FOLIO 1

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 04/2019
DEL 21 DE ENERO DE 2019

En la Ciudad de México, a las trece horas con treinta minutos del veintiuno de enero de dos mil diecinueve, en el edificio ubicado en avenida Cinco de Mayo, número dieciocho, colonia Centro, alcaldía Cuauhtémoc, se reunieron María Teresa Muñoz Arámburu, Titular de la Unidad de Transparencia; Erik Mauricio Sánchez medina, Director Jurídico y Víctor Manuel de la Luz Puebla, Director de Seguridad y Organización de la Información, todos integrantes del Comité de Transparencia de este Instituto Central, así como Rodrigo Villa Collins, Gerente de Análisis y Promoción de Transparencia, en su carácter de Secretario de dicho órgano colegiado. ----------

También estuvieron presentes, como invitados de este Comité, en términos de los artículos 4o. y 31, fracción XIV, del Reglamento Interior del Banco de México (RIBM), así como la Tercera, 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, (en adelante las Reglas), 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.----------

Al estar presentes los integrantes mencionados, quien ejerce en este acto las funciones del Secretariado del Comité de Transparencia manifestó que existe quórum para la celebración de la presente sesión, de conformidad con lo previsto en los artículos 43 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 64, párrafos segundo y tercero, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO); 4o. del RIBM; así como Quinta, párrafo primero, inciso d), y Sexta, párrafo primero, inciso b), de las Reglas. Por lo anterior, se procedió en los términos siguientes: ----------

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

El Secretario 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 43, párrafo segundo, 44, fracción IX, de la LGTAIP; 64, párrafo segundo; 65, fracción IX, de la LFTAIP; 83 de la LGPDPPSO; 4o. y 31, fracciones III y XX, del RIBM, y Quinta, de las Reglas, 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 CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE RECURSOS MATERIALES, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000000119.----------

El Secretario dio lectura al oficio con referencia W40/004/2019, suscrito por el titular de la Gerencia de Soporte Legal y Mejora Continua, en suplencia por ausencia del Director de Recursos Materiales del Banco de México; el cual se agrega a la presente acta como **ANEXO "C"**, por medio del cual hizo del conocimiento de este Comité de Transparencia la determinación de clasificar como confidencial diversa información contenida en los documentos que se indican en el mismo oficio, en términos de la motivación y fundamentación señaladas en el oficio referido, y solicitó a este órgano colegiado confirmar dicha clasificación. ----------

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; 1, 9, 64 y 65 fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia, vigentes, resolvió confirmar la clasificación de la información, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "D"**. ----------

BANCO DE MÉXICO

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA GERENCIA DE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN, Y DE LA SUBGERENCIA DE SEGURIDAD INFORMÁTICA, ASÍ COMO DEL TITULAR DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000074618. ----------

El Secretario dio lectura al oficio con referencia GSTI-01.2019, suscrito por los titulares de la Gerencia de Seguridad de Tecnologías de la Información, y de la Subgerencia de Seguridad Informática, unidades administrativas adscritas a la Dirección General de Tecnologías de la Información; así como al oficio de once de enero de dos mil diecinueve, suscrito por el titular de la Dirección de Apoyo a las Operaciones; los cuales se agregan en un solo legajo a la presente acta como **ANEXO "E"**, por medio de los cuales hicieron del conocimiento de este Comité de Transparencia la determinación de clasificar como reservada diversa información que se indica en dichos oficios, en términos de la motivación y fundamentación señaladas en las correspondientes pruebas de daño, y solicitaron a este órgano colegiado confirmar dicha clasificación. --------

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; 1, 9, 64 y 65 fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia, vigentes, resolvió confirmar la clasificación de la información, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "F"**.----------

TERCERO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR LOS TITULARES DE LA DIRECCIÓN DE REGULACIÓN Y SUPERVISIÓN, Y DE LA DIRECCIÓN DE SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000074318. ----------

El Secretario dio lectura al oficio de dieciocho de enero de dos mil diecinueve, suscrito por los titulares de la Dirección de Regulación y Supervisión, y de la Dirección de Sistemas de Pagos; el cual se agrega a la presente acta como **ANEXO "G"**, por medio del cual hicieron del conocimiento de este Comité de Transparencia la determinación de clasificar como reservada diversa información que se indica en dichos oficios, en términos de la motivación y fundamentación señaladas en el oficio señalado y en la correspondiente prueba de daño, y solicitaron a este órgano colegiado confirmar dicha clasificación.----------

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; 1, 9, 64 y 65 fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia, vigentes, resolvió confirmar la clasificación de la información, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "H"**. ----------

CUARTO. SOLICITUD DE CONFIRMACIÓN DE CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN DE SISTEMAS DE PAGOS, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO LT-BM-26213. ----------

El Secretario dio lectura al oficio con referencia D01/C391/2018, suscrito por el titular de la Dirección de Sistemas de Pagos, el cual se agrega a la presente acta como **ANEXO "I"**, por medio del cual hizo del conocimiento de este Comité de Transparencia que el documento referido en dicho oficio contiene información que en su momento fue clasificada para la atención de diversa solicitud, y que el mismo documento es materia de la solicitud con folio LT-BM-26213. Asimismo, informó que con motivo de una nueva reflexión, así como en consideración a los recientes criterios emitidos por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales en la substanciación de diversos recursos de revisión en materia de acceso a la información pública, así como el contexto actual en materia de ciberseguridad y ataques realizados por medios electrónicos a las instituciones financieras en todo el mundo, por lo que dicha unidad administrativa determinó modificar la clasificación realizada previamente, de conformidad con los fundamentos y motivos expresados en la prueba de daño que se puso a disposición

BANCO DE MÉXICO

de este órgano colegiado en su momento, extendiendo ahora la protección a la totalidad de la información contenida en el documento clasificado, y solicitó a este órgano colegiado confirmar dicha clasificación.--------
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; 1, 9, 64 y 65 fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Quinta de las Reglas de Operación del Comité de Transparencia, vigentes, resolvió confirmar la clasificación de la información, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "J"**. ----------
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 Secretario. Conste.----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

RODRIGO VILLA COLLINS
Secretario

ANEXO "A"

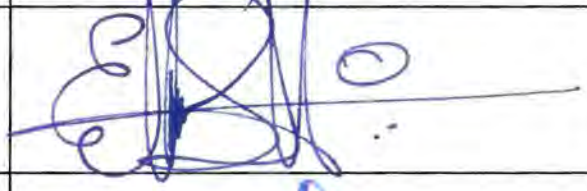
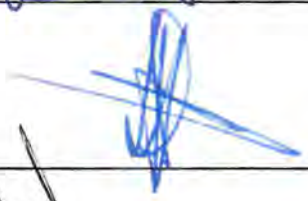
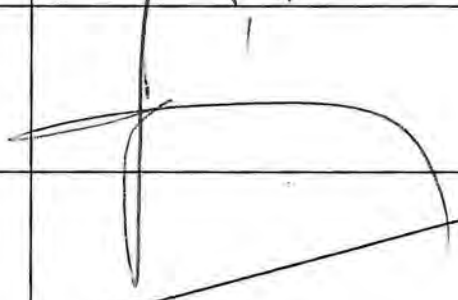
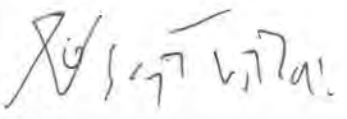
BANCO DE MÉXICO

LISTA DE ASISTENCIA

SESIÓN ORDINARIA 04/2019

21 DE ENERO DE 2019

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU Directora de la Unidad de Transparencia	
ERIK MAURICIO SÁNCHEZ MEDINA Director Jurídico	
VICTOR MANUEL DE LA LUZ PUEBLA Director de Seguridad y Organización de la Información	
CARLOS EDUARDO CICERO LEBRIJA Gerente de Gestión de Transparencia	
ENRIQUE ALCÁNTAR MENDOZA Abogado Especialista nivel Gerente	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información	
RODRIGO VILLA COLLINS Secretario del Comité de Transparencia	
SERGIO ZAMBRANO HERRERA Subgerente de Análisis Jurídico y Promoción de Transparencia	

BANCO DE MÉXICO

INVITADOS PERMANENTES

OSCAR JORGE DURÁN DÍAZ Dirección de Vinculación Institucional y Comunicación	
FRANCISCO CHAMÚ MORALES Director de Administración de Riesgos	

INVITADOS

RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
EDGAR MIGUEL SALAS ORTEGA Gerente Jurídico Consultivo	
JONATHAN NAVARRO VILLEGAS Abogado en Jefe en la Subgerencia de Apoyo Jurídico a la Transparencia	
MARGARITA LISSETE PONCE GUARNEROS Gerente de Riesgos No Financieros	

BANCO DE MÉXICO

IGNACIO JAVIER ESTÉVEZ GONZÁLEZ Director de Recursos Materiales	
GUILLERMO JOSÉ MARTÍNEZ VILLARREAL Gerente de Soporte Legal y Mejora Continua de Recursos Materiales	
KATYA ALVARADO YÁÑEZ Subgerente de Programación de Contratación y Mejora Continua	
PABLO ESCOBAR BRAVO Analista Administrativo	
JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN Director de Apoyo a las Operaciones	
CLAUDIA TAPIA RANGEL Especialista Investigador	
MARTÍN CAMPOS FERNÁNDEZ Analista de Información	

BANCO DE MÉXICO

OCTAVIO BERGÉS BASTIDA Director General de Tecnologías de la Información	
ALICIA ADRIANA AYALA ROMERO Subgerente de Planeación y Regulación	
RICARDO ALFREDO GONZÁLEZ FRAGOSO Líder de Especialidad	
ARTURO GARCÍA HERNÁNDEZ Gerente de Seguridad de Tecnologías de la Información	
FAUSTO CEPEDA GONZÁLEZ Subgerente de Seguridad Informática	
MANUEL MIGUEL ÁNGEL DÍAZ DÍAZ Director de Sistemas de Pagos	
OTHÓN MARTINO MORENO GONZÁLEZ Gerente de Política y Vigilancia de los Sistemas de Pagos	

CLAUDIA TAPIA RANGEL Especialista Investigador	
LILIANA GARCÍA OCHOA Líder de Especialidad	
XIMENA AIDEE DOMÍNGUEZ HERNÁNDEZ Investigador	
EDSEL ALEJANDRO CARMONA SANABRIA Analista de Información	
VIVIANA GARZA SALAZAR Directora de Regulación y Supervisión	
JOSÉ ALFREDO PANTOJA ZAMBRANO Gerente de Supervisión y Vigilancia de Intermediarios Financieros	
JORGE ERIK QUIROZ ROBLES Estudios y Proyectos Especiales	

BANCO DE MÉXICO

MARTHA MARISOL CAPILLA GUTIÉRREZ Subgerente de Identificación y Evaluación de Riesgos Operativos	
HÉCTOR GARCÍA MONDRAGÓN Jefe de la Oficina de Análisis Jurídico y Promoción de Transparencia	
Martín Campos Fernández	

ANEXO "B"

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

Sesión Ordinaria 04/2019
21 de enero de 2019

PRIMERO. Solicitud de confirmación de clasificación de información realizada por el Titular de la Dirección de Recursos Materiales, relacionada con la solicitud de acceso a la información con folio 6110000000119.

SEGUNDO. Solicitud de confirmación de clasificación de información realizada por los Titulares de la Gerencia de Seguridad de Tecnologías de la Información y de la Subgerencia de Seguridad Informática; y de la Dirección de Apoyo a las Operaciones, relacionada con la solicitud de acceso a la información con folio 6110000074618.

TERCERO. Solicitud de confirmación de clasificación de información realizada por los Titulares de la Dirección de Regulación y Supervisión, y de la Dirección de Sistemas de Pagos, relacionada con la solicitud de acceso a la información con folio 6110000074318.

CUARTO. Solicitud de confirmación de clasificación de información realizada por el Titular de la Dirección de Sistemas de Pagos, relacionada con la solicitud de acceso a la información con folio LT-BM-26213.

ANEXO "C"

BANCO DE MÉXICO

Ref: W40/004/2019

Ciudad de México, a 11 de enero de 2019.

Se recibe oficio constante en dos páginas

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000000119,** que turnó la Unidad de Transparencia a la Dirección de Recursos Materiales el día 3 de enero de 2019, 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.

> *"Muy atentamente se solicitan todas las pólizas de seguros contratadas por Banco de México que se hubiesen encontrado vigentes al 8 de mayo de 2018."*

Sobre el particular, con motivo de la atención de una solicitud de acceso diversa, la Dirección de Recursos Materiales clasificó diversa información contenida en los documentos que se señalan más adelante como confidencial, y generó las versiones públicas respectivas, junto con las carátulas que las distinguen e indican los datos concretos que fueron clasificados, con los motivos y fundamentos respectivos. Dicha clasificación y las correspondientes versiones públicas fueron aprobadas por el Comité de Transparencia mediante resolución emitida en su sesión del 19 de octubre de 2018.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
19 Póliza de seguro E01-2-71-1063-T.pdf	19	N/A
20 Póliza de seguro E01-2-71-1065-T.pdf	20	N/A

En el caso concreto, hacemos de su conocimiento que los documentos señalados en el cuadro precedente se ubican en el supuesto antes mencionado, y son materia de la presente solicitud.

Asimismo, en los documentos señalados, subsisten las causas que dieron origen a la clasificación como confidencial de la información relativa a "Correo electrónico de persona física y/o personal de los servidores públicos", de conformidad con la fundamentación y motivación señaladas en las carátulas correspondientes.

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 III, 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", vigentes, 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.

BANCO DE MÉXICO

Asimismo, de conformidad con el Décimo de los señalados Lineamientos, informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a los documentos señalados es el siguiente:

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

Sin otro particular, quedamos a sus órdenes para cualquier aclaración al respecto.

Atentamente,

GUILLERMO JOSÉ MARTÍNEZ VILLARREAL
Gerente de Soporte Legal y Mejora Continua de Recursos Materiales
Con fundamento en el artículo 66, párrafo primero del Reglamento Interior del Banco de México

ANEXO "D"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000000119

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

RESULTANDO

PRIMERO. Que el tres de enero de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000000119,** la cual se transcribe a continuación:

> *"Muy atentamente se solicitan todas las pólizas de seguros contratadas por Banco de México que se hubiesen encontrado vigentes al 8 de mayo de 2018."*

SEGUNDO. Que el mismo tres de enero, la solicitud de información en comento, fue turnada a la Dirección Recursos Materiales, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que el titular de la Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales, en suplencia por ausencia del Director de Recursos Materiales, mediante oficio con referencia W40/004/2019, hizo del conocimiento de este Comité que subsisten las causas que dieron origen a la clasificación de los documentos señalados en dicho oficio, en términos de la motivación y fundamentación señaladas en las carátulas que en su momento pusieron a disposición de este órgano colegiado.

Asimismo, a través de dicho oficio, señaló que dichas versiones públicas son materia de la solicitud señalada al rubro, y solicitó 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 (LGTAIP); 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción II, del Reglamento Interior del Banco de México (RIBM).

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 (Lineamientos).

SEGUNDO. Enseguida se analiza la clasificación referida en el resultando Tercero, conforme a lo siguiente:

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, 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 LGTAIP, 117 de la LFTAIP, y 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Este Comité de Transparencia **confirma la clasificación de la información testada y referida como confidencial.**

Por lo expuesto con fundamento en los artículos 44, fracción II, y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; 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 confidencial,** conforme a la fundamentación y motivación expresada en las correspondientes carátulas.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintiuno de enero de dos mil diecinueve.----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

ANEXO "E"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
Comité de Transparencia
Por: 715585 Hora: 11:01

se anexa oficio contenido de tres páginas y una prueba de daño

Ciudad de México, a 11 de enero de 2019

REF: GSTI-01.2019

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio **6110000074618**, que nos turnó la Unidad de Transparencia el 10 de diciembre del 2017, 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:

> *"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. Por numero de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero: a) Nombres comerciales de los sistemas operativos instalados. b) Nombres comerciales y versiones de los antivirus o software de seguridad en Internet, instalados. c) Inicio y termino de la vigencia de cada licencia utilizada en los software mencionados en el anterior inciso b). 2. Por dirección web o URL (Localizador Uniforme de Recursos), de los protocolos HTTP (Protocolo de Transferencia de Hipertexto) y HTTPS (Protocolo seguro de transferencia de hipertexto), cual es utilizado en cada una de sus paginas electrónicas o webs oficiales, así como el tipo de protocolo de seguridad implementado, SSL (Capa de sockets seguros) o TLS (Seguridad de la capa de transporte). 3. De cada una de sus actuales paginas electrónicas o webs oficiales, fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) padecidos."*

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, 113, Fracciones I, IV y VII y 114 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, IV y VII 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, Vigésimo sexto, primer párrafo,

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 siguiente información:**

a) Los números de serie de cada uno de los equipos de cómputo en posesión del Banco de México.
b) Los nombres comerciales y versiones de los antivirus o software de seguridad en Internet instalados.
c) El inicio y término de la vigencia de cada licencia utilizada en el software citado en el inciso b).
d) De cada una de sus actuales páginas electrónicas o webs oficiales, la fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) padecidos.

Lo anterior en virtud de que esta información corresponde a especificaciones y mecanismos de seguridad informática 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 desde el momento en que se lleve a cabo la confirmación de la clasificación correspondiente.

Por lo expuesto, solicito atentamente a este Comité de Transparencia confirmar la señalada clasificación de la información realizada por esta unidad administrativa.

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 quinto 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**
Inciso a)	• Funcionarios de la Dirección de Infraestructura de Tecnologías de la Información • Gerencia de Cómputo (Todo el personal) • Subgerencia de Planeación y Regulación (Todo el personal)

De cada uno de los equipos de cómputo: Inciso b)	• Gerencia de Seguridad de Tecnologías de la Información (Gerente) • Subgerencia de Seguridad Informática (Todo el personal)
Inciso c)	• Gerencia de Seguridad de Tecnologías de la Información (Gerente) • Subgerencia de Seguridad Informática (Todo el personal)
Inciso d)	• Gerencia de Seguridad de Tecnologías de la Información (Gerente) • Subgerencia del Centro de Defensa de Ciberseguridad (Todo el personal)

Atentamente.

ING. ARTURO GARCIA HERNÁNDEZ
Gerente de Seguridad de Tecnologías de la Información

ING. FAUSTO CEPEDA GONZÁLEZ
Subgerente de Seguridad Informática

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 6o., apartado A, sexto párrafo, 28, párrafo sexto y séptimo de la Constitución Política de los Estados Unidos Mexicanos, 113, fracciones I, IV y VII de la Ley General de Transparencia y Acceso a la información Pública (LGTAIP); y 110, fracciones I, IV y VII de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como el Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, y Vigésimo sexto, párrafo primero, 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 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.

e) Obstruya la prevención de delitos

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, de seguridad electrónica y de seguridad informática, sus números de serie, configuraciones, los números de teléfonos celulares asignados por el Banco a su personal, 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; la información relacionada con las evaluaciones y análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes, referente a 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; 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 o con algún elemento de seguridad informática, incluyendo la marca, el modelo, fabricante e información del proveedor de dicho elemento de seguridad que da protección a la referida infraestructura tecnológica; es clasificada como reservada.

Cabe aclarar que como parte de las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México se incluye lo siguiente:

- Los números de serie de cada uno de los equipos de cómputo en posesión del Banco de México.
- Nombres comerciales y versiones de los antivirus o software de seguridad en Internet instalados.
- El periodo de vigencia de las licencias del software citadas en el punto anterior, y
- De cada una de sus actuales paginas electrónicas o webs oficiales, la fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) padecidos.

En consecuencia, la referida información es 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; y obstruiría la prevención de delitos informáticos[1] en contra del Banco de México cuya planeación y ejecución se facilitarían con la divulgación de la información referida, 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

[1] Cfr. Cassou Ruiz, Jorge Esteban, "Delitos informáticos en México", *Revista del Instituto de la Judicatura Federal*, México, núm. 28, julio-diciembre de 2008, pp. 220-225. https://www.ijf.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

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 Décimo séptimo, fracción VIII, de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, señala que se considera 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 de Banco de México, representa una amenaza a la seguridad nacional, ya que publicar la información materia de la presente prueba de daño, 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.

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 Central.

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 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 los 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 **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.

