FOLIO 1

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ORDINARIA 24/2018
DEL 28 DE JUNIO DE 2018

En la Ciudad de México, a las doce horas con treinta minutos del veintiocho de junio de dos mil dieciocho, en el edificio ubicado en avenida Cinco de Mayo, número seis, colonia Centro, delegación Cuauhtémoc, se reunieron Claudia Álvarez Toca, Directora de la Unidad de Transparencia, Humberto Enrique Ruiz Torres, Director Jurídico, y José Ramón Rodríguez Mancilla, Gerente de Organización de la Información, suplente del Director de Coordinación de la Información, todos integrantes del Comité de Transparencia de este Instituto Central, así como Rodolfo Salvador Luna de la Torre, 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, así como la Tercera, párrafos primero y segundo, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis, las personas que se indican en la lista de asistencia que se adjunta a la presente como **ANEXO "A",** quienes también son servidores públicos del Banco de México. ----------

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

---

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

El 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 51, párrafo segundo, y 83 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados; 43, párrafo segundo, 44, fracción IX, de la Ley General de Transparencia y Acceso a la Información Pública; 4o. y 31, fracciones III y XX, del Reglamento Interior del Banco de México, y Quinta, párrafo primero, inciso e), de las Reglas de Operación del Comité de Transparencia del Banco

BANCO DE MÉXICO

de México, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente como **ANEXO "B"** y procedió a su desahogo, conforme a lo siguiente: ----------

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000030118. ----------

El Secretario dio lectura al oficio con referencia W40/159/2018, suscrito por el titular de la Dirección de Recursos Materiales del Banco de México, que se agrega a la presente acta como **ANEXO "C",** por medio del cual dicha unidad administrativa solicitó a este Comité de Transparencia confirmar la ampliación del plazo ordinario de respuesta para la solicitud de acceso a la información citada, por los motivos expuestos en el oficio referido.----------

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, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64, 65 fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Vigésimo octavo de los "*Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública*", vigentes, confirma la ampliación del plazo de respuesta, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "D"**. ----------

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE INEXISTENCIA REALIZADA POR LOS TITULARES DE LA GERENCIA DE CONTABILIDAD E INFORMACIÓN FINANCIERA, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE CONTABILIDAD, PLANEACIÓN Y PRESUPUESTO, Y DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000030618. ----------

El Secretario dio lectura a los oficios de veintidós de junio de dos mil dieciocho, suscritos por los titulares de la Gerencia de Contabilidad e Información Financiera, unidad administrativa adscrita a la Dirección de Contabilidad, Planeación y Presupuesto, y de la Dirección de Apoyo a las Operaciones, que se agregan a la presente acta en un solo legajo como **ANEXO "E"**, por medio de los cuales dichas unidades administrativas solicitaron a este órgano colegiado confirmar la declaración de inexistencia de la información que señala en los citados oficios, materia de la solicitud de acceso a la información identificada con el número de folio 6110000030618, en virtud de los motivos expuestos en los citados oficios, así como en las correspondientes Actas circunstanciadas de búsqueda exhaustiva.----------

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, 44, fracción II, 138, fracción II, y 139, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64, 65 fracción II, 141, fracción II, y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México; Vigésimo séptimo de los "*Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública*", vigentes; así como Quinta, segundo párrafo, 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, confirma la declaración de inexistencia de la información, realizada por los titulares de las unidades

administrativas referidas, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "F".** ----------

TERCERO. SOLICITUD DE CONFIRMACIÓN DE INEXISTENCIA REALIZADA POR LOS TITULARES DE LA GERENCIA DE CONTABILIDAD E INFORMACIÓN FINANCIERA, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE CONTABILIDAD, PLANEACIÓN Y PRESUPUESTO, Y DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-24006. ----------

El Secretario dio lectura a los oficios de veintidós de junio de dos mil dieciocho, suscritos por los titulares de la Gerencia de Contabilidad e Información Financiera, unidad administrativa adscrita a la Dirección de Contabilidad, Planeación y Presupuesto, y de la Dirección de Apoyo a las Operaciones, que se agregan a la presente acta en un solo legajo como **ANEXO "G"**, por medio de los cuales dichas unidades administrativas solicitaron a este órgano colegiado confirmar la declaración de inexistencia de la información que señala en los citados oficios, materia de la solicitud de acceso a la información identificada con el número de folio CTC-BM-24006, en virtud de los motivos expuestos en los citados oficios, así como en las correspondientes Actas circunstanciadas de búsqueda exhaustiva. ----------

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, 44, fracción II, 138, fracción II, y 139, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64, 65 fracción II, 141, fracción II, y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México; Vigésimo séptimo de los "*Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública*", vigentes; así como Quinta, segundo párrafo, 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, confirma la declaración de inexistencia de la información, realizada por los titulares de las unidades administrativas referidas, en términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "H".** ----------

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA GERENCIA DE OPERACIONES Y CONTINUIDAD DE NEGOCIO DE LOS SISTEMAS DE PAGOS, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE SISTEMAS DE PAGOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000028418. ----------

El Secretario dio lectura al oficio con referencia D50/1158-2018, suscrito por el titular de la Gerencia de Operaciones y Continuidad de Negocios de los Sistemas de Pagos, unidad administrativa adscrita a la Dirección de Sistemas de Pagos del Banco de México, mismo que se agrega a la presente acta como **ANEXO "I"**, por virtud del cual dicha unidad administrativa ha determinado clasificar la información que se señala en dicho oficio, conforme a la fundamentación y motivación expresadas en la prueba de daño señalada en el referido oficio, y solicitó a este órgano colegiado confirmar tal clasificación. ----------

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

BANCO DE MÉXICO

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

QUINTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFROMACIÓN DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000027118. ----------

El Secretario dio lectura al oficio con referencia DGTI-90/2018, suscrito por el titular de la Dirección General de Tecnologías de Información del Banco de México, mismo que se agrega a la presente acta como **ANEXO "K"**, por virtud del cual dicha unidad administrativa ha determinado clasificar la información que se señala en dicho oficio, conforme a la fundamentación y motivación expresadas en la prueba de daño señalada en el referido oficio, y solicitó a este órgano colegiado confirmar tal clasificación.----------

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

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

SEXTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFROMACIÓN DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000027618. ----------

El Secretario dio lectura al oficio con referencia DGTI-91/2018, suscrito por el titular de la Dirección General de Tecnologías de Información del Banco de México, mismo que se agrega a la presente acta como **ANEXO "M"**, por virtud del cual dicha unidad administrativa ha determinado clasificar la información que se señala en dicho oficio, conforme a la fundamentación y motivación expresadas en la prueba de daño señalada en el referido oficio, y solicitó a este órgano colegiado confirmar tal clasificación.----------

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

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

BANCO DE MÉXICO

clasificación de la información realizada por la unidad administrativa citada, en los términos de la resolución que se agrega al apéndice de la presente acta como **ANEXO "N"**. ----------
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

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

RODOLFO SALVADOR LUNA DE LA TORRE
Secretario

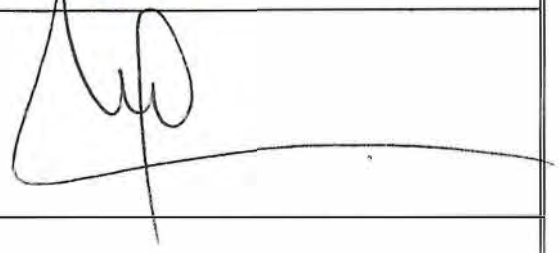
BANCO DE MÉXICO

LISTA DE ASISTENCIA

SESIÓN ORDINARIA 24/2018

28 DE JUNIO DE 2018

COMITÉ DE TRANSPARENCIA

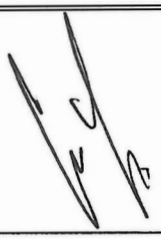
CLAUDIA ÁLVAREZ TOCA Directora de la Unidad de Transparencia Integrante	
HUMBERTO ENRIQUE RUIZ TORRES Director Jurídico Integrante	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información Integrante suplente	
RODOLFO SALVADOR LUNA DE LA TORRE Secretario del Comité de Transparencia	

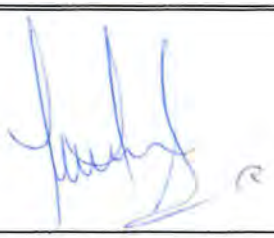
INVITADOS PERMANENTES

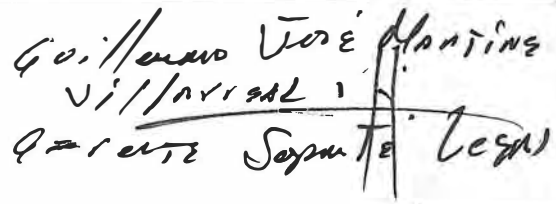
OSCAR JORGE DURÁN DÍAZ Director de Vinculación Institucional	
FRANCISCO CHAMÚ MORALES Director de Administración de Riesgos	

INVITADOS

ERIK MAURICIO SÁNCHEZ MEDINA Gerente Jurídico Consultivo	
ALAN CRUZ PICHARDO Subgerente de Apoyo Jurídico a la Transparencia	

CARLOS EDUARDO CICERO LEBRIJA Gerente de Gestión de Transparencia	
MARÍA DEL CARMEN REY CABARCOS Gerente de Riesgos No Financieros	
RODRIGO MÉNDEZ PRECIADO Abogado Especialista en la Dirección General de Relaciones Institucionales	
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 de la Subgerencia de Planeación y Regulación	
ÁNGEL MELESIO FUENTES Gerente de Operación y Continuidad de Negocio de los Sistemas de Pagos	

LILIANA GARCÍA OCHOA Líder de Especialidad de la Gerencia de Estudios de Sistemas de Pagos	
XIMENA AIDEE DOMÍNGUEZ HERNÁNDEZ Investigador de la Gerencia de Estudios de Sistemas de Pagos	
VÍCTOR MOISÉS SUÁREZ PICAZO Director de Contabilidad, Planeación y Presupuesto	
FLÉRIDA GUTIÉRREZ VIDAL Gerente de Contabilidad e Información Financiera	
MARÍA LUISA SEGOVIA MARTÍNEZ Subgerente de Contabilidad	
CLAUDIA TORRES TAPIA Jefa de la Oficina de Soporte Contable y Administrativo	
MIRNA CORTES CAMPOS Directora de Administración de Emisión	

CLAUDIA TAPIA RANGEL Especialista Investigador de la Dirección General de Operaciones y Sistemas de Pagos	
MARTÍN CAMPOS FERNÁNDEZ Analista de Información de la Oficina de Servicios Administrativos	
SERGIO ZAMBRANO HERRERA Subgerente de Análisis Jurídico y Promoción de Transparencia	
HÉCTOR GARCÍA MONDRAGÓN Jefe de la Oficina de Análisis Jurídico y Promoción de Transparencia	
	
	

ANEXO "B"

BANCO DE MÉXICO

Comité de Transparencia

ORDEN DEL DÍA
Sesión Ordinaria 24/2018
28 de junio de 2018

PRIMERO. SOLICITUD DE CONFIRMACIÓN DE AMPLIACIÓN DEL PLAZO DE RESPUESTA A LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000030118.

SEGUNDO. SOLICITUD DE CONFIRMACIÓN DE INEXISTENCIA REALIZADA POR LOS TITULARES DE LA GERENCIA DE CONTABILIDAD E INFORMACIÓN FINANCIERA, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE CONTABILIDAD, PLANEACIÓN Y PRESUPUESTO, Y DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000030618.

TERCERO. SOLICITUD DE CONFIRMACIÓN DE INEXISTENCIA REALIZADA POR LOS TITULARES DE LA GERENCIA DE CONTABILIDAD E INFORMACIÓN FINANCIERA, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE CONTABILIDAD, PLANEACIÓN Y PRESUPUESTO, Y DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO CTC-BM-24006.

CUARTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA GERENCIA DE OPERACIONES Y CONTINUIDAD DE NEGOCIO DE LOS SISTEMAS DE PAGOS, UNIDAD ADMINISTRATIVA ADSCRITA A LA DIRECCIÓN DE SISTEMAS DE PAGOS DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000028418.

QUINTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFROMACIÓN DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000027118.

SEXTO. SOLICITUD DE CONFIRMACIÓN DE LA CLASIFICACIÓN DE INFORMACIÓN REALIZADA POR EL TITULAR DE LA DIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFROMACIÓN DEL BANCO DE MÉXICO, RELACIONADA CON LA SOLICITUD DE ACCESO A LA INFORMACIÓN CON FOLIO 6110000027618.

ANEXO "C"

BANCO DE MÉXICO
RECIBIDO
21 JUN 2018
Comité de Transparencia
Por: J15310 Hora: 17:35

Recibí un oficio constante en una página

BANCO DE MÉXICO

Ciudad de México, a 21 de junio de 2018
W40/159/2018

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 **6110000030118**, que nos turnó la Unidad de Transparencia el cuatro de junio del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual en su parte conducente señala lo siguiente:

> *"Con base en mi derecho a la información, solicito conocer los tipos de seguros con los que cuentan los trabajadores de la dependencia (Seguro de Gastos Médicos Mayores, Seguro básico de accidentes personales, Seguro de autos, Seguro de Responsabilidad Civil, etc.) y cuánto se ha gastado en esto desde diciembre de 2006 a la fecha. Favor de detallar los tipos de seguros, montos que se pagan, a qué tipo y cantidad de trabajadores se les otorga, así como las empresas que otorgan estos servicios. Gracias."*

Sobre el particular, solicitamos a ese órgano colegiado que confirme la ampliación del plazo de respuesta a la solicitud de acceso indicada, por un plazo adicional de 10 días. Lo anterior en virtud de que, dada la naturaleza y complejidad de la solicitud referida, al interior de la Dirección de Recursos Materiales estamos localizando la información relacionada con los años 2006 y 2007 toda vez que no se encuentra en formato electrónico, misma que se entregará al solicitante para que ésta sea accesible, confiable, verificable, veraz y oportuna y que, de igual forma, se atienda en todo momento el requerimiento de acceso a la información del particular.

Esta solicitud de ampliación se presenta con fundamento en los artículos 44, fracción II, y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como el Vigésimo Octavo de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública".

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

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

IGNACIO JAVIER ESTÉVEZ GONZÁLEZ
Director de Recursos Materiales

ANEXO "D"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

AMPLIACIÓN DE PLAZO
Folio: 6110000030118

VISTOS, para resolver sobre la ampliación del plazo de respuesta relativa a la solicitud de acceso a la información al rubro indicada; **y**

RESULTANDO

PRIMERO. Que el cuatro de junio de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000030118**, la cual se transcribe a continuación:

> *"Con base en mi derecho a la información, solicito conocer los tipos de seguros con los que cuentan los trabajadores de la dependencia (Seguro de Gastos Médicos Mayores, Seguro básico de accidentes personales, Seguro de autos, Seguro de Responsabilidad Civil, etc.) y cuánto se ha gastado en esto desde diciembre de 2006 a la fecha. Favor de detallar los tipos de seguros, montos que se pagan, a qué tipo y cantidad de trabajadores se les otorga, así como las empresas que otorgan estos servicios. Gracias"*

SEGUNDO. Que la Unidad de Transparencia del Banco de México remitió para su atención a la Dirección de Recursos Materiales del Banco de México, el mismo cuatro de junio del presente año, la solicitud de acceso a la información referida en el resultando anterior, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que el titular de la Dirección de Recursos Materiales del Banco de México, mediante oficio con referencia W40/159/2018, sometió a la consideración del Comité de Transparencia la determinación de ampliación del plazo de respuesta a la referida solicitud de acceso a la información. Al respecto, en dicho documento manifestaron de manera medular lo siguiente:

> *"...solicitamos a ese órgano colegiado que confirme la ampliación del plazo de respuesta a la solicitud de acceso indicada, por un plazo adicional de 10 días. Lo anterior en virtud de que, dada la naturaleza y complejidad de la solicitud*

referida, al interior de la Dirección de Recursos Materiales estamos localizando la información relacionada con los años 2006 y 2007 toda vez que no se encuentra en formato electrónico, misma que se entregará al solicitante para que ésta sea accesible, confiable, verificable, veraz y oportuna y que, de igual forma, se atienda en todo momento el requerimiento de acceso a la información del particular."

CONSIDERANDO

PRIMERO. De conformidad con lo previsto en los artículos 44, fracción II, 131 y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Vigésimo octavo de los "*Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública*", este Comité de Transparencia cuenta con facultades para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las unidades administrativas del Banco.

SEGUNDO. Mediante el oficio referido en la sección de resultandos de la presente determinación, el titular de la Dirección de Recursos Materiales, expuso las razones para ampliar el plazo de respuesta a la solicitud de acceso a la información citada al rubro, particularmente, debido a que dada la naturaleza y complejidad de la misma, se encuentran realizando una búsqueda exhaustiva de la información. Lo anterior, con la finalidad de que la respuesta que se entregue al solicitante sea accesible, confiable, verificable, veraz y oportuna y que, de igual forma, se atienda en todo momento el requerimiento de acceso a la información del particular.

TERCERO. Que de conformidad con los artículos 131 de la Ley General de Transparencia y Acceso a la Información Pública y 133 de la Ley Federal de Transparencia y Acceso a la Información Pública, es necesario que las áreas competentes de los sujetos obligados realicen una búsqueda exhaustiva y razonable de la información solicitada, con la finalidad de garantizar el efectivo derecho de acceso a la información. En consecuencia, es necesario que cuente con un plazo adecuado, acorde a las circunstancias particulares, como pueden ser la complejidad técnica, material o jurídica, así como las cargas de trabajo.

Por lo anterior, atendiendo a las razones expuestas por el área mencionada, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 132, párrafo segundo, de la Ley General de Transparencia y Acceso a la Información Pública; 1, 9, 64, 65, fracción II, y 135, párrafo segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública; 31, fracción III, del Reglamento Interior del Banco de México, y Vigésimo octavo de los "*Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública*", vigentes, este Comité de Transparencia:

RESUELVE

ÚNICO. Se confirma la ampliación del plazo de respuesta, por **diez días hábiles adicionales** al plazo original, respecto de la solicitud de acceso a la información citada al rubro, en términos de lo expuesto en los considerandos Segundo y Tercero de la presente determinación.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "E"

BANCO DE MÉXICO

Ciudad de México, a 22 de junio de 2018.

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Nos referimos a la solicitud identificada con el número de folio **6110000030618**, y a su documento anexo, la cual fue turnada el trece de junio del año en curso por la Unidad de Transparencia a la Dirección de Contabilidad, Planeación y Presupuesto, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, de la Ley Federal de Transparencia y Acceso a la Información Pública, y demás disposiciones aplicables en la materia, y que refieren, la cual en su parte conducente, lo siguiente:

Descripción de la solicitud:

"PAGO DEL DECRETO EXPROPIATORIO AL EJIDO DE TEPEPAN DEL 4 DE FEBRERO DE 1972. SOLICITA SABER A QUIEN SE LE DEPOSITO DICHO PAGO, MONTO Y FECHA DEL DEPOSITO. Y QUE OTRA INSTITUCIÓN TIENE LA LISTA DE PAGO. ASI COMO LA INFORMACIÓN RELACIONADA CON BANCO NACIONAL DE CREDITO EJIDAL SA DE CV Y/ONACONAL FINANCIERA POR EL PAGO DE LA EXPROPIACIÓN DEL 4 DE FEBRERO DE 1972"

Datos adicionales de la solicitud.

"DE CONFORMIDAD CON LA INFORMACIÓN SOLICITADA. SE ADJUNTA EL PRESENTE DOCUMENTO"

Contenido del documento anexo a la solicitud:

"... nos informe con respecto al pago del **Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972**, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces Solícito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria.

- **Una parte a la Construcción del Cuarto tramo de anillo periférico**
- **Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco**
- **Otra para el colector del desagüe de la misma Ciudad de Xochimilco**

Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en **28-44-12Hs, (Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas)**, fueron valuadas en la cantidad de **$501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS).**

Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C.V y/o Nacional Financiera, S.N.C por el pago de la Expropiación **de fecha 04 de Febrero de 1972.**"

Sobre el particular, con fundamento en los artículos 19, 20, 44, fracción II, 138, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 13, 65, fracción II, 141, y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, 27, fracción II, del Reglamento Interior del Banco de México; así como Primero, párrafo primero, Segundo, fracción VIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, me permito informarles que esta Unidad Administrativa ha determinado declarar la inexistencia de **registros contables relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972**.

Lo anterior, en razón de lo siguiente:

1. Los artículos 139 de la Ley General de Transparencia y Acceso a la Información Pública y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen que la resolución del Comité de Transparencia que confirme la **inexistencia de la información solicitada contendrá los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y señalará al servidor público responsable de contar con la misma.**

2. En cumplimiento al citado precepto, con objeto de garantizar al solicitante que se realizaron las gestiones necesarias para la ubicación de la información y que estas se llevaron a cabo de conformidad con un criterio exhaustivo y fueron adecuadas para atender la particularidad del caso concreto, la Unidad de Transparencia nos turnó la solicitud en razón de que conforme a lo previsto en el artículo 27, fracción IV, del Reglamento Interior del Banco de México, esta Unidad Administrativa tiene, entre otras, las atribuciones siguientes:

   > IV.- Normar y supervisar el registro contable de las operaciones que realice el Banco y el cumplimiento de las obligaciones fiscales correspondientes;

   En este sentido, se llevó a cabo la revisión total de cada uno de los archivos que posee esta unidad administrativa correspondientes a los ejercicios 1972 y 1973, con base en la información proporcionada por el solicitante, sin haberse encontrado ninguno que se refiera a **registros contables relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972**.

3. Lo anterior se hizo constar en el acta levantada por esta unidad administrativa, la cual se adjunta al presente oficio (**Anexo Único**).

4. Por lo que respecta a **las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión**, es necesario señalar que no consta en los archivos de esta unidad administrativa correspondiente a los ejercicios 1972 y 1973, documento alguno relacionado con **registros contables relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972**.

BANCO DE MÉXICO

5. **En relación con el servidor público responsable de contar con la misma,** conforme a lo expuesto anteriormente, no existe dentro de los archivos documentales de esta unidad administrativa ningún **registro contable relativo a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972**. Por lo anterior, **no se puede determinar si algún servidor público pudo haber sido responsable de contar con ella.**

En atención a las consideraciones anteriores, concurren los elementos necesarios que acreditan de manera clara y evidente la inexistencia de la información contenida en la documentación solicitada.

Por lo expuesto, en términos de los artículos 44, fracción II, 138, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 141, y 143, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como 31, fracción III, del Reglamento Interior del Banco de México, **se solicita a ese Comité de Transparencia confirmar la declaración de inexistencia de la información referida**.

Atentamente,

FLÉRIDA GUTIÉRREZ VIDAL

Gerente de Contabilidad e Información Financiera

En suplencia por ausencia del Director de Contabilidad, Planeación y Presupuesto, con fundamento en el artículo 66, del Reglamento Interior del Banco de México

BANCO DE MÉXICO
RECIBIDO
22 JUN 2018
Comité de Transparencia
Por: BL2311 Hora: 13:55

Recibo este oficio consistente en tres páginas, y un acta circunstanciada.--

BANCO DE MÉXICO

ACTA CIRCUNSTANCIADA

En la Ciudad de México, siendo las 10:25 horas del día 22 de junio de dos mil dieciocho, se encuentran presentes en las instalaciones del Banco de México donde se localizan los archivos documentales físicos y electrónicos, correspondientes a los expedientes de la Dirección de Contabilidad, Planeación y Presupuesto, incluidos los de la Gerencia de Contabilidad e Información Financiera y de la Oficina de Soporte Contable y Administrativo, la C.P. Flérida Gutiérrez Vidal, Gerente de Contabilidad e Información Financiera, así como, en carácter de testigos, la Mtra. María Luisa Segovia Martínez, Subgerente de Contabilidad, y la Mtra. Claudia Torres Tapia, Jefe de la Oficina de Soporte Contable y Administrativo, todas ellas, trabajadoras del Banco de México, adscritas a la Dirección de Contabilidad, Planeación y Presupuesto, para hacer constar lo siguiente:-

---

PRIMERO. Que la Gerente de Contabilidad e Información Financiera de la Dirección de Contabilidad, Planeación y Presupuesto de este Instituto Central, C.P. Flérida Gutiérrez Vidal, con motivo de la solicitud identificada con el número de folio **CTC-BM-24006**, la cual refiere en su parte conducente, lo siguiente: *"... nos informe con respecto al pago del Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces, Solícito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria. •Una parte a la Construcción del Cuarto tramo de anillo periférico •Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco •Otra para el colector del desagüe de la misma Ciudad de Xochimilco. Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en 28-44-12Hs, (Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas), fueron valuadas en la cantidad de $501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS). Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C.V y/o Nacional Financiera, S.N.C por el pago de la Expropiación de fecha 04 de Febrero de 1972."*; instruyó al personal de la Oficina de Soporte Contable y Administrativo, con base en la información proporcionada por el solicitante, a realizar la revisión total de cada uno de los documentos contenidos en los archivos de la Dirección de Contabilidad, Planeación y Presupuesto, incluidos los de la Gerencia de Contabilidad e Información Financiera y de la Oficina de Soporte Contable y Administrativo, de manera exhaustiva, así como a que realizaran las acciones de búsqueda necesarias de la información que se solicitó.----------

---

SEGUNDO. Que la revisión de los expedientes físicos y electrónicos de la Dirección de Contabilidad, Planeación y Presupuesto, incluidos los de la Gerencia de Contabilidad e Información Financiera y de la Oficina de Soporte Contable y Administrativo, los cuales forman parte del Sistema Institucional de Archivos del Banco de México conforme a lo dispuesto en la Ley Federal de Archivos, se llevó a cabo durante el **período del 19 al 21 de junio de 2018**, en días hábiles bancarios y dentro del horario de trabajo.----------

---

TERCERO. Que como resultado de la búsqueda exhaustiva de la información solicitada por el particular en los archivos de la Dirección de Contabilidad, Planeación y Presupuesto, incluidos los de la Gerencia de Contabilidad e Información Financiera y de la Oficina de Soporte Contable y Administrativo del Banco de México, **no se localizó documento** alguno que contenga información relativa a **registros contables relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.**----------

---

CUARTO. Previa lectura de la presente acta y no habiendo otro asunto que tratar, se da por concluida la misma, siendo las 10:50 horas del mismo día de su celebración; firmándola las personas que en ella intervinieron, lo que hacen constar en este momento para todos los efectos legales a que hubiere lugar.----------

C.P. Flérida Gutiérrez Vidal
Gerente de Contabilidad e Información Financiera

Mtra. María Luisa Segovia Martínez Subgerente de Contabilidad	Mtra. Claudia Torres Tapia Jefe de la Oficina de Soporte Contable y Administrativo

BANCO DE MÉXICO
RECIBIDO
22 JUN 2018
Comité de Transparencia
Por: 215390 Hora: 13:46

Recibí un oficio constante en tres páginas y un acta circunstanciada.

BANCO DE MÉXICO

Ciudad de México, a 22 de junio de 2018.

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

Nos referimos a la solicitud identificada con el número de folio **6110000030618**, y a su documento anexo, la cual fue turnada el trece de junio del año en curso por la Unidad de Transparencia a la Dirección General de Operaciones y Sistemas de Pagos, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, de la Ley Federal de Transparencia y Acceso a la Información Pública, y demás disposiciones aplicables en la materia, y que refieren, en su parte conducente, lo siguiente:

Descripción de la solicitud:

"PAGO DEL DECRETO EXPROPIATORIO AL EJIDO DE TEPEPAN DEL 4 DE FEBRERO DE 1972. SOLICITA SABER A QUIEN SE LE DEPOSITO DICHO PAGO, MONTO Y FECHA DEL DEPOSITO. Y QUE OTRA INSTITUCIÓN TIENE LA LISTA DE PAGO. ASI COMO LA INFORMACIÓN RELACIONADA CON BANCO NACIONAL DE CREDITO EJIDAL SA DE CV Y/ONACONAL FINANCIERA POR EL PAGO DE LA EXPROPIACIÓN DEL 4 DE FEBRERO DE 1972"

Datos adicionales de la solicitud.

"DE CONFORMIDAD CON LA INFORMACIÓN SOLICITADA. SE ADJUNTA EL PRESENTE DOCUMENTO"

Contenido del documento anexo a la solicitud:

"… nos informe con respecto al pago del **Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972**, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces Solícito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria.