Finalmente, los riesgos aludidos tienen mayor probabilidad de materializarse con la entrega de la información referida, debido a que se proporcionaría a individuos o grupos con intenciones hostiles elementos que falicitarían el diseño y la ejecución de estrategias para llevar a cabo ataques cibernéticos dirigidos específicamente a la infraestructura tecnológica de este Banco Central, mismos que pueden ser constitutivos de delitos. Dichos ataques focalizados podrían tener mayor probailidad de éxito debido a que personas con intenciones delincuenciales tendrían la posibilidad de dedicar todos sus recursos a la realización de ataques específicos identificados con base en la información en comento.

Al respecto, la divulgación de la información relativa a las especificaciones de la infraestructura de tecnologías de la información y comunicación del Banco de México, implica la puesta a disposición de elementos importantes a las personas o grupos con intenciones delictivas para la realización de conductas constitutivas de delitos.

En consecuencia, la divulgación de la información clasificada, representa un obstáculo para la prevención de conductas constitutivas de delitos, por lo que se actualiza la causal de reserva prevista en el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a al 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, las redes de datos públicas, las redes de datos privadas, 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.[2] 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 las manos equivocadas, estas herramientas se convierten en armas para atacar o extorsionar a cualquier organización, gobierno o dependencia, ya 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.

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[3].

---

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

[3] https://www.computerworld.com/article/3257225/microsoft-windows/intel-releases-more-meltdownspectre-firmware-fixes-microsoft-items-an-sp3-patch.html, consultada el 3 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "B"**

- 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[4].
- 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.[5]
- 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[6]
- 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[7].
- 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 diseñado específicamente para la infraestructura tecnológica de la víctima.[8]
- 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)" [9]. 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.
- El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse a esta Infraestructura de Mercados Financieros (IMF), inyectando órdenes de transferencia apócrifas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes afectados. lo cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.

---

[4] 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"**

[5] 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"**

[6] 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"**.

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

[8] 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"**.

[9] 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"**.

A la fecha de elaboración de la presente prueba de daño, se estima un daño a los participantes del SPEI de aproximadamente 300 millones de pesos.

- 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.[10]
- En relación a dar a conocer el número telefónico de un teléfono celular proporcionado por la Institución, como parte de la infraestructura de cómputo y telecomunicaciones, con el fin de que sus empleados realicen sus funciones asignadas, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto del usuario del dispositivo móvil , puede poner al descubierto información de actividades del personal en cumplimiento de sus funciones para el Banco, o aspectos de su ámbito personal, con el simple hecho de llevar consigo este dispositivo móvil[11]. Por este mismo problema, recientemente un senador de los Estados Unidos de Norte América envió una carta al presidente de la Comisión Federal de Comunicaciones de ese mismo país en donde le advierte de los riesgos a los que los dispositivos móviles están expuestos[12] .
- Las tecnologías que proporcionan seguridad informática a las organizaciones, no están exentas de presentar, como cualquier otra tecnología, vulnerabilidades, por lo que no es recomendable difundir la marca, el fabricante y las característica que tiene un cierto elemento de seguridad informática, para evitar el facilitar que un posible atacante aproveche dicha información con propósitos delictivos o disruptivos, dirigidos a las instituciones que usan estos elementos de seguridad informática.

  Por otro lado, el dar a conocer marcas, modelos o fabricantes de los controles de seguridad informática puede dar una ventaja a un atacante para fabricar un ataque especialmente diseñado (dirigido), sabiendo de antemano la serie de controles presentes en una organización con el fin de evadirlos, aumentando así la probabilidad de éxito del ciber ataque.

  A manera de ejemplo se cita un caso en que dos de los grandes proovedores de seguridad informática a nivel mundial presentaban vulnerabilidades que pudieron comprometer a esas organizaciones[13] .

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[14] 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.

---

[10] 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"**.

[11] http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338, se anexa como **ANEXO "J"**

[12] https://www.wyden.senate.gov/imo/media/doc/wyden-fcc-ss7 letter-may 2018.pdf, se anexa como **ANEXO "K"**

[13] "Google Found Disastrous Symantec and Norton Vulnerabilities" http://fortune.com/2016/06/29/symantec-norton-vulnerability consultada el 14 de septiembre de 2018. Se adjunta impresión como **ANEXO "L"**

[14] 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"**.

En este mismo sentido, dar a conocer los **números de serie** de los equipos de cómputo del Banco de México, facilitaría que terceros identifiquen posibles vulnerabilidades asociadas a estos equipos, con las consecuentes afectaciones que pudieran suscitarse, que van desde el acceso a información financiera o personal, la modificación de los datos que se procesan en ellos o, incluso, dejar fuera de operación a los sistemas de información del Banco. Por lo que, no divulgar los números de serie asociados a estos dispositivos es en sí una medida básica de seguridad, ya que continuamente se publican vulnerabilidades asociadas a los números de serie de distintas tecnologías. Como un ejemplo de lo anterior mencionamos que en el año 2015 fue descubierta una operación llamada "Equation Group"[15] que infectó con código malicioso algunos modelos de los discos duros "Seagate" y "Western Digital" durante su etapa de fabricación. Estos discos duros comprometidos fueron incluidos en diferentes equipos de cómputo que fueron vendidos a diferentes empresas alrededor del mundo. Dicho código malicioso tiene la característica de que no puede ser detectado ni erradicado con herramientas tradicionales y por lo tanto fue utilizado por atacantes para espiar sin ser detectados. El conocer los números de serie de los equipos de cómputo facilitaría conocer las especificaciones con las que fue construido y eventualmente identificar que hubiera sido armado con uno de estos discos duros infectados.

Del mismo modo, al dar a conocer información relacionada a **nombres y versiones de los antivirus o software de seguridad en internet, así como la vigencia de sus correspondientes licencias**, utilizados en los sistemas de Banco de México implicaría multiplicar los riesgos de seguridad al dar a conocer los controles de seguridad informática con los que cuenta el Banco, de forma que los atacantes contarían con información sensible que le permitiría intentar vulnerar los sistemas de seguridad que protegen la infraestructura del Banco. Si bien no es posible afirmar si determinado antivirus o software de seguridad es más seguro que otro, existen otros factores que podrían incrementar la posibilidad de un ataque a la infraestructura, como vulnerabilidades sobre los mismos controles de seguridad o incluso nuevas amenazas que se den a conocer que incentiven a ejecutar ataques sobre la infraestructura del Banco. Incluso el propio atacante podría desarrollar una serie de pruebas en un laboratorio de análisis que le permitiría identificar la forma de esquivar las protecciones de un antivirus o software de seguridad en internet, ya que los controles de seguridad podrían contener defectos o vulnerabilidades, que pueden ser aprovechados por un atacante para evadir los controles de seguridad, e incluso desarrollar un código malicioso para evadir o deshabilitar fácilmente dichos controles.

Por otro lado, dar a conocer la información referente a la **fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) padecidos en cada una de las actuales páginas electrónicas o webs oficiales del Banco de México**, aumentaría la posibilidad de que un atacante pueda inferir las capacidades de mitigación y umbrales configurados en los controles de seguridad, lo cual implica un riesgo en la seguridad y comunicación web.

---

[15] https://en.wikipedia.org/wiki/Equation_Group. Se adjunta una impresión del artículo como **ANEXO "N"**

Si bien la información de ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) se puede considerar estadística, en el mundo existen organizaciones dedicadas a la extorsión en la cual un grupo de "hackers" exige un pago económico a una institución financiera a cambio de no realizar ataques DDoS hacia su infraestructura tecnológica, tal es el caso del grupo denominado "Armada Collective"[16] (anteriormente autodenominado "DD4BC") el cual surgió en el año 2015 y que durante el mes de diciembre del mismo año diferentes medios de comunicación informaron que dicho grupo lanzó ataques DDoS contra 3 bancos griegos que no realizaron el pago solicitado, como resultado de dicho ataque lograron interrumpir temporalmente las transacciones bancarias en linea por un corto período de tiempo. Por lo anterior un atacante podría utilizar la información de los ataques DDoS con el objetivo de extorsionar y dimensionar un ataque DDoS dirigido a Banco de México tomando como referencia las fechas, duraciones y número de incidencias pasadas.

Asimismo, proporcionar datos exactos sobre este tipo de eventos suscitados con anterioridad, podría ser utilizado por grupos cibercriminales para conocer la periodicidad con la que se manifiestan, así como los periodos en los cuales el Banco de México presenta una mayor incidencia de dichos eventos, por lo que atacantes pueden aprovechar dicha información para generar otro tipo de ataques informáticos durante los periodos mencionados, empleando los ataques DDoS como distractores para enmascarar otro tipo de ataques que puedan comprometer la integridad, confidencialidad y disponibilidad de la infraestructura del Banco.

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 arquitectura), así como mensajes de correo electrónico. La empresa Deloitte dio a conocer

[16] http://securityaffairs.co/wordpress/46702/cyber-crime/armada-collective.html. Se adjunta una impresión del artículo como **ANEXO "O"**

este incidente en septiembre de 2017[17], aunque varios medios reportan que la intrusión sucedió en otoño de 2016[18].

- 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[19], 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[20]. 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.

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 causar indisponibilidad en 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 2018, nuestros registros indican un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 1500 intentos en un único mes.

Durante el año 2018, en el sector financiero mundial han sucedido incidentes de seguridad informática en diversas instituciones, tal es el caso del Banco de Chile, el cual fue víctima de un ciberataque que derivó en pérdidas económicas para dicha organización[21]; y cuyo modus operandi ha sido observado en otros ataques informáticos durante al menos los últimos tres años (por

---

[17] https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html. Se adjunta una impresión del artículo como **ANEXO "P"**

[18] https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails. Se adjunta una impresión del artículo como **ANEXO "Q"**

[19] 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. Se adjunta una impresión del artículo como **ANEXO "R"**

[20] https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01. Se adjunta una impresión del artículo como **ANEXO "S"**

[21] https://ww3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/carta-a-clientes-sobre-incidente-tecnologico. Se adjunta una impresión del artículo como **ANEXO "T"**

ejemplo el Banco Central de Bangladesh[22]). Asimismo, se puede tomar como referencia un incidente suscitado en el continente europeo, el cual ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios web de los bancos centrales[23]. El colectivo Anonymous 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 "OpIcarus 2.0"[24], que tuvo lugar durante el presente mes de diciembre de 2018, y cuyos objetivos nuevamente fueron los sitios públicos de bancos centrales alrededor del mundo.

El panorama de amenazas de ciberseguridad en el ecosistema financiero mexicano ha cambiado, lo cual quedó de manifiesto al consumarse los ciberataques que afectaron a algunos participantes del sector financiero mexicano durante el 2018, como por ejemplo: en el mes de enero el ataque cibernético al Banco de Nacional de Comercio Exterior (Bancomext) con una afectación en su plataforma de pagos internacionales provocada por un tercero. En esta caso, las autoridades confirmaron que el modus operandi de los presuntos "hackers" es similar a intromisiones ocurridas en otras instituciones en México y América Latina[25]. Por otro lado, en los meses de abril y octubre, 6 instituciones financieras que operan con el Sistema de Pagos Electrónicos Interbancarios (SPEI) fueron vulneradas con el objetivo de realizar trasferencias bancarias no autorizadas hacia terceros, lo que ocasionó una pérdida económica para dichas instituciones[26] [27]. Considerando lo anterior, es evidente que el riesgo de sufrir ciberataques es considerable.

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 SPEI, 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[28]; 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

---

[22] https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html. Se adjunta una impresión del artículo como **ANEXO "U"**

[23] http://www.reuters.com/article/us-greece-centbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR. Se adjunta una impresión del artículo como **ANEXO "V"**

[24] https://rogueemedialabs.com/2018/12/13/anonymous-launches-opicarus-2-0/. Se adjunta una impresión del artículo como **ANEXO "W"**

[25] https://www.bancomext.com/comunicados/18443. Se adjunta una impresión del artículo como **ANEXO "X"**

[26] http://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B82AA2232-6078-F306-C66A-94868230AE4A%7D.pdf. Se adjunta una impresión del artículo como **ANEXO "Y"**

[27] https://axa.mx/web/blog/postura-de-axa-mexico?utm_source=twitter&utm_medium=comunicado-oficial&utm_campaign=ciberataque&utm_content=banxico. Se adjunta una impresión del artículo como **ANEXO "Z"**

[28] http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es . Se adjunta una impresión del artículo como **ANEXO "AA"**

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 materia de la presente prueba de daño, 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 **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** contenida en el documento que se clasifica, 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, divulgar **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México**, 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.

Adicionalmente, se obstaculizaría la prevención de hechos constitutivos de delitos, pues de divulgarse la información en cuestión se proporcionarían elementos relevantes para que personas o grupos de personas con intenciones delictivas lleven a cabo un ataque exitoso en contra de de la infraestructura de tecnologías de la información y comunicaciones que utiliza este Banco Central.

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, 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.

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. Finalmente, la divulgación de la información obstruiría la prevención de delitos.

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, IV y VII, y 114 de la LGTAIP; 1, 97, 100, 102, 103, 104, 105, 106, 110, fracciones I, IV y VII, 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, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Vigésimo sexto, párafo primeroTrigésimo 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, del Banco de México,** se han determinado clasificar como reservadas.

ANEXO "A"

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]

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.]

¿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»] *Rapid7*. Consultado el esta fecha esta pasada lo le agan caso por favor y gracias por su atencion chausmu.
3. ↑ [a] [b] Plantilla Citan 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

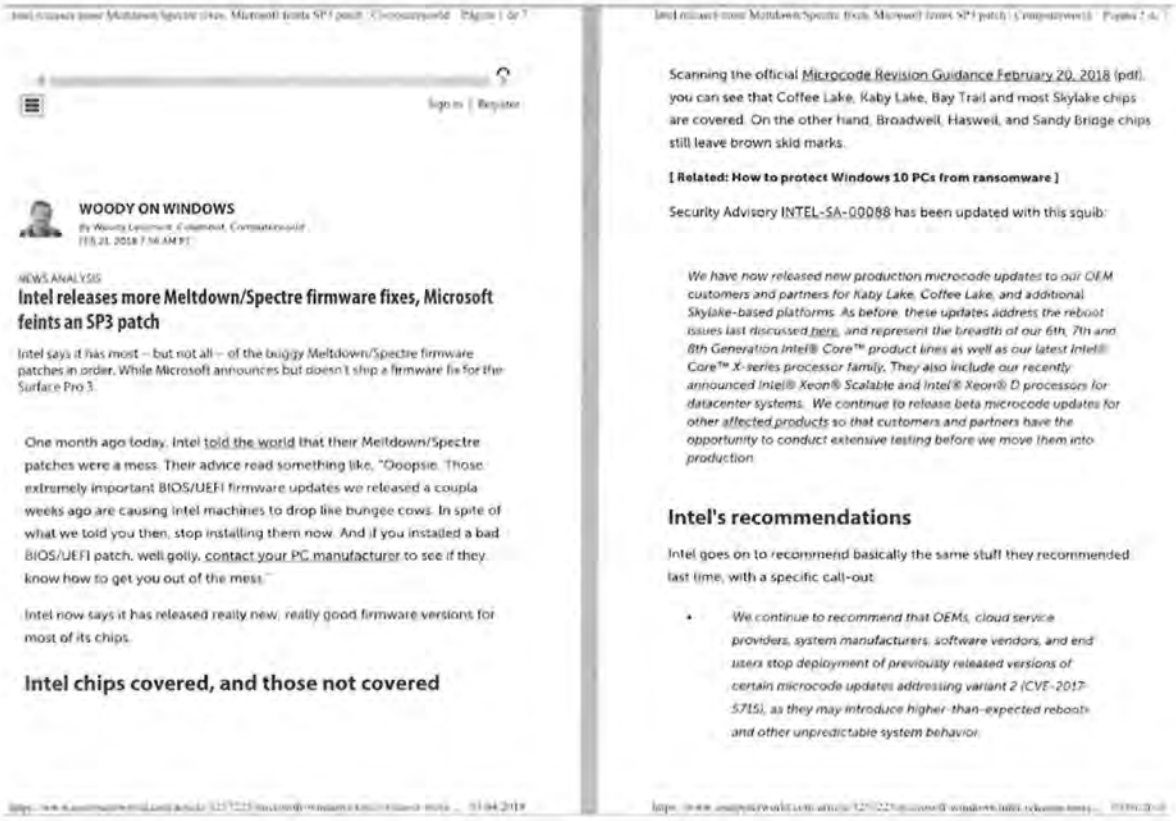
Metasploit - Wikipedia, la enciclopedia libre

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

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

ANEXO "B"

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 23, 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:

> *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

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, 8GB RAM, 256GB) – Newest Version $1047.75

ANEXO "C"

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 CLIE... Página 1 de 1

(http://www.gob.mx) › Banco Nacional de Comercio Exterior, S.N.C. (Bancomext) › **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

El Banco Nacional de Comercio Exterior (Bancomext) informa que, a pesar de las [illegible] medidas de seguridad con que cuenta, el día 9 de enero fue víctima de un [illegible] en su plataforma de pagos internacionales provocado 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 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 reanudando operaciones para sus clientes y contrapartes.

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

Teléfono Comunicación Social: (55) 1924

Comparte: 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=+Descargar en PDF la página completa

[illegible]

https://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-l... 15/01/2018

ANEXO "D"

https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/

Consultada el 22 de enero de 2018

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

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. ®

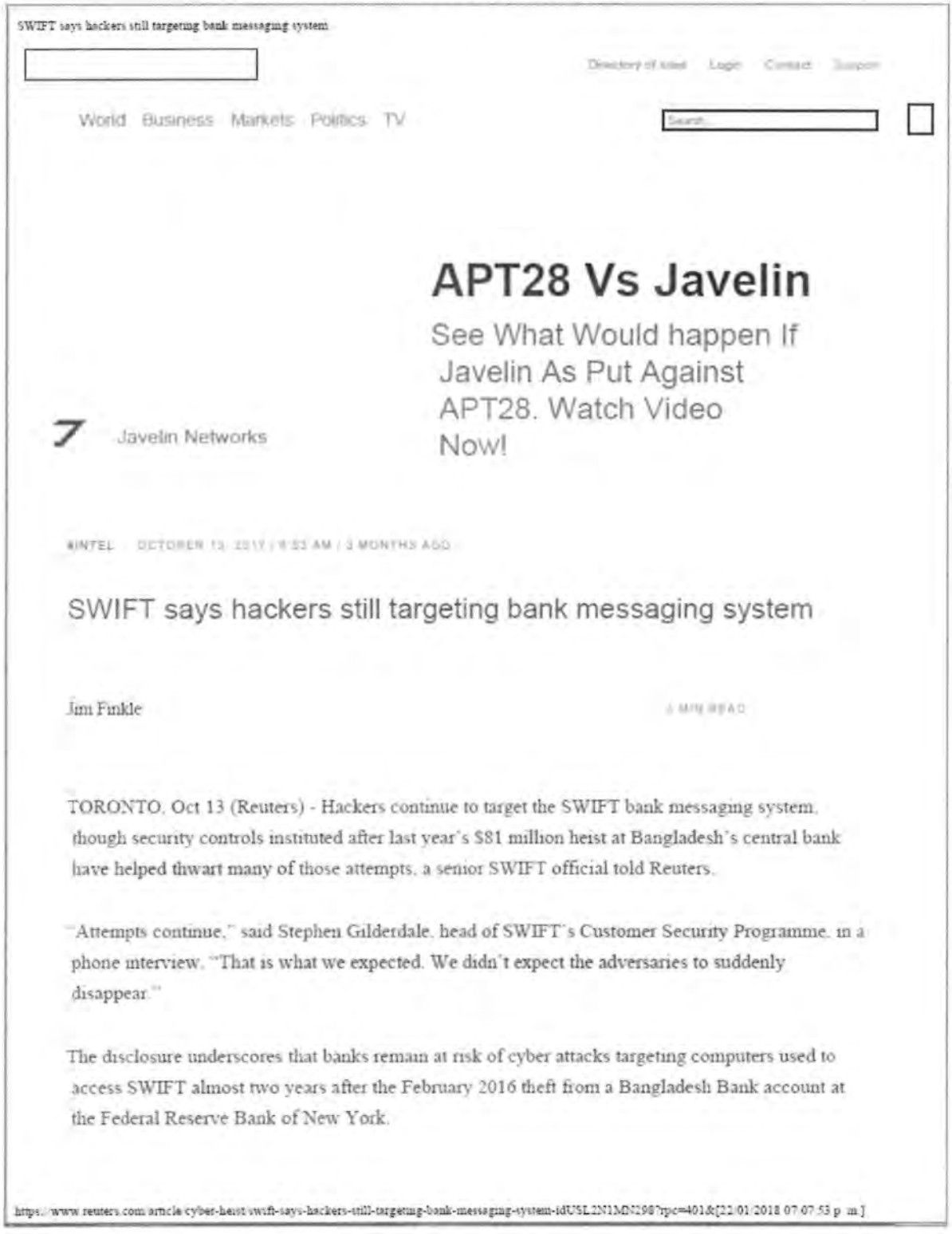
Updated to add

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

ANEXO "E"

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



SWIFT says hackers still targeting bank messaging system

World Business Markets Politics TV

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.*

ANEXO "F"

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

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

Features

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."