- **Una parte a la Construcción del Cuarto tramo de anillo periférico**
- **Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco**
- **Otra para el colector del desagüe de la misma Ciudad de Xochimilco**

Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en **28-44-12Hs, (Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas**), fueron valuadas en la cantidad de **$501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS).**

Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C.V y/o Nacional Financiera, S.N.C por el pago de la Expropiación **de fecha 04 de Febrero de 1972**."

Sobre el particular, con fundamento en los artículos 19, 20, 44, fracción II, 138, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 13, 65, fracción II, 141, y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública; 19 Bis 1, fracción II, del Reglamento Interior del Banco de México; así como Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, me permito informarles que esta Unidad Administrativa ha determinado declarar la inexistencia de la información relativa a algún depósito a nombre del **ejido de "TEPEPAN"** o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.

Lo anterior, en razón de lo siguiente:

1. Los artículos 139 de la Ley General de Transparencia y Acceso a la Información Pública y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen que la resolución del Comité de Transparencia que confirme la **inexistencia de la información solicitada contendrá los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y señalará al servidor público responsable de contar con la misma.**

2. En cumplimiento al citado precepto, con objeto de garantizar al solicitante que se realizaron las gestiones necesarias para la ubicación de la información y que estas se llevaron a cabo de conformidad con un criterio exhaustivo y fueron adecuadas para atender la particularidad del caso concreto, la Unidad de Transparencia nos turnó la solicitud en razón de que en términos del artículos 19 BIS 1, fracción II, del Reglamento Interior del Banco de México, la Dirección de Apoyo a las Operaciones, está facultada para atender, verificar y registrar las operaciones que efectúen los cuentahabientes del Banco.

   En relación con lo anterior, se consideró que el "DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal", publicado en el Diario Oficial de la Federación el 2 de febrero de 1972, estableció:

   *"...PRIMERO.- Por causa de utilidad pública, exprópiese al **ejido de " TEPEPAN"**, Delegación de Xochimilco, del Distrito Federal, a favor del Departamento del Distrito Federal,...*

   ...

   *SEGUNDO.- Queda a cargo del Departamento del Distrito Federal, el **pago por concepto de indemnización** de la cantidad de $501,276.15, (QUINIENTOS UN MIL, DOSCIENTOS SETENTA Y SEIS PESOS, QUINCE CENTAVOS), que ingresará al Fondo Común del Ejido, a fin de que se aplique como lo dispone la Ley Federal de Reforma Agraria, para cuyo efecto previamente a la ejecución de este Decreto, depositará a nombre del ejido afectado, **en el Banco de México, S. A.**, la cantidad de referencia, en la inteligencia de que si a los terrenos expropiados se les dá un fin distinto al que motivó este Decreto o no cumplen la función asignada en el término de cinco años contados a partir del acto expropiatorio, quedará sin efecto la expropiación y dichos terrenos pasarán de inmediato a ser propiedad del Fondo Nacional de Fomento Ejidal, sin que proceda la devolución de las sumas o bienes entregados por concepto de indemnización...".*

   Énfasis añadido

En este sentido, se llevó a cabo la revisión total de cada uno de los archivos que posee esta unidad administrativa, sin haberse encontrado información relativa a algún depósito a nombre del **ejido de "TEPEPAN"** o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal…",* publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.

3. Lo anterior se hizo constar en el acta levantada por esta unidad administrativa, la cual se adjunta al presente oficio (**Anexo Único**).

4. Por lo que respecta a **las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión**, es necesario señalar que no consta en los archivos de esta unidad administrativa documento alguno que contenga información relativa a algún depósito a nombre del **ejido de "TEPEPAN"** o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal…",* publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.

5. **En relación con el servidor público responsable de contar con la misma,** conforme a lo expuesto anteriormente, no existe dentro de los archivos documentales de esta unidad administrativa ningún registro relacionado con pago de decretos expropiatorios. Por lo anterior, **no se puede determinar si algún servidor público pudo haber sido responsable de contar con ella.**

En atención a las consideraciones anteriores, concurren los elementos necesarios que acreditan de manera clara y evidente la inexistencia de la información contenida en la documentación solicitada.

Por lo expuesto, en términos de los artículos 44, fracción II, 138, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 141, y 143, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como 31, fracción III, del Reglamento Interior del Banco de México, **se solicita a ese Comité de Transparencia confirmar la declaración de inexistencia de la información referida**.

Atentamente,

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

BANCO DE MÉXICO

ACTA CIRCUNSTANCIADA

En la Ciudad de México, siendo las 10:00 horas del día 22 de junio de dos mil dieciocho, se encuentran presentes en las instalaciones del Banco de México donde se localizan los archivos documentales físicos y electrónicos, correspondientes a los expedientes de la Dirección de Apoyo a las Operaciones, la Act. Norma Juliana Castro Roa, Gerente de Gestión de Operaciones, así como, en carácter de testigos, el Lic. Ignacio Alfredo Flores Luna, Jefe de la Oficina de Servicios Bancarios a Cuentahabientes y el Lic. Juan Cesar Peralta Sandoval, Jefe de la Oficina de Operaciones con Valores, Créditos y Depósitos, todos ellos, trabajadores del Banco de México, adscritos a la Dirección de Apoyo a las Operaciones, para hacer constar lo siguiente:----------

---

PRIMERO. Que la Gerente de Gestión de Operaciones de este Instituto Central, Act. Norma Juliana Castro Roa, con motivo de la solicitud identificada con el número de folio **6110000030618**, y de su anexo, que refieren en su parte conducente, lo siguiente: **Descripción de la solicitud:** *"PAGO DEL DECRETO EXPROPIATORIO AL EJIDO DE TEPEPAN DEL 4 DE FEBRERO DE 1972. SOLICITA SABER A QUIEN SE LE DEPOSITO DICHO PAGO, MONTO Y FECHA DEL DEPOSITO. Y QUE OTRA INSTITUCIÓN TIENE LA LISTA DE PAGO. ASI COMO LA INFORMACIÓN RELACIONADA CON BANCO NACIONAL DE CREDITO EJIDAL SA DE CV Y/ONACONAL FINANCIERA POR EL PAGO DE LA EXPROPIACIÓN DEL 4 DE FEBRERO DE 1972"*. **Datos adicionales de la solicitud:** *"DE CONFORMIDAD CON LA INFORMACIÓN SOLICITADA. SE ADJUNTA EL PRESENTE DOCUMENTO"*. **Contenido del documento anexo a la solicitud:** "... nos informe con respecto al pago del Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces Solícito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria. •Una parte a la Construcción del Cuarto tramo de anillo periférico •Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco •Otra para el colector del desagüe de la misma Ciudad de Xochimilco. Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en 28-44-12Hs, (Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas), fueron valuadas en la cantidad de $501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS). Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C.V y/o Nacional Financiera, S.N.C por el pago de la Expropiación de fecha 04 de Febrero de 1972."; instruyó al personal de la Oficina de Servicios Bancarios a Cuentahabientes y de la Oficina de Operaciones con Valores, Créditos y Depósitos, a realizar la revisión total de cada uno de los documentos contenidos en los expedientes relacionados con los pagos a cuentahabientes de este Instituto Central, de manera exhaustiva, así como a que realizaran las acciones de búsqueda necesarias de la información que se solicitó.----------

---

SEGUNDO. Que la revisión de los expedientes físicos y electrónicos de la Dirección de Apoyo a las Operaciones, los cuales forman parte del Sistema Institucional de Archivos del Banco de México conforme a lo dispuesto en la Ley Federal de Archivos, se llevó a cabo durante el **período del 13 al 21 de junio de 2018**, en días hábiles bancarios y dentro del horario de trabajo.----------

---

TERCERO. Que como resultado de la búsqueda exhaustiva de la información solicitada en los archivos de la Gerencia de Gestión de Operaciones del Banco de México, **no se localizó documento** o registro alguno que contenga información relativa a algún depósito a nombre del **ejido de "TEPEPAN"** o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.--------

---

CUARTO. Previa lectura de la presente acta y no habiendo otro asunto que tratar, se da por concluida la misma, siendo las 10:05 horas del mismo día de su celebración; firmándola las personas que en ella intervinieron, lo que hacen constar en este momento para todos los efectos legales a que hubiere lugar.----------

Act. Norma Juliana Castro Roa Gerente Gerencia de Gestión de Operaciones	Lic. Ignacio Alfredo Flores Luna Jefe Oficina de Servicios Bancarios a Cuentahabientes
Lic. ~~Juan Cesar Peralta Sandoval~~ Jefe Oficina de Operaciones con Valores, Créditos y Depósitos	---------- ---------- ---------- ---------- ---------- ---------- ----------

ANEXO "F"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

DECLARACIÓN DE INEXISTENCIA
FOLIO:6110000030618

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

RESULTANDO

PRIMERO. Que el siete de junio de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000030618,** que se transcribe a continuación:

> ***Descripción:*** *"PAGO DEL DECRETO EXPROPIATORIO AL EJIDO DE TEPEPAN DEL 4 DE FEBRERO DE 1972. SOLICITA SABER A QUIEN SE LE DEPOSITO DICHO PAGO, MONTO Y FECHA DEL DEPOSITO. Y QUE OTRA INSTITUCIÓN TIENE LA LISTA DE PAGO. ASI COMO LA INFORMACIÓN RELACIONADA CON BANCO NACIONAL DE CREDITO EJIDAL SA DE CV Y/ONACONAL FINANCIERA POR EL PAGO DE LA EXPROPIACIÓN DEL 4 DE FEBRERO DE 1972."*

SEGUNDO. Que el mismo siete de junio del presente año, la Unidad de Transparencia turnó, para su atención, la citada solicitud a la Dirección General de Operaciones y Sistemas de Pagos el mismo siete de junio; y a la Dirección de Contabilidad, Planeación y Presupuesto, el trece de junio del presente año, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que los titulares de la Dirección de Apoyo a las Operaciones, unidad administrativa adscrita a la Dirección General de Operaciones y Sistemas de Pagos, y de la Gerencia de Contabilidad e Información Financiera, en suplencia por ausencia del Director de Contabilidad, Planeación y Presupuesto, mediante oficios de veintidós de junio de dos mil dieciocho, ambas unidades administrativas, hicieron del conocimiento de este Comité de Transparencia, su declaración de inexistencia respecto de la información requerida a través de la referida solicitud, adjuntando cada una de dichas unidades administrativas del Banco Central sus respectivas actas circunstanciadas en la que se hacen constar que realizaron una búsqueda exhaustiva de dicha información, sin encontrarla en sus archivos. Asimismo, las mencionadas unidades administrativas señalaron las circunstancias de modo, tiempo, y lugar que generaron la inexistencia de que se trata, y se pronunciaron coincidentemente respecto a que en virtud de no existir registro alguno dentro de los archivos documentales correspondientes, no se puede determinar si algún servidor público pudo haber sido responsable de contar con lo requerido por el particular, y solicitaron a este Comité confirmar la inexistencia señalada.

CONSIDERANDO

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

Transparencia y Acceso a la Información Pública, y 31, fracción III, del Reglamento Interior del Banco de México.

SEGUNDO. En términos de los artículos 139 de la Ley General de Transparencia y Acceso a la Información Pública y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité analiza que la declaración de inexistencia contenga los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y señalará al servidor público responsable de contar con la misma.

A este respecto, se analizan enseguida los oficios señalados en el resultando Tercero de la presente resolución, a través de los cuales la Dirección de Apoyo a las Operaciones y la Gerencia de Contabilidad e Información Financiera, en suplencia por ausencia del Director de Contabilidad, Planeación y Presupuesto señalan, entre otras cosas, lo siguiente:

1. Que con objeto de garantizar al solicitante que realizaron las gestiones necesarias para la ubicación de lo requerido por el particular y que estas las llevaron a cabo de conformidad con un criterio exhaustivo y que fueron adecuadas para atender la particularidad del caso concreto, la Unidad de Transparencia les turnó la citada solicitud en razón de sus atribuciones previstas en el Reglamento Interior del Banco de México.

2. Que realizaron la revisión de sus archivos y, en su caso, de manera específica cada unidad administrativa argumentó diversas consideraciones en sus colaboraciones a la solicitud que nos ocupa, sin haberse encontrado en sus archivos: ***"… registros … relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el "DECRETO" que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D.F., a favor del Departamento del Distrito Federal…", publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.***

3. Que en cuanto a **las circunstancias de tiempo, modo y lugar,** las unidades administrativas de este Banco Central señalaron en sus respectivos oficios las razones por las cuales determinaron la inexistencia de información.

4. **Que en relación con el servidor público responsable de contar con la misma,** no existe registro alguno dentro de los archivos documentales de dichas unidades administrativas relacionado con la información cuya inexistencia se ha declarado, por lo que **no se puede determinar si algún servidor público pudo haber sido responsable de contar con ella.**

5. Todo lo anterior, en términos de lo que detalla cada una de las unidades administrativas que declararon la inexistencia a través de su respectivo oficio y acta circunstanciada adjunta.

Este órgano colegiado estima que concurren los elementos necesarios para acreditar la inexistencia de lo requerido por el particular en su solicitud, en atención a lo señalado en los oficios presentados por las unidades administrativas mencionadas en el resultando Tercero.

Por lo anterior, y de conformidad con los artículos 44, fracción II, 138, fracción II, y 139, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 141, fracción II, y 143, de la Ley Federal de Transparencia y Acceso a la Información Pública; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, y 31, fracción II, del Reglamento Interior del Banco de México, este Comité de Transparencia **confirma la declaración de inexistencia realizada por** la la Dirección de Apoyo a las Operaciones y la Gerencia de Contabilidad e Información Financiera, en suplencia por ausencia del Director de Contabilidad, Planeación y Presupuesto, respecto de:***"… registros … relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el "DECRETO" que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D.F., a favor del Departamento del Distrito Federal…", publicado en el Diario Oficial de la Federación el 4 de febrero de 1972***, al que se hace referencia en la solicitud **6110000030618.**

Por lo expuesto, con fundamento en los artículos 1, 23, 43 y 44, fracción II, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos primero, segundo, tercero y quinto y 65, en su fracciones II y IX, y 143, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracciones III y XX, del Reglamento Interior del Banco de México; así como Quinta, de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

ÚNICO. Se **confirma la declaración de inexistencia** de la información a la que se refieren los oficios señalados en el resultando Tercero de la presente resolución, en relación con la información requerida en la solicitud con folio **6110000030618**, en términos de lo expuesto en la presente resolución.

Así lo resolvió, por unanimidad de los integrantes presentes de este Comité de Transparencia del Banco de México, en sesión celebrada el veintiocho de junio de dos mil diecisiete.----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "G"

BANCO DE MÉXICO

Ciudad de México, a 22 de junio de 2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Nos referimos a la solicitud identificada con el número de folio **CTC-BM-24006**, la cual fue turnada el quince de junio del año en curso por la Unidad de Transparencia a la Dirección de Contabilidad, Planeación y Presupuesto, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, de la Ley Federal de Transparencia y Acceso a la Información Pública, y demás disposiciones aplicables en la materia, la cual en su parte conducente señala lo siguiente:

> *"*
> *... nos informe con respecto al pago del* ***Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972****, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces, Solicito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria.*
> - ***Una parte a la Construcción del Cuarto tramo de anillo periférico***
> - ***Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco***
> - ***Otra para el colector del desagüe de la misma Ciudad de Xochimilco***
>
> *Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en* ***28-44-12Hs, (Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas), fueron valuadas en la cantidad de $501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS).***
> *Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C.V y/o Nacional Financiera, S.N.C por el pago de la Expropiación de* ***fecha 04 de Febrero de 1972****."*

Sobre el particular, con fundamento en los artículos 19, 20, 44, fracción II, 138, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 13, 65, fracción II, 141, y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, 27, fracción II, del Reglamento Interior del Banco de México; así como Primero, párrafo primero, Segundo, fracción VIII, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, me permito informarles que esta Unidad Administrativa ha determinado declarar la inexistencia de **registros contables relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el "*DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal...*", publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.**

Lo anterior, en razón de lo siguiente:

1. Los artículos 139 de la Ley General de Transparencia y Acceso a la Información Pública y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen que la resolución del Comité de Transparencia que confirme la **inexistencia de la información solicitada contendrá los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y señalará al servidor público responsable de contar con la misma.**

2. En cumplimiento al citado precepto, con objeto de garantizar al solicitante que se realizaron las gestiones necesarias para la ubicación de la información y que estas se llevaron a cabo de conformidad con un criterio exhaustivo y fueron adecuadas para atender la particularidad del caso concreto, la Unidad de Transparencia nos turnó la solicitud en razón de que conforme a lo previsto en el artículo 27, fracción IV, del Reglamento Interior del Banco de México, esta Unidad Administrativa tiene, entre otras, las atribuciones siguientes:

   > IV. Normar y supervisar el registro contable de las operaciones que realice el Banco y el cumplimiento de las obligaciones fiscales correspondientes;

   En este sentido, se llevó a cabo la revisión total de cada uno de los archivos que posee esta unidad administrativa correspondientes a los ejercicios 1972 y 1973, con base en la información proporcionada por el solicitante, sin haberse encontrado ninguno que se refiera a **registros contables relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972**.

3. Lo anterior se hizo constar en el acta levantada por esta unidad administrativa, la cual se adjunta al presente oficio (**Anexo Único**).

4. Por lo que respecta a **las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión**, es necesario señalar que no consta en los archivos de esta unidad administrativa correspondiente a los ejercicios 1972 y 1973, documento alguno relacionado con **registros contables relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972**.

5. **En relación con el servidor público responsable de contar con la misma,** conforme a lo expuesto anteriormente, no existe dentro de los archivos documentales de esta unidad administrativa ningún **registro contable relativo a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972**. Por lo anterior, **no se puede determinar si algún servidor público pudo haber sido responsable de contar con ella.**

En atención a las consideraciones anteriores, concurren los elementos necesarios que acreditan de manera clara y evidente la inexistencia de la información contenida en la documentación solicitada.

BANCO DE MÉXICO

Por lo expuesto, en términos de los artículos 44, fracción II, 138, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 141, y 143, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como 31, fracción III, del Reglamento Interior del Banco de México, **se solicita a ese Comité de Transparencia confirmar la declaración de inexistencia de la información referida**.

Atentamente,

FLÉRIDA GUTIÉRREZ VIDAL
Gerente de Contabilidad e Información Financiera
En suplencia por ausencia del Director de Contabilidad, Planeación y Presupuesto, con fundamento en el artículo 66, del Reglamento Interior del Banco de México

BANCO DE MÉXICO
RECIBIDO
22 JUN 2018
Comité de Transparencia
Por: BL1322 Hora: 13:56
Recibo de Fisa constante en tres páginas y una acta circunstanciada.

BANCO DE MÉXICO

ACTA CIRCUNSTANCIADA

En la Ciudad de México, siendo las 10:25 horas del día 22 de junio de dos mil dieciocho, se encuentran presentes en las instalaciones del Banco de México donde se localizan los archivos documentales físicos y electrónicos, correspondientes a los expedientes de la Dirección de Contabilidad, Planeación y Presupuesto, incluidos los de la Gerencia de Contabilidad e Información Financiera y de la Oficina de Soporte Contable y Administrativo, la C.P. Flérida Gutiérrez Vidal, Gerente de Contabilidad e Información Financiera, así como, en carácter de testigos, la Mtra. María Luisa Segovia Martínez, Subgerente de Contabilidad, y la Mtra. Claudia Torres Tapia, Jefe de la Oficina de Soporte Contable y Administrativo, todas ellas, trabajadoras del Banco de México, adscritas a la Dirección de Contabilidad, Planeación y Presupuesto, para hacer constar lo siguiente:-

---

PRIMERO. Que la Gerente de Contabilidad e Información Financiera de la Dirección de Contabilidad, Planeación y Presupuesto de este Instituto Central, C.P. Flérida Gutiérrez Vidal, con motivo de la solicitud identificada con el número de folio **CTC-BM-24006**, la cual refiere en su parte conducente, lo siguiente: *"... nos informe con respecto al pago del Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces, Solicito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria. •Una parte a la Construcción del Cuarto tramo de anillo periférico •Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco •Otra para el colector del desagüe de la misma Ciudad de Xochimilco. Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en 28-44-12Hs, (Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas), fueron valuadas en la cantidad de $501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS). Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C.V y/o Nacional Financiera, S.N.C por el pago de la Expropiación de fecha 04 de Febrero de 1972."*; instruyó al personal de la Oficina de Soporte Contable y Administrativo, con base en la información proporcionada por el solicitante, a realizar la revisión total de cada uno de los documentos contenidos en los archivos de la Dirección de Contabilidad, Planeación y Presupuesto, incluidos los de la Gerencia de Contabilidad e Información Financiera y de la Oficina de Soporte Contable y Administrativo, de manera exhaustiva, así como a que realizaran las acciones de búsqueda necesarias de la información que se solicitó.----------

---

SEGUNDO. Que la revisión de los expedientes físicos y electrónicos de la Dirección de Contabilidad, Planeación y Presupuesto, incluidos los de la Gerencia de Contabilidad e Información Financiera y de la Oficina de Soporte Contable y Administrativo, los cuales forman parte del Sistema Institucional de Archivos del Banco de México conforme a lo dispuesto en la Ley Federal de Archivos, se llevó a cabo durante el **período del 19 al 21 de junio de 2018**, en días hábiles bancarios y dentro del horario de trabajo.----------

---

TERCERO. Que como resultado de la búsqueda exhaustiva de la información solicitada por el particular en los archivos de la Dirección de Contabilidad, Planeación y Presupuesto, incluidos los de la Gerencia de Contabilidad e Información Financiera y de la Oficina de Soporte Contable y Administrativo del Banco de México, **no se localizó documento** alguno que contenga información relativa a **registros contables relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.**----------

---

CUARTO. Previa lectura de la presente acta y no habiendo otro asunto que tratar, se da por concluida la misma, siendo las 10:50 horas del mismo día de su celebración; firmándola las personas que en ella intervinieron, lo que hacen constar en este momento para todos los efectos legales a que hubiere lugar.----------

C.P. Flérida Gutiérrez Vidal
Gerente de Contabilidad e Información Financiera

Mtra. María Luisa Segovia Martínez Subgerente de Contabilidad	Mtra. Claudia Torres Tapia Jefe de la Oficina de Soporte Contable y Administrativo

BANCO DE MÉXICO
RECIBIDO
22 JUN 2018
Comité de Transparencia
Por: JL5390 Hora: 13:45

Recibí un oficio constante en tres páginas y un acta circunstanciada.-

BANCO DE MÉXICO

Ciudad de México, a 22 de junio de 2018.

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

Nos referimos a la solicitud identificada con el número de folio **CTC-BM-24006**, la cual fue turnada el quince de junio del año en curso por la Unidad de Transparencia a la Dirección General de Operaciones y Sistemas de Pagos, a través del sistema electrónico de atención a solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, de la Ley Federal de Transparencia y Acceso a la Información Pública, y demás disposiciones aplicables en la materia, la cual en su parte conducente señala lo siguiente:

> "
> *... nos informe con respecto al pago del **Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972**, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces, Solícito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria.*
> - ***Una parte a la Construcción del Cuarto tramo de anillo periférico***
> - ***Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco***
> - ***Otra para el colector del desagüe de la misma Ciudad de Xochimilco***
>
> *Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en **28-44-12Hs, (Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas), fueron valuadas en la cantidad de $501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS).***
> *Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C.V y/o Nacional Financiera, S.N.C por el pago de la Expropiación de **fecha 04 de Febrero de 1972**."*

Sobre el particular, con fundamento en los artículos 19, 20, 44, fracción II, 138, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 13, 65, fracción II, 141, y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública; 19 Bis 1, fracción II, del Reglamento Interior del Banco de México; así como Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México, me permito informarles que esta Unidad Administrativa ha determinado declarar la inexistencia de la información relativa a algún depósito a nombre del **ejido de "TEPEPAN"** o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.

Lo anterior, en razón de lo siguiente:

1. Los artículos 139 de la Ley General de Transparencia y Acceso a la Información Pública y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública, establecen que la resolución del Comité de Transparencia que confirme la **inexistencia de la información solicitada contendrá los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y señalará al servidor público responsable de contar con la misma.**

2. En cumplimiento al citado precepto, con objeto de garantizar al solicitante que se realizaron las gestiones necesarias para la ubicación de la información y que estas se llevaron a cabo de conformidad con un criterio exhaustivo y fueron adecuadas para atender la particularidad del caso concreto, la Unidad de Transparencia nos turnó la solicitud en razón de que en términos del artículos 19 BIS 1, fracción II, del Reglamento Interior del Banco de México, la Dirección de Apoyo a las Operaciones, está facultada para atender, verificar y registrar las operaciones que efectúen los cuentahabientes del Banco.

   En relación con lo anterior, se consideró que el "DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal", publicado en el Diario Oficial de la Federación el 2 de febrero de 1972, estableció:

   > *"…PRIMERO.- Por causa de utilidad pública, exprópiese al **ejido de " TEPEPAN"**, Delegación de Xochimilco, del Distrito Federal, a favor del Departamento del Distrito Federal,…*
   >
   > …
   >
   > *SEGUNDO.- Queda a cargo del Departamento del Distrito Federal, el **pago por concepto de indemnización** de la cantidad de $501,276.15, (QUINIENTOS UN MIL, DOSCIENTOS SETENTA Y SEIS PESOS, QUINCE CENTAVOS), que ingresará al Fondo Común del Ejido, a fin de que se aplique como lo dispone la Ley Federal de Reforma Agraria, para cuyo efecto previamente a la ejecución de este Decreto, depositará a nombre del ejido afectado, **en el Banco de México, S. A.**, la cantidad de referencia, en la inteligencia de que si a los terrenos expropiados se les dá un fin distinto al que motivó este Decreto o no cumplen la función asignada en el término de cinco años contados a partir del acto expropiatorio, quedará sin efecto la expropiación y dichos terrenos pasarán de inmediato a ser propiedad del Fondo Nacional de Fomento Ejidal, sin que proceda la devolución de las sumas o bienes entregados por concepto de indemnización…".*
   >
   > Énfasis añadido

   En este sentido, se llevó a cabo la revisión total de cada uno de los archivos que posee esta unidad administrativa, sin haberse encontrado información relativa a algún depósito a nombre del **ejido de "TEPEPAN**" o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal…",* publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.

3. Lo anterior se hizo constar en el acta levantada por esta unidad administrativa, la cual se adjunta al presente oficio (**Anexo Único**).

4. Por lo que respecta a **las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión**, es necesario señalar que no consta en los archivos de esta unidad administrativa documento alguno que contenga información relativa a algún depósito a nombre del **ejido de "TEPEPAN"** o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal…",* publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.

5. **En relación con el servidor público responsable de contar con la misma,** conforme a lo expuesto anteriormente, no existe dentro de los archivos documentales de esta unidad administrativa ningún registro relacionado con pago de decretos expropiatorios. Por lo anterior, **no se puede determinar si algún servidor público pudo haber sido responsable de contar con ella.**

En atención a las consideraciones anteriores, concurren los elementos necesarios que acreditan de manera clara y evidente la inexistencia de la información contenida en la documentación solicitada.

Por lo expuesto, en términos de los artículos 44, fracción II, 138, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 141, y 143, de la Ley Federal de Transparencia y Acceso a la Información Pública; así como 31, fracción III, del Reglamento Interior del Banco de México, **se solicita a ese Comité de Transparencia confirmar la declaración de inexistencia de la información referida**.

Atentamente,

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

BANCO DE MÉXICO

ACTA CIRCUNSTANCIADA

En la Ciudad de México, siendo las 10:05 horas del día 22 de junio de dos mil dieciocho, se encuentran presentes en las instalaciones del Banco de México donde se localizan los archivos documentales físicos y electrónicos, correspondientes a los expedientes de la Dirección de Apoyo a las Operaciones, la Act. Norma Juliana Castro Roa, Gerente de Gestión de Operaciones, así como, en carácter de testigos, el Lic. Ignacio Alfredo Flores Luna, Jefe de la Oficina de Servicios Bancarios a Cuentahabientes y el Lic. Juan Cesar Peralta Sandoval, Jefe de la Oficina de Operaciones con Valores, Créditos y Depósitos, todos ellos, trabajadores del Banco de México, adscritos a la Dirección de Apoyo a las Operaciones, para hacer constar lo siguiente:----------

---

PRIMERO. Que la Gerente de Gestión de Operaciones de este Instituto Central, Act. Norma Juliana Castro Roa, con motivo de la solicitud identificada con el número de folio **CTC-BM-24006**, la cual refiere en su parte conducente, lo siguiente: *"… nos informe con respecto al pago del Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces, Solícito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria. •Una parte a la Construcción del Cuarto tramo de anillo periférico •Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco •Otra para el colector del desagüe de la misma Ciudad de Xochimilco. Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en 28-44-12Hs, (Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas), fueron valuadas en la cantidad de $501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS). Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C.V y/o Nacional Financiera, S.N.C por el pago de la Expropiación de fecha 04 de Febrero de 1972.";* instruyó al personal de la Oficina de Servicios Bancarios a Cuentahabientes y de la Oficina de Operaciones con Valores, Créditos y Depósitos, a realizar la revisión total de cada uno de los documentos contenidos en los expedientes relacionados con los pagos a cuentahabientes de este Instituto Central, de manera exhaustiva, así como a que realizaran las acciones de búsqueda necesarias de la información que se solicitó.----------

---

SEGUNDO. Que la revisión de los expedientes físicos y electrónicos de la Dirección de Apoyo a las Operaciones, los cuales forman parte del Sistema Institucional de Archivos del Banco de México

conforme a lo dispuesto en la Ley Federal de Archivos, se llevó a cabo durante el **período del 18 al 21 de junio de 2018**, en días hábiles bancarios y dentro del horario de trabajo.----------

---

TERCERO. Que como resultado de la búsqueda exhaustiva de la información solicitada en los archivos de la Gerencia de Gestión de Operaciones del Banco de México, **no se localizó documento** o registro alguno que contenga información relativa a algún depósito a nombre del **ejido de "TEPEPAN"** o relacionado con el *"DECRETO que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D. F., a favor del Departamento del Distrito Federal..."*, publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.--------

---

CUARTO. Previa lectura de la presente acta y no habiendo otro asunto que tratar, se da por concluida la misma, siendo las 10:10 horas del mismo día de su celebración; firmándola las personas que en ella intervinieron, lo que hacen constar en este momento para todos los efectos legales a que hubiere lugar.----------

Act. Norma Juliana Castro Roa Gerente Gerencia de Gestión de Operaciones	Lic. Ignacio Alfredo Flores Luna Jefe Oficina de Servicios Bancarios a Cuentahabientes
Lic. Juan Cesar Peralta Sandoval Jefe Oficina de Operaciones con Valores, Créditos y Depósitos	---------- ---------- ---------- ---------- ---------- ---------- ----------

ANEXO "H"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

DECLARACIÓN DE INEXISTENCIA
FOLIO:CTC-BM-24006

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

RESULTANDO

PRIMERO. Que el quince de junio de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **CTC-BM-24006,** que se transcribe a continuación:

> *"... nos informe con respecto al pago del Decreto expropiatorio al Ejido de Tepepan de fecha 04 cuatro de Febrero de 1972, que en oficio número1329 de fecha 09 de febrero de 1966 el Jefe de Gobierno del Departamento del Distrito Federal, de ese entonces, Solicito al Titular del Departamento de Asuntos Agrarios y Colonización la Expropiación del Ejido de Tepepan que se destinaria.*
>
> *• Una parte a la Construcción del Cuarto tramo de anillo periférico*
> *• Otra para la avenida que ligara este anillo con la Ciudad de Xochimilco*
> *• Otra para el colector del desagüe de la misma Ciudad de Xochimilco*
>
> *Comprometiéndose el Departamento del Distrito Federal a pagar la indemnización conforme a la ley. Que por Resolución del Presidencial de 9 marzo 1938 publicada en el Diario Oficial de la Federación el 11 de Julio 1938 Y ejecutada el 2 septiembre de1939 se concedió a TEPEPAN por concepto de Ampliación una superficie de; 127-14-95 Hs. Habiéndose aprobado el plano y expediente para dar cumplimiento al Acuerdo Presidencial de 15 de Abril 1933 publicado en el Diario Oficial de la Federación el 10 de Junio de 1933, se nombró un perito valuador de la Secretaria del Patrimonio Nacional quien manifiesta que la superficie a expropiar consiste en 28-44-12Hs, {Veintiocho hectáreas cuarenta y cuatro áreas doce centiáreas}, fueron valuadas en la cantidad de $501,276.15, (QUINIENTOS UN MIL MILLONES DOSCIENTOS SETENTA Y SEIS MIL PESOS CON QUINCE CENTAVOS).*
>
> *Y dado el caso se nos informe las fechas de los depósitos realizados en ese entonces a Banco Nacional de Crédito Ejidal S.A de C. V y/o Nacional Financiera, S.N. C por el pago de la Expropiación de fecha 04 de Febrero de 1972."*

SEGUNDO. Que el mismo quince de junio del presente año, la Unidad de Transparencia turnó, para su atención, la citada solicitud, a la Dirección General de Operaciones y Sistemas de Pagos y a la Dirección de Contabilidad, Planeación y Presupuesto, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que los titulares de la Gerencia de Contabilidad e Información Financiera, en suplencia por ausencia del Director de Contabilidad, Planeación y Presupuesto, y de la Dirección de Apoyo a las Operaciones, unidad administrativa adscrita a la Dirección General de Operaciones y Sistemas de Pagos mediante oficios de veintidós de junio de dos mil dieciocho, hicieron del conocimiento de este Comité de Transparencia, su declaración de inexistencia respecto de la información requerida a través de la referida solicitud, adjuntando cada una de dichas unidades administrativas sus respectivas actas circunstanciadas en la que se hacen constar que realizaron una búsqueda exhaustiva de dicha información, sin encontrarla en sus archivos. Asimismo, las mencionadas unidades administrativas señalaron las circunstancias de modo, tiempo, y lugar que generaron la inexistencia de que se trata, y se pronunciaron coincidentemente respecto a que en virtud de no existir registro alguno dentro de los archivos documentales correspondientes, no se puede determinar si algún servidor público pudo haber sido responsable de contar con lo requerido por el particular, y solicitaron a este Comité confirmar la inexistencia señalada.

CONSIDERANDO

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

SEGUNDO. En términos de los artículos 139 de la Ley General de Transparencia y Acceso a la Información Pública y 143 de la Ley Federal de Transparencia y Acceso a la Información Pública, este Comité analiza que la declaración de inexistencia contenga los elementos mínimos que permitan al solicitante tener la certeza de que se utilizó un criterio de búsqueda exhaustivo, además de señalar las circunstancias de tiempo, modo y lugar que generaron la inexistencia en cuestión y señalará al servidor público responsable de contar con la misma.

A este respecto, se analizan enseguida los oficios señalados en el resultando Tercero de la presente resolución, a través de los cuales la Dirección de Apoyo a las Operaciones y la Gerencia de Contabilidad e Información Financiera, en suplencia por ausencia del Director de Contabilidad, Planeación y Presupuesto señalan, entre otras cosas, lo siguiente:

1. Que con objeto de garantizar al solicitante que realizaron las gestiones necesarias para la ubicación de lo requerido por el particular y que estas las llevaron a cabo de conformidad con un criterio exhaustivo y que fueron adecuadas para atender la particularidad del caso concreto, la Unidad de Transparencia les turnó la citada solicitud en razón de sus atribuciones previstas en el Reglamento Interior del Banco de México.

2. Que realizaron la revisión de sus archivos y, en su caso, de manera específica cada unidad administrativa argumentó diversas consideraciones en sus colaboraciones a la solicitud

que nos ocupa, sin haberse encontrado en sus archivos: ***"... registros ... relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el "DECRETO" que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D.F., a favor del Departamento del Distrito Federal...", publicado en el Diario Oficial de la Federación el 4 de febrero de 1972.***

3. Que en cuanto a **las circunstancias de tiempo, modo y lugar,** las unidades administrativas de este Banco Central señalaron en sus respectivos oficios las razones por las cuales determinaron la inexistencia de información.

4. **Que en relación con el servidor público responsable de contar con la misma,** no existe registro alguno dentro de los archivos documentales de dichas unidades administrativas relacionado con la información cuya inexistencia se ha declarado, por lo que **no se puede determinar si algún servidor público pudo haber sido responsable de contar con ella.**

5. Todo lo anterior, en términos de lo que detalla cada una de las unidades administrativas que declararon la inexistencia a través de su respectivo oficio y acta circunstanciada adjunta.

Este órgano colegiado estima que concurren los elementos necesarios para acreditar la inexistencia de lo requerido por el particular en su solicitud, en atención a lo señalado en los oficios presentados por las unidades administrativas mencionadas en el resultando Tercero.

Por lo anterior, y de conformidad con los artículos 44, fracción II, 138, fracción II, y 139, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, 141, fracción II, y 143, de la Ley Federal de Transparencia y Acceso a la Información Pública; 4o., párrafo primero, 8o., párrafos primero, segundo y tercero, 10, párrafo primero, y 31, fracción II, del Reglamento Interior del Banco de México, este Comité de Transparencia **confirma la declaración de inexistencia realizada por** la la Dirección de Apoyo a las Operaciones y la Gerencia de Contabilidad e Información Financiera, en suplencia por ausencia del Director de Contabilidad, Planeación y Presupuesto, respecto de:***"... registros ... relativos a algún depósito a nombre del ejido de "TEPEPAN" o relacionado con el "DECRETO" que expropia por causa de utilidad pública una superficie de 28-44-12 hectáreas del ejido Tepepan, Delegación de Xochimilco, D.F., a favor del Departamento del Distrito Federal...", publicado en el Diario Oficial de la Federación el 4 de febrero de 1972***, al que se hace referencia en la solicitud **CTC-BM-24006.**

Por lo expuesto, con fundamento en los artículos 1, 23, 43 y 44, fracción II, y 139 de la Ley General de Transparencia y Acceso a la Información Pública; 64, párrafos primero, segundo, tercero y quinto y 65, en su fracciones II y IX, y 143, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracciones III y XX, del Reglamento Interior del Banco de México; así como Quinta, de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

ÚNICO. Se **confirma la declaración de inexistencia** de la información a la que se refieren los oficios señalados en el resultando Tercero de la presente resolución, en relación con la información requerida en la solicitud con folio **CTC-BM-24006**, en términos de lo expuesto en la presente resolución.

Así lo resolvió, por unanimidad de los integrantes presentes de este Comité de Transparencia del Banco de México, en sesión celebrada el veintiocho de junio de dos mil diecisiete. ----------

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "I"

BANCO DE MÉXICO

Ciudad de México, a 22 de junio de 2018

Ref. D50/1158-2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio 6110000028418 que nos turnó la Unidad de Transparencia el veintidós de mayo del presente año, a través del sistema electrónico de atención de solicitudes en el marco de la Ley General de Transparencia y Acceso a la Información Pública, la cual se transcribe a continuación:

> *"Solicito las fechas de comunicación y documentos que se emitieron para avisar a cada uno participantes del SPEI que migraran a una plataforma alterna por un riesgo de ciberataque durante este año."*

Al respecto, me permito informarle que la Dirección de Sistemas de Pagos, de conformidad con los artículos 100, 106, fracción I, 108 último párrafo, de la Ley General de Transparencia y Acceso a la Información Pública; 97, 98, fracción I, y 105 último párrafo, de la Ley Federal de Transparencia y Acceso a la Información Pública; ha determinado clasificar la información contenida en los documentos que se indican más adelante.

En consecuencia, esta área ha generado la correspondiente prueba de daño respecto de los documentos clasificados, la cual establece los motivos y fundamentos considerados para realizar la clasificación. Dichos documentos se encuentran disponibles a partir de esta fecha en la carpeta compartida ubicada en la red interna del Banco de México, a la que se puede acceder a través de la siguiente liga:

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

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título del documento clasificado y la liga respectiva al repositorio institucional en el que reside la versión digitalizada de dicho documento original. Es importante señalar que, por tratarse de información altamente sensible, dichas ligas son de acceso restringido; no obstante lo anterior, dichos documentos se pondrán a disposición de los miembros del Comité de Transparencia, en caso de que lo requieran.

BANCO de MÉXICO
RECIBIDO
22 JUN 2018
Comité de Transparencia
Por: [illegible] Hora: 11:20

Recibo este oficio con dos páginas y una Prueba de daño

BANCO DE MÉXICO

TÍTULO DEL DOCUMENTO CLASIFICADO	PRUEBA DE DAÑO	DIRECCIÓN URL AL ADMINISTRADOR INSTITUCIONAL DE DOCUMENTOS DE ARCHIVO (AIDA)
Comunicado a las instituciones (26 de abril)	**Anexo único**	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Sistemas%20de%20pagos/Operaci%C3%B3n/Sistemas%20de%20Pago/SPEI/Contingencia/Comunicados
Comunicado a las instituciones (30 de abril)	**Anexo único**	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Sistemas%20de%20pagos/Operaci%C3%B3n/Sistemas%20de%20Pago/SPEI/Contingencia/Comunicados
Comunicado a las instituciones (10 de mayo)	**Anexo único**	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Sistemas%20de%20pagos/Operaci%C3%B3n/Sistemas%20de%20Pago/SPEI/Contingencia/Comunicados
Comunicado a las instituciones (8 de mayo)	**Anexo único**	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Sistemas%20de%20pagos/Operaci%C3%B3n/Sistemas%20de%20Pago/SPEI/Contingencia/Comunicados
Comunicado a las instituciones (7 de mayo)	**Anexo único**	http://archivo/sitio/atac/DocumentosBM/DGSPSC/Sistemas%20de%20pagos/Operaci%C3%B3n/Sistemas%20de%20Pago/SPEI/Contingencia/Comunicados

Por lo expuesto, en términos de los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México; atentamente solicito a ese Comité de Transparencia confirmar la clasificación total de la información realizada por esta unidad administrativa, indicada en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso a los referidos documentos clasificados, es el adscrito a la Dirección de Sistemas de Pagos (Director), la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos (Gerente) y la Subgerencia de Continuidad de la Operación de Sistemas de Pagos (Subgerente).

Atentamente,

Mtro. Ángel Melesio Fuentes
Gerente de Operación y Continuidad de Negocio de los Sistemas de Pagos
Con fundamento en el Artículo 66 del Reglamento Interior del Banco de México

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información relacionada con las comunicaciones dirigidas a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) en caso de Contingencia

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

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

- Ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país;

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

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

En este sentido, la ***Información relacionada con las comunicaciones dirigidas a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) en caso de Contingencia*** contenida en los documentos que amparan la presente prueba de daño, es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público ya que pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; menoscabaría la efectividad de las medidas implementadas en los sistemas financiero o económico del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto; comprometería las acciones encaminadas a proveer el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos; y generaría incumplimiento en las obligaciones de un participante en un sistema de pagos que dé lugar a que otros participantes incumplan, a su vez, con sus respectivas obligaciones que pueda afectar seriamente al sistema financiero, toda vez que dicho riesgo es:

1. **Real**, en razón de **revelar o divulgar la *Información*** *relacionada con las comunicaciones dirigidas a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) en caso de Contingencia* **facilita a una persona o grupo de personas con intenciones**

delincuenciales identificar aspectos de seguridad informática, especificaciones técnicas en materia de seguridad, procesos de continuidad operativa y, en general, información relacionada con la infraestructura informática de los sistemas de pago administrados por este Instituto Central, lo cual posibilita la realización de acciones hostiles en contra de las tecnologías de la información de este Banco Central, así como de las infraestructuras que administra, opera y supervisa este Banco Central, lo cual, podría menoscabar la efectividad de las infraestructuras a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero y económico, del país, arriesgando el funcionamiento de esos sistemas y, en consecuencia, de la economía nacional en su conjunto.

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 al SPEI, 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.

Por lo anterior, exponer a los participantes de las infraestructuras de los mercados financieros así como al Banco Central que las administra, opera y supervisa, a estos riesgos cibernéticos **puede 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-.**

Incluso, los ataques cibernéticos pueden provocar la alteración de las órdenes de transferencia entre las cuentas bancarias de los participantes o la disrupción de los servicios de estos sistemas, lo cual pondría en riesgo el funcionamiento del sistema financiero y de la economía nacional en su conjunto, dañaría el buen funcionamiento de las infraestructuras de los mercados financieros, entre ellas los sistemas de pagos.

En efecto, proporcionar la información materia de la presente prueba de daño, **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 dichas tecnologías.

Asimismo, 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 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, seguridad informática, especificaciones técnicas en materia de seguridad, procesos de continuidad operativa y, en general, información relacionada con los sistemas correspondientes e infraestructura informática.

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

En el caso en concreto, la información materia de esta prueba de daño contiene información relacionada con especificaciones técnicas en materia de seguridad, procesos de continuidad operativa, información sobre los componentes de los sistemas informáticos así como especificaciones de equipos de cómputo y telecomunicaciones, entre otros, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los puntos débiles de las infraestructuras de los mercados financieros, entre ellas, los sistemas de pagos, y en consecuencia llevar a cabo ataques informáticos más certeros con la finalidad de causar daños o disrupción de servicios, obtener información, o realizar operaciones ilícitas como fraudes a través de infraestructuras.

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.[2] 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.[3] 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.[4] Asimismo, los sistemas de empresas como Google, Facebook, PayPal y el New York Times se han visto comprometidos por ataques cibernéticos.[5] 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.[6]

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

---

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

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

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

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

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

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

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

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;[9]

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;[10]

d) 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;[11]

e) 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;[12]

f) 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

---

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

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

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

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

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

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

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;[13]

g) 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;[14]

h) 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.[15]

i) 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 estima un daño a los participantes del SPEI de aproximadamente 300 millones de pesos.[17]

Ahora bien, 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 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.[18]

---

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

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

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

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 14 de junio de 2018.

17 Acorde con los "Puntos importantes sobre la situación actual del SPEI" publicados en la página de internet del Banco de México consultados el 13 de junio de 2018. http://www.banxico.org.mx/inicio/banner/informacion-importante-sobre-la-situacion-del-spei/%7B022CD9D7-11A9-68E6-D1A5-965F57A23F60%7D.pdf

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

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,**[19] 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.

En este sentido, la divulgación de la información materia de la presente prueba de daño, potencializaría que hechos como los mencionados ocurran en las infraestructuras de los mercados financieros, entre ellas, las que administra y opera el Banco de México, puesto que de divulgarse la información requerida por el solicitante, los cibercriminales contarían con los elementos necesarios para perpetrar un ataque informático directo a este Instituto Central. Lo anterior, 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,** ya 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.

   En ese sentido, **un ataque informático derivado de proporcionar la Información relacionada con las comunicaciones dirigidas a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) en caso de Contingencia, podría resultar en la afectación de las órdenes de transferencia en las cuentas bancarias de los distintos participantes y de los usuarios del sistema en comento**. A su vez, estas afectaciones en las órdenes de transferencia podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país y demás participantes de los sistemas de pagos, sino en perjuicio de la población usuaria de los pagos electrónicos interbancarios, es decir **millones de personas físicas y morales, incluyendo aquellos empleados del sector público o privado que reciben su pago de salario vía transferencia electrónica que realizan sus patrones.**

---

[19] Ver por ejemplo las 10 medidas básicas de ciberseguridad de la Security Information Center, en particular la relacionada con "Implementar un programa de capacitación en seguridad cibernética para empleados" en donde recomiendan sensibilizar sobre los temas de ingeniería social que buscan obtener información mediante diversos canales de comunicación solicitando información sensible.
https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf consultado el 13 de junio de 2018.

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

Por lo anterior, un ataque perpetrado directamente al SPEI o a sus participantes, ocasionado por dar a conocer la ***Información relacionada con las comunicaciones dirigidas a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) en caso de Contingencia,*** representa un perjuicio significativo para **el sistema financiero del país y para la población usuaria de los servicios de transferencias electrónicas interbancarias**, pues de acuerdo con la información del Banco de México, de marzo de 2017 a marzo de 2018, se realizaron aproximadamente 544 millones de pagos electrónicos interbancarios por un monto de 293 billones de pesos; lo anterior equivale a más de 62 mil operaciones por un monto de 33 mil millones de pesos por hora, únicamente para lo que respecta al SPEI.[20]

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

En relación con lo anterior, es importante señalar que México ocupa el tercer lugar mundial en crímenes cibernéticos, después de China y Sudáfrica[21] y que tan sólo en México, el costo causado por el *cibercrimen* ascendió a $5,500 millones de dólares y afectó alrededor de 22.4 millones de personas; mientras que a nivel mundial, el costo ascendió a $125,900 millones de dólares y afectó

---

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

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

a 689.4 millones de personas.[22] Por lo anterior, este Instituto Central[23] y autoridades como la Secretaría de Hacienda y Crédito Público[24] 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 materia de esta prueba de daño, supera el interés público general de que se difunda**, pues el interés público se centra en que no se comprometa la efectividad en las medidas implementadas en los sistemas financiero y económico, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto, la estabilidad en los mercados financieros y en los sistemas de pagos. Por lo que, la *Información relacionada con las auditorías internas realizadas al Sistema de Pagos Electrónicos Interbancarios (SPEI)*, no satisface un interés público, por el contrario, es información que pone en riesgo el buen funcionamiento de los sistemas de pagos y de la economía nacional en su conjunto. Asimismo al realizar una interpretación sobre la alternativa que más satisface dicho interés, se puede concluir que debe prevalecer el derecho más favorable a las personas, esto es, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste, en particular el SPEI, el cual es la infraestructura de los mercados financieros más importante del país.

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

Por otra parte, la limitación se adecua al principio de proporcionalidad, toda vez que debe prevalecer el interés que más beneficie a la colectividad, y como se ha dicho, proteger la ***Información relacionada con las comunicaciones dirigidas a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) en caso de Contingencia*** evitará poner en riesgo el buen funcionamiento de los sistemas de pagos, del sistema financiero y de la economía nacional en su conjunto.

---

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

23 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

24 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.

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar el buen funcionamiento de los sistemas de pagos, así como la estabilidad del sistema financiero, **puesto que el propio legislador determinó que el medio menos restrictivo es la clasificación de la información cuando actualice las causales prevista en la Ley**, tal y como se demostró en el presente caso.

En razón de lo anterior, y vistas las consideraciones expuestas en el presente documento, con fundamento en lo establecido en los artículos 6o., apartado A, fracciones I y VIII, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 100, 103, segundo párrafo, 104, 105, 106, fracción III, 107, 108, último párrafo, 109, 113, fracciones IV, y 114 de la LGTAIP; 110, fracciones IV, y 111 de la LFTAIP, 1o., 2o. y 3o., fracción I, de la Ley del Banco de México; 4o., párrafo primero, 8o., párrafos primero, y tercero, 10, párrafo primero, 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, Cuarto, Sexto, párrafo segundo, Séptimo, fracción I, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I, II y IV, de los Lineamientos, se clasifica como reservada, la ***Información relacionada con las comunicaciones dirigidas a los Participantes del Sistema de Pagos Electrónicos Interbancarios (SPEI) en caso de Contingencia por el plazo de 5 años a partir de la fecha de clasificación,*** toda vez que, como se ha manifestado esta acción atiende a la protección de las medidas de seguridad informática, con la finalidad de evitar intrusiones que puedan inhabilitar los sistemas de tecnologías de la información y comunicaciones, por lo que, en caso de revelarse, permitiría el desarrollo de estrategias para la realización de ataques informáticos, no solo de las vulnerabilidades identificadas sino de aquellas que no se encuentran reconocidas provocando afectaciones a las infraestructuras de los mercados financieros que opera y administra este Instituto Central, entre ellas los sistemas de pagos, menoscabaría la efectividad de las medidas implementadas en relación con las políticas en materia del sistema financiero del país, y ponga en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, así como comprometería las acciones encaminadas a propiciar el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

BANCO DE MÉXICO

REFERENCIA 1

United States Government Accountability Office

GAO

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

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

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO

Accountability * Integrity * Reliability

GAO-10-230T

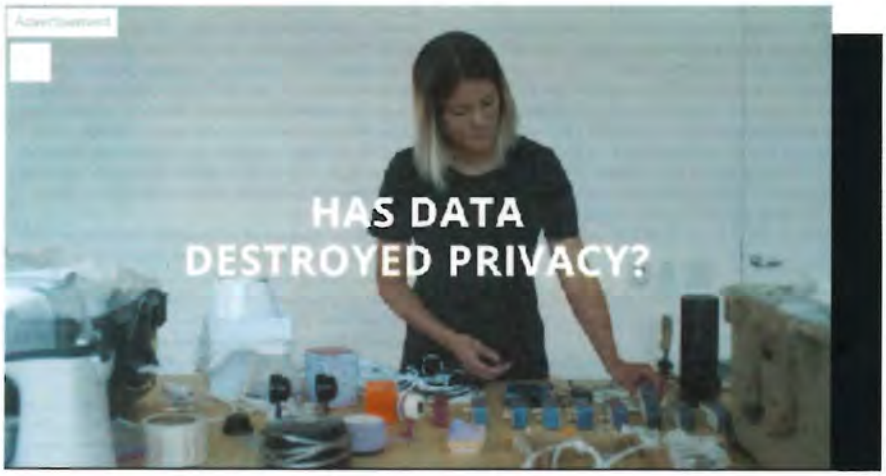
REFERENCIA 2

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.

REFERENCIA 3

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.

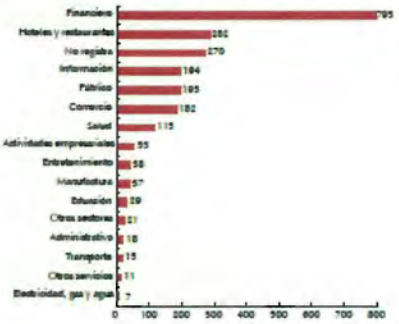
La forma más común como se ha materializado el riesgo cibernético en años recientes ha sido mediante lo que se conoce como ataques cibernéticos. En esencia, estos son acciones ilegales realizadas por *hackers*, con el objetivo principal de obtener cierto beneficio, al generar daños en los sistemas tecnológicos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

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



Fuente: Verizon (2016).

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

REFERENCIA 4

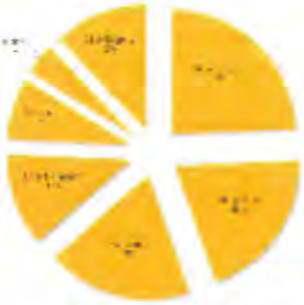
18 May, 2017

banking technology

tec reveals more hack attempts on Swift network

banking techno; 2016 Written by Antony Peyton

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



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

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

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

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

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

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

It's not just Swift

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

BANCO DE MÉXICO

REFERENCIA 5

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

The Economic Impact of Cyber-Attacks

April 1, 2004

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

REFERENCIA 7

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:

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.

BANCO DE MÉXICO

REFERENCIA 9

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

Article World Neurosurgery · June 2017

REFERENCIA 10

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 •

Imagen: Bjorn 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.

BANCO DE MÉXICO

REFERENCIA 11

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

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

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

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

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

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

Teléfono de Comunicación Social: 15551024

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

REFERENCIA 12

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

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 7, 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.arkseid.com to enroll in the free protection services being offered.**

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

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

› Click to enlarge

FREQUENTLY ASKED QUESTIONS

1. **How did [24]7.ai's cyber incident occur?**
   - [24]7.ai is a company that provides online chat services for many companies, including Delta.
   - We understand malware present in [24]7.ai's software between Sept. 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 5 at noon ET, which we will be updating regularly to address customer questions and concerns.
   - Delta will be working diligently to directly contact customers, including by first-class postal mail, who may have been impacted by the [24]7.ai cyber incident.

BANCO DE MÉXICO

REFERENCIA 16

BANCO DE MÉXICO

REFERENCIA 17

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.**

REFERENCIA 18

Social Engineering Fundamentals, Part I: Hacker Tactics

Sarah Granger 2001-12-18

Social Engineering Fundamentals, Part I: Hacker Tactics

by Sarah Granger
last updated December 18, 2001

A True Story

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

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

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

Definitions

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

BANCO DE MÉXICO

REFERENCIA 19

WaterISAC
Security Information Center

10 Basic Cybersecurity Measures

Best Practices to Reduce Exploitable Weaknesses and Attacks

June 2015

Developed in partnership with the U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the FBI, and the Information Technology ISAC. WaterISAC also acknowledges the Multi-State ISAC for its contributions to this document.

BANCO DE MÉXICO

REFERENCIA 20

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real.