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
336

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"

http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html,
Consultada el 22 de enero de 2018

22/1/2018 BAE Systems Threat Research Blog: Two bytes to $951m

Más Siguiente blog» Crear un blog Acceder

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers

SEARCH

THREAT RESEARCH BLOG

BAE SYSTEMS
INSPIRED WORK

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
625a8e3ae4e3df8c9c61f2a49e3b541d196e9228	2016-02-05 11:46:20	65,536	evtdiag.exe
76bab478dcc70f979ce62cd306e6ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
7bbf16597e375ad6911c2c1e6a194dbe7f60e4eeb	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 625a8e3ae4e3df8c9c61f2a49e3b541d196e9228 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.

http://baesystemsai.blogspot.mx/2016/04/two-bytes-to-951m.html 1/7

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 1f a7 7f 08 cc aa 0d 84 ed ef f9 ed 38 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):

```
196.202.168.174
```

The sample also uses the following file for logging:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\rmcas.dat
```

Module patching

The malware enumerates all processes, and if a process has the module `ibora4b.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 `liboradb.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\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_UNID) that corresponds to the transfer reference and sender address retrieved earlier:

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

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

```
DELETE FROM SAAOWNER.MESG_%s WHERE MESG_S_UNID = '%s';
DELETE FROM SAAOWNER.TEXT_%s WHERE TEXT_S_UNID = '%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 BBHOBDDMA: 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\Allians\mcp\in\*.*
{ROOT_DRIVE}:\Users\Administrator\AppData\Local\Allians\mcp\out\*.*
{ROOT_DRIVE}:\Users\Administrator\AppData\Local\Allians\mcp\ank\*.*
{ROOT_DRIVE}:\Users\Administrator\AppData\Local\Allians\mcs\nfsp
{ROOT_DRIVE}:\Users\Administrator\AppData\Local\Allians\mcs\nfsf
{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:"
"60M:"
"62M:"
"Credit"
"Debit"
":61:"
":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 `gpta.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_## WHERE MESG_S_UMID = '##';
```

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_## 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_UNID =
'%s';
UPDATE SAAOWNER.TEXT_%s SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UNID = '%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 `prdff.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"

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

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

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.]

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"

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...

About ▾ Membership ▾ Events ▾ Training/Certification ▾ Standards & Best Practices ▾ Committees ▾ Programs ▾ Gov Affairs ▾ Store ▾

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,

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

https://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 2018

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"

http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338

Consultada el 8 de octubre de 2018

CBC

Hackers only needed a phone number to track this MP's cellphone

Tests show Canada's two largest telecoms vulnerable to international hackers

NDP MP Matthew Dubé looks at a map showing that hackers tracked his movements through his cellphone for days.

One marker shows Dubé near Parliament Hill. Another marks the place he lives when he's working in Ottawa. One more shows an early morning trip to the airport to pick up his partner from a business trip.

"That's creepy. That doesn't make you feel very comfortable," said the Quebec MP.

He looks down at the laptop showing the map again and laughs nervously.

"I guess it's not something to joke about but I guess you think, 'Good thing I wasn't doing anything inappropriate.'"

It wasn't just his movements. Hackers were able to record Dubé's calls, too.

- **Someone is spying on cellphones in Ottawa**
- **RCMP, CSIS launch investigations into phone spying**

It was all part of a CBC/Radio-Canada demonstration of just how vulnerable Canada's phone networks are. With Dubé's consent and the help of cybersecurity experts based in Germany, CBC/Radio-Canada learned that Canada's two largest cellphone networks are vulnerable to attack.

How can hackers access your phone?

This is all possible because of vulnerability in the international telecommunication network. It involves what's known as Signalling System No. 7 — or SS7.

SS7 is the way cellphone networks around the world communicate with one another. It's a hidden layer of messages about setting up and tearing down connections for a phone call, exchanging billing information or allowing a phone to roam. But hackers can gain access to SS7, too.

"Those commands can be sent by anybody," said Karsten Nohl, a Berlin-based cybersecurity expert whose team helped CBC/Radio-Canada hack into Dubé's phone.

That can go beyond spying on phone conversations or geolocating a phone. SS7 attacks can also be used to alter, add or delete content.

For example, Nohl said he could set up a person's cellphone voicemail so all messages went directly to him. The user might never know the messages were missing.

"The technology is built with good intentions to make a very useful phone network and good user experience but it lacks any kind of security and it's open to abuse."

- **RCMP used cellphone tracking technology unlawfully 6 times, says privacy watchdog**

It's not just Nohl sounding the alarm. The U.S. Department of Homeland Security put out a report in April warning that "significant weaknesses in SS7 have been known for more than a decade."

The report notes that potential abuses of SS7 include eavesdropping, tracking and fraud, with "tens of thousands of entry points worldwide, many of which are controlled by countries or organizations that support terrorism or espionage."

SS7 abuse

SS7 attacks can easily go completely undetected. However, German journalists reported on an incident earlier this year where customers of Telefonica bank had untold amounts of money drained from their accounts because of phishing emails and SS7 attacks.

In that case, the bank used four-digit codes sent to customers' phones in order to complete money transfers. Hackers used SS7 to get those codes and take the funds for themselves.

The sheer number of SS7 attacks becomes clear when networks beef up their security, said Nohl.

"When they start blocking this abuse, they're blocking millions of otherwise abusive messages. That's for a single network in a single country. So you can imagine the magnitude of abuse worldwide."

Hacking a Canadian phone

Nohl said some telecom companies, primarily in Europe, have beefed up their defences to ward off SS7 attacks.

CBC/Radio-Canada wanted to know just how well Canadian cellphone networks would fare and asked Dubé to be part of a demonstration.

Dubé, the vice-chair of the House of Commons standing committee on public safety and national security, went to the mall and picked up a new phone for the experiment. CBC/Radio-Canada agreed not to use his current work phone in order to protect the privacy of those phone calls.

Dubé's new phone number was given to Nohl and his team of hackers in Berlin. It didn't take long for them to access his calls.

First, the hackers were able to record a conversation between Dubé in his office on Parliament Hill and our Radio-Canada colleague Brigitte Bureau, who was sitting at a café in Berlin.

Next, it was a conversation between Dubé and his assistant, who were both in Ottawa.

Nohl's team also tracked the geolocation data from the phone, painting a picture of Dubé's whereabouts.

When the CBC/Radio-Canada team was back in Canada, the calls were played for Dubé and he was shown a map of his movements.

"It's exactly what I did that day. Just phone calls are bad enough. When you start knowing where you are, that's pretty scary stuff," said Dubé.

Dubé's phone was on the Rogers Network, but CBC/Radio-Canada also ran a similar test with phones on the Bell network.

'Easy to hack'

Nohl offered his assessment of the results.

"Relative to other networks in Europe and elsewhere in the world, the Canadian networks are easy to hack."

He believes there's much more that Rogers and Bell could be doing.

"I think the two Canadian networks we tested have about 10 per cent of the security that they need to do to protect from SS7 attacks."

It's a source of concern for Pierre Roberge, too. He spent more than 10 years with Canada's Communications Security Establishment — the electronic spy agency charged with protecting Canadian digital security. He's now the CEO of Arcadia Cyber Defence.

The CBC/Radio-Canada demonstration raises questions about personal security, he said, and also about who else might want to spy on sensitive discussions.

"To know other nations or criminal groups can eavesdrop on Canadian communication is really worrisome, especially at the political level."

Companies say security a priority

Bell, Rogers and the Canadian Wireless Telecommunications Association declined to sit down with CBC/Radio-Canada and speak about the test results.

Via email, CBC/Radio-Canada sent a series of questions about what the networks were doing to prevent SS7 attacks and why customers weren't being told conversations could be compromised. Both networks responded with general statements about their security efforts.

Rogers Communications said security is a top priority and that it has a cybersecurity team monitoring threats and is introducing new measure to protect customers.

"On SS7, we have already introduced and continue to implement the most advanced technologies but we are unable to share specific details for security reasons."

Bell sent a two-line response.

"Bell works with international industry groups such as the GSMA [an international mobile phone operators association] to identify and address emerging security risks, including those relating to SS7."

A spokesperson added that Bell is "an active participant" in the Canadian Security Telecommunications Advisory Committee.

The group that represents Canadian telecoms was also fairly tight-lipped. The Canadian Wireless Telecommunications Association said it works with domestic and international bodies on security standards. It also said it works with law enforcement to "actively monitor and address risks."

Government reaction

CBC/Radio-Canada also reached out to Public Safety Minister Ralph Goodale's office to ask what was being done to protect Canadians and was directed to the Communication Security Establishment.

In a statement, CSE said its role is to provide "advice and guidance to help protect systems of importance to the Government of Canada."

"CSE has been actively working with Canada's telecom industry and critical infrastructure operators to address issues related to SS7 to develop best practices, advice and guidance that can help mitigate the risks associated with SS7."

How to protect yourself

There are ways to minimize the chance someone will spy on your communications, said Nohl.

He recommends encryption software.

"If you're using Signal, WhatsApp, Skype, you're certainly protected from SS7 attacks.... But there's other types of attacks that could happen against you, your computer, your phone. So you're never fully safe."

When it comes to having your movements tracked, Nohl said the only protection is to turn your phone off — something that's not always practical.

"We're so dependent on our phones. The networks should protect us from these attacks rather than us having to forgo all the benefits of carrying a phone."

Dubé said that dependency is what makes this most troubling.

"The scariest thing of all is that I know that tonight or tomorrow morning, when I make calls to friends to go out for a drink or when I make calls to colleagues to resolve a political or professional issue — I'm still going to have to use the phone."

Corrections

ANEXO "K"

https://www.wyden.senate.gov/imo/media/doc/wyden-fcc-ss7-letter-may-2018.pdf

Consultada el 8 de octubre de 2018

RON WYDEN
OREGON

COMMITTEES:

United States Senate

WASHINGTON, DC 20510-3703

May 29, 2018

The Honorable Ajit Pai
Chairman
Federal Communications Commission
445 12th Street Southwest
Washington, DC 20554

Dear Chairman Pai:

One year ago I urged you to address serious cybersecurity vulnerabilities in U.S. telephone networks. To date, your Federal Communications Commission has done nothing but sit on its hands, leaving every American with a mobile phone at risk.

Mobile telephone networks connect to each other through Signaling System 7 (SS7), which is riddled with long-standing cybersecurity vulnerabilities that pose a major national security threat. SS7's flaws expose U.S. telephone networks to hacking by criminals and foreign governments. Hackers can exploit SS7 flaws to track Americans, intercept their calls and texts, and hack their phones to steal financial information, know when they are at home or away, and otherwise prey on unsuspecting consumers. Moreover, according to multiple news reports, SS7 spying products are widely available to both criminals and foreign governments.

Over the past year, my office has consulted with mobile security experts, the major wireless carriers, and the Department of Homeland Security (DHS) to discuss these vulnerabilities. These meetings have made clear that SS7 vulnerabilities pose a major threat that must be addressed immediately, a conclusion the DHS 2017 *Study on Mobile Device Security* shares.

This threat is not merely hypothetical—malicious attackers are already exploiting SS7 vulnerabilities. One of the major wireless carriers informed my office that it reported an SS7 breach, in which customer data was accessed, to law enforcement through the government's Customer Proprietary Network Information (CPNI) Reporting Portal. This is a legal requirement for wireless providers who believe that private consumer information has been illegally accessed. Submissions via the portal are automatically delivered to the FCC, the U.S. Secret Service, and the Federal Bureau of Investigation.

Although the security failures of SS7 have long been known to the FCC, the agency has failed to address this ongoing threat to national security and to the 95% of Americans who have wireless service. In 2016, the FCC created a new working group under the Communications Security, Reliability and Interoperability Council (CSRIC) to explore and address SS7 vulnerabilities. However, the working group was dominated by wireless industry insiders with serious conflicts of interest. CSRIC appointed a senior official from the wireless industry's trade association,

CTIA, to be lead editor of the group's report. Of the fifteen non-government members, twelve worked for telecommunications companies or industry associations. No academic experts or representatives from civil society were members of the working group. Likewise, although personnel from DHS's National Coordinating Center for Communications (NCC) participated, DHS has informed my office that the vast majority of the edits to the final report suggested by NCC's subject matter experts were rejected. DHS also informed my office that those same subject matter experts from the NCC were not invited back to participate in the subsequent CSRIC SS7 working group, created in late 2017.

The FCC deferred to the wireless industry to assess the same security vulnerabilities that the industry has long ignored. CSRIC's final report, published in March 2017 openly acknowledged that "the attack surface for a bad actor to potentially exploit... [SS7] has increased" and "there is reported evidence of attacks being launched against U.S. carriers." While some of the working group's technical recommendations were constructive, it let the wireless industry off the hook for ignoring these issues for decades and did not recommend that the FCC use its regulatory authority to force the industry to fix these and other long-standing security flaws. That the working group appointed by the FCC to study this issue did not recommend a more forceful response is, I believe, not a coincidence.

In a prior letter to me, you dismissed my request for the FCC to use its regulatory authority to force the wireless industry to address the SS7 vulnerabilities. You cited the work of the CSRIC as evidence that the FCC is addressing the threat. But neither CSRIC nor the FCC have taken meaningful action to protect hundreds of millions of Americans from potential surveillance by hackers and foreign governments. The FCC must now take swift action, using its regulatory authority over the wireless carriers, to address the market failure that has enabled the industry to ignore this and other serious cybersecurity issues for decades. I also ask that you provide me with answers to the following questions by July 9, 2018:

- The DHS's 2017 report *Study on Mobile Device Security* stated "all U.S. carriers are vulnerable… resulting in risk to national security." In response to one of my letters, then-Director of the NSA Admiral Michael Rogers agreed with me that "the security of mobile networks needs to improve and securing the vulnerabilities of SS7 must be part of that work." Do you agree with DHS and NSA that SS7 vulnerabilities pose a significant national security threat?
    - If you do not, please explain why your assessment differs.
- The CSRIC-V working group 10 was charged with the creation of a Risk Assessment Report, as noted in each of their presentations. The working group's publicly available final report only summarizes the findings of the Risk Assessment Report. Please provide me with a copy of the full Risk Assessment Report.
- In each of the past five calendar years, how many breaches have been reported to the FCC through the CPNI breach portal?
    - How many of these were breaches in which SS7 was used to access subscriber information?
- In each of the past five calendar years, how many breaches of customer location data have been reported to the FCC by wireless carriers.

- How many of these were breaches in which SS7 was used to access subscriber information?
- For each SS7-related breach, please describe what steps, if any, the FCC took to investigate the breach.
- For each SS7-related breach, did the FCC notify the individuals whose information was stolen?
  - If not, please explain why the FCC did not notify these individuals.

If you have any questions regarding this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden
United States Senator

ANEXO "L"

http://fortune.com/2016/06/29/symantec-norton-vulnerability/

Consultada el 18 de septiembre de 2018

MPW
Wage Gap, Meet Equity Gap: Women Hold Only 9% of Startup Equity

BRIEFING
FCC Head Ajit Pai Compares California's Net Neutrality Regulations to Plastic Straw Bans

AUTOS
Tesla Said to Be Facing Criminal Probe Over Elon Musk Statements

AUTOS
Audi's All-Electric SUV Is Germany's First Serious Shot Across Tesla's Bow

TECH · CHANGING FACE OF SECURITY

Google Found Disastrous Symantec and Norton Vulnerabilities That Are 'As Bad As It Gets'

By ROBERT HACKETT

Google's "project zero" team, a group of security analysts tasked with hunting for computer bugs, discovered a heap of critical vulnerabilities in Symantec (SYMC, +3.21%) and Norton security products. The flaws allow hackers to completely compromise people's machines simply by sending them malicious self-replicating code through unopened emails or un-clicked links.

The vulnerabilities affect millions of people who run the company's endpoint security and antivirus software, rather ironically to protect their devices. Indeed, the flaws rendered all 17 enterprise products (Symantec brand) and eight consumer and small business products (Norton brand) open to attack.

In the words of Tavis Ormandy, an English hacker who works on the Google (GOOG, +1.15%) team: "These vulnerabilities are as bad as it gets"—and have "potentially devastating consequences."

Get Data Sheet, Fortune's technology newsletter.

"An attacker could easily compromise an entire enterprise fleet using a vulnerability

like this," Ormandy writes on a Google blog. "Network administrators should keep scenarios like this in mind when deciding to deploy Antivirus, it's a significant tradeoff in terms of increasing attack surface."

Ormandy's post published soon after Symantec issued advisories of its own, which credit him for reporting the bugs. "An attacker could potentially run arbitrary code by sending a specially crafted file to a user," the notice warns, before mentioning that the company has "verified these issues and addressed them in product updates."

For more on Symantec, watch:

The vulnerabilities affect a "decomposer engine"—a program that unpacks compressed files in order to help scan for potentially malicious ones—that's used across Symantec's products. "It's extremely challenging to make code like this safe," Ormandy writes. To avoid such problems, Ormandy recommends that security vendors use sandboxing, a technique that detonates suspicious code in a secure, virtual environment, as well as security-first software development strategies.

Ormandy further demonstrated that the flaws can be exploited to propagate

computer worms, meaning virally infectious malware. "Just emailing a file to a victim or sending them a link to an exploit is enough to trigger it," he says, "the victim does not need to open the file or interact with it in anyway."

Symantec, which recently purchased the Bain Capital-backed cybersecurity firm Blue Coat for $4.65 billion, also employed open source code that it failed to update even after seven years of use, Ormandy notes. He lists the additional vulnerabilities in that code here.

Ormandy has been on a tear rooting out similarly nasty computer bugs. He helped identify comparable flaws—known technically as buffer overflows and memory corruption vulnerabilities—in products developed by the cybersecurity companies Comodo, ESET, Kaspersky, Fireeye (FEYE, +2.50%), Intel (INTC, +2.16%) Security's McAfee, Trend Micro (TMICY, +3.46%), and others in recent years.

Customers of Symantec should visit the company's website to learn which products have been updated automatically, and which require manual updates.

ANEXO "M"

https://www.offensive-security.com/metasploit-unleashed/information-gathering/,
Consultada el 22 de enero de 2018

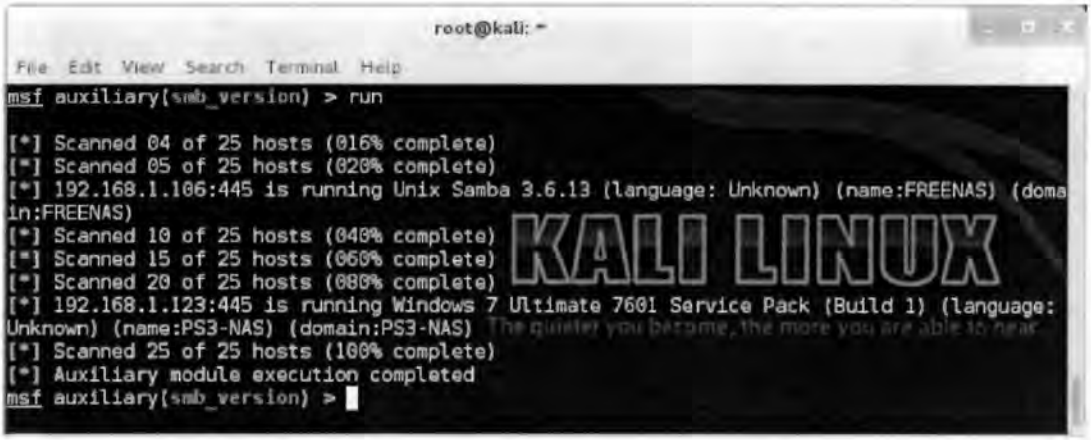
Information Gathering in Metasploit

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:

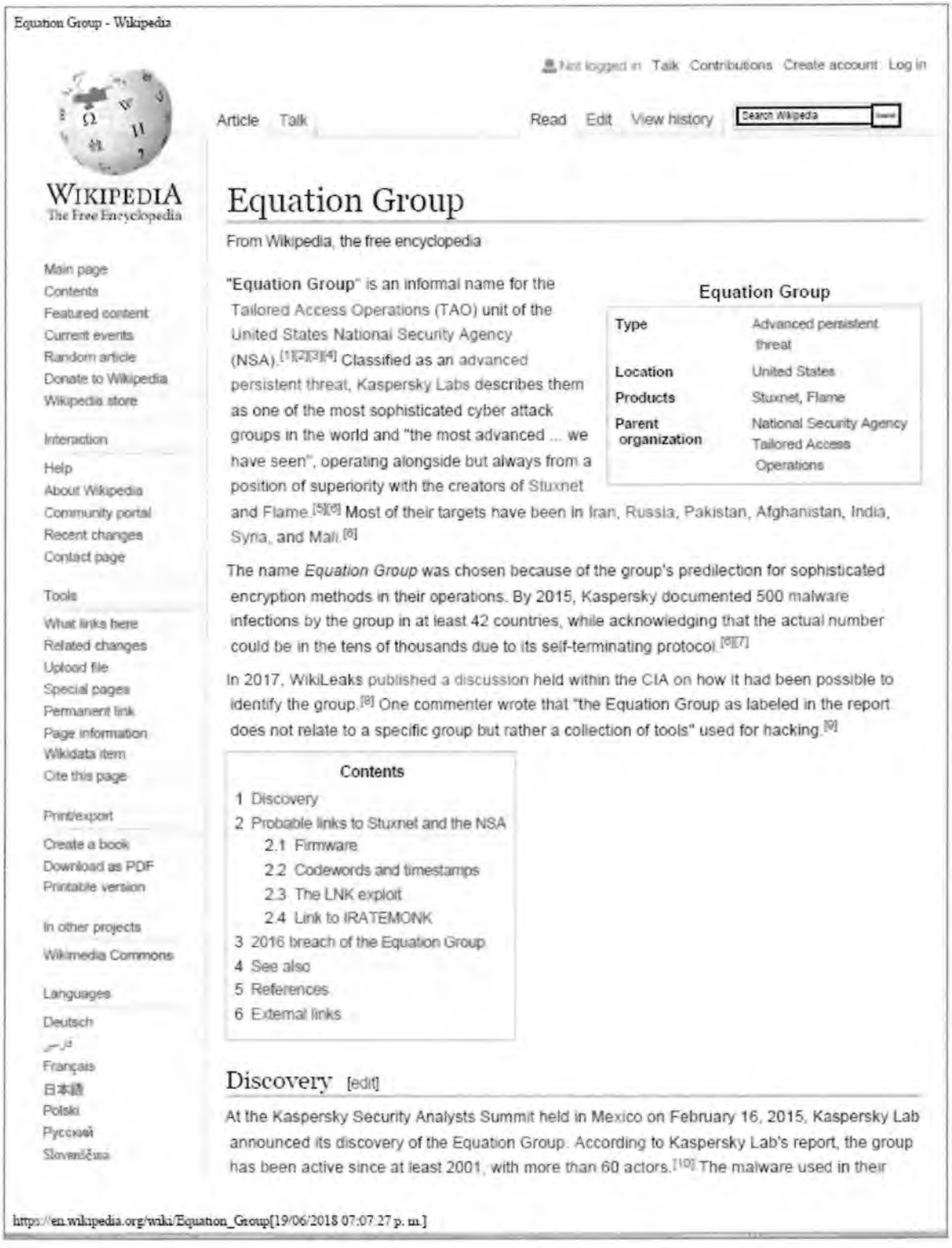
- Port Scanning
- Hunting for MSSQL
- Service Identification
- Password Sniffing
- SNMP sweeping



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

ANEXO "N"

https://en.wikipedia.org/wiki/Equation_Group,
Consultada el 19 de junio de 2018



Equation Group - Wikipedia

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

In other projects
Wikimedia Commons

Languages
Deutsch
فارسی
Français
日本語
Polski
Русский
Slovenščina

Equation Group

From Wikipedia, the free encyclopedia

Equation Group

Type	Advanced persistent threat
Location	United States
Products	Stuxnet, Flame
Parent organization	National Security Agency Tailored Access Operations

"**Equation Group**" is an informal name for the Tailored Access Operations (TAO) unit of the United States National Security Agency (NSA).[1][2][3][4] Classified as an advanced persistent threat, Kaspersky Labs describes them as one of the most sophisticated cyber attack groups in the world and "the most advanced ... we have seen", operating alongside but always from a position of superiority with the creators of Stuxnet and Flame.[5][6] Most of their targets have been in Iran, Russia, Pakistan, Afghanistan, India, Syria, and Mali.[6]

The name *Equation Group* was chosen because of the group's predilection for sophisticated encryption methods in their operations. By 2015, Kaspersky documented 500 malware infections by the group in at least 42 countries, while acknowledging that the actual number could be in the tens of thousands due to its self-terminating protocol.[6][7]

In 2017, WikiLeaks published a discussion held within the CIA on how it had been possible to identify the group.[8] One commenter wrote that "the Equation Group as labeled in the report does not relate to a specific group but rather a collection of tools" used for hacking.[9]

Contents

1 Discovery
2 Probable links to Stuxnet and the NSA
  2.1 Firmware
  2.2 Codewords and timestamps
  2.3 The LNK exploit
  2.4 Link to IRATEMONK
3 2016 breach of the Equation Group
4 See also
5 References
6 External links

Discovery [edit]

At the Kaspersky Security Analysts Summit held in Mexico on February 16, 2015, Kaspersky Lab announced its discovery of the Equation Group. According to Kaspersky Lab's report, the group has been active since at least 2001, with more than 60 actors.[10] The malware used in their

https://en.wikipedia.org/wiki/Equation_Group[19/06/2018 07:07:27 p. m.]

operations, dubbed EquationDrug and GrayFish, is found to be capable of reprogramming hard disk drive firmware.[5] Because of the advanced techniques involved and high degree of covertness, the group is suspected of ties to the NSA, but Kaspersky Lab has not identified the actors behind the group.

Probable links to Stuxnet and the NSA [edit]

In 2015 Kaspersky's research findings on the Equation Group noted that its loader, "Grayfish", had similarities to a previously discovered loader, "Gauss", from another attack series, and separately noted that the Equation Group used two zero-day attacks later used in Stuxnet; the researchers concluded that "the similar type of usage of both exploits together in different computer worms, at around the same time, indicates that the EQUATION group and the Stuxnet developers are either the same or working closely together".[11]:13

Firmware [edit]

They also identified that the platform had at times been spread by interdiction (interception of legitimate CDs sent by a scientific conference organizer by mail),[11]:15 and that the platform had the "unprecedented" ability to infect and be transmitted through the hard drive firmware of several of the major hard drive manufacturers, and create and use hidden disk areas and virtual disk systems for its purposes, a feat demanding access to the manufacturer's source code of each to achieve,[11]:16–18 and that the tool was designed for surgical precision, going so far as to exclude specific countries by IP and allow targeting of specific usernames on discussion forums.[11]:23–26

Codewords and timestamps [edit]

The NSA codewords "STRAITACID" and "STRAITSHOOTER" have been found inside the malware. In addition, timestamps in the malware seem to indicate that the programmers worked overwhelmingly Monday–Friday in what would correspond to a 08:00–17:00 workday in an Eastern United States timezone.[12]

The LNK exploit [edit]

Kaspersky's global research and analysis team, otherwise known as GReAT, claimed to have found a piece of malware that contained Stuxnet's "privLib" in 2008.[13] Specifically it contained the LNK exploit found in Stuxnet in 2010. Fanny is classified as a worm that affects certain Windows operating systems and attempts to spread laterally via network connection or USB storage. Kaspersky stated that they suspect that because of the recorded compile time of Fanny that the Equation Group has been around longer than Stuxnet.[5]

Link to IRATEMONK [edit]

F-Secure claims that the Equation Group's malicious hard drive firmware is TAO program "IRATEMONK",[14] one of the items from the NSA ANT catalog exposed in a 2013 *Der Spiegel* article. IRATEMONK provides the

attacker with an ability to have their software application persistently installed on desktop and laptop computers, despite the disk being formatted, its data erased or the operating system re-installed. It infects the hard drive firmware, which in turn adds instructions to the disk's master boot record that causes the software to install each time the computer is booted up.[15] It is capable of infecting certain hard drives from Seagate, Maxtor, Western Digital, Samsung,[15] IBM, Micron Technology and Toshiba.[5]

The NSA's listing of its Tailored Access Operations program named IRATEMONK from the NSA ANT catalog.

2016 breach of the Equation Group [edit]

In August 2016, a hacking group calling itself "The Shadow Brokers" announced that it had stolen malware code from the Equation Group.[16] Kaspersky Lab noticed similarities between the stolen code and earlier known code from the Equation Group malware samples it had in its possession including quirks unique to the Equation Group's way of implementing the RC6 encryption algorithm, and therefore concluded that this announcement is legitimate.[17] The most recent dates of the stolen files are from June 2013, thus prompting Edward Snowden to speculate that a likely lockdown resulting from his leak of the NSA's global and domestic surveillance efforts stopped The Shadow Brokers' breach of the Equation Group. Exploits against Cisco Adaptive Security Appliances and Fortinet's firewalls were featured in some malware samples released by The Shadow Brokers.[18] EXTRABACON, a Simple Network Management Protocol exploit against Cisco's ASA software, was a zero-day exploit as of the time of the announcement.[18] Juniper also confirmed that its NetScreen firewalls were affected.[19] The EternalBlue exploit was used to conduct the damaging worldwide WannaCry ransomware attack.

See also [edit]

- Global surveillance disclosures (2013–present)
- United States intelligence operations abroad
- Firmware hacking

References [edit]

1. ^ Fox-Brewster, Thomas (February 16, 2015). "Equation = NSA? Researchers Uncloak Huge 'American Cyber Arsenal'". *Forbes*. Retrieved November 24, 2015.
2. ^ Menn, Joseph (February 17, 2015). "Russian researchers expose breakthrough U.S. spying program". Reuters. Retneved November 24, 2015.
3. ^ "The nsa was hacked snowden documents confirm". *The Intercept*. 19 August 2016.

ANEXO "O"

http://securityaffairs.co/wordpress/46702/cyber-crime/armada-collective.html

Consultada el 31 de diciembre de 2018

Businesses pay $100k to alleged Armada Collective to avoid DDoSSecurity Affairs

Businesses pay $100k to alleged Armada Collective to avoid DDoS

April 26, 2016 By Pierluigi Paganini

Businesses have already paid more than $100.000 to DDoS extortionists who claim to be the dreaded Armada Collective, but that never DDoS anyone.

A criminal organization made $100,000 from a number of businesses across the globe my threatening them of distributed denial-of-service (DDoS) attack. The criminals requested to the victims the payment of a ransomware to avoid being targeted by powerful DDoS, the worrying aspect of the story is that they is that they never launched a single attack.

The extortion is a consolidated practice in the criminal ecosystem, groups like DD4BC used a consolidated scheme to convince victims to pay the ransomware. Typically attackers launch a demonstrative attack that temporarily shut down the victim's website then the crooks send a message to the victims requesting the payment of the ransom.

In September 2015, Akamai published samples of the extortion emails sent by the DD4BC group to the victims demanding ransom ranging from 25 Bitcoins to 50 Bitcoins ($6,000 and $12,000 at current currency exchange rates).

"Your site is going under attack unless you pay 25 Bitcoin," one email stated. "Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother."

The attackers promise never to threaten the victim twice if they will pay the ransom. In the case victims ignore the first message they will receive a subsequent email to warn them against ignoring the ransom demand.

"And you are ignoring us. Probably because you don't want to pay extortionists. And you believe that after sometime we will give up. But we never give up," the follow-up messages read.

Back to the present, a group called Armada Collective is threatening companies worldwide, the crew is the same that shut down the popular encrypted mail service ProtonMail in November 2015 and extorted $6,000 to stop a prolonged DDoS attack that knocked it offline.

A hundred companies have received emails from the alleged members of Armada Collective demanding as much as $23,000

http://securityaffairs.co/wordpress/46702/cyber-crime/armada-collective.html[31/12/2018 03:27:35 p. m.]

Businesses pay $100k to alleged Armada Collective to avoid DDoSSecurity Affairs

in Bitcoins in exchange for not being attacked.

A number of members of the Armada Collective were arrested in January 2016, so many experts speculate that someone is abusing the reputation of the Armada Collective for profit, and it works!

"We heard from more than 100 existing and prospective CloudFlare customers who had received the Armada Collective's emailed threats. We've also compared notes with other DDoS mitigation vendors with customers that had received similar threats," states a blog post published by Cloudflare.

"Our conclusion was a bit of a surprise: we've been unable to find a single incident where the current incarnation of the Armada Collective has actually launched a DDoS attack. In fact, because the extortion emails reuse Bitcoin addresses, there's no way the Armada Collective can tell who has paid and who has not. In spite of that, the cybercrooks have collected hundreds of thousands of dollars in extortion payments."

04/18/2016 11:20 pm Armada Collective

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.
http://rmgtfy.com/?q=Armada+Collective

Most importantly, we have launched largest DDoS in Swiss history and one of the largest DDoS attacks ever. Search for "ProtonMail DDoS"

All your servers will be DDoS-ed starting Monday (April 25) if you don't pay protection fee - exactly 10.08 Bitcoins @ 1Fz3DXGH6aa16sEBLBBXfZfFFNCfc3Pu2

If you don't pay by Monday, attack will start, yours service going down permanently price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

This is not a joke.
Our attacks are extremely powerful - peak over 1 Tbps per second.

Do not reply, we will not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!
Bitcoin is anonymous, nobody will ever know you cooperated.

At the time I was writing, no DDoS attack was launched by the criminal organizations against the victims.

Pierluigi Paganini

(Security Affairs – Armada Collective, DDoS attacks)

Share this...

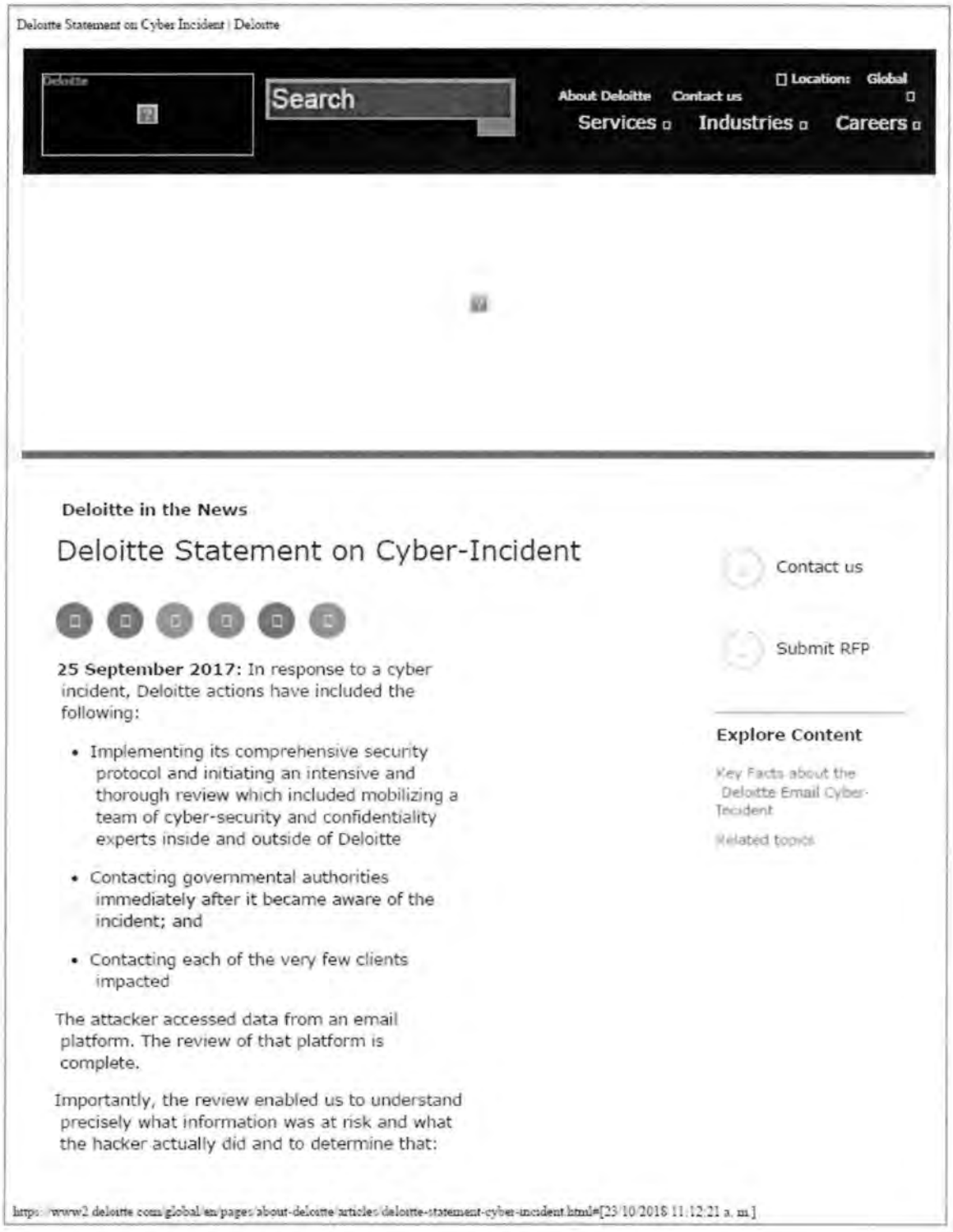
SHARE ON

http://securityaffairs.co/wordpress/46702/cyber-crime/armada-collective.html[31/12/2018 03:27:35 p. m.]

ANEXO "P"

https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html

Consultada el 23 de octubre de 2018



Deloitte Statement on Cyber Incident | Deloitte

Deloitte

Search

About Deloitte Contact us Location: Global

Services Industries Careers

Deloitte in the News

Deloitte Statement on Cyber-Incident

Contact us

Submit RFP

Explore Content

Key Facts about the Deloitte Email Cyber-Incident

Related topics

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:

https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html#[23/10/2018 11:12:21 a. m.]

- 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 distinct and

separate from other Deloitte platforms, including those that host client data, collaborative work among Deloitte professionals, engagement systems and other non-cloud based email systems. None of these were impacted. We know from the forensic review conducted by our own cyber professionals, working alongside outside experts, that the attacker was specifically focused on obtaining active credentials.

- **Reviewed materials targeted by the hacker.** This incident involved unstructured data; namely, email. Through a detailed review of logs, Deloitte was able to determine what the attacker actually did and that the number of 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

Partnering for cyber resilience

Risk & responsibility in a hyperconnected world

Deloitte social media

Join the conversation

Related topics

Conduct Risk

Cyber Risk

Brand & Reputation Risk

Cyber Resilience

Cyber Vigilance

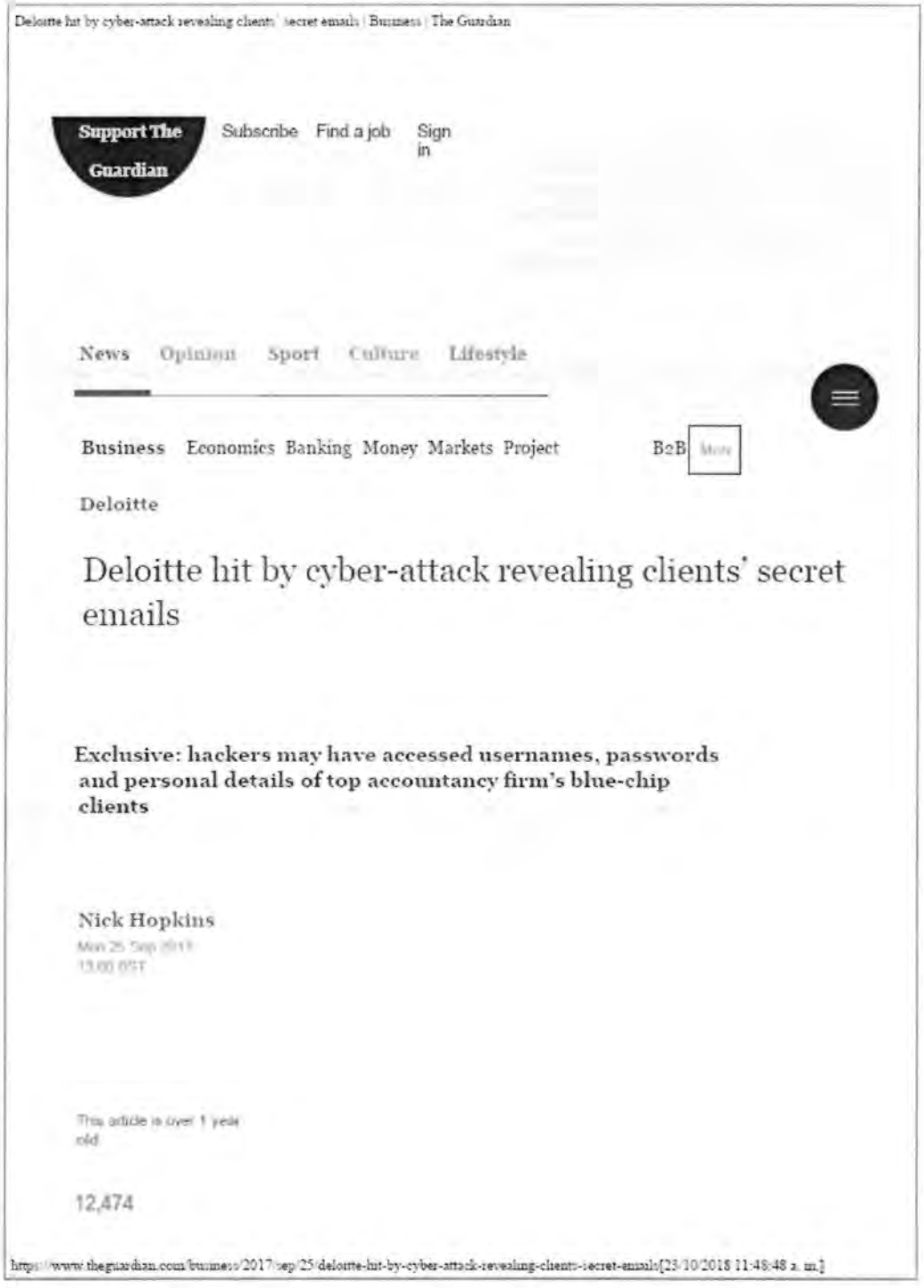
Contact us | Submit RFP | Job search

Get Connected	Services	Industries	Careers	Legal
Newsroom	Audit & Assurance	Consumer	Job search	About Deloitte
Home	Consulting	Energy, Resources & Industrials	Experienced hires	Terms of use
Social media	Risk Advisory	Financial Services	Students	Cookies
Leadership blog	Financial Advisory	Government & Public	Life at Deloitte	Privacy
Press releases	Legal		Alumni	Privacy Shield

ANEXO "Q"

https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails

Consultada el 23 de octubre de 2018



Deloitte hit by cyber-attack revealing clients' secret emails | Business | The Guardian

Support The Guardian Subscribe Find a job Sign in

News Opinion Sport Culture Lifestyle

Business Economics Banking Money Markets Project B2B More

Deloitte

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

This article is over 1 year old

12,474

https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails[23/10/2018 11:48:48 a. m.]

Deloitte hit by cyber-attack revealing clients' secret emails | Business | The Guardian

Deloitte provides auditing, tax consultancy and cybersecurity advice to banks, multinational companies and government agencies. Photograph: Alamy Stock Photo

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.

https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails[23/10/2018 11:48:48 a. m.]

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.

ANEXO "R"

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 23 de octubre de 2018

Israel hacked Kaspersky, then tipped the NSA that its tools had been breached - The Washington Post

Sections

The Washington Post
Democracy Dies in Darkness

Sign In | Try 1 month for $1

National Security

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

People walk past the headquarters of the anti-virus firm Kaspersky Lab in Moscow in September. (Sergei Karpukhin/Reuters)

By Ellen Nakashima
October 10, 2017

In 2015, Israeli government hackers saw something suspicious in the computers of a Moscow-based cybersecurity firm: hacking

https://www.washingtonpost.com/.../0/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?noredirect=on&utm_term=.24315eeeec5b[23/10/2018 12:12:00 p. m.]

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.

[Local governments keep using this software — but it might be a back door for Russia]

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."

Eugene Kaspersky, chief executive of Russia's Kaspersky Lab. (Pavel Golovkin/AP)

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.

Ellen Nakashima Ellen Nakashima is a national security reporter for The Washington Post. She covers cybersecurity, surveillance, counterterrorism and intelligence issues. She has also served as a Southeast Asia correspondent and covered the White House and Virginia state politics. She joined The Post in 1995. Follow

ANEXO "S"

https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01

Consultada el 23 de octubre de 2018

Homeland Security

News

Search

Blog Data Events Fact Sheets Homeland Security LIVE

In Focus Media Contacts Multimedia

National Terrorism Advisory System Podcasts

Press Releases Publications Library Social Hub

Social Media Speeches Testimony News Archive

Comunicados de Prensa

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: Cybersecurity
Keywords: cyber security, information

Last Published Date: July 17, 2018

Anexo "T"

https://ww3.bancochile.cl/wps/wcm/connect/nuestro-banco/portal/sala-de-prensa/noticias-y-comunicados/carta-a-clientes-sobre-incidente-tecnologico

Consultada el 23 de octubre de 2018

12 JUN 2018 | Carta a clientes sobre incidente tecnológico

En nuestro permanente interés por mantener informados a nuestros clientes, nos referimos al incidente de seguridad tecnológica que afectó a Banco de Chile y a las medidas adoptadas para resolverlo.

El día jueves 24 de mayo pasado se detectó que terceros, delincuentes internacionales altamente sofisticados, a través de acciones ilícitas sustrajeron desde cuentas propias de Banco de Chile en bancos corresponsales del exterior, una cifra aproximada a US$10 millones, dinero que corresponde a fondos del Banco y no de sus clientes. Respecto de dicha suma, el Banco inició las gestiones tendientes a obtener su recuperación.

Para facilitar la perpetración del delito, y para dificultar su detección, este grupo delictual introdujo un virus (Malware Swapq) que afectó algunos sistemas del Banco, impidiendo su normal funcionamiento.

Ante esta situación se activaron nuestros protocolos de seguridad y el plan de contingencia, lo que permitió controlar el incidente, continuar con la operación del Banco y asegurar la integridad de los datos e información, de manera que no se vieran perjudicadas las transacciones, registros, fondos y productos de nuestros clientes.

Lo anterior afectó principalmente la calidad de servicio en sucursales y banca telefónica, considerando especialmente que dentro de las medidas adoptadas se incluyó la desconexión de la mayoría de los terminales computacionales, quedando plenamente restablecidos nuestros servicios a comienzo de la semana siguiente. Nuestra página web y el resto de los canales móviles, así como nuestra red de cajeros automáticos se mantuvieron operativos.