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

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

REFERENCIA 21

Javier Arreola (https://www.forbes.com.mx/author/javier-arreola/)
Mayo 23rd, 2016 @ 12:29 pm

Ciberseguridad (casi) a prueba del enemigo 'invisible'

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

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

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/gene motors-se-despide-sudafrica/)
MAYO 18, 2017

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

REFERENCIA 22

Informe Norton sobre Ciberseguridad 2016

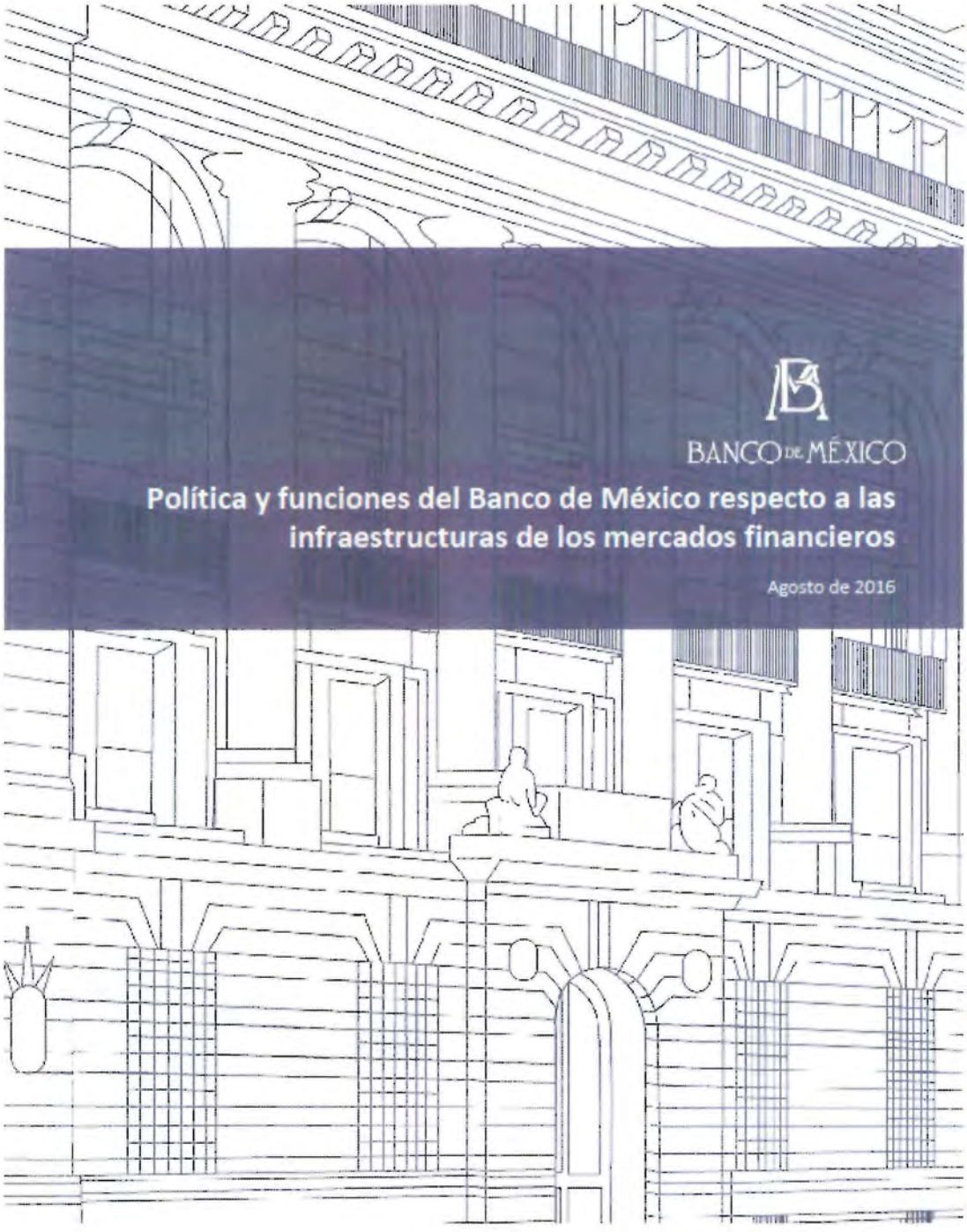
Comparaciones Globales

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

REFERENCIA 23



(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

Contesta nuestra encuesta de satisfacción

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

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

ANEXO "J"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000028418

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

RESULTANDO

PRIMERO. El veintidós de mayo de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000028418,** la cual se transcribe a continuación:

> *"Solicito las fechas de comunicación y documentos que se emitieron para avisar a cada uno participantes del SPEI que migraran a una plataforma alterna por un riesgo de ciberataque durante este año."*

SEGUNDO. Que la solicitud de información mencionada en el resultando anterior, fue turnada para su atención el mismo veintidós de mayo del presente año, a la Dirección de Sistemas de Pagos del Banco de México, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que el titular de la Dirección de Sistemas de Pagos del Banco de México, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la referida solicitud de acceso a la información.

CUARTO. Que este órgano colegiado, mediante resolución de catorce de junio del presente año, confirmó la ampliación del plazo ordinario de respuesta por diez días, para la atención de la solicitud al rubro citada. Dicha resolución, fue notificada al solicitante dentro del plazo ordinario.

QUINTO. Que el titular de la Gerencia de Operación y Continuidad de Negocio de los Sistemas de Pagos del Banco de México, mediante oficio con referencia D50/1158-2018, hizo del conocimiento de este Comité de Transparencia que dicha unidad administrativa determinó clasificar la información que señala en el mismo oficio, y solicitó a este órgano colegiado confirmar dicha clasificación como reservada, en términos de la fundamentación y motivación señalados en la prueba de daño referida en dicho oficio.

CONSIDERANDOS

PRIMERO. Este Comité de Transparencia es competente para confirmar, modificar o revocar las determinaciones que en materia de ampliación del plazo de respuesta, clasificación de la información y declaración de inexistencia o de incompetencia realicen los titulares de las áreas del

Banco de México, de conformidad con lo previsto en los artículos 44, fracción II, de la Ley General de Transparencia y Acceso a la Información Pública; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública; y 31, fracción III, del Reglamento Interior del Banco de México.

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa señalada en el resultando Quinto de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que los datos clasificados que se señalan en el oficio referido en el resultando Quinto de la presente, se tratan de información reservada, y es procedente dicha clasificación conforme a la fundamentación y motivación expresados en la correspondiente prueba de daño, la cual se tiene aquí por reproducida a la letra, en obvio de repeticiones innecesarias.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresada en la correspondiente prueba de daño, adjunta en el oficio precisado en el resultando Quinto de la presente determinación.**

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

RESUELVE

ÚNICO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresados en la correspondiente prueba de daño, referida en el oficio precisado en el resultando Quinto de la presente determinación.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "K"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
21 JUN 2018
Comité de Transparencia
Por: JIS36 Hora: 17:30

Recibí un oficio constante en tres páginas y una prueba de daño.

Ciudad de México, a 21 de junio de 2018

REF: DGTI-90/2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio 6110000027118, que nos turnó la Unidad de Transparencia el 21 de mayo 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:

> *"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. Ordenado por Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado. a. Una relación de todos los puertos de red abiertos. b. Nombre y versión, del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall (en ingles). c. Si se encuentra habilitada la conexión de red IPv6 (Protocolo de Internet versión 6)".*

Sobre el particular, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, sexto y séptimo párrafos, de la Constitución Política de los Estados Unidos Mexicanos; 103, 104, 105, 106, fracción I, 108, último párrafo, y 113, Fracciones I y IV de la Ley General de Transparencia y Acceso a la Información Pública; 97, segundo, tercero y sexto párrafos, 98, fracción I, y 110, fracciones I y IV de la Ley Federal de Transparencia y Acceso a la Información Pública; 2º y 3º, fracción I, de la Ley del Banco de México; 4, 8, primero y segundo párrafos, 10, 15 Bis 1, 18 Bis, 29 del Reglamento Interior del Banco de México, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como el Cuarto, párrafo primero, Séptimo, fracción I, y último párrafo, Octavo, párrafos primero al tercero, Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Trigésimo tercero, y Trigésimo cuarto, primer y segundo párrafos, de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, nos permitimos informarles que **esta unidad administrativa clasifica como reservada la siguiente información:**

- Los números de serie de cada uno de los equipos de cómputo, routers y puntos de acceso inalámbricos.
- Todos los puertos de red abiertos.
- La respuesta a la pregunta respecto a si se encuentra habilitada la conexión de red IPv6 (Protocolo de Internet versión 6).
- Nombre y versión del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall.

Lo anterior en virtud de que esta información corresponde a especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México, lo cual se fundamenta y motiva en la prueba de daño que se anexa.

Considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años, esta información deberá ser reservada, al menos, por cinco años.

Por lo expuesto, solicito atentamente a este Comité de Transparencia confirmar la 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 quito de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigentes.

Asimismo, de conformidad con el Décimo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, informamos que el personal que, por la naturaleza de sus atribuciones, tiene acceso a la información clasificada es el siguiente:

Información clasificada	Personal de la DGTI con acceso a la información clasificada
Los números de serie de cada uno de los equipos de cómputo.	Funcionarios de la Dirección de Sistemas Gerencia de Cómputo (Todo el personal) Subgerencia de Planeación y Regulación (Todo el personal)
Los números de serie de cada uno de los routers y puntos de acceso inalámbricos.	Gerencia de Telecomunicaciones (Gerente) Subgerencia de Operación de Servicios de Telecomunicaciones (Todo el personal) Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente) Oficina de Soporte a la Gestión Presupuestal (Todo el personal). Subgerencia de Planeación y Regulación (Todo el personal)
• Todos los puertos de red abiertos. • La respuesta a la pregunta respecto a si se encuentra habilitada la conexión de red IPv6 (Protocolo de Internet versión 6). • Nombre y versión del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall.	Gerencia de Telecomunicaciones (Gerente) Subgerencia de Operación de Servicios de Telecomunicaciones (Todo el personal) Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente) Oficina de Soporte a la Gestión Presupuestal (Todo el personal).

Atentamente.

ING. OCTAVIO BERGÉS BASTIDA
Director General de Tecnologías de la Información

PRUEBA DE DAÑO

Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México.

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

a) Comprometer la seguridad nacional;

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

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

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

Por lo que, la información relativa a las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones** referente a la arquitectura de los componentes, que conforman la infraestructura, es decir, la organización y relación entre los equipos de cómputo, de telecomunicaciones y de seguridad electrónica, sus configuraciones, las actualizaciones de seguridad de estos componentes; la ubicación en donde se emplean estos componentes en las instalaciones del Banco de México, incluyendo los centros de datos y telecomunicaciones; los análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes; los manuales y procedimientos de operación de recuperación y de continuidad operativa para restablecer su funcionamiento; el diseño, el código fuente y los algoritmos que se desarrollan o se configuran para operar en ellos; así como toda información derivada de estas especificaciones que, de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con los procesos del Banco de México en que éste participa; es clasificada como reservada.

Cabe aclarar que como parte de las **especificaciones de la infraestructura de comunicaciones** se incluye lo siguiente:

- Los números de serie de cada uno de los equipos de cómputo, ruteadores (routers) y puntos de acceso inalámbricos, así como las unidades administrativas, conforme al organigrama institucional, que hacen uso de cada uno de estos equipos.

- Información sobre las contraseñas para acceder a la configuración y administración de los ruteadores (routers) y puntos de acceso inalámbrico.
- Información que identifique la configuración o el estado de los puertos de red (identificador de los servicios a los cuales se dirige un paquete de datos determinado) del Banco de México.
- Información relacionada con los protocolos de Internet utilizados.
- Nombre y versiones de los programas utilizados para administrar los cortafuegos (firewall) de red.
- Información sobre las tecnologías de red inalámbrica utilizadas y sus mecanismos de seguridad.

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, toda vez que dicho riesgo es:

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

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

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

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

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

Asimismo, el artículo décimo séptimo, fracción VIII, señala que se considera considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

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

En efecto, proporcionar las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, indudablemente facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco.

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

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se

fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

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

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

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

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

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

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de la **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**.

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

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, 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.[1] Como ésta existen numerosas herramientas que, si bien su propósito original es realizar pruebas a las infraestructuras de tecnologías de la información y comunicaciones para corregir errores en sus configuraciones e identificar posibles vulnerabilidades, en malas manos permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier sistema de cómputo fabricado en los últimos años. Estas son conocidas como "Meltdown" y "Spectre" y permiten ataques denominados "side-channel", en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando "Meltdown", un atacante puede utilizar un

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

programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. "Spectre" requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS[2].

- Un ataque a la plataforma de pagos internacionales del Banco Nacional de Comercio Exterior (Bancomext) que obligó a la institución a suspender sus operaciones de manera preventiva[3].
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.[4]
- De acuerdo a Reuters, el Director del Programa de Seguridad del Clientes de SWIFT, Stephen Gilderdale, dijo que los hackers continúan apuntando al sistema de mensajería bancaria de SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos[5]
- Dos ataques realizados contra la infraestructura crítica que provee energía eléctrica en la capital de Ucrania en diciembre de 2015, y diciembre de 2016, dejando sin electricidad a 225,000 personas[6].
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.[7]
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que

---

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

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

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

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

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

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

ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)" [8]. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.

- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.[9]
- Además de los ataques tradicionales y comunes de usurpación de direcciones MAC, el posible rastreo de equipos móviles empleando esta dirección, hace que no solo se pueda identificar cuando estos equipos se conectan a redes Wi-Fi, sino que además se pudiera estar siguiendo a la persona que lo usa[10], ocurriendo lo mismo con solo proporcionar el número telefónico de un celular, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto[11].
- Respecto a la adopción del protocolo para la comunicación en Internet "IPv6", el cual permite la comunicación entre los diferentes elementos de la red y nuestra propia computadora o dispositivo móvil, existen indicios de que los agentes malintencionados han comenzado las pruebas y la investigación de "IPv6" basados en métodos de ataque DDoS[12] (Denial of service – Denegación de servicio), el cual provoca que un servicio o recurso en una red de computadoras sea inaccesible a usuarios legítimos .
- El conocer el nombre y la versión del programa que administra los cortafuegos o "firewalls" (dispositivos para bloquear los accesos no autorizados a una red de computadoras, permitiendo al mismo tiempo comunicaciones autorizadas), puede llevar a conocer las vulnerabilidades de estos dispositivos, las cuales inclusive se llegan a publicar en páginas de Internet[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? (cuyas especificaciones de fabricación, y por consiguiente posibles vulnerabilidades se pueden obtener indirectamente a través de sus números de serie accediendo a la información que los fabricantes tengan de cada uno de estos dispositivos, teniendo como ejemplo la operación llamada "Equation Group")[15], ¿qué puertos de comunicaciones usan? (Si se encuentran abiertos o inactivos), ¿qué

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

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

[10] http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/, consultada el 4 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "J"**.

[11] http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338. Se adjunta una impresión del artículo como **ANEXO "K"**

[12] https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2312, se adjunta una impresión del artículo como **ANEXO "L"**

[13] https://www.lomasnuevo.net/noticias/detectan-vulnerabilidad-en-firewalls-fortinet/. Se adjunta una impresión del artículo como **ANEXO "M"**

[14] https://www.offensive-security.com/metasploit-unleashed/information-gathering. Se adjunta una impresión del artículo como **ANEXO "N"**.

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

servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Por otro lado, el uso de la tecnología "WiFi", que permite la interconexión inalámbrica de dispositivos electrónicos (computadoras, teléfonos, etc), ya sea entre ellos o hacia Internet, puede implicar riesgos importantes, ya que sin los adecuados mecanismos de seguridad, terceros pueden acceder a estas redes sin autorización, con la posibilidad de acceder y controlar los dispositivos "WiFi", tales como los ruteadores (o "routers" en inglés) encargados de encaminar los datos trasmitidos entre diferentes redes o subconjuntos de dispositivos, con tan solo conocer su identificador en la red. Por otro lado, el acceso no autorizado a un dispositivo "WiFi" permite supervisar y registrar toda la información que se trasmite a través de éste.

Dentro del uso de redes inalámbricas, el estándar "WPS" (WiFi Protected Setup) define diversos mecanismos para configurar una red local inalámbrica apoyados en el sistema de seguridad conocido como "WPA2" (WiFi Protected Access 2 – Acceso Protegido WiFi 2). El conocer los mecanismos de protección utilizados también permitiría a un atacante identificar las vulnerabilidades asociadas a éstos.[16].

A partir de lo mencionado anteriormente, el dar a conocer la unidad, área u órgano del Banco de México que hace uso de cada uno de ruteadores y puntos de acceso inalámbricos, facilitaría direccionar a algún área funcional que sea del interés del atacante cibernético materializar los riesgos recién señalados.

En resumen, de la misma manera que el resto de las especificaciones de tecnologías de la información y telecomunicaciones, el conocimiento de las tecnologías utilizadas para la comunicación inalámbrica y sus mecanismos de seguridad y cifrado tales como el estándar WPS, y por obvias razones, el uso de contraseñas para acceder a los dispositivos WiFi, tales como los ruteadores y puntos de acceso inalámbricos, así como las unidades administrativas que hacen uso de esta tecnología, permitiría a un atacante identificar y aprovechar vulnerabilidades asociadas a ellas.

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.

[16] https://www.krackattacks.com/. Se adjunta una impresión del artículo como **ANEXO "P"**

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

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados "hacktivistas", como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: "Anonymous attack Greek central bank, warns others"[17]. El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo "Anonymous", conocida como "OpIcarus" y que desde 2016 ha presentado actividad; siendo la más reciente la denominada "OpSacred" o "OpIcarus – Phase 5", que tuvo lugar en Junio de 2017, y cuyos objetivos nuevamente fueron los sitios públicos de bancos centrales alrededor del mundo[18].

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2017, se realizaron más de 480 millones de operaciones por un monto mayor a 270 billones de pesos[19]; lo que equivale a más de 54 mil operaciones por un monto de 30 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

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

---

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

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

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

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

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

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

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

Las consecuencias de que tenga éxito un ataque a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendrían 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, **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

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

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

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

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular del interés que pudiera existir en el dar a conocer dicha información.

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

Además de que su divulgación posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional y, en consecuencia menoscaba la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto. Asimismo comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

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

ANEXO "A"

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
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.

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

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]

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 Cyber 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 libero 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[2]

Cargas útiles [editar]

Metasploit ofrece muchos tipos de cargas útiles, incluyendo:

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

Lista de los desarrolladores originales:

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

Referencias [editar]

1. ↑ «Rapid7 Prensa». *Rapid7*. Consultado el 18 de febrero de 2015.
2. ↑ [http://www.metasploit.com/download «Herramienta de Pruebas de Penetración Metasploit, gratuito Descargar - Rapid7»].
3. ↑ [a b] Plantilla Cita web
4. ↑ Plantilla Cite noticias

Rapid7. Consultado el esta fecha esta pasada lo le agan caso por favor y gracias por su atencion chauuuu

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

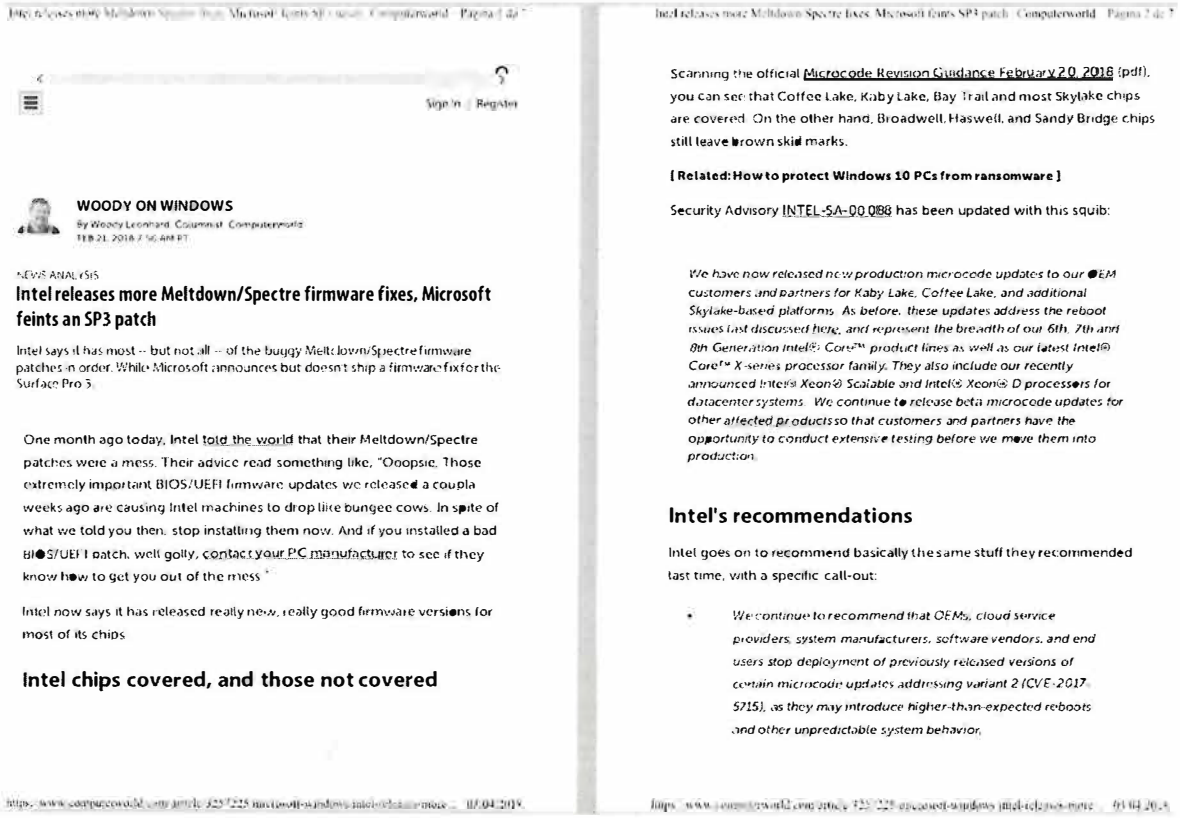
Metasploit - Wikipedia, la enciclopedia libre

Se editó esta página por última vez el 12 nov 2017 a las 05:13.

http://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 21, 2018 7:56 AM PT

NEWS ANALYSIS

Intel releases more Meltdown/Spectre firmware fixes, Microsoft feints an SP3 patch

Intel says it has most -- but not all -- of the buggy Meltdown/Spectre firmware patches in order. While Microsoft announces but doesn't ship a firmware fix for the Surface Pro 3.

One month ago today, Intel told the world that their Meltdown/Spectre patches were a mess. Their advice read something like, "Ooopsie. Those extremely important BIOS/UEFI firmware updates we released a coupla weeks ago are causing Intel machines to drop like bungee cows. In spite of what we told you then, stop installing them now. And if you installed a bad BIOS/UEFI patch, well golly, contact your PC manufacturer to see if they know how to get you out of the mess."

Intel now says it has released really new, really good firmware versions for most of its chips.

Intel chips covered, and those not covered

Scanning the official Microcode Revision Guidance February 20, 2018 (pdf), you can see that Coffee Lake, Kaby Lake, Bay Trail and most Skylake chips are covered. On the other hand, Broadwell, Haswell, and Sandy Bridge chips still leave brown skid marks.

[Related: How to protect Windows 10 PCs from ransomware]

Security Advisory INTEL-SA-00086 has been updated with this squib:

> *We have now released new production microcode updates to our OEM customers and partners for Kaby Lake, Coffee Lake, and additional Skylake-based platforms. As before, these updates address the reboot issues last discussed here, and represent the breadth of our 6th, 7th and 8th Generation Intel® Core™ product lines as well as our latest Intel® Core™ X-series processor family. They also include our recently announced Intel® Xeon® Scalable and Intel® Xeon® D processors for datacenter systems. We continue to release beta microcode updates for other affected products so that customers and partners have the opportunity to conduct extensive testing before we move them into production.*

Intel's recommendations

Intel goes on to recommend basically the same stuff they recommended last time, with a specific call-out:

- *We continue to recommend that OEMs, cloud service providers, system manufacturers, software vendors, and end users stop deployment of previously released versions of certain microcode updates addressing variant 2 (CVE-2017-5715), as they may introduce higher-than-expected reboots and other unpredictable system behavior.*

- *We also continue to ask that our industry partners focus efforts on evaluating the beta microcode updates.*
- *For those concerned about system stability while we finalize these updated solutions, earlier this week we advised that we were working with our OEM partners to provide BIOS updates using previous versions of microcode not exhibiting these issues, but that also removed the mitigations for 'Spectre' variant 2 (CVE-2017-5715).*
- *Microsoft also provided two resources for users to disable original microcode updates on platforms exhibiting unpredictable behavior.*
- ***For most users** – An automatic update available via the Microsoft® Update Catalog which disables 'Spectre' variant 2 (CVE-2017-5715) mitigations without a BIOS update. This update supports Windows 7 (SP1), Windows 8.1, and all versions of Windows 10 - client and server.*
- ***For advanced users** – Refer to the following Knowledge Base (KB) articles:*
- *KB4073119: IT Pro Guidance*
- *KB4072698: Server Guidance*
- *Both of these options eliminate the risk of reboot or other unpredictable system behavior associated with the original microcode update and retain mitigations for 'Spectre' variant 1 and 'Meltdown' variant 3 until new microcode can be loaded on the system.*

The "For most users" update is KB 4078130, the surprise Friday evening patch, released on Jan. 26, which I discussed almost a month ago:

> *On Friday night, Microsoft released a strange patch called KB 4078130 that "disables mitigation against Spectre, variant 2." The KB article goes to great lengths describing how Intel's the bad guy and its microcode patches don't work right.*
>
> *There aren't any details, but apparently this patch -- which isn't being sent out the Windows Update chute -- adds two registry settings that "manually disable mitigation against Spectre Variant 2."*

Rummaging through the lengthy Microsoft IT Pro Guidance page, there's an important warning:

[Got a spare hour? Take this online course and learn how to install and configure Windows 10 with the options you need.]

> *Customers who only install the Windows January and February 2018 security updates will not receive the benefit of all known protections against the vulnerabilities. In addition to installing the January and February security updates, a processor microcode, or firmware, update is required. This should be available through your OEM device manufacturer.*

Microsoft firmware update for Surface Pro 3

In what must be an amazing coincidence, last night Microsoft released a firmware update for the Surface Pro 3. It's currently available as a manual download ("MSI format") for Surface Pro 3. I haven't seen it come down the Windows Update chute. Perhaps Microsoft is beta testing it once again. Per Brandon Records on the Surface blog:

> *We've released a new driver and firmware update for Surface Pro 3. This update includes new firmware for Surface UEFI which resolves potential security vulnerabilities, including Microsoft security advisory 180002.*
>
> *This update is available in MSI format from the Surface Pro 3 Drivers and Firmware page at the Microsoft Download Center.*

Except, golly, the latest version of the patch on that page (as of 10 am Eastern US time) is marked "Date Published: 1/24/2018." The official Surface Pro 3 update history page lists the last firmware update for the SP3 as being dated Oct. 27, 2017.

And, golly squared, Microsoft Security Advisory 180002 doesn't even mention the Surface Pro 3. It hasn't been updated since Feb. 13; it links to the *Surface Guidance to protect against speculative execution side-channel vulnerabilities* page, KB 4073065, which doesn't mention the Surface Pro 3 and hasn't been updated since Feb. 2.

You'd have to be incredibly trusting -- of both Microsoft and Intel -- to manually install *any* Surface firmware patch at this point. Particularly when you realize that not one single Meltdown or Spectre-related exploit is in the wild. Not one.

Thx Bogdan Popa Softpedia News

Fretting over Meltdown and Spectre? Assuage your fears on the AskWoody

Lounge.

Woody Leonhard is a columnist at Computerworld and author of dozens of Windows books, including "Windows 10 All-in-One for Dummies."