Lamentamos profundamente los inconvenientes que generó esta situación que se reflejó en la lentitud operativa de nuestras sucursales (pagos de cheques y/o Vale Vistas, efectuar cambio de claves presenciales entre otros). Sin embargo, estamos convencidos que nuestra reacción permitió preservar la seguridad de sus datos, fondos y productos.

Durante los 125 años de trayectoria de Banco de Chile, nuestros clientes han sido siempre el centro de nuestro actuar, y en este incidente todas nuestras acciones estuvieron enfocadas en resguardar a todos y cada uno de ustedes.

Continuamos trabajando arduamente no sólo para que estos hechos no se repitan, sino que también para seguir entregando los mejores servicios financieros, de forma ágil, y con los mayores estándares de seguridad, para de esa forma responder a la confianza que ustedes han depositado en nosotros.

Un afectuoso saludo.

Eduardo Ebensperger O.
Gerente General
Banco de Chile

Anexo "U"

https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html

Consultada el 23 de octubre de 2018

BY JOSHUA HAMMER
ILLUSTRATIONS BY FRANCESCO FRANCAVILLA
MAY 3, 2018

IN 2016, A MYSTERIOUS SYNDICATE TRIED TO STEAL $951 MILLION FROM BANGLADESH'S CENTRAL BANK — AND LAID BARE A PROFOUND WEAKNESS IN THE SYSTEM BY WHICH MONEY MOVES AROUND THE WORLD.

At 8:45 in the morning on Friday, Feb. 5, 2016, Zubair Bin Huda, a director at Bangladesh's central bank, entered the 30-story, concrete-and-glass headquarters in Dhaka. Bin Huda, slim and soft-spoken, with a thin black mustache and beard, rode an elevator to the ninth floor and eventually walked into the back office of the Accounts and Budgeting Department's "dealing room," the most restricted area of the building, accessible to only a handful of employees.

Until about a decade ago, Bangladesh's central bank was stuck in the analog age: Staff members sent international payment instructions via a teleprinter, an electromechanical typewriter that sent and received messages over standard phone lines and other channels. But since a new bank governor took over in 2009, the institution had gone digital. Its international transfer orders are now dispatched via Swift, the Brussels-based electronic network used by 11,000 financial institutions in more than 200 countries and territories. Inside a 12-foot-by-8-foot glass-walled chamber, under the scrutiny of closed-circuit security cameras, staff members log into Swift and dispatch the payment orders with encrypted communications. With a few keystrokes, a complex process is set in motion that sends millions of dollars zipping across continents.

Bin Huda was the duty manager that morning, which meant he was tasked with scrutinizing printouts of transfer confirmations, routine queries and other Swift messages that had come in overnight. Friday is a bank holiday in Bangladesh, but a dedicated printer still generated hard copies of digital transfer messages. A few dozen would usually come in over the course of a day,

Bangladesh, but a dedicated printer still generated hard copies of digital transfer messages. A few dozen would usually come in over the course of a day, but that morning Bin Huda didn't see any on the printer. He assumed it was a technical glitch and decided to deal with it on Saturday.

At 9 o'clock the next morning, he returned to the office. This time, he found that the Swift software — the program that launches the messaging service — wasn't functioning, either. Each time he tried to open it, a disconcerting error message appeared: *A file is missing or changed.* He and his colleagues huddled over the dedicated Swift computer, following directions on the monitor on how to get the software running again. Shortly after noon, he was able to retrieve three messages from the Federal Reserve Bank of New York and to print them out one by one. The New York Fed is, in effect, the gatekeeper of much of world banking, and hosts accounts for 250 central banks and governments with deposits of about $3 trillion. A Fed employee had written to Bangladesh, asking for clarification about 46 payment instructions received over the past 24 hours. The Fed had never seen orders like that or a total so large from the bank — nearly $1 billion.

'IF THAT LINKAGE IS TRUE, THAT MEANS A NATION-STATE IS ROBBING BANKS. THAT'S A BIG DEAL; IT'S DIFFERENT.'

It had to be a mistake, Bin Huda thought. Bangladesh Bank, as the central bank is known, never sent payment instructions on weekends, and even during business hours, it rarely sent more than two or three to the Fed in a day. He scrolled through the message file in search of more information. Where was the money headed? The one debit statement he could find was corrupted and unreadable. Desperate to stop the transactions from moving forward, but unsure where to turn, Bin Huda emailed a Swift case manager at the organization's Brussels headquarters. He told bank officials that he had reported a "big accident" in the Swift system. He tried to reach the Fed in New York by telephone, but the bank was shut down for the weekend. Bin Huda emailed and faxed a demand to the Fed to stop processing all payments, including all those mentioned in the queries. Hoping that someone would get the message, Bin Huda then shut down his computer and went home to enjoy his weekend with his family.

ALTHOUGH NO ONE KNEW THIS YET, Bin Huda was in the middle of the most daring bank robbery ever attempted using Swift. And it would prove to be the most severe breach yet of a system designed to be unbreachable. Swift's transmission process — by which money moves through the dispatching of encrypted messages to multiple operating centers and then on to the receivers — has become the standard in the banking world, flawlessly processing more than three billion payment orders a year. It uses "military grade" security systems, says Adrian Nish, the head of Threat Intelligence for BAE Systems, a cybersecurity firm in Britain that investigated the attack on Bangladesh Bank. Swift (the acronym stands for the Society for Worldwide Interbank Financial Telecommunication, a cooperative founded in 1973 and owned by its member banks) recommends that its institutions use multifactor authentication to log on and that they segregate the Swift server from the rest of their internal network.

Even for skilled and dedicated hackers, the most viable path to penetrating Swift runs through the member banks, which operate the software that lets them log into the Swift system — providing "the technical handshake that opens the secure pipe," as one cybersecurity expert put it to me. During the past three years, a rash of smaller incidents have shown the vulnerabilities in the system, as cyberthieves broke into the computer networks of banks in Ecuador, Taiwan, Vietnam, Poland, India and Russia to send out phony payment instructions via the Swift network. Alert bank officials were able to call back some fake payments, but millions of dollars were lost. "A lot of institutions in emerging markets don't have the same security controls that more mature banks have," says Patrick Neighorn of FireEye, a U.S. cybersecurity firm. "In some the passwords aren't centrally managed, or they didn't know what all the devices connecting their network are."

ANEXO "V"

http://www.reuters.com/article/us-greece-cenbank-cyber/anonymous-attack-greek-central-bank-warns-others-idUSKCN0XV0RR

Consultada el 23 de octubre de 2018

Anonymous attack Greek central bank, warns others

Directory of sites Login Contact Support

World Business Markets Politics TV

Search

#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.

ANEXO "W"

https://roguemedialabs.com/2018/12/13/anonymous-launches-opicarus-2-0/
Consultada el 23 de Diciembre de 2018

Anonymous Launches #OpIcarus 2.0

BY BRIAN DUNN *on* DECEMBER 13, 2018 • (0)

Over the course of the last few weeks covering different hacking operations throughout the world, I've begun picking up on rumblings of the re-emergence of *#OpIcarus*. For those of you whom are not already aware, *#OpIcarus* was largely considered one of the most successful hacking operations of the last decade, targeting countless international banking and financial institutions worldwide – *even the US Stock Exchange was targeted*. Considering that the operation *garnered international front page headlines* for the better part of a year and a half, *#OpIcarus* is also generally considered to be one of, if not the single biggest Anonymous hacking operations of the 21st Century, resulting in anywhere from tens of millions to hundreds of millions dollars lost.

Back in 2015 – 2016, the operation was largely spear-headed by *Ghost Squad Hackers*, whom possessed the skills, tools and know-how necessary for hackers to pull of the majority of attacks. But truth be told, the operation actually had its origins in Pakistan through a small group of hackers known as the "*Anonymous Predators*," alleged to be the gate-keepers of Anonymous "*Red Cult*" – another (in)famous branch of Anonymous.

Fast forward to today however, the operation is largely being led by "***Lorian Synaro***" – perhaps Anonymous' single largest and most active/influential voice in 2018. While the operation hasn't fully caught on yet, various activists around the web are trying to spread the word and begin building followers/participants – with the majority of all hacks occurring over the course of the last 36 hours. "*This is an operation against the baking system worldwide. Aims to fight corruption and the criminals banking*" *Lorian Synaro* told *Rogue Media Labs*, "*We need a lot of people in this Op.*"

About *#OpIcarus2018*, in statements to *Rogue Media Labs* earlier today, "*M1r0x*" of *Ghost Squad Hackers* said "*Operation #OpIcarus 2016 was a success, many banks were touched for several hours or even days, the #OpIcarus 2018 version is rather a good idea to prove that banks are not secure. The operation will also target governments, if the operation against the banks in 2018 is a success as in 2016, yes why not participate, for the moment I observe in silence.*"

As of December 13th 2018 *Anonymous Pakistan* and *Red Cult* both have declined comment on the matter. For the time being, here's what we know about the operation so far:

Operation Hit List: *https://ghostbin.com/paste/m2uoc*

Banks Hit To Date:

hxxp://centralbankbahamas.com
hxxp://cbiraq.org/
hxxp://centralbank.org.bb
hxp://bcu.gub.uy/
hxxp://www.bkam.ma/
hxxp://banxico.org.mx/
hxxp://centralbankofindia.co.in
hxxps://bankofalbania.org/
hxxp://bankjerusalem.il
hxxps://www.bancaditalia.it
hxxps://www.rba.gov.au
hxxps://www.bis.org/

Example of Target Reconnaissance:

https://pastebin.com/vwmHy5Zf – rothchildandco.com
https://pastebin.com/hkSRufiy – bportugal.pt
https://pastebin.com/3VZ5JKGZ – boz.zm

> New attack for the OpIcarus:
> * Target: The Central Bank of Bahamas - https://t.co/r3k76Lo35v #Offline
> * #Down: https://t.co/m9ZaWZHO9c
> ——————————————————————#TangoDown - #Pryzraky - #OpIcarus2018 - @LorianSynaro pic.twitter.com/FFajUuCdYN
>
> — SHIZ3N ⊏ (@zglobal_) December 13, 2018

> #Anonymous #OpIcarus #ShutDownTheBanks #OpGlobalAwakening
>
> All #TangoDown:
> Central Bank of Albania
> Central bank of Mexico
> Vatican official Website
> Central Bank of Bahamas #Down by @zglobal_
>
> Sites:https://t.co/voC5tguIRihttps://t.co/dfScY3XjTMhttps://t.co/epghNhMbAJ pic.twitter.com/6OdrB6HvZY
>
> — Lorian Synaro (@LorianSynaro) December 13, 2018

> @StateBank_Pak You are one of a target of Anonymous. Prepare to defend yourself for DDoS like attacks or not. @ARYNEWSOFFICIAL @ExpressNewsPK @geonews_urdu https://t.co/2eHRZ6aLCI#Anonymous #OpIcarus #Pakistan
>
> — Waqar Ahmed (@W4444Q4444R) December 12, 2018

> "RT @LorianSynaro: #Anonymous #OpIcarus #YellowVests #ShutDownTheBanks #StopActa2 The official website of the Italian Central Bank #DOWN Re... https://t.co/unXlahflu7 ..."
>
> — Anti-control group (@AntiCtrl) December 12, 2018

> #Anonymous #Revolution #OpIcarus #YellowVests #StopActa2
>
> We begin hunting the Elite today. Vatican official site (The masters of corruption) and the Bank for International Settlements (Rothschild owned bank) both #DOWN.
>
> Sites: https://t.co/tNqoWl1PJIhttps://t.co/27gKdLdzZ9 pic.twitter.com/EopyYzZ5Tz
>
> — Lorian Synaro (@LorianSynaro) December 5, 2018

> #Pryzraky #OpIcarus #OpIcarus2018 @zglobal_
>
> The Central Bank Of India (@centralbank_in) has been downed by #Pryzraky Target: https://t.co/DpyXiq8Gp0#TangoDown#Offline #Down #NetNeutrality pic.twitter.com/Z4BjOmPfno
>
> — #Pryzraky (@Pryzraky) December 14, 2018

> Bank of Jerusalem site is #Offline #TangoDown ->https://t.co/G3UMiYsbL8<-
>
> Web: https://t.co/eUbp9WB22u
>
> ns1:https://t.co/eg0ILWXkC0
>
> ns2:https://t.co/yUenCOQsrk#Anonymous #OpIsrael #FreePalestine #FreeGaza #FckIsrael #GazaUnderAttack #Gaza pic.twitter.com/AxqVsdSUiJ
>
> — Gow_Th_ĕr (@Gow_Th_er) November 19, 2018

ANEXO "X"

https://www.bancomext.com/comunicados/18443

Consultada el 23 de Octubre de 2018

Ciudad de México a 10 de enero de 2018

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

--0-0--

ANEXO "Y"

http://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7B82AA2232-6678-F306-C66A-94868230AE4A%7D.pdf

Consultada el 23 de Octubre de 2018

BANCO DE MÉXICO

Comunicado de Prensa

14 de mayo de 2018

Acciones emprendidas por el Banco de México para mitigar los riesgos de ocurrencia de incidentes operativos en los participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI)

En seguimiento a los comunicados de prensa emitidos por este Banco Central el pasado 27 y 30 de abril del año en curso, en los que se informó sobre las afectaciones de algunos participantes en el servicio de transferencias electrónicas del Sistema de Pagos Electrónicos Interbancarios (SPEI), se destaca que, hasta la fecha, las afectaciones se han registrado en algunos aplicativos e infraestructura de cómputo de algunos participantes para preparar sus órdenes de pago y conectarse al SPEI.

Cabe destacar que la infraestructura y el sistema central del SPEI en el Banco de México no han sufrido afectación alguna. La infraestructura de pagos y el SPEI se han mantenido en operación y han seguido procesando los millones de transferencias que se generan de manera ordinaria cada día. En algunos casos, algunos participantes han visto retrasada su operación en la medida que han reforzado los procesos de revisión y mitigación de riesgos. Es muy importante señalar que, a la fecha, no hay indicios de que se hayan visto afectados los recursos de los clientes en ninguna de las instituciones participantes en el SPEI, toda vez que las incidencias se han presentado en cuentas de las propias instituciones financieras, las cuales han sido acotadas, se han mitigado y no han afectado la salud financiera de las mismas.

Asimismo, se considera conveniente hacer del conocimiento del público las acciones que ha realizado este Instituto Central, para coadyuvar a que las instituciones participantes en el sistema refuercen sus procesos e infraestructuras tecnológicas para mitigar el riesgo de ocurrencia de este tipo de incidentes.

BANCO DE MÉXICO

En el ámbito tecnológico, este Instituto Central tomó medidas para que los participantes en los que se detectaron los incidentes, operen por vías alternas y mantengan su capacidad para enviar órdenes de transferencias a la infraestructura del SPEI. Asimismo, se han tomado acciones para mitigar las vulnerabilidades detectadas en algunos participantes, además de requerirles establecer elementos adicionales de control para minimizar la probabilidad de que presenten otros incidentes.

En el ámbito operativo, se requirió a los participantes cuyos aplicativos e infraestructura de cómputo para conectarse al SPEI resultaron afectados, tomar medidas para renovar los elementos de seguridad de sus operadores para autenticarse en los sistemas de pagos operados por el Banco de México, al tiempo que este Instituto Central ha ampliado y fortalecido el esquema de soporte a todos los participantes del sistema.

En el ámbito regulatorio, el Banco de México ha decidido emitir disposiciones que otorguen a las instituciones de crédito y demás entidades que prestan el servicio de transferencias de fondos, espacio para que estas implementen medidas de control adicionales encaminadas a fortalecer sus sistemas de detección de transferencias irregulares, verificar la integridad de sus operaciones y evitar posibles afectaciones a dichas instituciones, al resto de los participantes y al sistema en su conjunto.

En particular, por medio de la Circular 4/2018, y hasta que el Banco de México lo considere conveniente, los participantes contarán con un día para entregar en efectivo o cheques de caja los recursos correspondientes a transferencias de fondos entre participantes o traspasos al interior de ellos, por montos iguales o superiores a 50 mil pesos, excepto en aquellos casos autorizados expresamente por los participantes, respecto de cada cliente, con base en sus características y operatividad. En todo caso, con esta norma, no se afectará la acreditación de los recursos de las transferencias y traspasos en las cuentas respectivas o su disposición por cualquier otra vía. Por otra parte, mediante la Circular 5/2018, a los participantes en el SPEI que reciban transferencias de fondos, y que así lo soliciten, se les podrá autorizar que puedan llevar a cabo las validaciones de dichas transferencias en periodos de tiempo superiores a los establecidos en las reglas aplicables para el abono de los recursos en las cuentas de los clientes beneficiarios (5 o 30 segundos, dependiendo del tipo

BANCO DE MÉXICO

de participante), hasta en tanto concluyan las automatizaciones de las verificaciones que deben desarrollar.

Finalmente, se reitera al público que las transferencias electrónicas procesadas a través del SPEI, así como a través del resto de los sistemas de pagos a cargo de este Instituto Central, son un medio seguro para realizar pagos. El Banco de México continuará ejerciendo sus facultades, para implementar las acciones necesarias y cumplir con su finalidad de propiciar el buen funcionamiento de los sistemas de pagos.

ANEXO "Z"

https://axa.mx/web/blog/postura-de-axa-mexico?utm_source=twitter&utm_medium=comunicado-oficial&utm_campaign=ciber-ataque&utm_content=banxico

Consultada el 23 de Octubre de 2018

AXA MÉXICO

Comunicado oficial

Sin afectaciones a datos o recursos de asegurados: AXA

Ciudad de México, 23 de octubre del 2018.- Tras el ataque detectado en contra de AXA, en torno a las incidencias en el Sistema de Pagos Electrónicos (SPEI) reportadas por el Banco de México, AXA confirma que la información y recursos de sus asegurados está en completo resguardo y no han sufrido ninguna afectación.

El pasado 22 de octubre, el monitoreo del funcionamiento del sistema financiero detectó algunos elementos que determinaron un ataque cibernético a AXA en el SPEI, lo cual llevó a las autoridades financieras a solicitar a los participantes de los sistemas de pagos el incremento de los niveles de alerta y esquemas de vigilancia. Asimismo, el Banco de México elevó a rojo el nivel de alerta de seguridad informática en la operación de los participantes en los sistemas de pagos.

Respecto a este tema, AXA informa lo siguiente:

- Desde el primer momento en que detectamos esta incidencia con SPEI, notificamos al Banco de México e implementamos diferentes acciones para robustecer y garantizar aún más nuestros procesos de seguridad.
- Diferentes equipos de la compañía están trabajando de manera coordinada con Instituciones y Autoridades para dar una rápida solución a esta incidencia.
- Los recursos y datos de nuestros clientes no han sufrido ninguna afectación y su seguridad está garantizada.

AXA es una compañía global con más de 30 años de historia y opera conforme a altos estándares de calidad y seguridad.

De igual manera, AXA seguirá atenta al tema e informará oportunamente sobre situación adicional respecto a esta incidencia.

ANEXO "AA"

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

Consultada el 23 de Octubre de 2018

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

Fecha de consulta: 15/01/2018 09:14:32

Título	Cámaras de pago. Sistemas con liquidación en tiempo real. Una operación	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 Bajo Amplitud. SPEBA. Número de operaciones	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Pagos Electrónicos de Bajo Amplitud. SPEBA. Importe	Sistemas de pago. Sistemas con liquidación en tiempo real. Sistema de Liquidación de Órdenes INDEVAL. Número de operaciones	Sistemas de pago. Sistemas con liquidación en tiempo real. Sistema de Liquidación de Órdenes 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 SPEUA. Número de operaciones	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios en Dólares SPEUA. 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	Jul 2017 - Dic 2017
Periodicidad	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual
Cifra	Sin tipo de Cifra	Volumen	Flujo	Volumen	Flujo	Volumen	Flujo	Volumen	Flujo	Volumen	Flujo	Volumen
Unidad	Días	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Dólares	Operaciones
Base												
Aviso												
Tipo de Información	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles
Fecha	SF41080	SF41083	SF41077	SF41084	SF41076	SF61953	SF61952	SF46188	SF46189	SF309374	SF309376	
Ene 2017	20	4,817	467,311	N/E	N/E	308,784	76,038,943	35,510,393	15,877,771	N/E	N/E	
Feb 2017	19	5,091	413,319	N/E	N/E	298,395	66,953,520	34,817,473	21,505,904	N/E	N/E	
Mar 2017	22	4,261	547,787	N/E	N/E	281,479	74,000,279	43,316,349	28,180,217	N/E	N/E	
Abr 2017	16	3,545	448,980	N/E	N/E	252,679	55,917,207	35,954,794	21,494,560	N/E	N/E	
May 2017	23	4,220	517,595	N/E	N/E	326,838	66,966,356	37,835,714	21,984,093	N/E	N/E	
Jun 2017	22	4,115	480,922	N/E	N/E	341,455	76,053,069	43,886,937	28,093,965	N/E	N/E	
Jul 2017	21	5,027	409,892	N/E	N/E	305,917	64,619,046	35,242,771	21,576,446	130,273.00	11,209.4	
Ago 2017	23	4,393	471,344	N/E	N/E	291,195	68,621,226	42,207,091	27,005,752	157,260.00	11,615.3	
Sep 2017	21	3,887	485,392	N/E	N/E	N/E	N/E	42,471,988	21,601,177	147,545.00	10,970.5	
Oct 2017	22	4,406	414,698	N/E	N/E	N/E	N/E	40,171,872	22,504,509	N/E	N/E	
Nov 2017	20	3,680	629,207	N/E	N/E	N/E	N/E	43,888,884	21,719,410	N/E	N/E	
Dic 2017	19	3,749	596,451	N/E	N/E	N/E	N/E	48,579,238	29,656,129	N/E	N/E	

BANCO DE MÉXICO

Ciudad de México, a 11 de enero de 2019

COMITÉ DE TRANSPARENCIA
DEL BANCO DE MÉXICO
Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio **6110000074618** que nos turnó la Unidad de Transparencia el tres de enero 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:

> *"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. Por numero de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero: a) Nombres comerciales de los sistemas operativos instalados. b) Nombres comerciales y versiones de los antivirus o software de seguridad en Internet, instalados. c) Inicio y termino de la vigencia de cada licencia utilizada en los software mencionados en el anterior inciso b). 2. Por dirección web o URL (Localizador Uniforme de Recursos), de los protocolos HTTP (Protocolo de Transferencia de Hipertexto) y HTTPS (Protocolo seguro de transferencia de hipertexto), cual es utilizado en cada una de sus paginas electrónicas o webs oficiales, así como el tipo de protocolo de seguridad implementado, SSL (Capa de sockets seguros) o TLS (Seguridad de la capa de transporte). 3. De cada una de sus actuales paginas electrónicas o webs oficiales, fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) padecidos."*

Sobre el particular, 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, último párrafo, 109, 113, fracciones I y IV, y 114 de la Ley General de Transparencia y Acceso a la Información Pública; 1, 97, 102, 103, 105, último párrafo, 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; 3, 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, 19 Bis 1 y 20, del Reglamento Interior del Banco de México; Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Décimo Séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Vigésimo sexto, párrafo primero, 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; nos permitimos informarles que estas unidades administrativas clasifican como reservada diversa ***"Información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos"***, en los términos de la fundamentación y motivación expresadas en la prueba de daño que se adjunta al presente.

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", la información

BANCO DE MÉXICO

clasificada es accesible a todos los empleados de las gerencias de Desarrollo de Sistemas Operativos y de Tecnología de los Sistemas de Pagos, a los directores de Apoyo a las Operaciones y de Sistemas de Pagos, así como al director, gerentes, subgerentes, especialistas y jefes de oficina de la Dirección de Sistemas.

Por lo expuesto, y con fundamento en los artículos 44, fracción II, y 137, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, y 140 de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México; solicitamos atentamente a ese Comité de Transparencia, confirme la clasificación de reserva señalada anteriormente.

Atentamente,

LIC. JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN
Director de Apoyo a las Operaciones

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos.

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; 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, fracciones I y II 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 pueda comprometer la seguridad nacional, así como afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país o el buen funcionamiento del sistema de pagos, por lo que la información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos, se clasifica como reservada, en virtud de lo siguiente:

La divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que revelar información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos que utiliza y requiere este Instituto Central, compromete la seguridad nacional, esto es, pone en riesgo de destrucción, inhabilitación o sabotaje de la infraestructura de tal importancia para el Estado Mexicano que su destrucción o incapacidad tendría un impacto debilitador en la seguridad nacional; y de afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país o el buen funcionamiento del sistema de pagos; **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, lo que puede menoscabar la infraestructura que en caso de ser destruida o inhabilitada provocaría un impacto debilitador a la seguridad nacional, así como afectar seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, o el buen funcionamiento de los sistemas de pagos, arriesgando el funcionamiento de esos sistemas y, por lo tanto, de la economía nacional en su conjunto.

Al respecto, 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 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 cuales comprenden sus funciones de banca. 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 dichos procesos.

En este sentido, el artículo 3 de la Ley de Seguridad Nacional, entiende como seguridad nacional, entre otras, las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a la preservación de la democracia, fundada en el **desarrollo económico** social y político del país y sus habitantes.

Por su parte, 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 que tiendan a mantener la integridad, estabilidad y permanencia del Estado Mexicano, entre las que se encuentra el propiciar el buen funcionamiento de los sistemas de pagos, actividad que depende en buena medida del **software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos.**

Consecuentemente, pretender atacar o inhabilitar los sistemas de tecnologías de la información y comunicaciones que utiliza el 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 la información referente software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos y el propósito de los mismos, posibilita la destrucción, inhabilitación o sabotaje de la infraestructura tecnológica indispensable para la preservación de la seguridad nacional, como lo es la del Banco de México, Banco Central del Estado Mexicano, por mandato constitucional.

Los riesgos aludidos tienen mayor probabilidad de materializarse con la entrega de la información, debido a que **los delincuentes podrían diseñar estrategias para llevar a cabo ataques cibernéticos** dirigidos específicamente a la infraestructura tecnológica de este Banco Central; dichos ataques focalizados podrían tener mayor probabilidad de éxito debido a que los delincuentes tendrían la

posibilidad de dedicar todos sus recursos a ataques específicos identificados con base en la información en cuestión.

Es importante destacar que los sistemas informáticos que utiliza el Banco de México, como lo es **el software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos,** son adquiridos, desarrollados o destinados para atender la implementación de las políticas en materia monetaria, cambiaria o del sistema financiero o el buen funcionamiento del sistema de pagos, por tal motivo, divulgar información relacionada con éstos, puede repercutir en su inhabilitación y en un extremo escenario, podría perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a los usuarios de los sistemas de pagos -tanto de las instituciones financieras como de las personas físicas y morales-.

En efecto, proporcionar la "***Información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos***", facilita que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a dichas tecnologías.

Asimismo, los ataques a las tecnologías de la información y de comunicaciones 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 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 y, en general, de cualquier información relacionada con los sistemas correspondientes e infraestructura informática.

Otra característica que debe destacarse de este tipo de ataques, es la propia evolución de los equipos y sistemas, pues con cada actualización, 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 ataque. 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, por lo que 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 materia de esta prueba de daño, la cual el Banco Central de la Nación emplea para dar soporte a los procesos de atención e implementación de las políticas en materia monetaria, cambiaria o del sistema financiero o el buen funcionamiento

del sistema de pagos, permite reducir sustancialmente 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 podría substraer, interrumpir o alterar información referente 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 como agente financiero del Gobierno Federal y las que lleva a cabo con propósitos de regulación monetaria y cambiaria; información que no debe ser alterada o divulgada de forma no autorizada, pues de hacerlo afectaría la efectividad de las medidas adoptadas en relación con el sistema financiero del país o el buen funcionamiento del sistema de pagos.

Por las razones expuestas, divulgar la referida información compromete la seguridad nacional, afecta la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país o el buen funcionamiento del sistema de pagos, en términos del artículo 113, fracciones I y IV, de la Ley General de Transparencia y Acceso a la Información Pública; 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, fracciones I y II de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" vigentes.

2) Demostrable, ya que es un hecho notorio que los sistemas de pagos de Bancos Centrales han sufrido ataques cibernéticos a través de estas infraestructuras, 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.[1] 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.[2] 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 y sistemas financieros.[3] Asimismo, los sistemas de empresas como Google, Facebook, PayPal y el New York Times se han visto comprometidos por ataques cibernéticos.[4] 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.[5]Esta serie de ataques se encuentra en una fase avanzada, que

---

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

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

3 Antony Peyton. "Symantec reveals more hack attempts on Swift network". Banking Technology. 11 de octubre de 2016.

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

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

comenzó con ensayos desde 2017 y que ha logrado la consecución de sus objetivos en algunos casos. En todos ellos, **la detección de vulnerabilidades a nivel aplicativo y sistema operativo son elementos en común**, por lo cual es totalmente demostrable que el entregar información precisamente sobre las vulnerabilidades de los sistemas de pagos permitiría a los delincuentes o grupos delictivos el llevar a cabo más ciberataques que pudieran dañar de forma más severa los sistemas de pagos de los cuales depende el sistema financiero mexicano.

Para demostrar lo anterior, se citan algunos de los ataques más relevantes:

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 polacos[6], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[7]

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;[8]

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;[9]

d) 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;[10]

---

6 Badcyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 de febrero de 2017, http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ consultado el 3 de agosto de 2018.

7 BAE Systems Applied Intelligence. "BAE Systems Threat Research Blog." Lazarus & Watering-Hole Attacks, 1 de enero de 1970, http://baesystemsai.blogspot.mx/2017/02/lazarus-watering-hole-attacks.html . consultado 3 de agosto de 2018.

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

9 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 de junio de 2017, http://es.gizmodo.com/descubren-que-petya-el-ataque-que-paralizo-empresas-de-1796492938 consultado el 3 de agosto de 2018.

10 Nussman, Chris. "DHS Bulletin on Denial of Service (TDoS) Attacks on PSAPs." NENA The 911 Association, 17 de marzo de 2013, www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm, consultada el 2 de mayo de 2018.

e) Los cibertataques reportados por la empresa de ciberseguridad S21sec realizados por el grupo cibercriminal llamado 'Cobalt', el cual consistió en un ataque realizado a los cajero automáticos basado en red, es decir que no se requiere acceso físico al cajero para perpetrarlos, sino que la infección se lleva a cabo desde la propia red interna del banco;[11]

f) El ciberataque basado en la modalidad de denegación de servicio distribuido (DDoS) en Holanda, en el cual diez millones de holandeses se quedaron sin firma digital por el bloqueo del portal como consecuencia de una avalancha de solicitudes;[12]

g) Los ciberataques a los que fue víctima *Delta Air Lines*, entre el 26 de septiembre al 12 de octubre de 2017, los cuales fueron informados a través de un comunicado que la compañía *[24]7.ai*, proveedora de servicios informáticos de ésta y otras compañías, suceso que causó que los datos bancarios de algunos de los usuarios de la aerolínea se hayan visto comprometidos durante ese periodo.[13]

h) El ataque 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;[14]

i) En febrero de 2018, el Banco Central Ruso, dio a conocer que un grupo de hackers de origen ruso sustrajo, aproximadamente $339,5 de rublos (US$ 6 millones), con motivo de un ataque informático perpetrado al sistema internacional de pagos SWIFT en Rusia;[15]

j) El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse al SPEI de algunos participantes, mediante código malicioso, el cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero.[16] A la fecha de elaboración de la presente prueba de daño, se

---

11 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 2 de mayo de 2018.

12 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 03 de agosto de 2018.

13 Delta Airlines. "INFORMATION ON [24]7.AI CYBER INCIDENT." Information on [24]7.Ai Cyber Incident, 7 de abril 2018, www.delta.com/content/www/en_US/response.html consultado el 2 de mayo de 2018.

14 BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución", http://www.bancomext.com/comunicados/18443, consultado el 7 de febrero de 2018.

15 Quijije, Jorge *"Hackers rusos robaron US$6 millones del sistema internacional de pago SWIFT"* Tekcrispy, Tekcrispy.com 16 feb 2018,https://www.tekcrispy.com/2018/02/16/hackeo-swift-6-millones-rusia/. Consultado el 17 de mayo.

16 Banco de México. "Información sobre los ataques a los Participantes del SPEI". http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B2B9BB8C6-D66B-38C4-CC90-F72A7BC335C9%7D.pdf, consultado el 03 de agosto de 2018.

estima un daño a los participantes del SPEI de aproximadamente 300 millones de pesos.[17] El ataque producido a las plataformas que son usadas por proveedores externos en algunos bancos en México, en relación con el SPEI, ha sido catalogado como similar al que ocurrió con el sistema de pagos internacional S.W.I.F.T. en Rusia.

k) La filtración a través de redes sociales de la base de datos de tarjetas de los clientes del Banco de Chile dada a conocer por el grupo de hackers llamado "TheShadowBrokers".[18]

Cabe señalar que 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".[19] 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.

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[20] 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 ellos, si ésta se les entregara directamente bajo la forma de acceso a la información.

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 la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros

---

17 Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de México: http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B022CD9D7-11A9-68E6-D1A5-965F57A23F60%7D.pdf consultados el 3 de agosto de 2018.

18 "Hackers Filtraron Base De Datos De Tarjetas De Crédito De Miles De Clientes." CNN Chile, 25 July 2018, www.cnnchile.com/economia/hackers-filtran-base-de-datos-de-tarjetas-de-credito-de-miles-de-clientes_20180725/. Consultado el 6 de Agosto de 2018.

19 Para mayor información consultar la siguiente dirección electrónica: https://en.wikipedia.org/wiki/Metasploit_Project. Consultado el 04 junio 2018

20 Para mayor información consultar la siguiente dirección electrónica: https://www.offensive-security.com/metasploit-unleashed/information-gathering/. Consultado el 6 de agosto de 2018

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.[21]

Inclusive, uno de los *modus operandi* de los ciberataques es precisamente a través de la obtención de información que no es pública, lo cual puede ocurrir mediante la complicidad con las personas que operan los sistemas, o bien, precisamente a través de solicitudes de acceso a la información que tienen por único objeto conocer las vulnerabilidades en los sistemas e infraestructura de tecnologías de la información.[22]

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 cuyo rol no esté autorizado,[23] en el entendido de que dicha información, al estar en posesión de personas no autorizadas, 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 o de los sistemas de pagos, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

3) Identificable, puesto que, a la fecha de realización de la presente prueba de daño, es un hecho notorio que los sistemas de pagos están siendo objeto de ciberataques a gran escala, como quedó demostrado en la sección anterior. Si bien dichos ataques no han logrado irrumpir en los sistemas del Banco de México, **resulta claramente identificable que el objeto final de dichos ataques son los sistemas de pagos que maneja el Banco de México**, cuya seguridad depende de la reserva de la información materia de la presente prueba de daño.

---

21 Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, 18 de diciembre de 2001.

22 Riquelme, Rodrigo. *"El sistema financiero mexicano fue víctima de una campaña de ciberataques."* El Economista, El Economista, 15 de mayo 2018, https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html. Consultado el 30 mayo 2018

23 Ver por ejemplo https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf Consultado el 04 de junio 2018

En ese sentido, cabe mencionar 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 registraron 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."[24]

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.

Por lo anterior, un ataque informático a los sistemas tecnológicos utilizados por el Banco de México, ocasionado por dar a conocer la información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos, representa un perjuicio significativo para el sistema financiero del país, el sistema de pagos y para la población usuaria de los mismos. En este punto cabe mencionar que, **México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica**[25] y que tan sólo en nuestro país, 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

---

24 http://pastebin.com/raw/y7JmsKVD Consultado el 04 junio de 2018

25 Arreola Javier. "Ciberseguridad (casi) a prueba del enemigo 'invisible'". Forbes México. http://www.forbes.com.mx/ciberseguridad-casi-prueba-del-enemigo-invisible/ consultado el 03 de agosto de 2018.

a 689.4 millones de personas.[26] Por lo anterior, este Instituto Central[27] y autoridades como la Secretaría de Hacienda y Crédito Público[28] se han pronunciado sobre la importancia de fortalecer la ciberseguridad para la estabilidad del sistema financiero.

Adicionalmente, 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 referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos***", 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.