Follow

5 tips for working with SharePoint Online

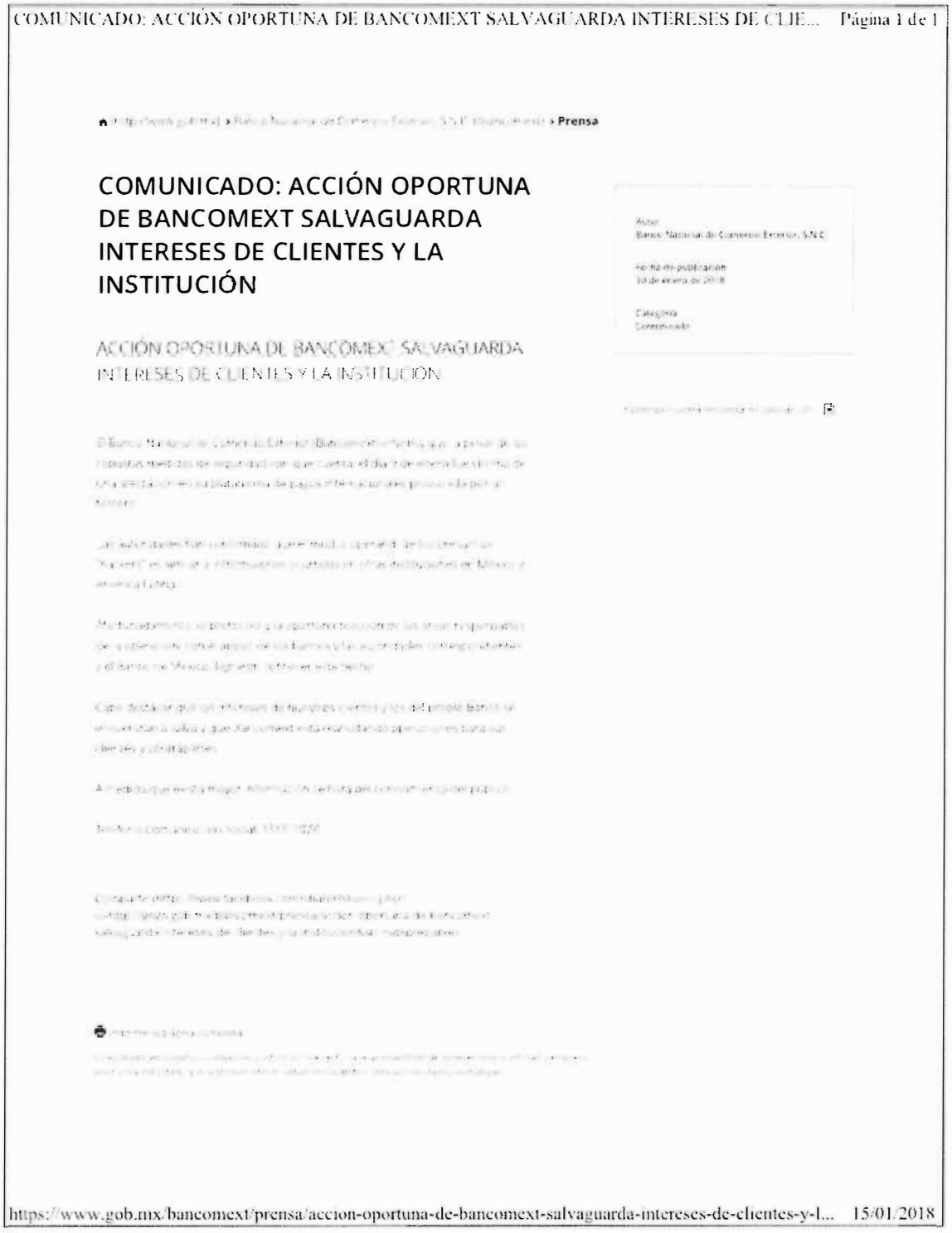
YOU MIGHT LIKE

SHOP TECH PRODUCTS AT AMAZON

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

› Prensa

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

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

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

Log in Sign up Forums Serverless | M³ | OLL | Events | Whitepapers | The Next Platform

Security

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

Arrests after customized malware apparently used to drain millions

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

11 SHARE

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

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

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

https://www.theregister.co.uk/2017/10/11/hackers_swift_taiwan/[22/01/2018 07:03:38 p. m.]

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

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

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

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

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

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

Updated to add

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

Tips and corrections

11 Comments

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

MORE Swift Hacking

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

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.

SWIFT says hackers still targeting bank messaging system

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

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

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

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

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

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

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

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

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

Reporting by Jim Finkle. Editing by Rosalba O'Brien

Our Standards: The Thomson Reuters Trust Principles.

ANEXO "F"

http://www.bbc.com/news/technology-38573074

Consultada el 15 de enero de 2018

Technology

Ukraine power cut 'was cyber-attack'

11 January 2017 Share

UK-NATO military unit has been attacked twice by hackers

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

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

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

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

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

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

Top Stories

Raid on Venezuela pilot ends in bloodshed
4 hours ago

Turkey denounces US 'terror army' plan
5 hours ago

Cranberries singer Dolores O'Riordan dies
1 hour ago

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.

"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
738

1,000 young people charged over sex video
12 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

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

625a8e3de4e9df8dac61f2a4ee39541af4e6e9228	2016-02-05 11:48:20	95,536	evtdiag.exe
78bab478dcc70f979ce82cd306e9ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
70bf16597e375ad891f2c1efa194dbe7f10e4eeb	2016-02-05 08:55:19	24,576	msft_b.exe
6207b82842b28a438330a2bf0ee8dcab7ef0a193	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 625a8e3de4e9df8dac61f2a4ee39541af4e6e228 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 8am on 8th February 2016. This is significant given the transfers are believed to have occurred in the two days prior to this time. The tool was custom made for this job and shows a significant level of knowledge of SWIFT Alliance Access software as well as good malware coding skills.

Malware config and logging

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

```
4e 35 b6 a7 7d 03 cc aa 1a 89 ed ad d9 ed 31 ef
```

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

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

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

```
185.230.103.174
```

The sample also uses the following file for logging:

```
[BOOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\wcaa.dat
```

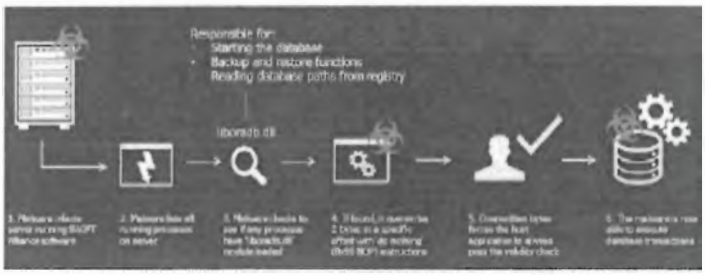
Module patching

The malware enumerates all processes, and if a process has the module `oracle.exe` loaded in it, it will patch 2 bytes in its memory at a specific offset. The patch will replace 2 bytes `0x75` and `0x0a` with the bytes `0x90` and `0xE9`.

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 fooling 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 `libora9.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\msn\in\
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\msn\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

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

```
"FIN 103 Single Customer Credit Transfer"
":32A: Transaction"
"Sender :"
(additional failures from the decrypted configuration file gpse.ini)
```

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 SAACONFP.MESG_FS WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '######%' AND MESG_TRN_REF LIKE '######';
```

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

```
DELETE FROM SAACONFP.MESG_FS WHERE MESG_S_UNID = 'ke';
DELETE FROM SAACONFP.TEXT_FS WHERE TEXT_S_UNID = 'ke';
```

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

```
set heading off;
set linesize 9999;
SET FEEDBACK OFF;
SET ECHO OFF;
SET PAGE OFF;
SET TERMOUT 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 `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
SAACONFP.JRNL_FS WHERE JRNL_DISPLAY_TEXT LIKE '%AIT BBRKBDDH%: Login%'
ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWNUM = 1;
```

NOTE: "BBRKBDDH" is the SWIFT code for the Bangladesh Bank in Dhaka.

If it fails to find the "Login" record, it falls asleep for 6 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_address]/ait[data]
```

The malware notifies the remote C&C each hour of events, sending "----1" if the "Login" (open) event occurred, "----0" in case "Logout" (close) event occurred or "----9" if neither of the events

occurred, e.g.

```
[lod_served] all====
```

Manipulating balances

The malware monitors all SWIFT messages found in

```
[ROOT_DRIVE]:  \Users\Administrator\AppData\Local\Alliance\mop\in\*.*
[ROOT_DRIVE]:  \Users\Administrator\AppData\Local\Alliance\mop\out\*.*
[ROOT_DRIVE]:  \Users\Administrator\AppData\Local\Alliance\mop\unk\*.*
[ROOT_DRIVE]:  \Users\Administrator\AppData\Local\Alliance\mos\mfan
[ROOT_DRIVE]:  \Users\Administrator\AppData\Local\Alliance\mos\mfaf
[ROOT_DRIVE]:  \Users\Administrator\AppData\Local\Alliance\mos\dofp
[ROOT_DRIVE]:  \Users\Administrator\AppData\Local\Alliance\mos\doff
```

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

```
":19A:"Amount"
":  Debit"
"Debit Credit :"
"Sender :"
"Amount :"
"FEDERAL RESERVE BANK"
" D"
" C"
":61F: "
":60F: "
":62M: "
":62M: "
"Credit"
"Debit"
" 64: "
" 20: Transaction"
":32B: Value"
```

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

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

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

```
SELECT MESG_FIN_CCY_AMOUNT FROM BAACONFER.MESG_es WHERE MESG_S_UNID = '**';
```

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

```
SELECT MESG_S_UNID FROM BAACONFER.MESG_es WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '******' AND MESG_FIN_CCY_AMOUNT LIKE '******';
```

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

```
UPDATE SAACONFER.MESG_## SET MESG_FIN_XXX_AMOUNT = '##' WHERE MESG_S_UNID =
'##';
UPDATE SAACONFER.TEXT_## SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('##') WHERE TEXT_S_UNID = '##';
```

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 ##### .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' actors). 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

GIZMODO univision

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

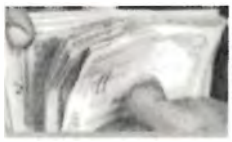
Matias S. Zavia

5/26/16 7:19am · Archivar en ATAQUES INFORMÁTICOS

Share Tweet

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

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



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

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

Read more

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

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

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

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

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

Síguenos también en Twitter, Facebook y Flipboard.

Click here

ABOUT THE AUTHOR

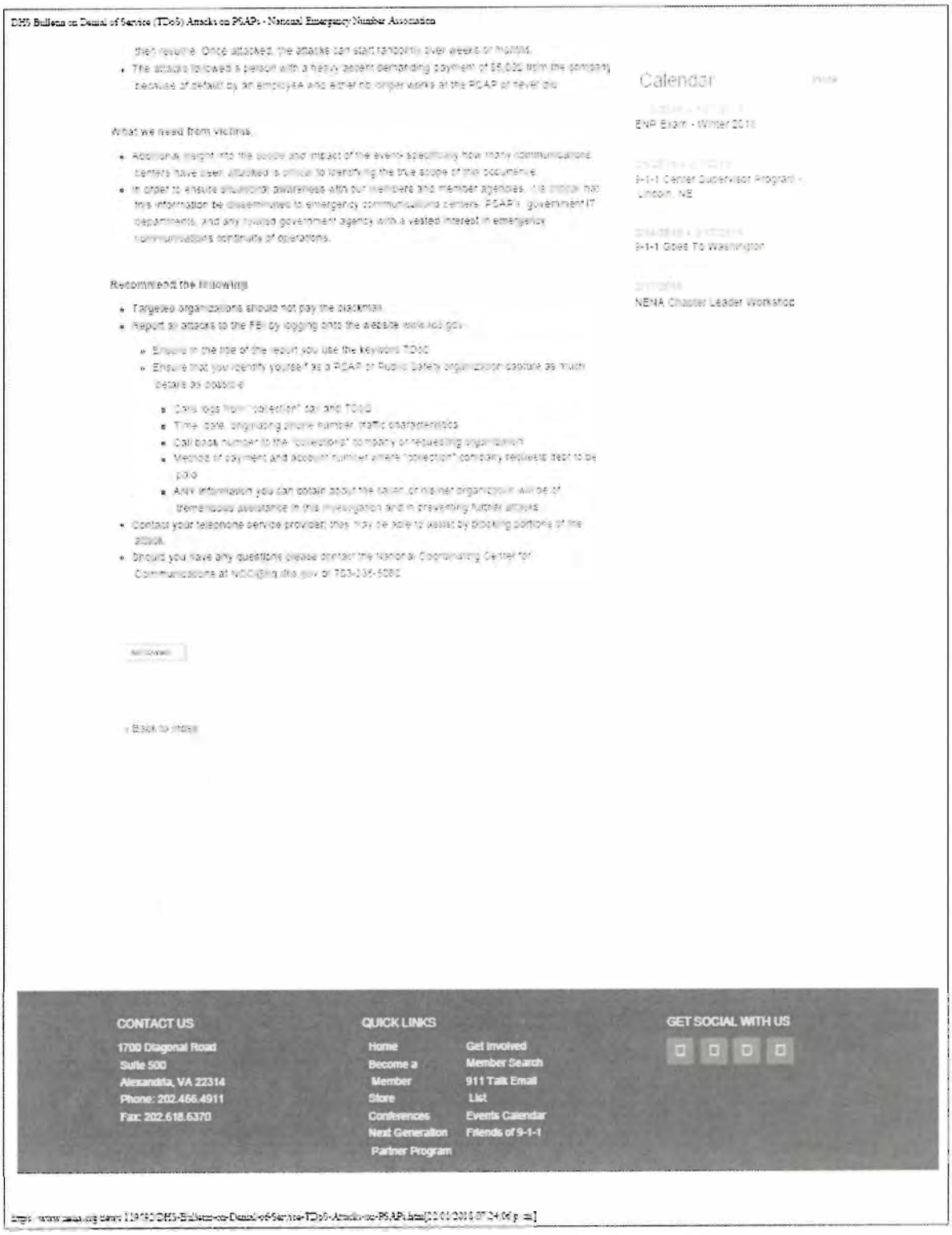
Matías S. Zavia

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

Email Twitter Posts Keys

ANEXO "I"

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

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 and 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 in order to identify the true scope of the occurrence.
- In order to ensure situational awareness with our members and member agencies, we ask that this information be disseminated to emergency communications centers, PSAPs, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operations.

Recommend the following:

- Targeted organizations should not pay the blackmail.
- Report all attacks to the FBI by logging onto the website www.ic3.gov.
  - Ensure in the title of the report you use the keywords TDoS.
  - Ensure that you identify yourself as a PSAP or Public Safety organization capture as much details as possible.
    - Caller ID 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 the 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

ENP Exam - Winter 2016

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

9-1-1 Goes To Washington

NENA Chapter Leader Workshop

CONTACT US

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

QUICK LINKS

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

GET SOCIAL WITH US

ANEXO "J"

http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/,

Consultada el 4 de marzo de 2018

CDM
CYBER DEFENSE MAGAZINE

JNQ™ is safely and securely bringing SMB v3 file Sharing to any Java Application

SIGN UP FOR FREE MONTHLY E-MAGAZINES

SUBSCRIBE

802.1X Authentication Has Never Been Easier!

READ NOW

portnox

Flaws in MAC address randomization implemented by vendors allow mobile tracking

on March 14, 2017

Read all past editions here

"First, we show that devices at random make impossible use of randomization by sending wireless frames with the true, global address when they should be using a randomized address." reads the paper published by the experts.

"We move on to extend the passive identification techniques of Vanhoef et al. to effectively defeat randomization in nearly all Android phones. Finally, we show a method that can be used to track 100% of devices using randomization, regardless of manufacturer, by exploiting a previously unknown flaw in the way existing wireless chipsets handle low-level power-saving frames."

The experts also analyzed so-called **Karma attacks**, a method that leverages on rogue access points (AP) for attacking their prey as known and trusted networks.

They researchers developed a new method that relies on Request-to-Send (RTS) and Clear-to-Send (CTS) control frames to expose the global MAC address for any kind of device.

According to the IEEE 802.11 specification, the RTS and CTS control frames are used to avoid collisions, basically every time a node using the channel to send data, it transmits also an RTS frame to inform other nodes that the channel should not be used in order to avoid collisions. Once a node in using the channel to send data, it transmits also an RTS frame to inform other nodes that the channel should not be used in order to avoid collisions. Once a node in time a node in

The recipient node responds with a CTS frame when it is ready to receive data.

The knowledge of this mechanism could be exploited by attackers that can send an RTS frame to any 802.11 capable devices, then analyzing the CTS response it can derive the global MAC address of the target. Once obtained the global MAC address, the attacker can use it to track the target device in the future by sending it RTS frames containing the global MAC.

The group of experts successfully tested the technique on over a models from multiple vendors, including iPhone 5s, iPhone 6s, iPad Air, Google Pixel, LG Nexus 5X, LG G4 and G5, Motorola Nexus 6, Moto Z Play and OnePlus 3.

Experts speculate RTS/CTS frequencies are managed within the 802.11 chipset, instead of the operating system, this means the only way to prevent the attacks is to develops a firmware patch that have to be distributed by manufactures.

"There are multiple scenarios in which a motivated attacker could use this method to violate the privacy of an unsuspecting user. If the global MAC address for a user is ever known, it can then be added to a database for future tracking." added the researchers. *"Concretely, an adversary with a sufficiently large database of advanced transmission capabilities could render randomization protections moot."*

The experts highlighted the importance to adopt a universal randomization policy with clear requirements for the implementation of the protection mechanism.

"We propose the following best practices for MAC address randomization. Firstly, mandate a universal randomization policy to be used across the spectrum of 802.11 client devices. We have illustrated that when vendors implement unique MAC address randomization schemes it becomes easier to identify and track those devices." concluded the experts. *"A randomization policy must include a minimum ruleset for randomized MAC address byte structure, 802.11 IE usage, and sequence number behavior."*

Pierluigi Paganini

Share this story

Recent Posts

UPCOMING EVENTS

10 APR	11 APR	BLOCKCHAIN SUMMIT CANADA TORONTO ON
10 APR	12 APR	Cyber Risk & Data Security
11 APR	12 APR	Cyber Resilience & Info Security Seminar 2018
	16 APR	2018 Global Insider Threat Summit
18 APR	19 APR	MENA CISO Forum
23 APR	24 APR	IT & Digital Leaders Dialogue UK
23 APR	24 APR	Tech Infrastructure Dialogue UK

ANEXO "K"

http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 ,
Consultada el 18 de mayo 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

Brigitte Bureau, Catherine Cullen, Kristen Everson · CBC News
Posted: Nov 22, 2017 5:00 PM ET | Last Updated: November 24, 2017

NDP MP Matthew Dubé took part in an experiment with CBC/Radio-Canada that revealed vulnerabilities in Canadian telecom networks. (Marc Robichaud/CBC)

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

One marker shows Dube 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.

Ethical hackers were able to hack into Dube's phone starting with just his telephone number. (Marc Robichaud/CBC)

"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 Dube'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 Dube's phone.

Lex Gill, Research Fellow at the University of Toronto's Citizen Lab, weighs in 5:30

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.

Karsten Nohl, managing director of Security Research Labs, says the two main Canadian telecom networks have about 10 per cent of the security needed to protect from SS7 attacks. (Michel Aspirot/CBC)

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 Dube to be part of a demonstration.

Dube, 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.

Dube'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.

Ethical hacker Luca Melette is based in Berlin. With just a phone number, he was able to hack into Dube's phone, listen to his calls, track his whereabouts and intercept his text messages. (CBC)

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

Canadian telecoms told CBC News that security is a top priority and threats are monitored. (Andrew Lee/CBC)

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.

Using encrypted apps like Signal and WhatsApp can help protect you from SS7 attacks, according to Noni. But unless your phone is off, you're never fully safe. (Andrew Lee/CBC)

"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, Noni 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."

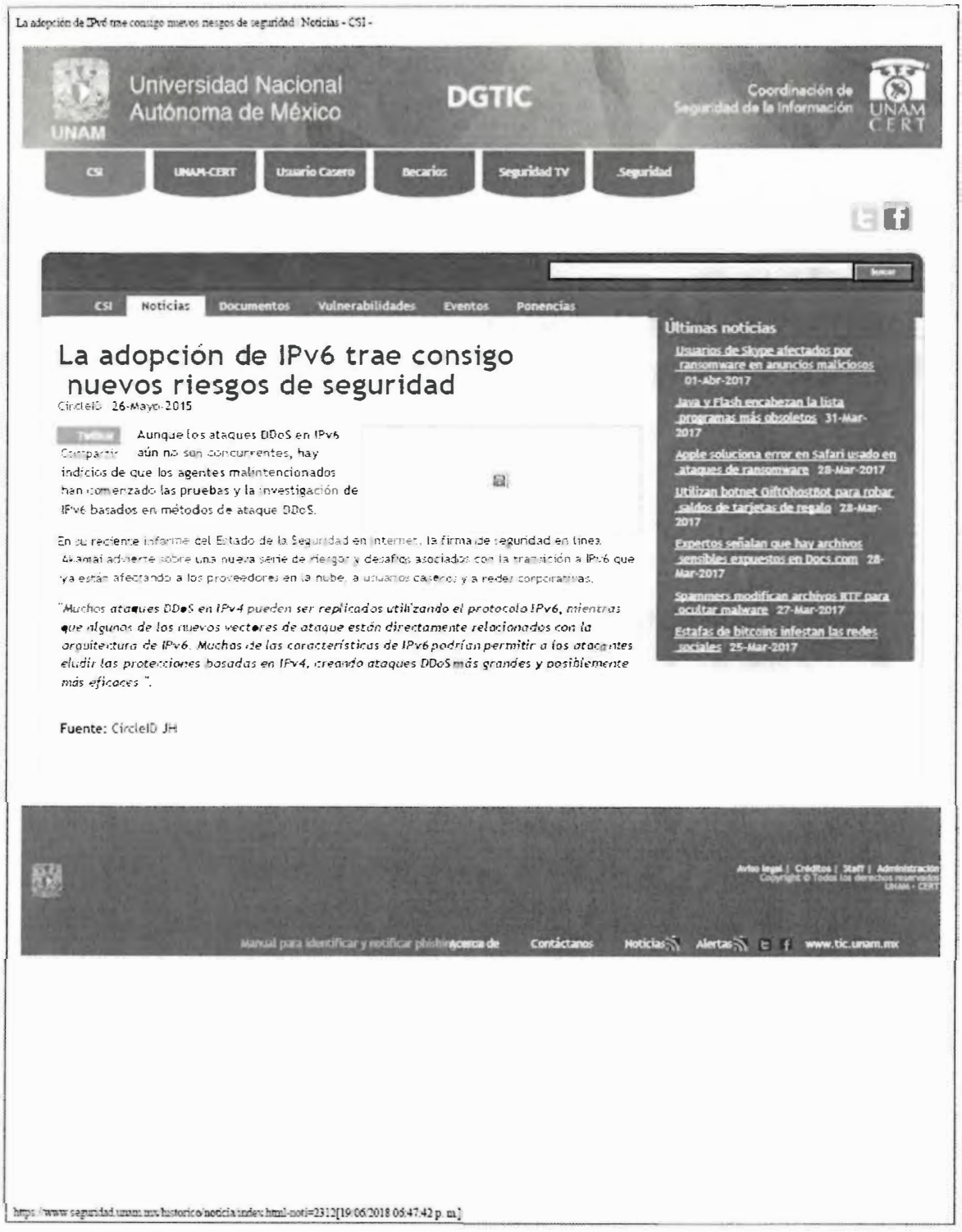
Hacking a cellphone has never been easier thanks to a vulnerability in the international telecommunication network, and tests have revealed two of Canada's largest telecom networks are at risk. All a hacker needs is your phone number, and they can track your movements and record your calls, all without your knowledge 4:51

Corrections

- A previous version of this story referred to a hacking incident involving a German Bank. The story originally said the incident happened in 2014. In fact it occurred earlier this year. *Nov 24, 2017 2:27 PM ET*

ANEXO "L"

https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2312,
Consultada el 19 de junio de 2018



ANEXO "M"

https://www.lomasnuevo.net/noticias/detectan-vulnerabilidad-en-firewalls-fortinet/,
Consultada el 19 de junio de 2018

Noticias | Infraestructura | Seguridad

Detectan vulnerabilidad en firewalls Fortinet

Por **Erwin** - Ene 13, 2016

Detectan vulnerabilidad en firewalls Fortinet

Se ha dado a conocer una nueva vulnerabilidad en los firewalls FortiGate 4.x-5.0.7 de la empresa Fortinet. La vulnerabilidad es grave ya que permite acceso total al firewall por ssh utilizando un usuario generico utilizado por el soporte de Fortinet y una clave que se genera con un script ya que es dinámica.

Los firewalls son pieza clave en la seguridad de las empresas y de internet en general ya que protegen para que gente externa (hackers) no pueda tener acceso sin autorización a los datos, servidores, aplicaciones y computadoras de la empresa.

Los firewalls Fortinet son muy utilizados por las empresas por su bajo costo comparado con otras empresas. Aunque las grandes del mundo de seguridad no están exentas de problemas como este, como ya lo demostró Juniper hace algunas semanas con algo similar.

Se aconseja a las empresas con estos firewalls actualizar lo antes posible los equipos. Y recordar que no es correcto habilitar el puerto ssh hacia el internet.

Fortinet emitió un comunicado indicando que luego de una investigación han determinado que no fue algo malintencionado de parte de sus empleados, pero es algo muy probable, poco a poco van saliendo a luz las posibles formas de cómo operaba la NSA.

Más información

Fuente

Etiquetas

5G Alcatel amazon Android Apple aws bigdata Blackberry Canon CES 2018 Cisco cloud Dell Dlink Docker Emc Facebook Galaxy S9 Google guatemala HP HPE huawei IBM Intel ios IoT iPhone Kingston lg Logitech Mediatek Microsoft Motorola Nintendo Nokia Oracle playstation Samsung smartphone Smartphones smartwatch Sony vmware Xbox

https://www.lounamuevo.net/noticias/detectan-vulnerabilidad-en-firewalls-fortinet/[19/06/2018 06:56:07 p. m.]

ANEXO "N"

https://www.offensive-security.com/metasploit-unleashed/information-gathering/,

Consultada el 22 de enero de 2018

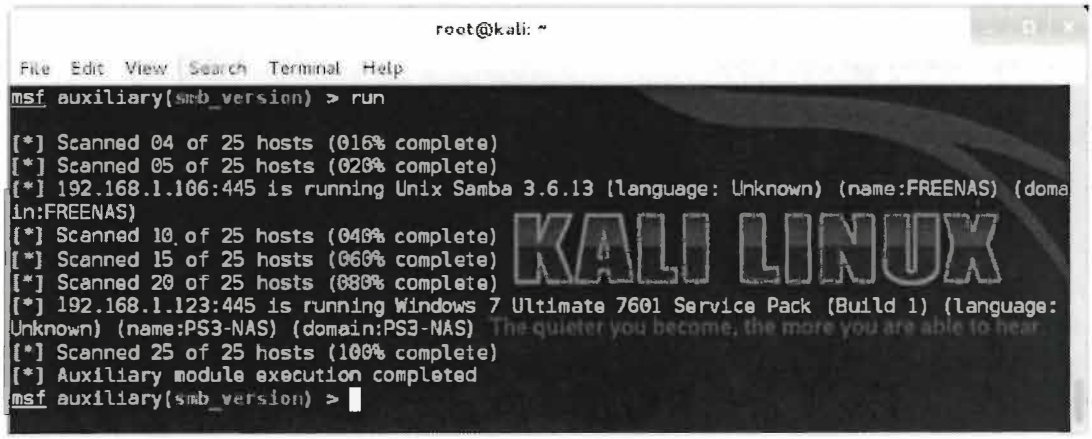
Information Gathering in Metasploit

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 "O"

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

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.[5]

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.[5][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

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

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]:23–28

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 2009.[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

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

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]

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. Retrieved November 24, 2015.
3. ^ "The nsa was hacked snowden documents confirm". *The Intercept*. 19 August 2016.

ANEXO "P"

https://www.krackattacks.com/ ,
Consultada el 19 de junio de 2018

KRACK : Attack:Breaking WPA2

Key Reinstallation Attacks

Breaking WPA2 by forcing nonce reuse

Discovered by Mathy Vanhoef of imec-DistriNet, KU Leuven

INTRO | DEMO | DETAILS | PAPER | TOOLS | Q&A

INTRODUCTION

We discovered serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. **The attack works against all modern protected Wi-Fi networks.** Depending on the network's configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

The weaknesses are in the Wi-Fi standard itself, and not in individual products or implementations. Therefore, any correct implementation of WPA2 is likely affected. To prevent the attack, users must update affected products as soon as security updates become available. Note that **if your device supports Wi-Fi, it is most likely affected.** During our initial research, we discovered ourselves that Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys, and others, are all affected by some variant of the attacks. For more information about specific products, consult the database of CERT/CC, or contact your vendor.

The research behind the attack will be presented at the Computer and Communications Security (CCS) conference, and at the Black Hat Europe conference. Our detailed research paper can already be downloaded.

https://www.krackattacks.com/[19/06/2018 07:12:36 p. m.]

ANEXO "Q"

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

Consultada el 22 de enero de 2018

#TECHNOLOGY NEWS MAY 4, 2013 / 3:50 AM / 2 YEARS AGO

Anonymous attack Greek central bank, warns others

Reuters Staff

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

Anonymous attack Greek central bank, warns others

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

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

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

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

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

Reporting by George Georgiopoulos; Editing by Angus MacSwan

Our Standards: The Thomson Reuters Trust Principles.

ANEXO "R"

https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/,

Consultada el 17 de enero de 2018

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

6/8/2017

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

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

Opicarus2017

Abstract

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

Figure 1: Operation Image of OpSacred

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

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

Download a Copy Now (/WorkArea/Downlc

OpSacred – Opicarus Phase 5

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

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

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

Figure 2: Opicarus Facebook Event Page

Reasons for Concern

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

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

Targets

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

Opicarus DDoS Arsenal

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

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

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

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

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

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

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

Other DDoS attack tools include:

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

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

Figure 3: OpicarusBot – A Layer 7 attack tool for Opicarus

Opicarus Github Pages

Opicarus - https://github.com/opicaruscollective/Opicarus (https://github.com/opicaruscollective/Opicarus/)
Documentation - https://github.com/opicaruscollective/Opicarus/tree/Documentation (https://github.com/opicaruscollective/Opicarus/tree/Documentation)
Tools - https://github.com/opicaruscollective/Opicarus/tree/Tools (https://github.com/opicaruscollective/Opicarus/tree/Tools)
YouTube channel - https://youtu.be/rk82RfPkTkY (https://youtu.be/rk82RfPkTkY)

Attack Vectors

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

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

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

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

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

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

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

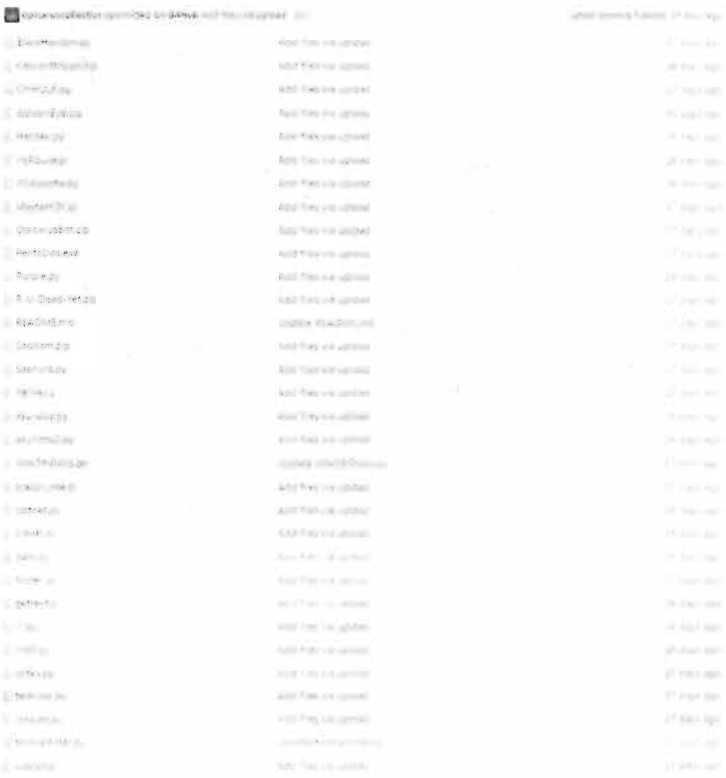


Figure 4: These tools can be found on GitHub at:https://github.com/opicarus/Opicarus/tree/Tools(https://github.com/opicarus/Opicarus/tree/Tools)

Effective DDoS Protection Essentials

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

Effective Web Application Security Essentials

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

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

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

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

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

https://www.facebook.com/HarveyHarris6/posts/421743798183945(https://www.facebook.com/HarveyHarris6/posts/421743798183945)

https://www.facebook.com/events/236685386815328(https://www.facebook.com/events/236685386815328/)

https://en.wikipedia.org/wiki/Maltego(https://en.wikipedia.org/wiki/Maltego)

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

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

DDoS Knowledge Center

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

DDoS Threats and Attacks

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

DDoS Experts' Insider

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

Under Attack and Need Emergency Assistance?

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

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

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

Community

- RadwareBlog (http://blog.radware.com/security/)
- Radware Connect (https://itunes.apple.com/us/app/radware-connect/id911124100?mt=8)

FOLLOW US:

Twitter (https://twitter.com/radware) LinkedIn (https://www.linkedin.com/companies/165642)

Google+ (https://plus.google.com/+radware)

YouTube (https://www.youtube.com/user/radwareinc)

Facebook (https://www.facebook.com/Radware)

slide-share (http://www.slideshare.net/Radware)

ANEXO "S"

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

Consultada el 15 de enero de 2018

Consulta de Series - Banxico

Banco de México

Sistemas de pago

Sistemascon liquidación en tiempo real.

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

Título	Sistemas de pago. Sistemas de liquidación en tiempo real. Días operados	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Atención a Cuentahabientes de Banco de México SIAC. Número de operaciones	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Atención a Cuentahabientes de Banco de México SIAC. Importe	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios (SPEI®). Ampliado. SPEUA. Número de operaciones	Sistemas de pago. Sistemas de liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios (SPEI®). Ampliado. SPEUA. Importe	Sistemas de pago. Sistemas con liquidación en tiempo real. Sistema de Liquidación de Valores INDEVAL. Número de operaciones	Sistemas de pago. Sistemas con liquidación en tiempo real. Sistema de Liquidación de Valores INDEVAL. Importe (millones de pesos)	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios (SPEI®). Número de operaciones	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios (SPEI®). Importe	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios (SPEI®). Número de operaciones	Sistemas con liquidación en tiempo real. Sistema de Pagos Electrónicos Interbancarios (SPEI®). Importe (millones de pesos)
Periodo disponible	Ene 1993 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1997 - Dic 2017	Ene 1997 - Dic 2017	Ene 1993 - Dic 2017	Ene 1993 - Dic 2017	Ene 1993 - Dic 2017	Ene 1993 - 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	Suma de Días	Valores	Flujo	Valores	Flujo	Valores	Flujo	Valores	Flujo	Valores	Flujo	Valores
Unidad	Días	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos
Base												
Aviso												
Tipo de información	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles
Fecha	SF41080	SF41083	SF41077	SF41084	SF41078	SF61053	SF61052	SF46188	SF46189	SF309374	SF309375
Ene 2017	22	4,617	407,311	N/E	N/E	336,184	78,018,647	38,316,737	21,637,771	N/E	N/E
Feb 2017	19	5,261	411,333	N/E	N/E	298,245	68,553,369	34,417,445	21,505,894	N/E	N/E
Mar 2017	22	4,261	5447,28	N/E	N/E	331,428	74,890,339	42,999,549	28,180,217	N/E	N/E
Abr 2017	18	5,535	445,390	N/E	N/E	290,035	68,312,022	36,954,704	27,494,055	N/E	N/E
May 2017	22	4,206	550,595	N/E	N/E	335,668	80,966,359	37,838,214	21,904,993	N/E	N/E
Jun 2017	22	4,115	468,872	N/E	N/E	341,433	76,058,055	43,405,087	24,093,365	N/E	N/E
Jul 2017	21	3,927	492,052	N/E	N/E	305,017	64,619,549	38,242,338	21,676,442	122,275,20	11,393,4
Ago 2017	23	4,164	421,344	N/E	N/E	333,109	68,671,479	40,307,961	22,008,779	136,352,30	11,819,3
Sep 2017	21	3,887	499,552	N/E	N/E	N/E	N/E	42,473,950	21,281,177	147,745,39	18,075,1
Oct 2017	22	4,306	404,014	N/E	N/E	N/E	N/E	43,173,873	24,899,886	N/E	N/E
Nov 2017	20	3,668	529,297	N/E	N/E	N/E	N/E	42,335,994	21,719,418	N/E	N/E
Dic 2017	19	3,749	574,454	N/E	N/E	N/E	N/E	46,076,738	24,058,191	N/E	N/E

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

15/01/2018

ANEXO "L"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000027118

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

RESULTANDO

PRIMERO. Que el veintiuno de mayo de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000027118,** la cual se transcribe a continuación:

> ***Descripción:*** *"*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. Ordenado por Número de serie, de cada uno de los equipos de cómputo, y de cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos, en posesión del sujeto obligado. a. Una relación de todos los puertos de red abiertos. b. Nombre y versión, del programa informático instalado para administrar o controlar lo referente al cortafuegos o firewall (en ingles). c. Si se encuentra habilitada la conexión de red IPv6 (Protocolo de Internet versión 6)."

SEGUNDO. Que la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección General de Tecnologías de la Información, el mismo veintiuno de mayo del presente año, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que el titular de la Dirección General de Tecnologías de la Información del Banco de México, mediante oficio con referencia DGTI-77/2018, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la solicitud de acceso a la información.

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

QUINTO. Que el Titular de la Dirección General de Tecnologías de la Información, mediante oficio DGTI-90/2018, informó a este órgano colegiado su determinación de clasificar la información precisada en dicho escrito, en los términos ahí señalados, respecto de la cual se elaboró la correspondiente prueba de daño, contenida en el cuerpo del oficio en comento, y solicitaron a este órgano colegiado confirmar tal clasificación.

BANCO DE MÉXICO

CONSIDERANDO

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

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa señalada en el resultando Quinto de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información señalada como **reservada,** toda vez que se ubica en los supuestos de reserva, en términos de **la fundamentación y motivación expresada en la prueba de daño** contenida en el oficio precisado en el resultando Quinto de la presente determinación, misma que se tiene por reproducida a la letra, en obvio de repeticiones innecesarias.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresada en la correspondiente prueba de daño, contenida en el cuerpo del respectivo oficio precisado en el resultando Quinto de la presente determinación.**

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

RESUELVE

ÚNICO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresada en la prueba de daño contenida en el oficio precisado en el resultando Quinto de la presente determinación.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "M"

BANCO DE MÉXICO

BANCO DE MÉXICO
RECIBIDO
21 JUN 2018
Comité de Transparencia
Por: JLS36 Hora: 17:30

Recibí un oficio constante en tres páginas y una prueba de daño.

Ciudad de México, a 21 de junio de 2018

REF: DGTI-91/2018

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

Presente.

Me refiero a la solicitud de acceso a la información, identificada con el número de folio 6110000027618, que nos turnó la Unidad de Transparencia el 21 de mayo 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:

> *"Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado: a. Número de serie, de parte y de modelo. b. Marca. c. Si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico. d. Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup). e. Si se encuentra activada la tecnología WIFI. f. Seguridad o cifrado implementado en la conexión WIFI (WEP -Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc). g. Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico."*

Sobre el particular, con fundamento en lo dispuesto por los artículos 6, apartado A, fracciones I y VIII, párrafo sexto, y 28, sexto y séptimo párrafos, de la Constitución Política de los Estados Unidos Mexicanos; 103, 104, 105, 106, fracción I, 108, último párrafo, y 113, Fracciones I y IV de la Ley General de Transparencia y Acceso a la Información Pública; 97, segundo, tercero y sexto párrafos, 98, fracción I, y 110, fracciones I y IV de la Ley Federal de Transparencia y Acceso a la Información Pública; 2º y 3º, fracción I, de la Ley del Banco de México; 4, 8, primero y segundo párrafos, 10, 15 Bis 1, 18 Bis, 29 del Reglamento Interior del Banco de México, Segundo, fracción IX, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como el Cuarto, párrafo primero, Séptimo, fracción I, y último párrafo, Octavo, párrafos primero al tercero, Décimo séptimo, fracción VIII, Vigésimo segundo, fracciones I y II, Trigésimo tercero, y Trigésimo cuarto, primer y segundo párrafos, de los *"Lineamientos generales en materia de clasificación y desclasificación de*

la información, así como para la elaboración de versiones públicas", vigentes, nos permitimos informarles que **esta unidad administrativa clasifica como reservada la siguiente información:**

- Número de serie de los routers y puntos de acceso inalámbricos.
- Si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico.
- Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup).
- Si se encuentra activada la tecnología WIFI.
- Seguridad o cifrado implementado en la conexión WIFI.
- Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso de los routers y puntos de acceso inalámbrico.

Lo anterior en virtud de que esta información corresponde a especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México, lo cual se fundamenta y motiva en la prueba de daño que se anexa.

Considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años, esta información deberá ser reservada, al menos, por cinco años.

Por lo expuesto, solicito atentamente a este Comité de Transparencia confirmar la 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 quito de los "Lineamientos que establecen los procedimientos internos de atención a solicitudes de acceso a la información pública", vigentes.

Asimismo, de conformidad con el Décimo de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, informamos que el personal que, por la naturaleza de sus atribuciones, tiene acceso a la información clasificada es el siguiente:

Información clasificada	Personal de la DGTI con acceso a la información clasificada
Los números de serie de cada uno de los routers y puntos de acceso inalámbricos.	Gerencia de Telecomunicaciones (Gerente) Subgerencia de Operación de Servicios de Telecomunicaciones (Todo el personal) Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente) Oficina de Soporte a la Gestión Presupuestal (Todo el personal). Subgerencia de Planeación y Regulación (Todo el personal)
• Si se cuenta con contraseña para acceder a la configuración o administración de los routers y puntos de acceso inalámbrico. • Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup). • Si se encuentra activada la tecnología WIFI. • Seguridad o cifrado implementado en la conexión WIFI. • Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso de los routers y puntos de acceso inalámbrico.	Gerencia de Telecomunicaciones (Gerente) Subgerencia de Operación de Servicios de Telecomunicaciones (Todo el personal) Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Subgerente) Oficina de Soporte a la Gestión Presupuestal (Todo el personal).

Atentamente.

ING. OCTAVIO BERGÉS BASTIDA
Director General de Tecnologías de la Información

PRUEBA DE DAÑO

Especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México.

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

a) Comprometer la seguridad nacional;

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

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

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

Por lo que, la información relativa a las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones** referente a la arquitectura de los componentes, que conforman la infraestructura, es decir, la organización y relación entre los equipos de cómputo, de telecomunicaciones y de seguridad electrónica, sus configuraciones, las actualizaciones de seguridad de estos componentes; la ubicación en donde se emplean estos componentes en las instalaciones del Banco de México, incluyendo los centros de datos y telecomunicaciones; los análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes; los manuales y procedimientos de operación de recuperación y de continuidad operativa para restablecer su funcionamiento; el diseño, el código fuente y los algoritmos que se desarrollan o se configuran para operar en ellos; así como toda información derivada de estas especificaciones que, de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con los procesos del Banco de México en que éste participa; es clasificada como reservada.

Cabe aclarar que como parte de las **especificaciones de la infraestructura de comunicaciones** se incluye lo siguiente:

- Los números de serie de cada uno de los equipos de cómputo, ruteadores (routers) y puntos de acceso inalámbricos, así como las unidades administrativas, conforme al organigrama institucional, que hacen uso de cada uno de estos equipos.

- Información sobre las contraseñas para acceder a la configuración y administración de los ruteadores (routers) y puntos de acceso inalámbrico.
- Información que identifique la configuración o el estado de los puertos de red (identificador de los servicios a los cuales se dirige un paquete de datos determinado) del Banco de México.
- Información relacionada con los protocolos de Internet utilizados.
- Nombre y versiones de los programas utilizados para administrar los cortafuegos (firewall) de red.
- Información sobre las tecnologías de red inalámbrica utilizadas y sus mecanismos de seguridad.

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, toda vez que dicho riesgo es:

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

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

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

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

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

Asimismo, el artículo décimo séptimo, fracción VIII, señala que se considera considerarse como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

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

En efecto, proporcionar las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, indudablemente facilitaría que terceros logren acceder a información financiera o personal, modifiquen los datos que se procesan en ellas o, incluso, dejen fuera de operación a los sistemas de información del Banco.

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

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales y más importantes instrumentos utilizados en el ámbito mundial para ingresar sin autorización a computadoras, aplicaciones, redes de comunicación, y diversos sistemas informáticos, con la finalidad de causar daños, obtener información o realizar operaciones ilícitas. Estos ataques se

fundamentan en (1) descubrir y aprovechar vulnerabilidades, basando cada descubrimiento en el análisis y estudio de la información de las especificaciones técnicas de diseño y construcción, incluyendo el código fuente de las aplicaciones, la arquitectura o servicios de tecnologías de información y de comunicaciones que se quieren vulnerar, y (2) tomar ventaja de cualquier información conocida para emplear técnicas de ingeniería social que les faciliten el acceso indebido a los sistemas, con el propósito de substraer información, alterarla, o causar un daño disruptivo.

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

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

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

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

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

En efecto, el funcionamiento seguro y eficiente de los sistemas de información depende de la **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**.

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

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, 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.[1] Como ésta existen numerosas herramientas que, si bien su propósito original es realizar pruebas a las infraestructuras de tecnologías de la información y comunicaciones para corregir errores en sus configuraciones e identificar posibles vulnerabilidades, en malas manos permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier sistema de cómputo fabricado en los últimos años. Estas son conocidas como "Meltdown" y "Spectre" y permiten ataques denominados "side-channel", en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando "Meltdown", un atacante puede utilizar un

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

programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. "Spectre" requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS [2].

- Un ataque a la plataforma de pagos internacionales del Banco Nacional de Comercio Exterior (Bancomext) que obligó a la institución a suspender sus operaciones de manera preventiva[3].
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.[4]
- De acuerdo a Reuters, el Director del Programa de Seguridad del Clientes de SWIFT, Stephen Gilderdale, dijo que los hackers continúan apuntando al sistema de mensajería bancaria de SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos[5]
- Dos ataques realizados contra la infraestructura crítica que provee energía eléctrica en la capital de Ucrania en diciembre de 2015, y diciembre de 2016, dejando sin electricidad a 225,000 personas[6].
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.[7]
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que

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

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

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

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

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

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

ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)" [8]. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.

- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.[9]
- Además de los ataques tradicionales y comunes de usurpación de direcciones MAC, el posible rastreo de equipos móviles empleando esta dirección, hace que no solo se pueda identificar cuando estos equipos se conectan a redes Wi-Fi, sino que además se pudiera estar siguiendo a la persona que lo usa[10], ocurriendo lo mismo con solo proporcionar el número telefónico de un celular, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto[11].
- Respecto a la adopción del protocolo para la comunicación en Internet "IPv6", el cual permite la comunicación entre los diferentes elementos de la red y nuestra propia computadora o dispositivo móvil, existen indicios de que los agentes malintencionados han comenzado las pruebas y la investigación de "IPv6" basados en métodos de ataque DDoS[12] (Denial of service – Denegación de servicio), el cual provoca que un servicio o recurso en una red de computadoras sea inaccesible a usuarios legítimos .
- El conocer el nombre y la versión del programa que administra los cortafuegos o "firewalls" (dispositivos para bloquear los accesos no autorizados a una red de computadoras, permitiendo al mismo tiempo comunicaciones autorizadas), puede llevar a conocer las vulnerabilidades de estos dispositivos, las cuales inclusive se llegan a publicar en páginas de Internet[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? (cuyas especificaciones de fabricación, y por consiguiente posibles vulnerabilidades se pueden obtener indirectamente a través de sus números de serie accediendo a la información que los fabricantes tengan de cada uno de estos dispositivos, teniendo como ejemplo la operación llamada "Equation Group")[15], ¿qué puertos de comunicaciones usan? (Si se encuentran abiertos o inactivos), ¿qué

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

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

[10] http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/, consultada el 4 de marzo de 2018. Se adjunta una impresión del artículo como **ANEXO "J"**.

[11] http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338. Se adjunta una impresión del artículo como **ANEXO "K"**

[12] https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2312, se adjunta una impresión del artículo como **ANEXO "L"**

[13] https://www.lomasnuevo.net/noticias/detectan-vulnerabilidad-en-firewalls-fortinet/. Se adjunta una impresión del artículo como **ANEXO "M"**

[14] https://www.offensive-security.com/metasploit-unleashed/information-gathering. Se adjunta una impresión del artículo como **ANEXO "N"**.

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

servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

Por otro lado, el uso de la tecnología "WiFi", que permite la interconexión inalámbrica de dispositivos electrónicos (computadoras, teléfonos, etc), ya sea entre ellos o hacia Internet, puede implicar riesgos importantes, ya que sin los adecuados mecanismos de seguridad, terceros pueden acceder a estas redes sin autorización, con la posibilidad de acceder y controlar los dispositivos "WiFi", tales como los ruteadores (o "routers" en inglés) encargados de encaminar los datos trasmitidos entre diferentes redes o subconjuntos de dispositivos, con tan solo conocer su identificador en la red. Por otro lado, el acceso no autorizado a un dispositivo "WiFi" permite supervisar y registrar toda la información que se trasmite a través de éste.

Dentro del uso de redes inalámbricas, el estándar "WPS" (WiFi Protected Setup) define diversos mecanismos para configurar una red local inalámbrica apoyados en el sistema de seguridad conocido como "WPA2" (WiFi Protected Access 2 – Acceso Protegido WiFi 2). El conocer los mecanismos de protección utilizados también permitiría a un atacante identificar las vulnerabilidades asociadas a éstos.[16].

A partir de lo mencionado anteriormente, el dar a conocer la unidad, área u órgano del Banco de México que hace uso de cada uno de ruteadores y puntos de acceso inalámbricos, facilitaría direccionar a algún área funcional que sea del interés del atacante cibernético materializar los riesgos recién señalados.

En resumen, de la misma manera que el resto de las especificaciones de tecnologías de la información y telecomunicaciones, el conocimiento de las tecnologías utilizadas para la comunicación inalámbrica y sus mecanismos de seguridad y cifrado tales como el estándar WPS, y por obvias razones, el uso de contraseñas para acceder a los dispositivos WiFi, tales como los ruteadores y puntos de acceso inalámbricos, así como las unidades administrativas que hacen uso de esta tecnología, permitiría a un atacante identificar y aprovechar vulnerabilidades asociadas a ellas.

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.

[16] https://www.krackattacks.com/. Se adjunta una impresión del artículo como **ANEXO "P"**

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

Lo anterior no es ajeno a la banca mundial, la cual, es continuamente asediada por grupos denominados "hacktivistas", como ocurrió durante el mes de mayo de 2016, donde se pretendía inutilizar los sitios Web de los bancos centrales. Se cita la fuente de la noticia: "Anonymous attack Greek central bank, warns others"[17]. El colectivo amenazó a los bancos centrales de todo el mundo, luego de afectar por más de seis horas la página del Banco Nacional de Grecia. Estos ataques formaron parte de una operación, orquestada originalmente por el colectivo "Anonymous", conocida como "OpIcarus" y que desde 2016 ha presentado actividad; siendo la más reciente la denominada "OpSacred" o "OpIcarus – Phase 5", que tuvo lugar en Junio de 2017, y cuyos objetivos nuevamente fueron los sitios públicos de bancos centrales alrededor del mundo[18].

Por ejemplo, en términos económicos, para dimensionar de manera más clara la posible afectación de un ataque informático dirigido al Banco de México, se puede identificar que mediante el sistema de pagos electrónicos interbancarios, desarrollado y operado por el Banco de México, en los meses de enero a diciembre de 2017, se realizaron más de 480 millones de operaciones por un monto mayor a 270 billones de pesos[19]; lo que equivale a más de 54 mil operaciones por un monto de 30 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

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

---

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

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

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

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

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

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

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

Las consecuencias de que tenga éxito un ataque a la infraestructura estratégica referida, que sustenta a los procesos fundamentales, tendrían 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, **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones**, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

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

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

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

Dicha determinación es además proporcional considerando que, como se ha explicado, dar a conocer **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones** generaría un riesgo o daño de perjuicio significativo, el cual sería claramente mayor al beneficio particular del interés que pudiera existir en el dar a conocer dicha información.

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

Además de que su divulgación posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional y, en consecuencia menoscaba la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto. Asimismo comprometer las acciones encaminadas a proveer a la economía del país de moneda nacional, dañando la estabilidad del poder adquisitivo de dicha moneda, el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos.

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

ANEXO "A"

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

Metasploit

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 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.

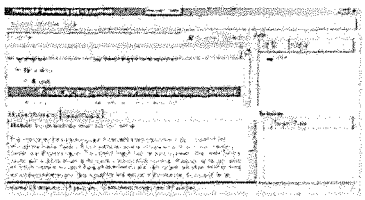
Índice [ocultar]

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

Metasploit Framework

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

metasploit®



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

[editar datos en Wikidata]

Historia [editar]

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

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

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

Metasploit - Wikipedia, la enciclopedia libre

Editar enlaces

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

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

Marco/Sistema Metasploit [editar]

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

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

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

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

Interfaces de Metasploit [editar]

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

Edición Metasploit [editar]

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

Edición Community Metasploit [editar]

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

Metasploit express [editar]

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

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

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

Metasploit Pro [editar]

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

Armitage [editar]

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

Cargas útiles [editar]

Metasploit ofrece muchos tipos de cargas útiles, incluyendo:

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

Lista de los desarrolladores originales:

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

Referencias [editar]

1. ↑ «Rapid7 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 chausmi.
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 21, 2018 7:56 AM PT

NEWSANALYSIS

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, Elay Trail and most Skylake chips are covered. On the other hand, Broadwell, Haswell, and Sandy Bridge chips still leave brown skid marks.

[Related: How to protect Windows 10 PCs from ransomware]

Security Advisory INTEL-SA-00088 has been updated with this squib:

> *We have now released new production microcode updates to our OEM customers and partners for Kaby Lake, Coffee Lake, and additional Skylake-based platforms. As before, these updates address the reboot issues last discussed here, and represent the breadth of our 6th, 7th and 8th Generation Intel® Core™ product lines as well as our latest Intel® Core™ X-series processor family. They also include our recently announced Intel® Xeon® Scalable and Intel® Xeon® D processors for datacenter systems. We continue to release beta microcode updates for other affected products so that customers and partners have the opportunity to conduct extensive testing before we move them into production.*

Intel's recommendations

Intel goes on to recommend basically the same stuff they recommended last time, with a specific call-out:

- *We continue to recommend that OEMs, cloud service providers, system manufacturers, software vendors, and end users stop deployment of previously released versions of certain microcode updates addressing variant 2 (CVE-2017-5715), as they may introduce higher-than-expected reboots and other unpredictable system behavior.*

- *We also continue to ask that our industry partners focus efforts on evaluating the beta microcode updates.*
- *For those concerned about system stability while we finalize these updated solutions, earlier this week we advised that we were working with our OEM partners to provide BIOS updates using previous versions of microcode not exhibiting these issues, but that also removed the mitigations for 'Spectre' variant 2 (CVE 2017-5715)*
- *Microsoft also provided two resources for users to disable original microcode updates on platforms exhibiting unpredictable behavior:*
- *For most users – An automatic update available via the Microsoft® Update Catalog which disables 'Spectre' variant 2 (CVE 2017-5715) mitigations without a BIOS update. This update supports Windows 7 (SP1), Windows 8.1, and all versions of Windows 10 - client and server*
- *For advanced users – Refer to the following Knowledge Base (KB) articles*
- *KB4073119: IT Pro Guidance*
- *KB4072698: Server Guidance*
- *Both of these options eliminate the risk of reboot or other unpredictable system behavior associated with the original microcode update and retain mitigations for 'Spectre' variant 1*

and 'Meltdown' variant 3 until new microcode can be loaded on the system.

The "For most users" update is KB 4078130, the surprise Friday evening patch, released on Jan. 26, which I discussed almost a month ago:

> *On Friday night, Microsoft released a strange patch called KB 4078130 that "disables mitigation against Spectre, variant 2." The KB article goes to great lengths describing how Intel's the bad guy and its microcode patches don't work right.*
>
> *There aren't any details, but apparently this patch — which isn't being sent out the Windows Update chute — adds two registry settings that "manually disable mitigation against Spectre Variant 2"*

Rummaging through the lengthy Microsoft IT Pro Guidance page, there's an important warning:

[Got a spare hour? Take this online course and learn how to install and configure Windows 10 with the options you need.]