Al respecto, debe destacarse que la información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos 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.

Loa anterior, máxime que las consecuencias de que tenga éxito un ataque a la infraestructura referida por dar a conocer la información materia de esta prueba de daño, la cual sustenta a los procesos fundamentales, tendrían muy probablemente, 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.

---

26 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 03 de agosto de 2018.

27 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

28 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.

Por otra parte, 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, del sistema de pagos y a sus usuarios, respecto de otorgar la "***información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos***". Asimismo, únicamente se reserva la información que se considera indispensable, en aras de propiciar el cumplimiento de los principios imperantes en la materia, por lo que la no divulgación de la misma representa el medio menos restrictivo disponible para evitar el perjuicio, tan es así que se elaboran versiones públicas de la información que se clasifica.

De otra forma, de entregarse la información solicitada, 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, es proporcional y resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, y en virtud de que la "***Información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas de pagos***" no está sujeta a cambios en específico, toda vez que atienden a la preservación de 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, 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, 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; 3, 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, 19 Bis 1 y 20, del Reglamento Interior del Banco de México; Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XIII, Cuarto, Sexto, párrafo segundo, 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; la ***"Información referente al software que soporta la implementación de las operaciones de banca central y el funcionamiento de los sistemas***

de pagos", es de clasificarse 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 monetaria, cambiaria o del sistema financiero del país o el buen funcionamiento del sistema de pagos.

Technology

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

By Michael Riley and Alan Katz
26 de mayo de 2016 8:36 GMT-5
Updated on 26 de mayo de 2016 15:21 GMT-5

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

Swift Hack Investigation Expands to Southeast Asia

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.

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.

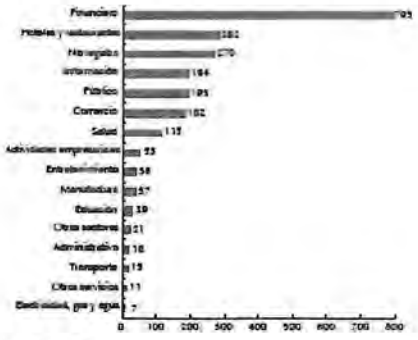
La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por *hackers*, con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos 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 exante. 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.

News

Symantec reveals more hack attempts on Swift network

Written by Antony Peyton (https://www.bankingtech.com/author/antonypeyton/) 11 Oct 2016

Symantec 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.

(https://www.bankingtech.com/file
1.png)
Odinaff attacks by region (IMAGE: Symantec) Click to enlarge

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 (https://www.bankingtech.com/455732/typo-spells-confusion-in-101m-cyber-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.

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 (https://www.bankingtech.com/595372/swift-issues-plea-to-collaborate-in-fight-against-cybercrime/) on the subject and recently unveiled SwiftSmart (https://www.bankingtech.com/602332/swift-smart-modules-seek-stronger-security/) 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

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]

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 6 Y 23

AFECTACIONES AL SPEI

El sistema financiero mexicano fue víctima de una campaña de ciberataques

Algunas instituciones del sistema financiero en México sufrieron una campaña de ciberataques, a principios del 2017, que afectó los aplicativos y la infraestructura de TI que dan soporte a los servicios de banca en línea.

Rodrigo Riquelme
15 de mayo de 2018, 16:34

Algunas instituciones del sistema financiero en México sufrieron una campaña de ciberataques, a principios del 2017, que afectó los aplicativos y la infraestructura de tecnologías de la información que dan soporte a los servicios de banca en línea, y que contó con elementos similares a los que se describen en la información que se conoce hasta el momento sobre el hackeo a las instituciones bancarias que afectó la operación del Sistema de Pagos Electrónicos Interbancarios (SPEI) las últimas semanas.

De acuerdo con Eduardo Espina, director de Ciberseguridad de Mnemo-CERT, ciertos elementos y tendencias de esta campaña de ataques de ciberseguridad que ocurrió durante varios meses del 2017 tiene elementos en común con el ciberataque ocurrido desde el pasado 27 abril. La nueva afrenta a los bancos fue calificada como un ataque que " no tiene precedentes en el país", de acuerdo con Alejandro Díaz de León, gobernador del Banco de México.

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 8

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:

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

Article World Neurosurgery · June 2017

CITATION 1

READS 142

1 author:

Eastern Maine Medical Center

164 PUBLICATIONS 604 CITATIONS

SEE PROFILE

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.

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

Email to a Friend (/members/send.asp?In=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.

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**.

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.

DELTA

MY TRIPS BOOK A TRIP FLIGHT STATUS CHECK IN

INFORMATION ON [24]7.AI CYBER INCIDENT

OVERVIEW

Last updated on April 3, 2018, 8:00am 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. 26 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 late 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. 26 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, CVV 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 3 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 [illegible] mail, who may have been impacted by the [24]7.ai cyber incident.

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 dia 9 de enero fue victima 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 16

INTERNET SEGURIDAD

Hackers rusos robaron US$ 6 millones del sistema internacional de pagos SWIFT

Por **Jorge Quijije** - Feb 16, 2018

Más allá de ser uno de los países de mayor influencia política en el mundo, Rusia es la cuna de una gran parte de los hackers que desarrollan las herramientas más sofisticadas de robo y espionaje del sector de la informática.

Selección del Editor


¿Por qué los cachorros despiertan más ternura a cierta edad?


Identifican genes implicados en el incremento del tamaño del cerebro humano


Identifican el fósil de la 'Madre de todos los Lagartos'


El agua líquida no es sólo un líquido, sino dos


Información sobre los ataques a los Participantes del SPEI
Banco de México
Mayo, 2018
BANCO DE MÉXICO

BANCO DE MÉXICO

REFERENCIA 18

BANCO DE MÉXICO

22 de mayo de 2018

Puntos Importantes sobre la Situación Actual del SPEI.

1. **Se tienen registrados 5 participantes con vulneraciones de ciberseguridad. Todos los ataques que se han observado han sido dirigidos hacia los bancos, casas de bolsa y otros participantes del sistema de pagos.** Estos han estado enfocados en los sistemas de los participantes con los que se conectan al SPEI.
2. **El sistema central del SPEI, que opera el Banco de México, no se ha visto afectado y no ha sido blanco de ningún ataque.** El sistema central opera de manera segura y eficiente como lo ha hecho desde su creación.
3. **Los recursos de los clientes de instituciones financieras están seguros, no estuvieron en peligro y no han sido el objetivo de los ataques.** Los recursos que se han extraído han sido de los participantes (bancos, casas de bolsa, etc.). Los atacantes han buscado vulnerar las conexiones de las instituciones con el SPEI, inyectando instrucciones de pago fraudulentas a partir de cuentas inexistentes, lo cual afecta la cuenta transaccional de los participantes en el SPEI, pero no las cuentas de los clientes finales. Los recursos de los clientes están seguros porque radican en un sistema separado con validaciones individuales por operación.
4. **Para salvaguardar la continuidad operativa, el Banco de México alertó a los participantes en el SPEI y solicitó a los participantes con un mayor perfil de riesgo migrar la operación a una plataforma contingente. Este esquema de operación contingente y las validaciones adicionales que han implementado los participantes han propiciado la ralentización de los flujos de pagos.**
5. Una vez recibidas en el SPEI, el 100% de las operaciones son procesadas y enviadas a los participantes receptores en segundos. Por otra parte, desde que se recibe la solicitud por parte de un cliente en los sistemas del participante hasta el abono final el 55% de las operaciones fluye por el sistema y los participantes con normalidad en cuestión de segundos, mientras que el 99% se opera en menos de dos horas. No obstante, en algunos casos estas acreditaciones pueden tardar uno o más días. **El Banco de México, consciente de la preocupación y malestar de los clientes, trabaja arduamente para que los participantes agilicen sus procesos para abonar en el menor tiempo posible los recursos de sus clientes y con ello minimizar la afectación a los mismos.**
6. **Con la información disponible, los montos involucrados en envíos irregulares y sujetos a revisión son de aproximadamente 300 millones de pesos.**

ECONOMÍA BANCO **25.07.2018 / 22:00**

Hackers filtraron base de datos de tarjetas de crédito de miles de clientes

Serían 14 mil los usuarios afectados. La recomendación es a bloquear los documentos además de realizar el aviso respectivo a las cadenas.

REFERENCIA 20

Metasploit Project

From Wikipedia, the free encyclopedia

? This article includes a list of references, but its sources remain unclear because it has insufficient inline citations. Please help to improve this article by introducing more precise citations. (November 2017) (Learn how and when to remove this template message)

The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Its best-known subproject is the open source[1] Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important subprojects include the Opcode Database, shellcode archive and related research.

The Metasploit Project is well known for its anti-forensics and evasion tools, some of which are built into the Metasploit Framework.

Contents [hide]

Metasploit

Metasploit Community showing three hosts, two of which were compromised by an exploit

Developer(s)	Rapid7, LLC
Stable release	4.16.[illegible] / February 24, 2017
Repository	[illegible]
Operating system	Cross-platform
Type	Security
License	Framework: BSD[2] Community Edition: Proprietary
Website	[illegible]

History [edit]

Metasploit was created by H. D. Moore in 2003 as a portable network tool using Perl. By 2007, the Metasploit Framework had been completely rewritten in Ruby.[3] On October 21, 2009, the Metasploit Project announced[4] that it had been acquired by Rapid7, a security company that provides unified vulnerability management solutions.

Like comparable commercial products such as Immunity's Canvas or Core Security Technologies' Core Impact, Metasploit can be used to test the vulnerability of computer systems or to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities. Since the acquisition of the Metasploit Framework, Rapid7 has added two open core proprietary editions called Metasploit Express and Metasploit Pro.

Metasploit's defining position as the de facto exploit development framework[5] is to the release of software vulnerability advisories often accompanied[6] by a proprietary Metasploit module that highlights the exploitability, risk and remediation of the particular bug.[7] Metasploit 2.0 began to include fuzzing tools to discover software vulnerabilities rather than just exploits for known bugs. The avenue can be seen with the integration of the fuzzer suite SMB.[8] Released Metasploit 3.0 in November 2006. Metasploit 4.0 was released in August 2011.[9]

Metasploit Framework [edit]

The basic steps for exploiting a system using the Framework include:

1. Choosing and configuring an exploit (code that enters a target system by taking advantage of one of the bugs; about 900 different exploits for Windows, Unix/Linux and Mac OS X systems are included)
2. Optionally checking whether the intended target system is susceptible to the chosen exploit
3. Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server)
4. Choosing the encoding technique so that the chosen payload will be accepted by the target software
5. Executing the exploit

This modular approach – allowing the combination of any exploit with any payload – is the major advantage of the Framework; it facilitates the tasks of attackers, exploit writers and payload writers.

Metasploit runs on Linux (including Linux and Mac OS X) and on Windows. The Metasploit Framework can be extended to use modules in multiple languages.

To choose an exploit and payload, some information about the target system is needed, such as operating system version and installed network services. This information can be gained with port scanning and OS fingerprinting tools such as Nmap. Vulnerability scanners such as Nessus, Nessus, and OpenVAS can detect target system vulnerabilities. Metasploit can import vulnerability scanner data and compare the identified vulnerabilities to existing exploit modules for possible exploitation.[10]

Metasploit interfaces [edit]

There are several interfaces for Metasploit available. The most popular are maintained by Rapid7 and Strategic Cyber LLC.[11]

Metasploit Framework Edition [edit]

OFFENSIVE SECURITY

Courses Certifications Online Labs Penetration Testing Projects Blog About

Information Gathering in Metasploit

MSFU Navigation

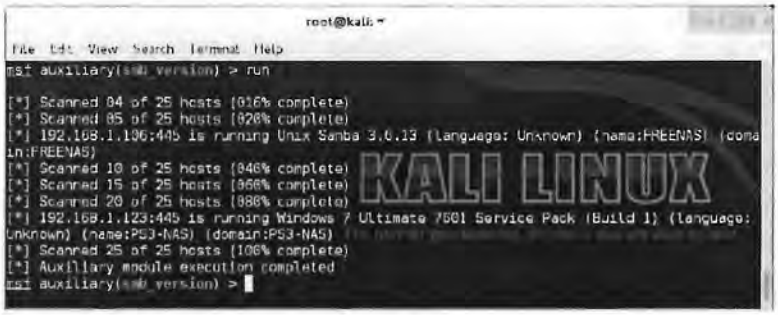
- Metasploit Unleashed
- Donate - Help Feed a Child
- Introduction
- Metasploit Fundamentals
- Information Gathering
- Vulnerability Scanning
- Writing a Simple Fuzzer
- Exploit Development
- Web App Exploit Dev
- Client Side Attacks
- MSF Post Exploitation
- Meterpreter Scripting
- Maintaining Access
- MSF Extended Usage
- Metasploit GUIs
- Post Module Reference
- Auxiliary Module Reference
- Recent Changes

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.

Social Engineering Fundamentals, Part I: Hacker Tactics

Sarah Granger

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

BANCO DE MÉXICO

WaterISAC

Security Information Center

10 Basic Cybersecurity Measures

Best Practices to Reduce Exploitable Weaknesses and Attacks

June 2015

REFERENCIA 25

World Banking Cartel Master Target List

#OpIcarus

.....

Federal Reserve of America
http://www.federalreserve.gov/
http://www.ny.frb.org/
http://www.federalreserveonline.org/
http://www.federalreserveeducation.org/
http://www.chicagofed.org/webpages/index.cfm
https://www.richmondfed.org/
http://www.frbservices.org/
http://www.stlouisfed.org/
https://www.minneapolisfed.org/index.cfm
http://www.dallasfed.org/
http://www.bostonfed.org/
http://www.newyorkfed.org/
http://www.frbsf.org/
http://www.philadelphiafed.org/
http://www.federalreservehistory.org/
http://www.ffiec.gov/
http://www.federalreserveconsumerhelp.gov/
http://www.frbatlanta.org/

IMF
https://www.imf.org/external/index.htm
https://imf.taleo.net/
http://imfsite.org/

World Bank
http://www.worldbank.org/
http://www.centralbanking.com/
www.centralbanksguide.com
http://www.doingbusiness.org/
http://ieg.worldbankgroup.org/
http://info.worldbank.org
http://www.globalexchange.org/
http://data.worldbank.org/
http://www.worldbankpresident.org/
http://www.ifc.org

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 21st, 2018 @ 12:19 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

EQUI

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/muere-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/genel 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

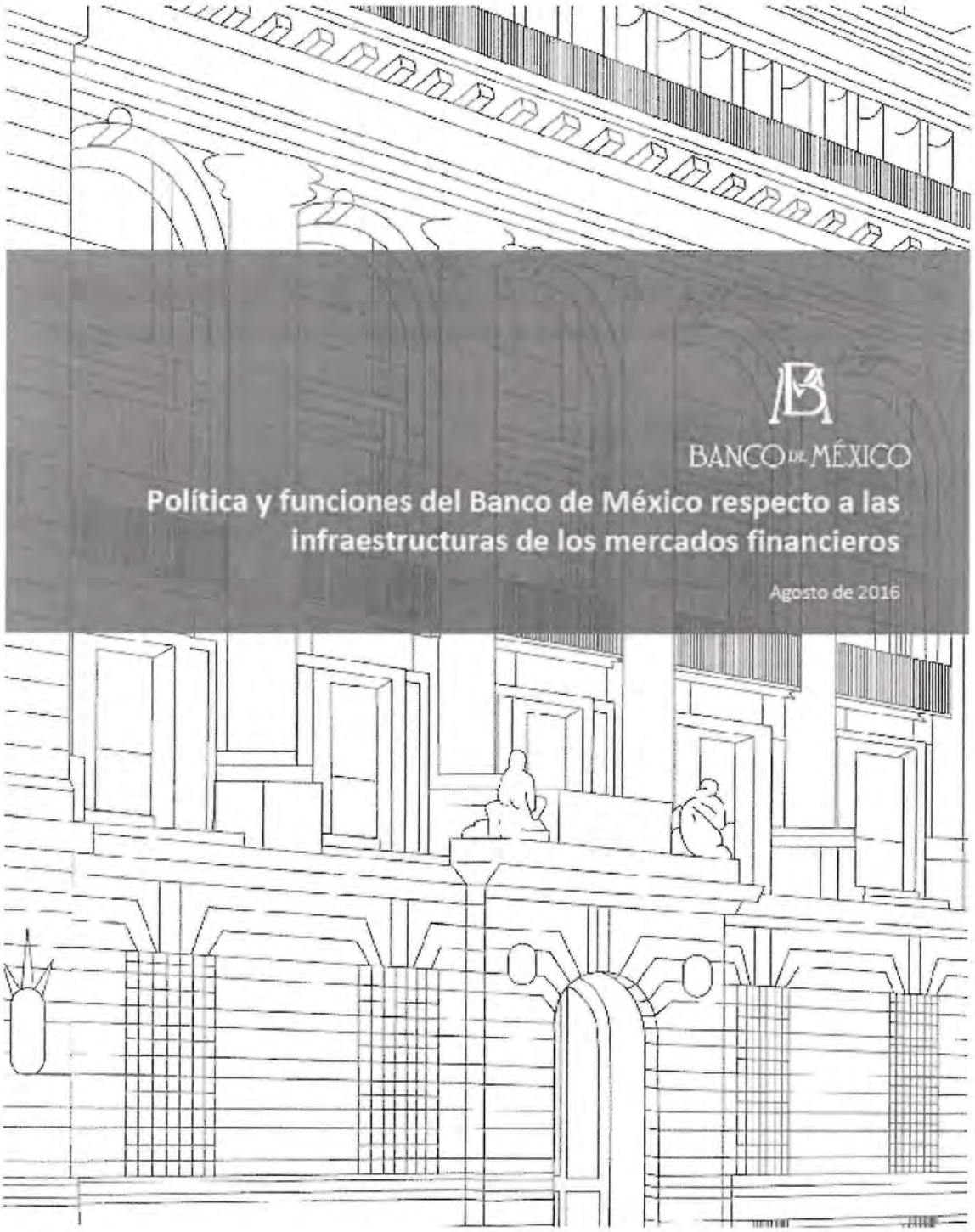
REFERENCIA 27

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%

Norton by Symantec


BANCO DE MÉXICO
Política y funciones del Banco de México respecto a las infraestructuras de los mercados financieros
Agosto de 2016

(http://www.gob.mx) › Secretaría de Hacienda y Crédito Público (/shcp) › **Prensa**

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

Comenta nuevo e 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.

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000074618

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

RESULTANDO

PRIMERO. Que el diez de diciembre de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000074618,** 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. Por numero de serie de cada uno de los equipos de cómputo en posesión del sujeto obligado requiero: a) Nombres comerciales de los sistemas operativos instalados. b) Nombres comerciales y versiones de los antivirus o software de seguridad en Internet, instalados. c) Inicio y termino de la vigencia de cada licencia utilizada en los software mencionados en el anterior inciso b). 2. Por dirección web o URL (Localizador Uniforme de Recursos), de los protocolos HTTP (Protocolo de Transferencia de Hipertexto) y HTTPS (Protocolo seguro de transferencia de hipertexto), cual es utilizado en cada una de sus paginas electrónicas o webs oficiales, así como el tipo de protocolo de seguridad implementado, SSL (Capa de sockets seguros) o TLS (Seguridad de la capa de transporte). 3. De cada una de sus actuales paginas electrónicas o webs oficiales, fecha exacta y duración de todos los ataques de Denegación de Servicio (DoS) ó Denegación de Servicio Distribuida (DDoS) padecidos."*

SEGUNDO. Que el mismo diez de diciembre, la solicitud de información en comento, fue turnada para su atención a la Dirección de Sistemas, unidad administrativa adscrita al a Dirección General de Tecnologías de la Información; y el tres de enero de dos mil diecinueve, fue turnada a la Dirección de Sistemas de Pagos, unidad administrativa adscrita a la Dirección General de Operaciones y Sistemas de Pagos, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que los titulares de la Subgerencia de Arquitectura de la Información, y de la Subgerencia de Coordinación de la Información, ambas unidades administrativas adscritas a la Dirección General de Tecnologías de la Información, mediante oficio con referencia I01/0001/2018, sometieron a consideración de este Comité la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud.

CUARTO. Que este órgano colegiado, mediante resolución de veintisiete de diciembre de dos mil dieciocho, confirmó la ampliación del plazo de respuesta por diez días, para la atención de la solicitud al rubro citada.

QUINTO. Que los titulares de la Gerencia de Seguridad de Tecnologías de la Información, y de la Subgerencia de Seguridad Informática, ambas unidades administrativas adscritas a la Dirección General de Tecnologías de la Información, mediante oficio con referencia GSTI-01.2019, hicieron del conocimiento de este Comité su determinación de clasificar como reservada la información referida en el mismo oficio, en términos de la motivación y fundamentación señaladas en la prueba de daño correspondiente, y solicitaron a este órgano colegiado confirmar dicha clasificación en sus términos.

SEXTO. Que el titular de la Dirección de Apoyo a las Operaciones, unidad administrativa adscrita a la Dirección General de Operaciones y Sistemas de Pagos, mediante oficio de once de enero de dos mil diecinueve, hizo del conocimiento de este Comité su determinación de clasificar como reservada la información referida en dicho oficio, en términos de la motivación y fundamentación señaladas en la prueba de daño correspondiente, y solicitó a este órgano colegiado confirmar dicha clasificación en sus términos.

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 (LGTAIP); 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción III, del Reglamento Interior del Banco de México (RIBM).

SEGUNDO. Enseguida se analiza la clasificación referida en los oficios señalados en los resultandos Quinto, y Sexto, conforme a lo siguiente:

Es procedente la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresadas en los oficios señalados en los resultandos Quinto y Sexto, así como en las correspondientes pruebas de daño, las cuales se tienen aquí por reproducidas como si a la letra se insertasen en obvio de repeticiones innecesarias.

Este Comité confirma la clasificación de la información referida como reservada.

Por lo expuesto con fundamento en los artículos 44, fracción II, y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; 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 expresadas en las correspondientes pruebas de daño señaladas en los oficios precisados en los resultandos Quinto y Sexto.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el día veintiuno de enero de dos mil diecinueve.----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

ANEXO "G"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
18 ENE 2019
Comité de Transparencia
Por: JJSRS Hora: 13:56

Se recibe oficio mencionado en tres páginas

Ciudad de México, a 18 de enero de 2019.

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Nos referimos a la solicitud de acceso a la información, identificada con el número de folio 6110000074318, que nos turnó la Unidad de Transparencia el siete de diciembre 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, la cual se transcribe a continuación:

> *" Solicito conocer lo siguiente de las visitas de inspección que hizo el banco central a los participantes del SPEI, previo al cambio de la circular 14/2017:1.- El número total de visitas de inspección y el número segmentado por cada entidad financiera.2.- Las observaciones y comentarios hechos a cada participante en el cumplimiento de dicha circular3.- El número de procedimientos de supervisión y el número de participantes que estuvieron involucrados en estos procedimientos de supervisión4.- El número de dictámenes generados y el número de participantes a los que le levantaron estos dictámenes 5.- El argumento para generar dichos dictámenes y su contenido.6.- Las sanciones y montos derivadas de estas supervisiones."*

Sobre el particular, hacemos del conocimiento de ese Comité de Transparencia lo siguiente:

A) Con motivo del recurso de revisión tramitado bajo el expediente RRA5211/18, promovido por el solicitante en contra la respuesta emitida por este instituto Central el 3 de agosto de 2018, y tomando en consideración los recientes criterios emitidos por este Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI) en la sustanciación de diversos recursos de revisión en materia de acceso a la información pública, estas unidades administrativas determinaron modificar la clasificación de reserva de información realizada mediante oficio de 10 de septiembre de 2018, misma que fue confirmada por ese órgano colegiado en resolución emitida en su sesión ordinaria 37/2018, de 11 de septiembre de 2018. Lo anterior, a fin de garantizar la seguridad jurídica y certidumbre del solicitante, al establecer con precisión el supuesto normativo de la clasificación que resulta aplicable al caso en concreto, y las expresiones documentales que comprende.

Cabe señalar que, derivado de los actos de supervisión que lleva a cabo este Banco Central, emite observaciones, las cuales, de ser el caso, se contienen en las actas parciales y/o de cierre que se levantan durante el desarrollo de las visitas de inspección (cabe aclarar que no en todas las visitas es necesario emitir actas parciales). Al concluir la visita se comunica a la Entidad Financiera el dictamen el cual invariablemente incluye los resultados de la revisión, incorporando de ser el caso las observaciones. Sin embargo, los resultados de la visita no se

consideran definitivos, toda vez que la Entidad en su respuesta puede ofrecer elementos que aclaren alguna observación. En caso de que en una visita de inspección se detecten presuntos incumplimientos a la regulación, el resultado final del ejercicio de las facultades de supervisión se genera hasta el momento en que es emitida la resolución definitiva correspondiente, determinando el incumplimiento e imponiendo la sanción aplicable. Al respecto, debe señalarse que en ninguno de los procedimientos que comprende el periodo de la solicitud se han emitido resultados definitivos.

Conforme a lo anterior, en su momento se determinó clasificar la información señalada en el oficio de tres de agosto de 2018, considerando las expresiones documentales en posesión de este sujeto obligado hasta ese momento, constantes en 39 actas parciales, 8 actas de cierre y 7 dictámenes generados con motivo del ejercicio de las facultades de supervisión del Banco de México a participantes del SPEI, durante el periodo comprendido entre el 17 de julio del 2017 y el 16 de mayo de 2018 (momento en que se modificó la circular 14/2017), los cuales contienen las observaciones y, en su caso, resultados preliminares correspondientes.

En el caso concreto, hacemos de su conocimiento que la información relativa a ***"de las visitas de inspección que hizo el banco central a los participantes del SPEI, previo al cambio de la circular 14/2017 [...] 2.- Las observaciones y comentarios hechos a cada participante en el cumplimiento de dicha circular [...]5.- El argumento para generar dichos dictámenes y su contenido.[...]"***, se ubica en el supuesto antes mencionado, y es materia de la presente solicitud.

Asimismo, en las expresiones documentales que comprenden o contienen dicha información, subsisten también las causas que dieron origen a la clasificación como reservada de la misma, de conformidad con los fundamentos y motivos señalados en la prueba de daño puesta a disposición de ese órgano colegiado en su momento.

En ese sentido, dicha información deberá permanecer clasificada en su totalidad como reservada por un plazo de cinco años, contados a partir de la fecha en que se confirmó dicha clasificación (el 3 de agosto de 2018), por las causas señaladas a ese órgano colegiado en su momento.

Atentó 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 III, 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", vigentes, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa.

B) De igual manera, de conformidad con lo dispuesto en los artículos 100 y 106, fracción I, de la Ley General de Transparencia y Acceso a la Información Pública; así como 97 y 98, fracción I, de la Ley Federal de Transparencia y Acceso a la Información Pública, ha determinado

clasificar como reservada la información relativa a ***"de las visitas de inspección que hizo el banco central a los participantes del SPEI, previo al cambio de la circular 14/2017. 2.- Las observaciones y comentarios hechos a cada participante en el cumplimiento de dicha circular [...]5.- El argumento para generar dichos dictámenes y su contenido."***, considerando las expresiones documentales adicionales a las mencionadas en el inciso **A)** generadas hasta la fecha de la presente solicitud, las cuales se encuentran en posesión de este sujeto obligado hasta ese momento, constantes de 4 dictámenes generados con motivo del ejercicio de las facultades de supervisión del Banco de México a participantes del SPEI, durante el periodo comprendido entre el 17 de julio del 2017 y el 16 de mayo de 2018 (momento en que se modificó la circular 14/2017), los cuales contienen las observaciones y, en su caso, resultados preliminares correspondientes. Lo anterior, de conformidad con la fundamentación y motivación señaladas en la prueba de daño que se puso a disposición de ese órgano colegiado para la clasificación de la información señalada en el inciso **A)** del presente oficio, en virtud de que su divulgación actualiza los riesgos señalados en dicha prueba de daño.

Dicha información, deberá permanecer clasificada como reservada, por el periodo de cinco años, contados a partir de la confirmación de dicha clasificación, de conformidad con lo señalado en la prueba de daño respectiva.

Por lo anterior, y en términos de los artículos 44 fracción II de la LGTAIP; 65, fracción II de la LFTAIP; así como 31, fracción III 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", vigentes, solicitamos a ese Comité de Transparencia confirmar la clasificación realizada por estas unidades administrativas.

Atentamente,

VIVIANA GARZA SALAZAR
Directora de Regulación y Supervisión

MANUEL MIGUEL ÁNGEL DÍAZ DÍAZ
Director de Sistemas de Pagos

ANEXO "H"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000074318

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

RESULTANDO

PRIMERO. Que el siete de diciembre de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000074318,** la cual se transcribe a continuación:

> *"Solicito conocer lo siguiente de las visitas de inspección que hizo el banco central a los participantes del SPEI, previo al cambio de la circular 14/2017:1.- El número total de visitas de inspección y el número segmentado por cada entidad financiera.2.- Las observaciones y comentarios hechos a cada participante en el cumplimiento de dicha circular3.- El número de procedimientos de supervisión y el número de participantes que estuvieron involucrados en estos procedimientos de supervisión4.- El número de dictámenes generados y el número de participantes a los que le levantaron estos dictámenes 5.- El argumento para generar dichos dictámenes y su contenido.6.- Las sanciones y montos derivadas de estas supervisiones."*

SEGUNDO. Que el mismo siete de diciembre, la solicitud de información en comento fue turnada a la Dirección de Sistemas de Pagos y a la Dirección General de Asuntos del Sistema Financiero, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que la titular de la Dirección de la Dirección General de Asuntos del Sistema Financiero, mediante oficio con referencia DGASF/92/2018, sometió a consideración de este Comité la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud.

CUARTO. Que este órgano colegiado, mediante resolución de siete de enero de dos mil diecinueve, confirmó la ampliación del plazo de respuesta por diez días., para la atención de la solicitud al rubro citada.

QUINTO. Que el titular de Dirección de Sistemas de Pagos, mediante oficio de dieciocho de enero de dos mil diecinueve hizo del conocimiento de este Comité de Transparencia que la información relativa a ***"de las visitas de inspección que hizo el banco central a los participantes del SPEI, previo al cambio***

de la circular 14/2017 [...] 2.- Las observaciones comentarios hechos a cada participante en el cumplimiento de dicha circular [...]5.- El argumento para generar dichos dictámenes y su contenido", fue clasificada previamente para la atención de una solicitud de acceso diversa, y que dicha clasificación fue modificada para la atención del recurso referido en el oficio en comento, en los términos de lo señalado en el mismo; que dicha información es materia de la solicitud citada al rubro, y que en ella subsisten las causas que dieron origen a su clasificación, por lo que igualmente solicitó a este órgano colegiado confirmar la clasificación referida.

Asimismo, también hizo del conocimiento de este órgano colegiado su determinación de clasificar por primera vez la información relativa a***"de las visitas de inspección que hizo el banco central a los participantes del SPEI, previo al cambio de la circular 14/2017 [...] 2.- Las observaciones comentarios hechos a cada participante en el cumplimiento de dicha circular [...]5.- El argumento para generar dichos dictámenes y su contenido"***, así como **las expresiones documentales adicionales, generadas con motivo del ejercicio de las facultades de supervisión del Banco de México a participantes del SPEI, durante el periodo comprendido entre el 17 de julio de 2017 y el 16 de mayo de 2018 (momento en que se modificó la circular 14/2017), constantes en 4 dictámenes, y solicitó a este órgano colegiado confirmar dicha clasificación,** en los términos de la fundamentación y motivación expresados en la prueba de daño referida.

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 (LGTAIP); 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción III, del Reglamento Interior del Banco de México (RIBM).

SEGUNDO. Enseguida se analiza la clasificación referida en el oficio señalado en el resultando Quinto, conforme a lo siguiente:

Es procedente la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresadas en el oficio señalado en el resultando Quinto, así como en la correspondiente prueba de daño, la cual se tiene aquí por reproducida como si a la letra se insertase en obvio de repeticiones innecesarias.

Este Comité confirma la clasificación de la información referida como reservada.

Por lo expuesto con fundamento en los artículos 44, fracción II, y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; 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 expresadas en la prueba de daño señalada en el oficio precisado en el resultando Quinto.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintiuno de enero de dos mil diecinueve. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante

ANEXO "I"

BANCO DE MÉXICO

Ciudad de México, a 11 de enero de 2018
D01/C391/2018

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 **LT-BM-26213** que nos turnó la Unidad de Transparencia el veintisiete de diciembre 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:

> *"Manual de Operación del SPEI, a que hace alusión la circular 17/2010, emitida por el Banco de México y sus modificaciones hasta la circular 13/2015"*

Sobre el particular, con motivo de la atención de una solicitud de acceso diversa, mediante oficio con referencia D01/C256/2016, esta unidad administrativa hizo del conocimiento de ese órgano colegiado la determinación de clasificar como reservada diversa información contenida en el documento que se señala más adelante, y generó la versión pública respectiva, junto con la carátula que la distingue e indica los datos concretos que fueron clasificados, al igual la prueba de daño con los motivos y fundamentos respectivos. Dicha clasificación y la correspondiente versión pública fueron confirmadas por el Comité de Transparencia mediante resolución emitida en su sesión de 15 de diciembre de 2016.

TÍTULO DEL DOCUMENTO CLASIFICADO	CLASIFICACIÓN DE LA INFORMACIÓN REALIZADA POR LA DIRECCIÓN DE SISTEMAS DE PAGOS	PLAZO DE RESERVA
Manual de Operación del SPEI® versión 4.11	Reservada	5 años, contados a partir de la confirmación de la clasificación (15 de diciembre de 2016)

Asimismo, el documento señalado se encuentra en el supuesto anterior y es materia d3e la presente solicitud de acceso a la información, por lo que con motivo de una nueva reflexión llevada a cabo para la atención de la solicitud materia del presente, y tomando en consideración los recientes criterios emitidos por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI) en la substanciación de diversos recursos de revisión en materia de acceso a la información pública[1], así como el contexto actual en materia de

[1] a) Resolución del Pleno del INAI en la sustanciación del recurso de revisión identificado con el número de expediente RRA 2537 /18, interpuesto en contra de la respuesta emitida por la Secretaría de Relaciones Exteriores, relativa a la solicitud de acceso a la información con folio 0000500059218;

BANCO DE MÉXICO

ciberseguridad ataques realizados por medios electrónicos a las instituciones financieras en todo el mundo, esta unidad administrativa ha determinado modificar la clasificación de la información reservada realizada mediante el referido oficio con referencia D01/C256/2016, de conformidad con los fundamentos y motivos expresados en la prueba de daño que se puso a disposición de ese órgano colegiado en su momento, extendiendo la protección de la información realizada en su momento, al resto de la información contenida en el documento materia del presente. Quedando la totalidad de la información contenida en el documento señalado en el cuadro precedente, clasificada como reservada, por el plazo de cinco años, contados a partir de la confirmación de la clasificación realizada mediante oficio con referencia D01/C256/2016..

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 III, 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", vigentes, atentamente solicitamos a ese Comité de Transparencia confirmar la clasificación de la información realizada por estas unidades administrativas y aprobar la clasificación correspondiente.

Asimismo, de conformidad con el Décimo de los señalados Lineamientos, informamos que el personal que por la naturaleza de sus atribuciones tiene acceso a los documentos señalados es el adscrito a la Dirección de Sistemas de Pagos.

Atentamente,

Manuel Miguel Ángel Díaz Díaz
Director de Sistemas de Pagos

Se recibe oficio constante en dos páginas

b) Resolución del Pleno del INAI en la sustanciación del recurso de revisión identificado con el número de expediente RRA 2747 /18, interpuesto en contra de la respuesta emitida por el Servicio de Protección Federal, relativa a la solicitud de acceso a la información con folio 3600100001718; y
c) Resolución del Pleno del INAI en la sustanciación del recurso de revisión identificado con el número de expediente RRA 2794/18, interpuesto en contra de la respuesta emitida por el INAI, relativa a la solicitud de acceso a la información con folio 067800063318.

ANEXO "J"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: LT-BM-26213

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

RESULTANDO

PRIMERO. Que el veintisiete de diciembre de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **LT-BM-26213**, que se transcribe a continuación:

> *"Manual de Operación del SPEI, a que hace alusión la circular 17/2010, emitida por el Banco de México y sus modificaciones hasta la circular 13/2015"*

SEGUNDO. Que el cuatro de noviembre de dos mil dieciséis, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **CTC-BM-17764,** que se transcribe a continuación:

> *"Buenos días quería solicitar si me podían hacer llegar el manual de SPEI así como la normativa que aplica al tema, de antemano gracias por su atención."*

TERCERO. Que el titular de la Dirección de Sistemas de Pagos del Banco de México, mediante oficio con referencia D01/C256/2016, informó a este Comité que determinó clasificar como reservada la información del *"Manual de Operación del SPEI® versión 4.11"* que detalla en la prueba de daño que adjuntó a dicho oficio, y solicitó confirmar tal clasificación y aprobar la versión pública respectiva.

CUARTO. Que este órgano colegiado confirmó la clasificación referida en el resultando anterior, mediante resolución de quince de diciembre de dos mil dieciséis.

QUINTO. Que el titular de la Dirección de Sistemas de Pagos, mediante oficio con referencia D01/C391/2018, hizo del conocimiento de este órgano colegiado que el *"Manual de Operación del SPEI® versión 4.11"* es materia de la solicitud citada al rubro, y que con motivo de una nueva reflexión, así como en consideración a los recientes criterios emitidos por el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales en la substanciación de diversos recursos de revisión en materia de acceso a la información pública, así como el contexto actual en materia de ciberseguridad y ataques realizados por medios electrónicos a las instituciones financieras en todo el mundo, dicha unidad administrativa ha determinado modificar la clasificación de la información reservada realizada mediante el referido oficio con referencia D01/C256/2016, de conformidad con los fundamentos y motivos expresados en la prueba de daño que se puso a disposición de este órgano colegiado en su momento, extendiendo la protección de la información realizada en su momento, a la totalidad de la información contenida en el Manual señalado, por el plazo de cinco años, contados a partir de la confirmación de la clasificación realizada mediante el citado oficio con referencia D0I/C256/2016.

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 (LGTAIP); 65, fracción

II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción III, del Reglamento Interior del Banco de México (RIBM).

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 (Lineamientos).

SEGUNDO. En seguida se analiza la clasificación señalada en el resultando Quinto, conforme a lo siguiente:

Es procedente confirmar la clasificación de la información identificada como reservada, en términos de la fundamentación y motivación expresadas en la correspondiente prueba de daño, misma que se tiene por reproducida a la letra, en obvio de repeticiones innecesarias.

Este Comité de Transparencia confirma la clasificación de la información referida como reservada.

Por lo expuesto, con fundamento en los artículos 44, fracción II, y 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; el Décimo Sexto, fracciones I y II, de los Lineamientos, vigentes; y la 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 expresadas en la correspondiente prueba de daño.

Así lo resolvió, por unanimidad de sus integrantes presentes, el Comité de Transparencia del Banco de México, en sesión celebrada el veintiuno de enero de dos mil diecinueve.---------- ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

ERIK MAURICIO SÁNCHEZ MEDINA
Integrante

VÍCTOR MANUEL DE LA LUZ PUEBLA
Integrante