> *Customers who only install the Windows January and February 2018 security updates will not receive the benefit of all known protections against the vulnerabilities. In addition to installing the January and February security updates, a processor microcode, or firmware, update is required. This should be available through your OEM device manufacturer.*

Microsoft firmware update for Surface Pro 3

In what must be an amazing coincidence, last night Microsoft released a firmware update for the Surface Pro 3. It's currently available as a manual download ("MSI format") for Surface Pro 3. I haven't seen it come down the Windows Update chute. Perhaps Microsoft is beta testing it once again. Per Brandon Records on the Surface blog:

> *We've released a new driver and firmware update for Surface Pro 3. This update includes new firmware for Surface UEFI which resolves potential security vulnerabilities, including Microsoft security advisory 180002.*
>
> *This update is available in MSI format from the Surface Pro 3 Drivers and Firmware page at the Microsoft Download Center.*

Except, golly, the latest version of the patch on that page (as of 10 am Eastern US time) is marked "Date Published 1/24/2018." The official Surface Pro 3 update history page lists the last firmware update for the SP3 as being dated Oct. 27, 2017.

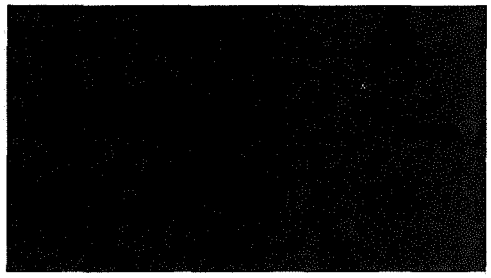
And, golly squared, Microsoft Security Advisory 180002 doesn't even mention the Surface Pro 3. It hasn't been updated since Feb. 13. It links to the *Surface Guidance to protect against speculative execution side-channel vulnerabilities* page, KB 4073065, which doesn't mention the Surface Pro 3 and hasn't been updated since Feb. 2.

You'd have to be incredibly trusting — of both Microsoft and Intel — to manually install *any* Surface firmware patch at this point. Particularly when you realize that not one single Meltdown or Spectre-related exploit is in the wild. Not one.

Thx Bogdan Popa Softpedia News.

Fretting over Meltdown and Spectre? Assuage your fears on the AskWoody

Lounge



Woody Leonhard is a columnist at Computerworld and author of dozens of Windows books, including "Windows 10 All-in-One for Dummies."

Follow

ANEXO "C"

https://www.gob.mx/bancomext/prensa/acción-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion,

Consultada el 15 de enero de 2018

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

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

Fecha de publicación
10 de enero de 2018

Categoría
Comunicado

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

El Banco Nacional de Comercio Exterior (Bancomext) informa que a partir de las conductas ilícitas de seguridad con que cuenta, el día 9 de enero fue viernes de una fecha de [illegible] de pago de [illegible] por lo [illegible] tercero.

Las autoridades han confirmado que el [illegible] de Bancomext "Bancomext en línea" no [illegible] por otros productos de Bancomext y Apoyo Futuro.

Afortunadamente, el [illegible] y la oportuna reacción de las áreas responsables para [illegible], como [illegible] de los Bancos y las autoridades correspondientes y el Banco de México, [illegible] normalidad esta mañana.

Cabe destacar que los intereses de nuestros clientes y [illegible] del propio Banco se encuentran a salvo y que Bancomext está [illegible] sus clientes y contrapartes.

A medida que [illegible] mayor información [illegible] de operación del portal de

Teléfono Comercial: 55 [illegible]

Compartir (Ligas Nuevas Ventanas) compartir en [illegible]
(http://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion?idiom=es)

Imprimir (Ligas Nuevas Ventanas)

[illegible]

ANEXO "D"

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

Consultada el 22 de enero de 2018

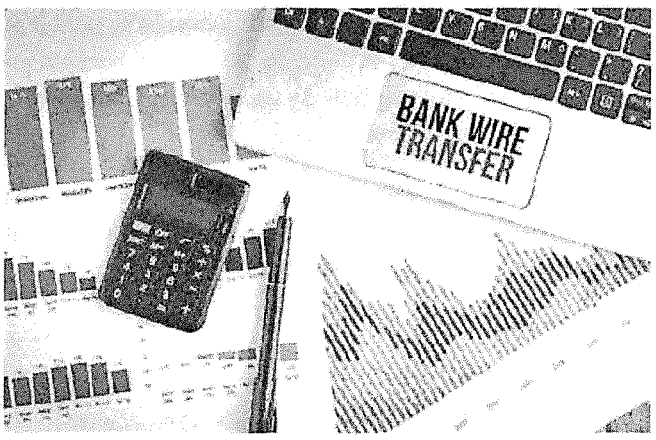
Security

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

Arrests after customized malware apparently used to drain millions

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

11 SHARE



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

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

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

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

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

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

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

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

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

Updated to add

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

Tips and corrections

11 Comments

MORE Swift Hacking

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

#INTEL OCTOBER 13, 2017 / 6:03 AM / 3 MONTHS AGO

SWIFT says hackers still targeting bank messaging system

Jim Finkle

3 MIN READ

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

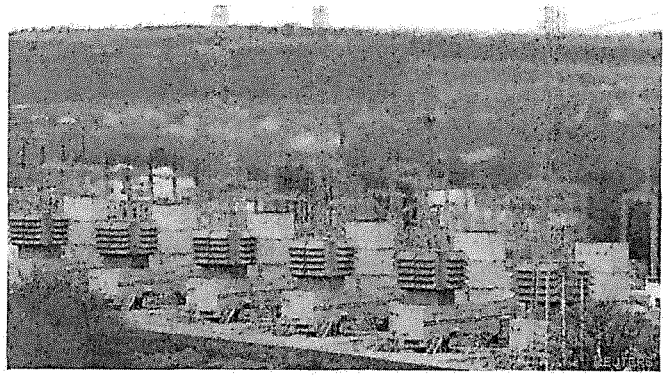
http://www.bbc.com/news/technology-38573074

Consultada el 15 de enero de 2018

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

ISSP

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

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

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

'Not much different'

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

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

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

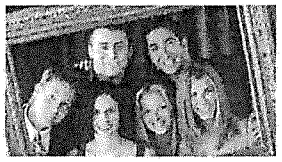
BRENDAN HOFFMAN

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

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

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

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



Still Friends? The trouble with old sitcoms

The Japanese star who taught China's young about sex

'Floating on air' after 19kg tumour is removed

The missing - aftermath of Trump's crackdown

The Israeli boy who survived Mumbai attack

Looking for my brother

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

'Acts of terrorism'

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

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

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

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

Related Topics

Cyber-security | Ukraine

Share this story About sharing

More on this story

Ukraine hackers claim huge Kremlin email breach
3 November 2016

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

Ukraine power 'hack attacks' explained
29 February 2016

Technology

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

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

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

More Videos from the BBC

Recommended by Outbrain

Desert temples of stone

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

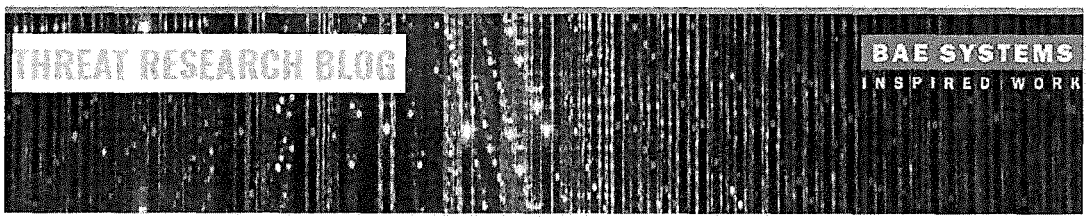
Elephant's trunk? The story of the @ sign

Most Read

1. Cranberries singer Dolores O'Riordan dies suddenly aged 46
2. Rape case collapses after 'cuddling' photos emerge
3. Denmark Facebook sex video: More than 1,000 young people charged
4. Black Death 'spread by humans not rats'
5. Still Friends? The trouble with old sitcoms
6. Carillion collapse: Ministers hold emergency meeting
7. Steven Seagal denies Bond girl assault
8. Peppi 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



Posted by Sergei Shevchenko - Monday, 25 April 2016

TWO BYTES TO $951M

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

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

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

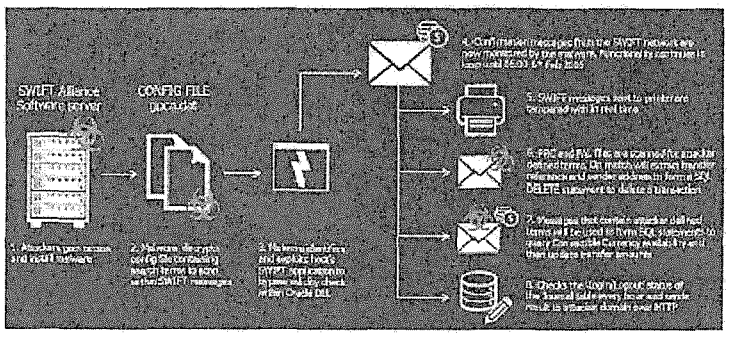
The tools are highly configurable and given the correct access could feasibly be used for similar attacks in the future.

Malware samples

[illegible]	[illegible]	[illegible]	[illegible]
525a8e3ae4e3df8c8c61f2a48e38541d198e9228	2016-02-05 11:46:29	65,536	evtdiag.exe
76bab478dcc70f979ce62cd308e9ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
70bf18597e375ad891f2c1efa194dbe7f60e4eeb	2016-02-05 08:55:19	24,576	nroff_b.exe
6207b92842b28a438330a2bf0ee8dcab7ed0a183	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 525a8e3ae4e3df8c8c61f2a48e38541d198e9228 as this is the component that contains logic for interacting with the SWIFT software

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



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

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

Malware config and logging

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

```
4e 38 16 a7 7f 03 cc aa 0d 56 ed ef 59 ed 18 ef
```

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

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

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

```
196.201.108.174
```

The sample also uses the following file for logging:

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

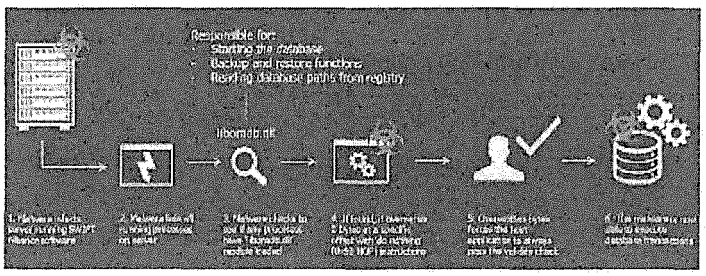
Module patching

The malware enumerates all processes, and if a process has the module `libcswdb.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 `liboraclb.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 910 Confirmation of Debit"
":20: Transaction"
"Sender :"
[additional filters from the decrypted configuration file cpos.dat]
```

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

```
SELECT MESG_S_UMID FROM SAACWNER.MESG_%% WHERE MESG_SENDER_SWIFT_ADDRESS
LIKE '******' AND MESG_TRN_REF LIKE '******';
```

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

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

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

```
set heading off;
set linesize 32767;
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
SAACWNER.JRNL_%% WHERE JRNL_DISPLAY_TEXT LIKE '%%LT BEXCBDDH: Log%%'
ORDER BY JRNL_DATE_TIME DESC) A WHERE ROWNUM = 1;
```

NOTE: 'BEXCBDDH' 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]:all[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 "---U" if neither of the events

occurred, e.g.:

```
IC&I_server;/all:::0
```

Manipulating balances

The malware monitors all SWIFT messages found in

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

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

```
":19A: Amount"
": Debit"
"Debit/Credit :"
"Sender :"
"Amount :"
"FEDERAL RESERVE BANK"
" I"
" I"
":62F: "
":60F: "
":60M: "
":62M: "
"Credit"
"Debit"
" 61: "
" 20: Transaction"
":20: Force"
```

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 `gpia.dat`.

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

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

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

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

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

```
UPDATE SAAJOURNER.MESG_%s SET MESG_FIN_CCY_AMOUNT = '%s' WHERE MESG_S_UNIQ =
'%s';
UPDATE SAAJOURNER.TEXT_%s SET TEXT_DATA_BLOCK =
UTL_RAW.CAST_TO_VARCHAR2('%s') WHERE TEXT_S_UNIQ = '%s';
```

Printer manipulation

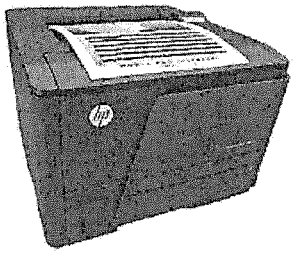
In order to hide the fraudulent transactions carried out by the attacker(s), the database/message manipulations are not sufficient. SWIFT network also generates confirmation messages, and these messages are sent by the software for printing. If the fraudulent transaction confirmations are printed out, 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 `nzofi.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"

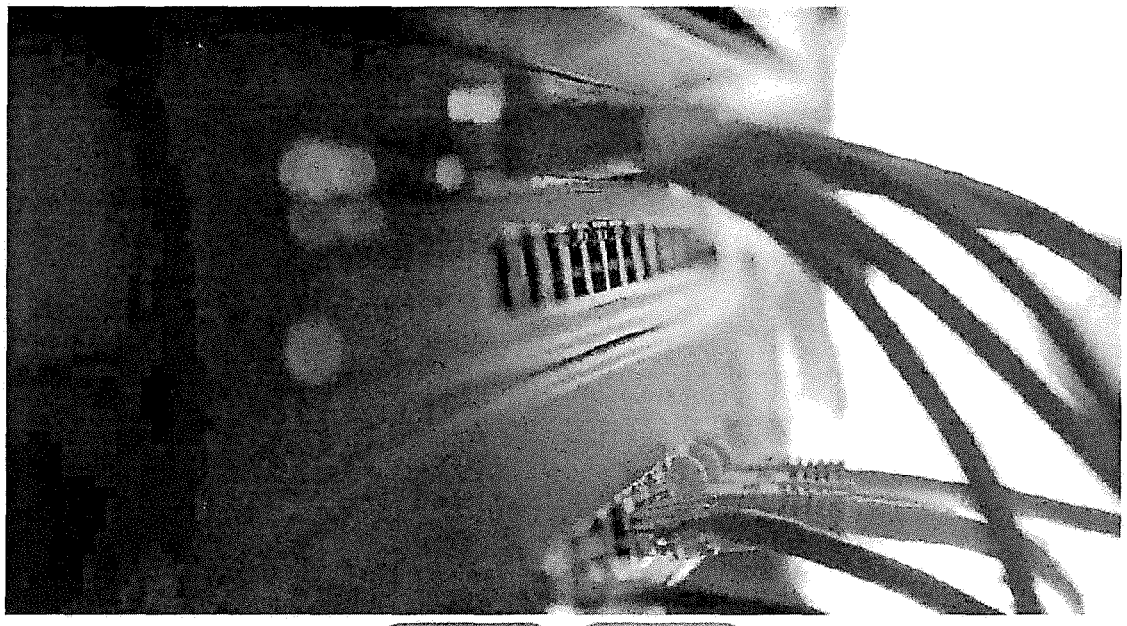
http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375,
Consultada el 22 de enero de 2018

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

Matias S. Zavia
3/29/16 7:19am • Archivado en: ATAQUES INFORMÁTICOS



Share Tweet

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

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

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

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

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

Read more

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

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

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

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

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

Síguenos también en Twitter, Facebook y Flipboard.

Click here

ABOUT THE AUTHOR

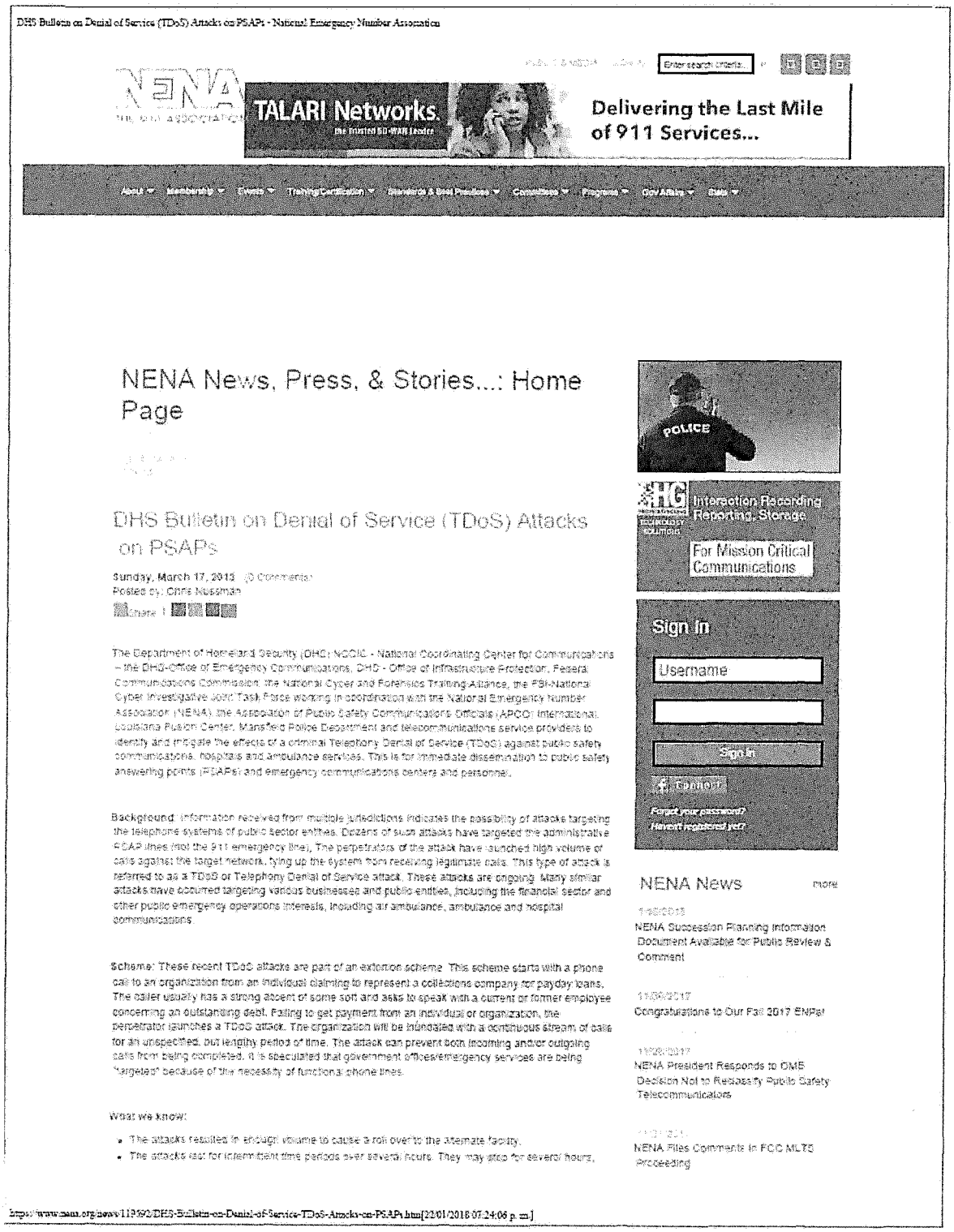
Matías S. Zavia

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
the trusted SD-WAN Leader

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 Hussman

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 Reassess Public Safety Telecommunications

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, PSAPs, government IT departments, and any related government agency with a vested interest in emergency communications continuity of operations.

Recommend the following:

- Targeted organizations should not pay the blackmail.
- Report all attacks to the FBI by logging onto the website *www.ic3.gov*
  - Ensure in the title of the report you use the keyword TDoS
  - Ensure that you identify yourself as a PSAP or Public Safety organization capture as much details as possible
    - Calls logs from "collection" call and TDoS
    - Time, date, originating phone number, traffic characteristics
    - Call back number to the "collections" company or requesting organization
    - Method of payment and account number where "collection" company requests 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

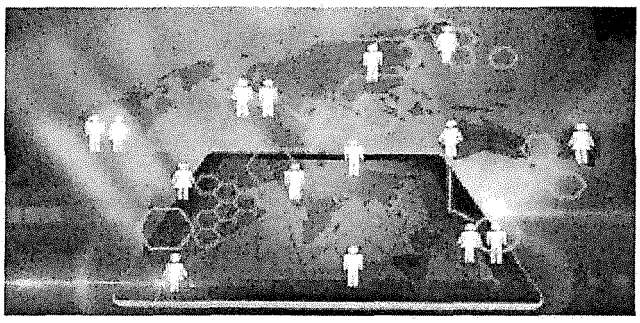
ANEXO "J"

http://www.cyberdefensemagazine.com/flaws-in-mac-address-randomization-implemented-by-vendors-allow-mobile-tracking/,

Consultada el 4 de marzo de 2018

Flaws in MAC address randomization implemented by vendors allow mobile tracking

on March 14, 2017



Researchers devised a new attack method that can be leveraged to track mobile devices that rely on MAC address randomization mechanism.

The MAC address is a unique and an hardcoded identifier assigned to a device's network interface. This characteristic makes it an excellent tool for the tracking of the devices. A group of researchers from the U.S. Naval Academy has devised a new attack method that can be leveraged to track mobile devices that rely on Media Access Control (MAC) address randomization mechanism used to protect the users' privacy.

The MAC address randomization uses broadcasting a random Wi-Fi MAC address making difficult the monitoring of the MAC addresses.

Starting from a previous research, the researchers have demonstrated that MAC address randomization is not sufficient to protect the users.

The MAC address randomization was introduced by Google for Android devices in 2015 with the release of Android's Marshmallow.

The experts discovered that many device manufacturers that use Android, including Samsung, have not enabled MAC address randomization.

Apple introduced the feature in mid-2014 with the release of iOS 8, but experts found that iOS 10 makes it easy to identify and track devices regardless of their use of MAC address randomization.

U.S. Naval Academy researchers identified serious flaws in a majority of the Android implementations of MAC randomization, allowing them to break the protection in the case of roughly 5% percent of mobile devices they have tested.

"First, we show that devices commonly make improper use of randomization by sending wireless frames with the true, global address when they should be using a randomized address," reads the paper published by the experts.

"We move on to extend the passive identification techniques of Vanhoef et al. to effectively defeat randomization in ~55% of Android phones. Finally, we show a method that can be used to track 100% of devices using randomization, regardless of manufacturer, by exploiting a previously unknown flaw in the way existing wireless chipsets handle low-level control frames."

The experts also analyzed so-called **Karma attacks**, a method that leverages on rogue access points (Evil AP attack) that pose as known and trusted networks.

They researchers devised a new method that relies on Request to Send (RTS) and Clear to Send (CTS) control frames to expose the global MAC address for any kind of device.

According to the IEEE 802.11 specification, the RTS and CTS control frames are used to avoid collisions, basically every time a node using the channel to send data, it transmits also an RTS frame to inform other nodes that the channel should not be used in order to avoid collisions. Every node in using the channel to send data, it transmits also an RTS frame to inform other nodes that the channel should not be used in order to avoid collisions. Every node in turn a node in

The recipient node responds with a CTS frame when it is ready to receive data.

The knowledge of this mechanism could be exploited by attackers that can send an RTS frame to IEEE 802.11 client devices, then analyzing the CTS response it can derive the global MAC address of the target device obtained the global MAC address, the attacker can use it to track the target device in the future by sending RTS frames containing the global MAC.

The group of experts successfully tested the technique on over a models from multiple vendors, including iPhone 5s, iPhone 6s, iPad Air, Google Pixel, LG Nexus 5X, OS 04 and G5, Motorola Nexus 6, Moto Z Play and OnePlus 3.

Experts speculate RTS/CTS responses are managed within the 802.11 chipset, instead of the operating system, this means the only way to prevent the attacks is to develop a firmware patch that have to be distributed by manufactures.

"There are multiple scenarios in which a motivated attacker could use this method to violate the privacy of an unsuspecting user. If the global MAC address for a user is ever known, it can then be added to a database for future tracking," added the researchers. "Conceivably, an adversary with a sufficiently large database and advanced transmission capabilities could render randomization protections moot."

The experts highlighted the importance to adopt a universal randomization policy with clear requirements for the implementation of the protection mechanism.

"We propose the following best practices for MAC address randomization. Firstly, mandate a universal randomization policy to be used across the spectrum of 802.11 client devices. We have illustrated that when vendors implement unique MAC address randomization schemes it becomes easier to identify and track these devices," concluded the experts. "A universal policy must include a minimum, rules for randomized MAC address byte structure, 802.11 IE usage, and sequence number behavior."

Pierluigi Paganini

UPCOMING EVENTS

TUE 10 APR 2018	WED 11 APR 2018	BLOCKCHAIN OPPORTUNITIES SUMMIT CANADA / Apr 10-11, 2018, Toronto ON
TUE 10 APR 2018	THU 12 APR 2018	Cyber Risk & Data Security
WED 11 APR 2018	THU 12 APR 2018	Cyber Resilience & Info Security Seminar 2018
	MON 16 APR 2018	2018 Global Insider Threat Summit
WED 18 APR 2018	THU 19 APR 2018	MENA CISO Forum
MON 23 APR 2018	TUE 24 APR 2018	IT & Digital Leaders Dialogue UK
MON 23 APR 2018	TUE 24 APR 2018	Tech Infrastructure Dialogue UK

Home

ANEXO "K"

http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 ,
Consultada el 18 de mayo 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

Brigitte Bureau, Catherine Cullen, Kristen Everson · CBC News ·
Posted: Nov 22, 2017 5:00 PM ET | Last Updated: November 24, 2017

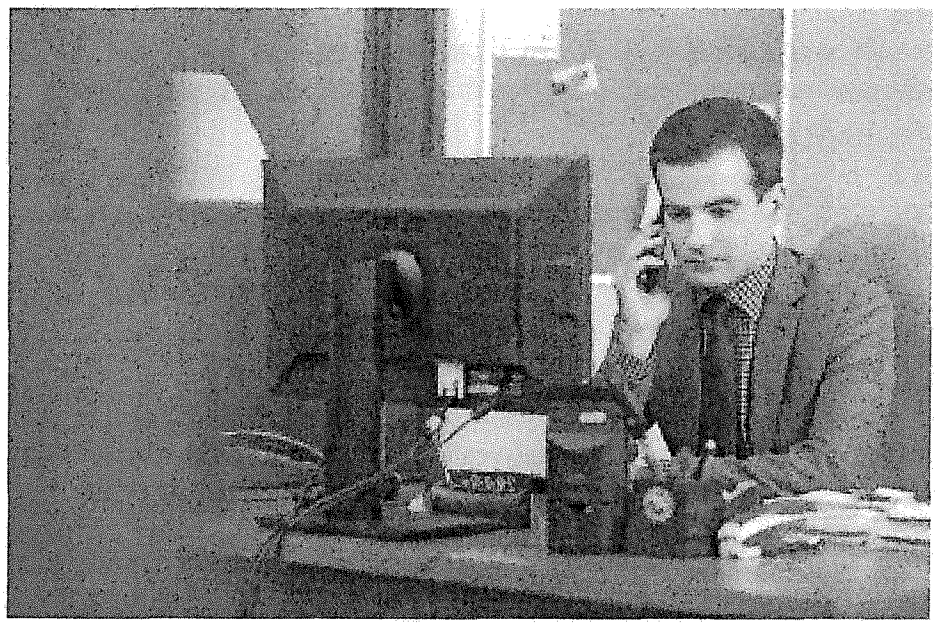
NDP MP Matthew Dubé took part in an experiment with CBC/Radio-Canada that revealed vulnerabilities in Canadian telecom networks. (Marc Robichaud/CBC)

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

One marker shows Dube 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.



Ethical hackers were able to hack into Dubé's phone starting with just his telephone number. (Marc Robichaud/CBC)

"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.

Lex Gill, Research Fellow at the University of Toronto's Citizen Lab, weighs in 5:30

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."

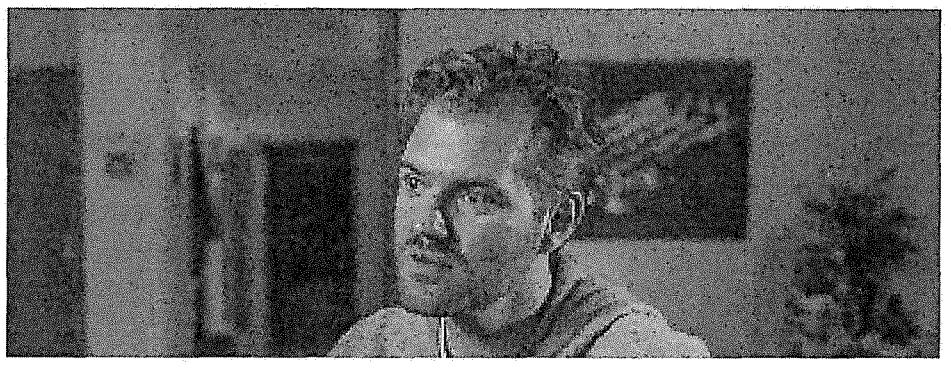
- RCMP used cellphone tracking technology unlawfully 6 times, says privacy watchdog

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.



Karsten Nohl, managing director of Security Research Labs, says the two main Canadian telecom networks have about 10 per cent of the security needed to protect from SS7 attacks. (Michel Aspirot/CBC)

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.

Ethical hacker Luca Melette is based in Berlin. With just a phone number, he was able to hack into Dubé's phone, listen to his calls, track his whereabouts and intercept his text messages. (CBC)

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 Dube'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.

Canadian telecoms told CBC News that security is a top priority and threats are monitored. (Andrew Lee/CBC)

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.

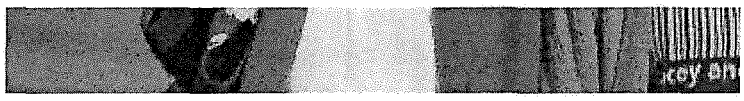
In a statement, CSE said its role is to provide "advice and guidance to help protect systems of importance to the Government of Canada."

"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.



Using encrypted apps like Signal and WhatsApp can help protect you from SS7 attacks, according to Noni. But unless your phone is off, you're never fully safe. (Andrew Lee/CBC)

"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, Noni 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."

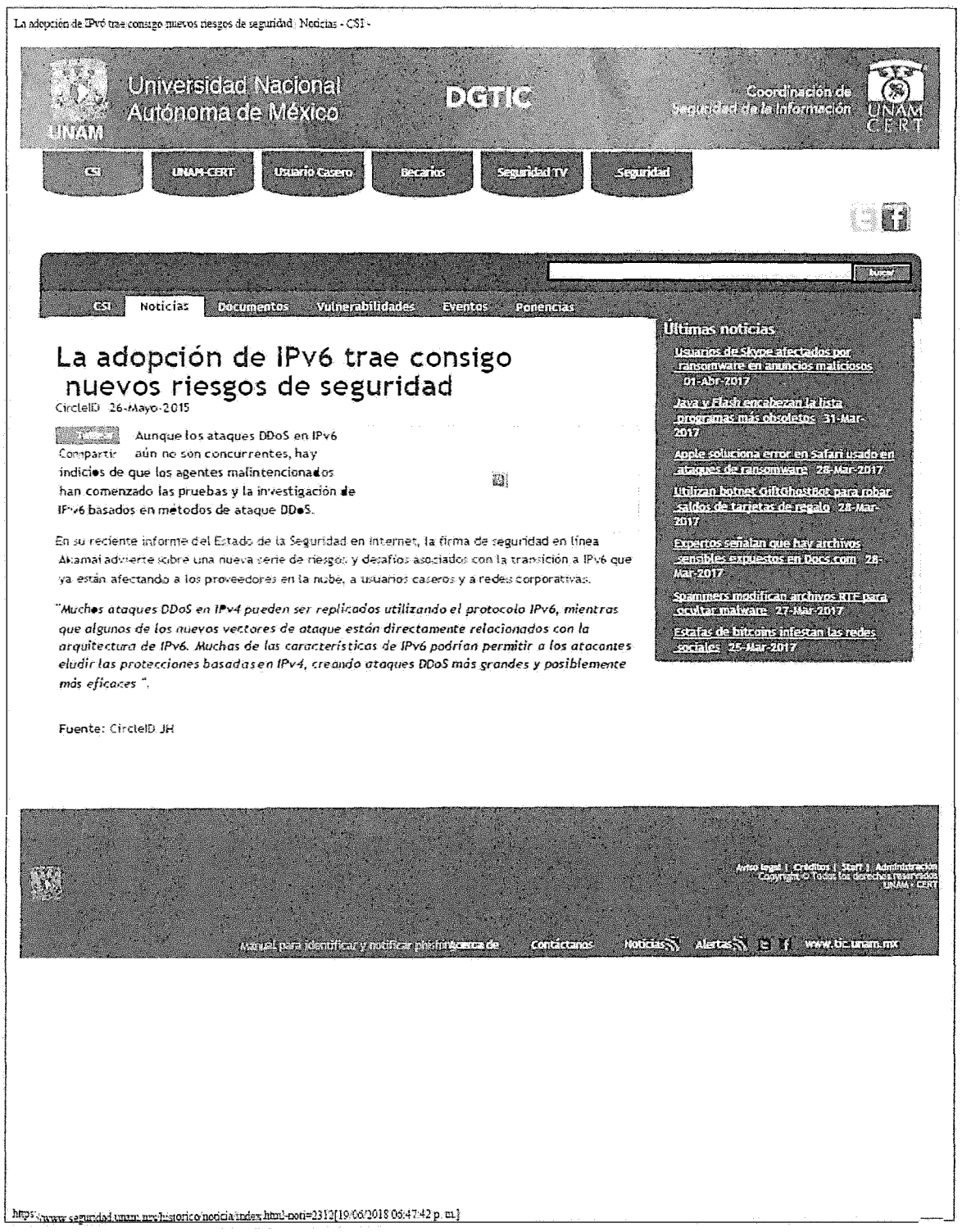
Hacking a cellphone has never been easier thanks to a vulnerability in the international telecommunication network, and tests have revealed two of Canada's largest telecom networks are at risk. All a hacker needs is your phone number, and they can track your movements and record your calls; all without your knowledge 4:51

Corrections

- A previous version of this story referred to a hacking incident involving a German Bank. The story originally said the incident happened in 2014. In fact it occurred earlier this year. *Nov 24, 2017 2:27 PM ET*

ANEXO "L"

https://www.seguridad.unam.mx/historico/noticia/index.html-noti=2312,
Consultada el 19 de junio de 2018



ANEXO "M"

https://www.lomasnuevo.net/noticias/detectan-vulnerabilidad-en-firewalls-fortinet/,
Consultada el 19 de junio de 2018

Noticias | Infraestructura | Seguridad

Detectan vulnerabilidad en firewalls Fortinet

Por Erwin - Ene 13, 2016

FORTINET®

https://www.lomasnuevo.net/noticias/detectan-vulnerabilidad-en-firewalls-fortinet/[19/06/2018 06:56:07 p. m.]

Detectan vulnerabilidad en firewalls Fortinet

Se ha dado a conocer una nueva vulnerabilidad en los firewalls FortiGate 4.x-5.0.7 de la empresa Fortinet. La vulnerabilidad es grave ya que permite acceso total al firewall por ssh utilizando un usuario generico utilizado por el soporte de Fortinet y una clave que se genera con un script ya que es dinámica.

Los firewalls son pieza clave en la seguridad de las empresas y de internet en general ya que protegen para que gente externa (hackers) no pueda tener acceso sin autorización a los datos, servidores, aplicaciones y computadoras de la empresa.

Los firewalls Fortinet son muy utilizados por las empresas por su bajo costo comparado con otras empresas. Aunque las grandes del mundo de seguridad no están exentas de problemas como este, como ya lo demostró Juniper hace algunas semanas con algo similar.

Se aconseja a las empresas con estos firewalls actualizar lo antes posible los equipos. Y recordar que no es correcto habilitar el puerto ssh hacia el internet.

Fortinet emitió un comunicado indicando que luego de una investigación han determinado que no fue algo malintencionado de parte de sus empleados, pero es algo muy probable, poco a poco van saliendo a luz las posibles formas de cómo operaba la NSA.

https://www.lomasnuevo.net/noticias/detectan-vulnerabilidad-en-firewalls-fortinet/[19/06/2018 06:56:07 p. m.]

ANEXO "N"

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

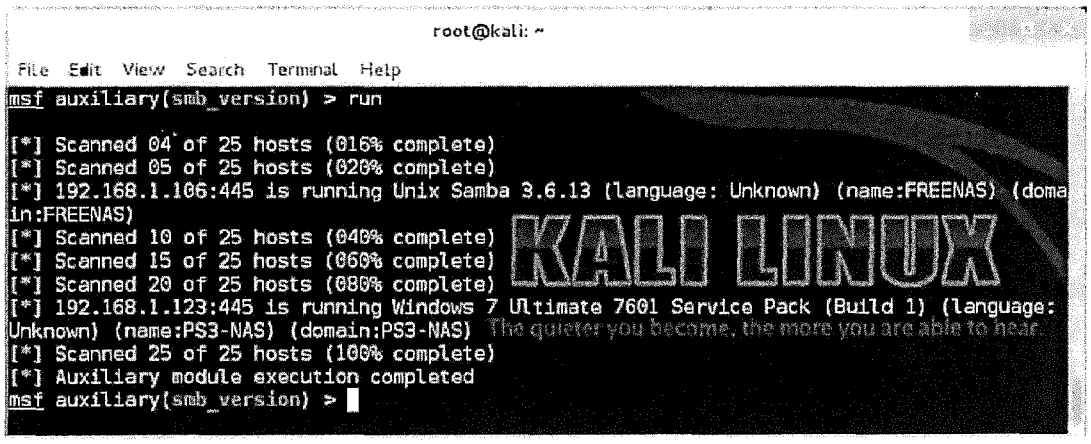
Information Gathering in Metasploit

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:

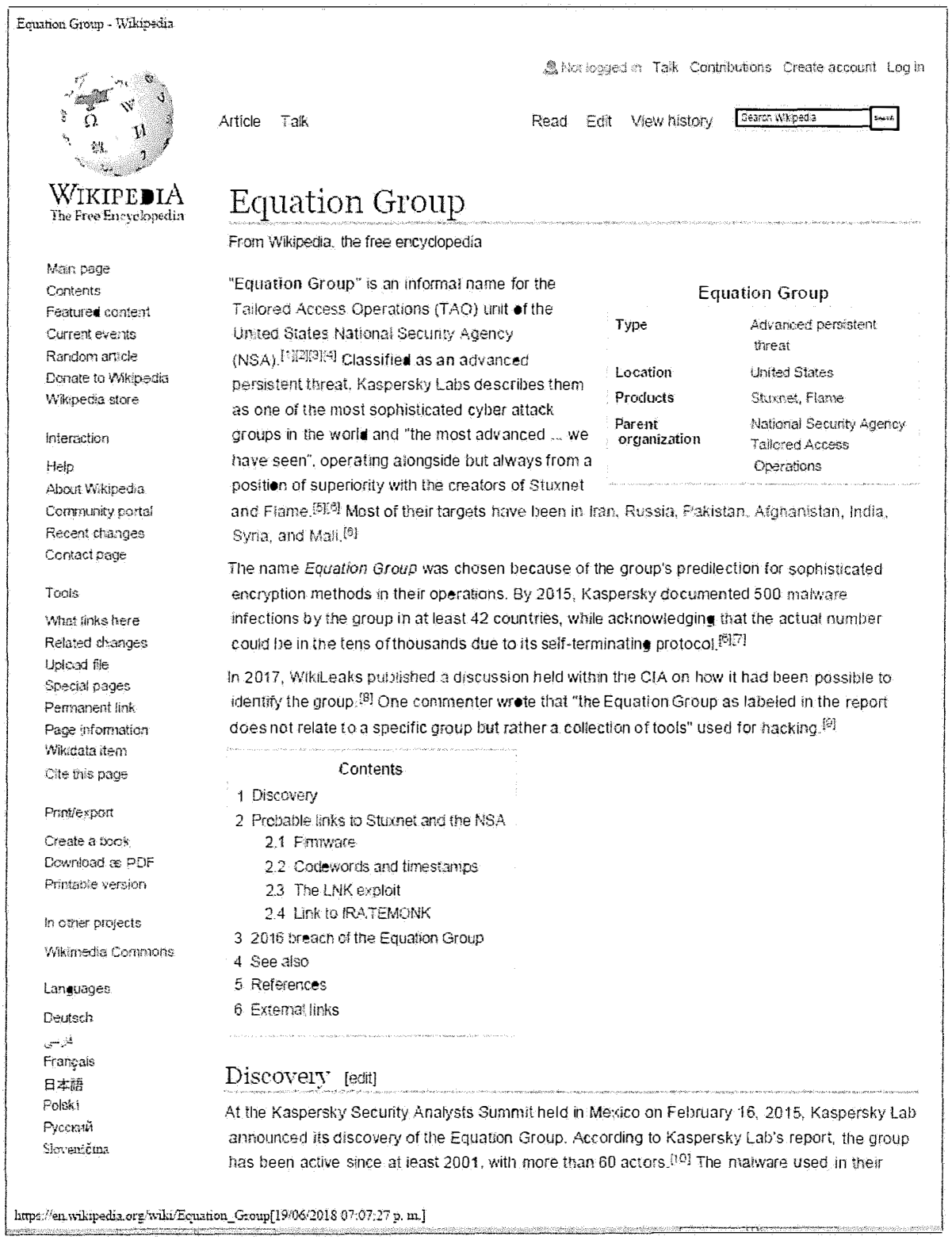
- Port Scanning
- Hunting for MSSQL
- Service Identification
- Password Sniffing
- SNMP sweeping



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

ANEXO "O"

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

Equation Group

From 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
Slovenčina

"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]

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

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.[5][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

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]

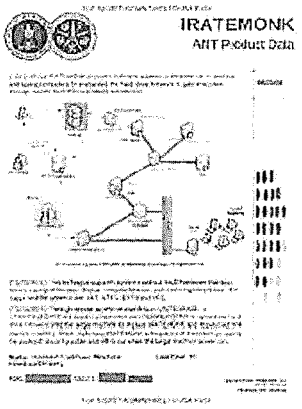
The NSA codewords "STRAITACID" and "STRAITSHOOTER" have been found inside the malware. In addition, timestamps in the malware seem to indicate that the programmers worked overwhelmingly Monday–Friday in what would correspond to a 08:00–17:00 workday in an Eastern United States timezone.[12]

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



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

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]

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

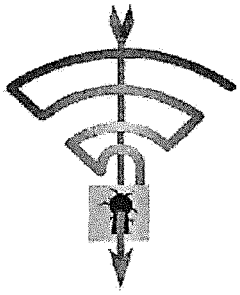
References [edit]

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. Retrieved November 24, 2015.
3. ^ "The nsa was hacked snowden documents confirm". *The Intercept*. 19 August 2016.

ANEXO "P"

https://www.krackattacks.com/ ,
Consultada el 19 de junio de 2018

KRACK Attacks: Breaking WPA2



Key Reinstallation Attacks

Breaking WPA2 by forcing nonce reuse

Discovered by Mathy Vanhoef of imec-DistriNet, KU Leuven

INTRO DEMO DETAILS PAPER TOOLS Q&A

INTRODUCTION

We discovered serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. **The attack works against all modern protected Wi-Fi networks.** Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

The weaknesses are in the Wi-Fi standard itself, and not in individual products or implementations. Therefore, any correct implementation of WPA2 is likely affected. To prevent the attack, users must update affected products as soon as security updates become available. Note that **if your device supports Wi-Fi, it is most likely affected.** During our initial research, we discovered ourselves that Android, Linux, Apple, Windows, OpenBSD, MediaTek, Linksys, and others, are all affected by some variant of the attacks. For more information about specific products, consult the database of CERT/CC, or contact your vendor.

The research behind the attack will be presented at the Computer and Communications Security (CCS) conference, and at the Black Hat Europe conference. Our detailed research paper can already be downloaded.

https://www.krackattacks.com/[19/06/2018 07:12:36 p. m.]

ANEXO "Q"

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

Consultada el 22 de enero de 2018

Anonymous attack Greek central bank, warns others

Directory of sites Login Contact Support

World Business Markets Politics TV

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.

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 "R"

https://security.radware.com/ddos-threats-attacks/threat-advisories-attack-reports/opicarus2017/,
Consultada el 17 de enero de 2018

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

6/8/2017

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

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

OpIcarus2017

Abstract

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

Figure 1: Operation image of OpSacred

(/WorkArea/DownloadAsset.aspx?id=1558)
Opicarus is a multiphase opetation originally launched by Ano is nowentering its fifth phase on June 11, 2017

Download a Copy Now (/WorkArea/Downlc

OpSacred – OpIcarus Phase 5

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

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

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

Figure 2: Opicarus Facebook Event Page

Reasons for Concern

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

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

Targets

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

Opicarus DDoS Arsenal

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

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

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

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

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

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

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

Other DDoS attack tools include:

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

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

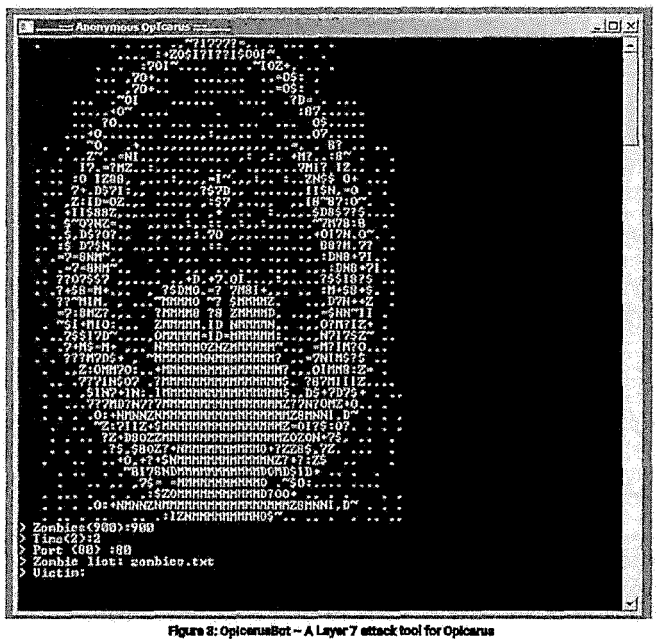


Figure 3: OpicarusBot – A Layer 7 attack tool for Opicarus

Opicarus Github Pages

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

Attack Vectors

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

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

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

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

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

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

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

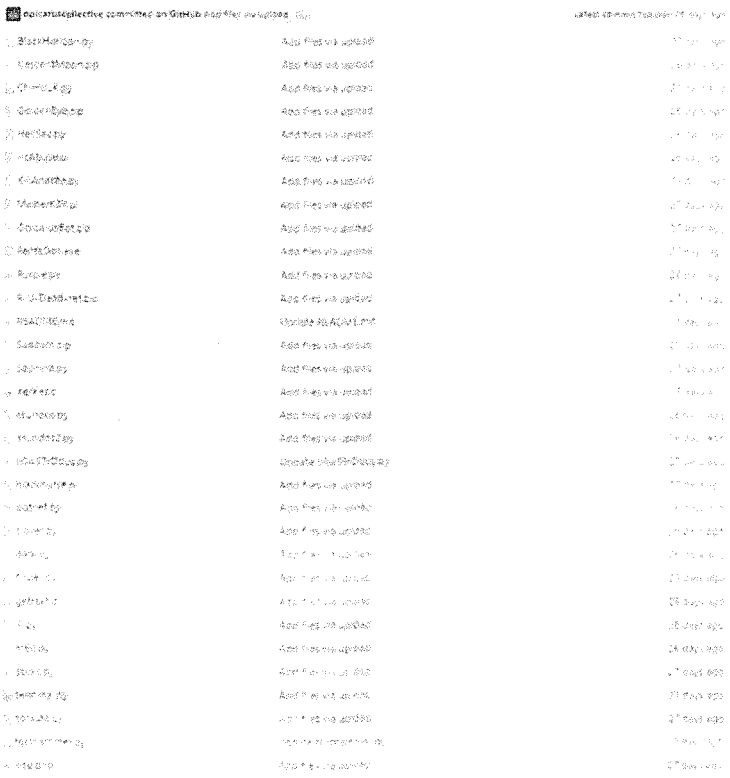


Figure 4: These tools can be found on GitHub at https://github.com/opicarus collective/Opicarus/tree/Tools(https://github.com/opicarus collective/Opicarus/tree/Tools)

Effective DDoS Protection Essentials

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

Effective Web Application Security Essentials

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

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

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

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

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

https://www.facebook.com/HarveyHarris6/posts/421743798188394(https://www.facebook.com/HarveyHarris6/posts/421743798188945)

https://www.facebook.com/events/236685386815328(https://www.facebook.com/events/236685386815328/)

https://en.wikipedia.org/wiki/Maltego(https://en.wikipedia.org/wiki/Maltego)

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

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

DDoS Knowledge Center

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

DDoS Threats and Attacks

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

DDoS Experts' Insider

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

Under Attack and Need Emergency Assistance?

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

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

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

Community

- Radware Blog (http://blog.radware.com/security/)
- Radware Connect (https://itunes.apple.com/us/app/radware-connect/id391124100?mt=8)

FOLLOW US:

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

ANEXO "S"

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

Consultada el 15 de enero de 2018

Consulta de Series - Banxico — Página 1 de 1

Banco de México

Sistemas de pago
Sistemas con liquidación en tiempo real

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

Título	Sistemas de pago, Sistemas de liquidación en tiempo real. Días operados	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Atención a Cuentahabientes de Banco de México SIAC, Número de operaciones	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Atención a Cuentahabientes de Banco de México SIAC, Importe	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos de Uso Amplio SPEUA, Número de operaciones	Sistemas de pago, Sistemas de liquidación en tiempo real, Sistema de Pagos Electrónicos de Uso Amplio, SPEUA, Importe	Sistemas de pago, Sistemas con liquidación en tiempo real, Sistema de Liquidación de Valores INDEVAL, Número de operaciones	Sistemas de pago, Sistemas con liquidación en tiempo real, Sistema de Liquidación de Valores INDEVAL, Importe (millones de pesos)	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI®, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios SPEI®, Importe (millones de pesos)	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios en Dólares SPID®, Número de operaciones	Sistemas con liquidación en tiempo real, Sistema de Pagos Electrónicos Interbancarios en Dólares SPID®, Importe (millones de dólares)
Periodo disponible	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1992 - Dic 2017	Ene 1997 - Dic 2017	Ene 1998 - Dic 2017	Ene 1998 - Dic 2017	Jul 2017 - Dic 2017	Jul 2017 - Dic 2017
Periodicidad	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual	Mensual
Cifra	Sin tipo de Cifra	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos	Volumen	Flujos
Unidad	Días	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Pesos	Operaciones	Millones de Dólares
Base											
Aviso											
Tipo de información	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles	Niveles
Fecha	SF41080	SF41083	SF41077	SF41084	SF41078	SF61953	SF61952	SF46188	SF46189	SF309374	SF309375
Ene 2017	22	4,617	467,515	N/E	N/E	738,784	79,018,943	35,316,765	24,877,271	N/E	N/E
Feb 2017	19	3,961	413,315	N/E	N/E	598,705	68,553,320	34,417,422	21,505,024	N/E	N/E
Mar 2017	22	4,263	542,787	N/E	N/E	731,478	74,850,270	40,316,545	25,180,217	N/E	N/E
Abr 2017	18	3,595	448,360	N/E	N/E	702,076	55,517,777	35,954,754	22,494,923	N/E	N/E
May 2017	22	4,226	532,095	N/E	N/E	726,828	66,956,550	37,331,714	23,984,590	N/E	N/E
Jun 2017	22	4,115	480,872	N/E	N/E	541,453	70,053,655	43,805,037	23,093,365	N/E	N/E
Jul 2017	21	3,927	499,052	N/E	N/E	595,917	64,619,646	35,242,331	21,576,446	122,275.00	11,309.4
Ago 2017	23	4,104	421,344	N/E	N/E	781,129	68,671,726	42,267,091	22,005,727	155,750.00	11,817.0
Sep 2017	21	3,937	495,592	N/E	N/E	N/E	N/E	42,473,503	21,881,177	147,745.00	10,920.0
Oct 2017	22	4,306	474,056	N/E	N/E	N/E	N/E	40,172,872	22,509,386	N/E	N/E
Nov 2017	20	3,963	429,207	N/E	N/E	N/E	N/E	43,888,364	21,719,413	N/E	N/E
Dic 2017	19	3,749	526,453	N/E	N/E	N/E	N/E	48,575,708	24,658,179	N/E	N/E

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

ANEXO "N"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

CLASIFICACIÓN DE INFORMACIÓN
FOLIO: 6110000027618

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

RESULTANDO

PRIMERO. Que el veintiuno de mayo de dos mil dieciocho, la Unidad de Transparencia del Banco de México recibió la solicitud de acceso a la información con folio **6110000027618**, la cual se transcribe a continuación:

> ***Descripción:*** *"*Con fundamento en el artículo 6 constitucional, atentamente requiero que en función de los principios constitucionales de máxima publicidad, transparencia, rendición de cuentas y gratuidad, me entregue a través de un medio gratuito derivado de los avances tecnológicos y en formato de documento portátil (PDF) comprimido o en diverso de naturaleza similar, la siguiente información pública documentada en el ejercicio de las facultades, competencias y funciones previstas en las normas jurídicas aplicables. 1. De cada uno de los MODEMS, ROUTERS (rúters) o Puntos de acceso inalámbricos en posesión del sujeto obligado: a. Número de serie, de parte y de modelo. b. Marca. c. Si se cuenta con contraseña para acceder a la configuración u administración del MÓDEM, ROUTER (rúter) o punto de acceso inalámbrico. d. Si se encuentra activada la tecnología WPS (por sus siglas en ingles Wi-Fi Protected Setup). e. Si se encuentra activada la tecnología WIFI. f. Seguridad o cifrado implementado en la conexión WIFI (WEP -Wired Equivalent Privacy, WPA -Wi-Fi Protected Access, WPA2 -Wi-Fi Protected Access 2, etc). g. Conforme al organigrama estructural, unidades, áreas u órganos que hacen uso del MODEM, ROUTER (rúter) o punto de acceso inalámbrico.*"*

SEGUNDO. Que la solicitud de información mencionada en el resultando anterior, fue turnada para su atención a la Dirección General de Tecnologías de la Información, el mismo veintiuno de mayo del presente año, a través del sistema electrónico de gestión interno de solicitudes de información previsto para esos efectos.

TERCERO. Que el titular de la Dirección General de Tecnologías de la Información del Banco de México, mediante oficio con referencia DGTI-78/2018, sometió a consideración de este Comité de Transparencia la determinación de ampliación del plazo ordinario de respuesta a la solicitud de acceso a la información.

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

QUINTO. Que el Titular de la Dirección General de Tecnologías de la Información, mediante oficio DGTI-91/2018, informó a este órgano colegiado su determinación de clasificar la información precisada en dicho escrito, en los términos ahí señalados, respecto de la cual se elaboró la correspondiente prueba de daño, contenida en el cuerpo del oficio en comento, y solicitó a este órgano colegiado confirmar tal clasificación.

BANCO DE MÉXICO

CONSIDERANDO

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

SEGUNDO. Enseguida se analiza la clasificación realizada por la unidad administrativa señalada en el resultando Quinto de la presente determinación, conforme a lo siguiente:

Este órgano colegiado advierte que es procedente la clasificación de la información señalada como **reservada,** toda vez que se ubica en los supuestos de reserva, en términos de **la fundamentación y motivación expresada en la prueba de daño** contenida en el oficio precisado en el resultando Quinto de la presente determinación, misma que se tiene por reproducida a la letra, en obvio de repeticiones innecesarias.

En consecuencia, **este Comité de Transparencia confirma la clasificación de la información referida como reservada, conforme a la fundamentación y motivación expresada en la correspondiente prueba de daño, contenida en el cuerpo del respectivo oficio precisado en el resultando Quinto de la presente determinación.**

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

RESUELVE

ÚNICO. Se **confirma la clasificación de la información referida como reservada,** conforme a la fundamentación y motivación expresada en la prueba de daño contenida en el oficio precisado en el resultando Quinto de la presente determinación.

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

COMITÉ DE TRANSPARENCIA

CLAUDIA ÁLVAREZ TOCA
Presidenta

HUMBERTO ENRIQUE RUIZ TORRES
Integrante

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente