REAL INSTITUTO elcano ROYAL INSTITUTE

JUNIO 2017
Nº 26

CIBERelcano

Informe mensual de ciberseguridad

Desarrollado por: THIBER

Copyright y derechos:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos-THIBER, the Cyber Security Think Tank

Todos los derechos de esta Obra están reservados a Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos y a THIBER, the Cyber Security Think Tank. Los titulares reconocen el derecho a utilizar la Obra en el ámbito de la propia actividad profesional con las siguientes condiciones:

a) Que se reconozca la propiedad de la Obra indicando expresamente los titulares del Copyright.
b) No se utilice con fines comerciales.
c) No se creen obras derivadas por alteración, trasformación y/o desarrollo de esta Obra.

Los titulares del Copyright no garantizan que la Obra esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados.

Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Obra son de propiedad exclusiva de los titulares correspondientes.

Informe editado en Madrid.

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank.

Índice

1 Comentario Ciberelcano 04

2 Análisis de actualidad internacional 06

3 Informes y análisis sobre ciberseguridad publicados en mayo de 2017..... 09

4 Herramientas del analista 10

5 Análisis de los ciberataques del mes de mayo de 2017.....12

6 Recomendaciones

6.1 Libros y películas 21

6.2 Webs recomendadas 24

6.3 Cuentas de Twitter.....24

7 Eventos.....25

1 COMENTARIO CIBERELCANO:

¿Estamos preparados para hacer frente a un ciberataque global?

AUTOR: Enrique Fojón Chamorro. Subdirector de THIBER, the cybersecurity think tank.

Fuente: NetworkWorld.com

Hace apenas tres semanas buena parte de la comunidad internacional sucumbió al caos provocado por el ransomware Wannacry. Cientos de compañías paralizaron su actividad -muchas de ellas de manera preventiva- con el consiguiente e incalculable impacto económico; los gabinetes de crisis convocados por la mayoría de los gobiernos del globo solo alcanzaban a transmitir un conjunto de recomendaciones que permitiesen mitigar los desconocidos efectos del ransomware; y la mayoría de los ciudadanos asistían desde el desconcierto y el desconocimiento a la última llamada de atención proveniente del ciberespacio.

Aunque será muy difícil (más bien imposible) determinar la autoría real de Wannacry, las principales potencias mundiales pusieron en marcha sus maquinarias informativas para influir en la opinión pública internacional, posicionando sus "teorías" en la batalla de las narrativas que se está librando. Corea del Norte, China, Rusia, Estados Unidos o bandas de cibercriminales de Europa del Este son solo algunos de los candidatos a "autores materiales" de Wannacry.

Aunque no hemos asistido aún a un ciberataque global de una capacidad destructiva relevante, ataques como Wannacry nos permiten conjeturar sobre las consecuencias que uno de

estos podría tener. En la actualidad, buena parte de los ciberataques globales siguen siendo pruebas de conceptos de agencias gubernamentales con un ámbito de actuación reducido y controlado. Quiza Wannacry fue una de esas pruebas de concepto que de una manera inesperada se descontroló.

Sea como fuere, resulta evidente que las principales potencias mundiales disponen de arsenales cibernéticos de primer nivel con capacidad para paralizar medio mundo. Un arsenal que está siendo utilizado ya en campañas de espionaje, información y desinformación y que quizá en un futuro sea utilizado para menoscabar las capacidades estratégicas de un adversario. Buena parte de estos arsenales están formados por las denominadas vulnerabilidades **0-Days**, aquellas que no son conocidas y, por tanto, son aprovechadas para menoscabar el funcionamiento de sistemas críticos de gobiernos y el sector privado. En este sentido, hace unos días Michael Daniel, coordinador de ciberseguridad de la Casa Blanca durante la época del presidente Obama, declaró:

"Revelar una vulnerabilidad puede significar que los Estados Unidos pierdan la oportunidad de recolectar inteligencia crucial que podría frustrar un ataque terrorista, detener el robo de propiedad intelectual de nuestro país e incluso descubrir las vulnerabilidades más peligrosas que están siendo utilizadas por hackers u otros adversarios para explotar nuestras redes. Por tanto, revelar las vulnerabilidades no es siempre la mejor opción"

En definitiva, la inmensa mayoría de la comunidad internacional no está preparada para responder ante un ciberataque global. Por tanto, no solo debe ser una prioridad política sobre el papel sino que muchos gobiernos deberán promover profundos cambios culturales que posibiliten acometer una importante transformación organizativa para maximizar las ventajas que el dominio cibernético puede proporcionar.

"las principales potencias mundiales disponen de arsenales cibernéticos de primer nivel con capacidad para paralizar medio mundo"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

La particular lucha de Irán para prevenir potenciales interferencias en sus elecciones

AUTORES: Miguel Ángel de Castro Simón. Senior Cybersecurity Analyst at ElevenPaths.
Yaiza Rubio. Analista de THIBER, the cybersecurity think tank. Analista de inteligencia en ElevenPaths

El uso de internet por parte de la población iraní es de un *68,5%* y al menos el 47% de la población se encuentra en la franja de edad de los *25 a los 54 años*. Acorde con estas estadísticas, los candidatos a la presidencia de Irán han utilizado las redes sociales como herramienta principal para la difusión de noticias. Pero, ¿qué medidas ha tomado Irán para prevenir cualquier tipo de interferencia de sus elecciones a la presidencia?

LA DELGADA LÍNEA ENTRE LA CENSURA Y LAS FAKE NEWS

Teniendo en cuenta que Twitter, Facebook y Youtube se encuentran bloqueados en Irán, la aplicación de mensajería Telegram e Instagram han sido las redes sociales más utilizadas por los candidatos, así como por sus ciudadanos, pero con ciertas limitaciones. En el caso de Telegram, aquellos grupos públicos con más de 5.000 usuarios debían ser notificados. A raíz de esta medida, a mediados de marzo se produjeron al menos doce arrestos de administradores de canales de Telegram, según el *Centro de Derechos Humanos en Irán.*

Candidato	Twitter	Facebook	Telegram	Aparat	Instagram
Rouhani	X	X	X		X
Jahangiri	X		X		X
Raisi			X	X	X
Ghalibaf			X	X	X
Hashemitaba					
Mirsalim	X	X	X	X	X

Con el objetivo de prevenir el impacto que tuvieron las noticias falsas en las elecciones presidenciales de Estados Unidos a través de Facebook, también llegaron a bloquear las llamadas de voz en Telegram, así como la funcionalidad de la retransmisión de los videos en directo de Instagram. Sin embargo, a pesar del control llevado a cabo, se registraron dos casos de noticias falsas a través de Telegram. El primero trataba sobre el asesinato de 27 personas en un centro comercial de Teherán y, el segundo, sobre supuestos avisos donde se alertaba de las actividades ilegales que estaban llevando a cabo la Policía de Internet de Irán (FATA) a través de esta red social.

No solo las redes sociales fueron objetivo de bloqueo. Ciertas páginas web han sido objetivo de la censura ejerciendo una represión continua contra los informadores, según afirma ***Reporteros sin Fronteras.*** De la misma forma, también se ha ejercido cierta represión sobre los movimientos estudiantiles procedentes de las universidades. 92 organizaciones de estudiantes escribieron una carta al presidente Rouhani expresando su preocupación por las amenazas a estudiantes después de la declaración de Alí Khamenei sobre la politización de los estudiantes. Decenas de estudiantes fueron expulsados por razones políticas entre ***2005 y 2016*** sin poder reanudar sus estudios.

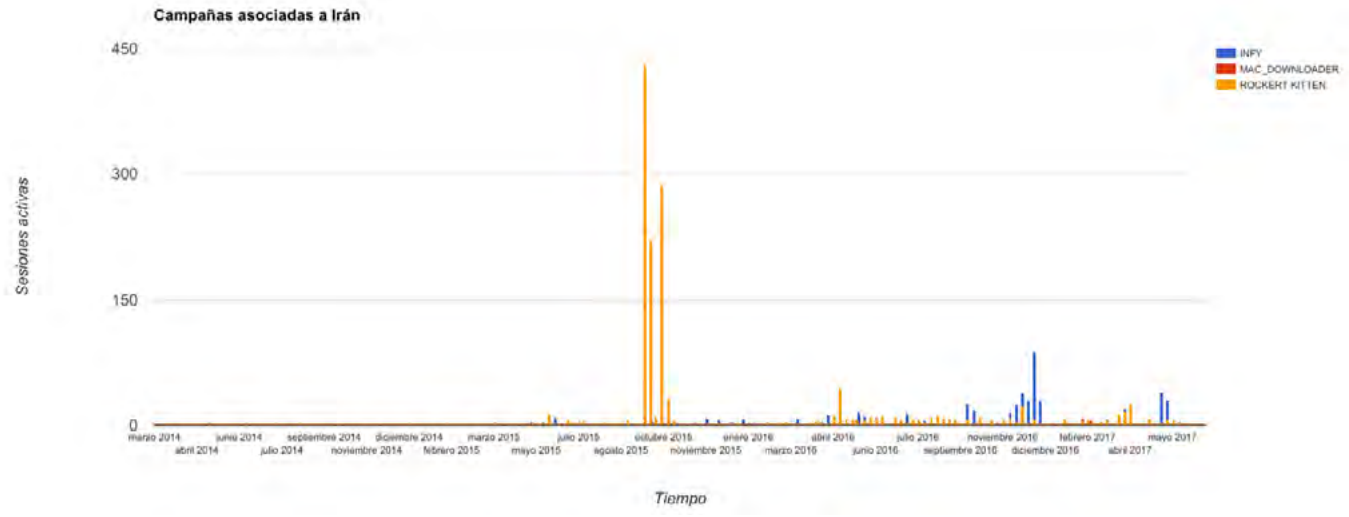
"Es necesario remontarse a 2010 con el descubrimiento de Stuxnet para identificar el primer ataque contra la República Islámica de Irán con impacto político, tanto interno como exterior."

DE VÍCTIMAS A VERDUGOS

Es necesario remontarse a 2010 con el descubrimiento de Stuxnet para identificar el primer ataque conocido contra la República Islámica de Irán con impacto político, tanto interno como exterior. Un año después, se detectó Duqu, muy parecido a Stuxnet, con la diferencia de que su cometido era obtener información sobre sistemas de control industrial. Ambos afectaban a infraestructuras críticas, especialmente, al desarrollo del programa nuclear iraní. Asimismo, también en 2012, se identificó Flame. *Malware* destinado a operaciones de ciberespionaje en Oriente Medio, en el que se encontraba a Irán entre sus objetivos, capaz de propagarse a otros sistemas través de la red local (LAN) y mediante memorias USB.

Sin embargo, esta situación ha cambiado. Recientemente, Irán ha sido señalado por diferentes ***investigadores de seguridad*** como autor de la creación de diferentes herramientas que les permitirían obtener información sensible o hacerse con el control de sistemas de individuos o de potencias extranjeras. Un ejemplo es MacDownloader, una pieza de *malware* desarrollada para sistemas Mac y que ha sido utilizada para atacar a contratistas de defensa de Estados Unidos y a defensores de los derechos humanos.

Otra herramienta perteneciente a su arsenal es Infy. Según investigadores de Palo Alto llevaría diez años en funcionamiento. En su diseño se incluyeron funcionalidades de obtención de datos y exfiltración de los mismos mediante técnicas de *keylogging* incluyendo en las últimas variantes funcionalidades de control remoto del sistema infectado. Las últimas muestras datan del 19 de marzo de 2017, apareciendo en multitud de sectores empresariales, principalmente en empresas orientadas a la venta mayorista, alta tecnología, telecomunicaciones y gobiernos. Por otro lado, también ha sido atribuida a Irán la campaña RocketKitten I y II en donde se utilizaba la navegación web como vía de infección con sectores afectados similares al resto de herramientas.



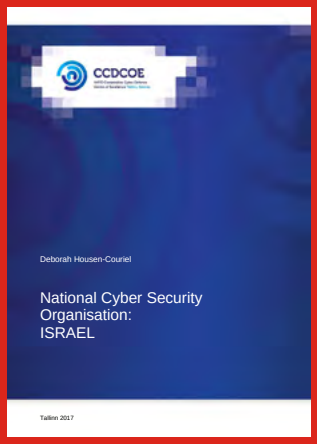
Evolución sobre el número de sesiones activas de cada pieza de *malware* o campaña.
Fuente: Elaboración propia.

Hassan Rouhani fue candidato a presidente en 2013 centrando su mensaje sobre la promesa de mejorar el acceso a internet y a la información. El pasado mayo volvió a salir reelegido y la política de internet sigue siendo clave para la población. Su éxito en este sentido ha sido mixto ya que el Consejo Supremo del Ciberespacio es el último órgano en la toma de decisiones sobre internet, en el que se incluye al poder judicial y a la Guardia Revolucionaria, pero se rinde cuentas directamente a Alí Jamenei.

3 Informes y análisis sobre ciberseguridad publicados en mayo de 2017

2017 CyberSecurity Annual Report (CISCO)

National Cyber Security Organization: ISRAEL (NATO CCD COE)



Risk or reward: What lurks within your IoT? (KPMG)

Worldwide Threat Assessment of US Intelligence Community (US ODNI)

Penquin´s Moonlit Maze (Kaspersky Lab)

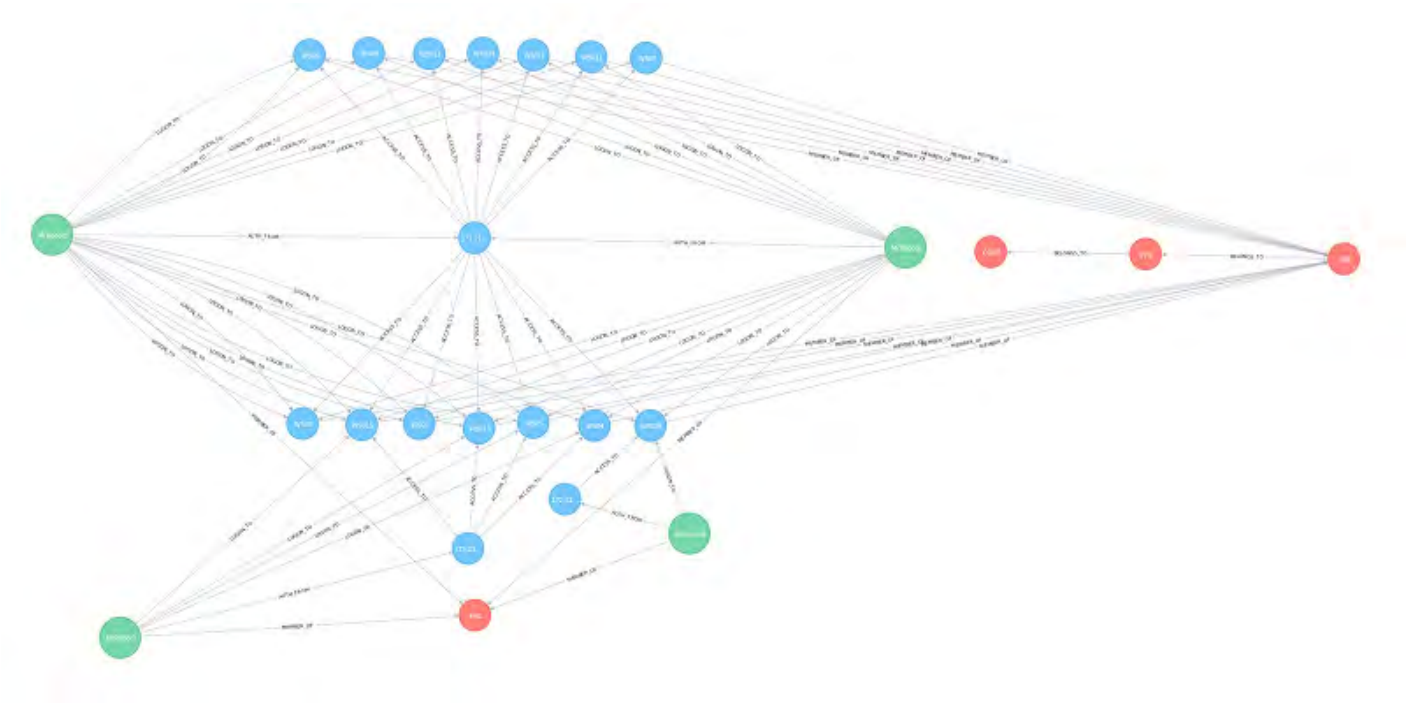
M-Trends 2017 (Mandiant)

Chinese cyber diplomacy in a new Era of Uncertainty (Hoover Institution)

Hacking UK Trident: A growing threat (BASIC)

4 HERRAMIENTAS DEL ANALISTA:
UserLine

Userline, es una herramienta de especialidad utilidad para analistas de seguridad y especialistas forenses informáticos para responder al quién, dónde y cuándo al analizar una actuación ilegítima de un insider en entornos Microsoft.



Esta herramienta de código abierto gratuita, desarrollada por Chema García, analista de *THIBER, the cybersecurity think tank*, automatiza el proceso de creación de relaciones de inicio de sesión desde eventos de seguridad de Microsoft Windows mostrando una relación gráfica entre los dominios de los usuarios, los inicios de sesión de origen y de destino, la duración de la sesión, quién ha iniciado sesión en los sistemas en una fecha determinada, etc. Proporciona diferentes modos de salida como la generación de un fichero CSV, inserción en una base de datos de grafos Neo4j, inserción en un SQLite, Gephi y Graphviz.

La herramienta *será presentada* en la afamada conferencia BlackHat 2017 que tendrá lugar en las Vegas en Julio.

```
$ ./userline.py -i ir-1329585-events-security-windows --last-shutdown

 /\ /\  ___  ___ _ __ / /(_)_ __   ___
/ / \ \/ __|/ _ \ '__/ / | | '_ \ / _ \
\ \_/ /\__ \  __/ | / /__| | | | |  __/
 \___/ |___/\___|_| \____/_|_| |_|\___|  v0.2.3b

Author: Chema Garcia (aka sch3m4)
        @sch3m4
        https://github.com/thiber-org/userline

INFO - Last shutdown:
INFO - Computer: ws01.evil.corp
INFO -  - Datetime: 2016-07-12 18:56:33+00:00
INFO -  - Uptime:   124 days, 23:24:03
INFO -  - EvtIndex: ir-1329585-events-security-windows
INFO -  - EvtId:    AVsRMBloEoASMdQErSf-
```

5 Análisis de los Ciberataques del mes de mayo de 2017

AUTOR: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.

CIBERCRIMEN

A comienzos de mes, la revista *Fortune* comunicó haber identificado a las dos empresas tecnológicas que se cree han sido víctimas de una estafa de unos 100 millones de dólares a través de un phishing. Las compañías no fueron identificadas en la primera nota pública del Departamento de Justicia estadounidense en marzo.

El Departamento de Justicia afirmó que, Evaldas Rimasauskas, de 48 años, se convirtió en un fabricante con sede en Asia y convenció a diversos empleados de las empresas víctimas de transferir dinero a cuentas bajo su control entre los años 2013 y 2015. Registró una compañía en Letonia que compartía el nombre con un fabricante asiático de hardware informático y abrieron cuentas en su nombre en múltiples bancos. A continuación, envió correos electrónicos de phishing a los empleados seleccionados en los que solicitaba el pago de los bienes y servicios legítimos ofrecidos por el fabricante asiático de ordenadores.

La revista Fortune afirma que las víctimas fueron Facebook y Google. En respuesta a un e-mail a Fortune, Facebook confirmó que fue una de las víctimas y dijo que recuperó la mayor parte de los fondos. Google posteriormente anunció que era la otra víctima. Rimasauskas fue detenido en Lituania en marzo y está a la espera de juicio.

Esta estafa de phishing que supuestamente impactó a Facebook y Google es un ejemplo de un vector de ataque conocido como Compromiso de Correo Electrónico Corporativo (BEC por sus siglas en inglés). Los actores involucrados en este tipo de esquemas utilizan múltiples métodos de ingeniería social para engañar a las empresas a enviar dinero o datos a actores maliciosos. Los criminales a menudo tienen un conocimiento significativo de las operaciones comerciales normales de la empresa objetivo y utilizan este conocimiento para adaptar sus operaciones a sus víctimas. Este vector de ataque es uno de los más lucrativos para el cibercrimen en Europa, siendo centenares sus víctimas.

Funcionamiento del Business Email Compromise (BEC) attack

Desde el 12 de mayo, se ha vivido una campaña de ransomware de la cepa WannaCry muy agresiva que ha estado impactando a organizaciones en todo el mundo y continúa planteando riesgos significativos a día de hoy. WannaCry explota una vulnerabilidad del protocolo SMB de Windows para permitir la propagación después de haber establecido un punto de pivotaje en un entorno informático (comportamiento típico de un gusano informático).

Inicialmente, algunas de las variantes distribuidas de WannaCry incluían un *killswitch* que el sector de la ciberseguridad aprovechó con éxito para ralentizar la propagación del malware.

Sin embargo, los operadores del malware han eliminado esta característica, como lo demuestra la aparición de diversas muestras que no incorporan esa funcionalidad.

El 14 de mayo, se identificó una nueva variante que no parece contener la funcionalidad *killswitch*. Sin embargo, diversos informes sugieren que este cambio puede haber sido implementado por un tercero después de que el malware fue complilado por sus operadores originales. El componente de ransomware de esta variante aparentemente parece mal programado y no funciona en algunos entornos.

Se estima que ha podido afectar a más de 200.000 equipos en tan solo tres días. El malware se propaga a versiones de Microsoft Windows que no aplicaron la actualización de seguridad de marzo de 2017 (MS17-010). El ataque deshabilitó operaciones en miles de entidades, en España y en otros países, como el Sistema Nacional de Salud del Reino Unido. El presidente de Microsoft, Brad Smith, afirmó que la vulnerabilidad explotada fue robada a la Agencia de Seguridad Nacional de Estados Unidos a principios de año por parte del grupo Shadow Brokers.

Ventana de Wannacry 2.0 pidiendo el rescate

A mediados de mes, se hacían públicos *diversos informes* que apuntaban a que varios atacantes externos robaron la próxima película de Disney "Piratas del Caribe: la venganza de Salazar", exigiendo un rescate, y que Disney se negaba a pagar la cantidad solicitada. Bob Iger, director ejecutivo de ABC (que es propiedad de Disney), comunicó a sus empleados que los cibercriminales habían amenazado con liberar los primeros cinco minutos de la película antes de la fecha de estreno para, posteriormente, publicar sucesivamente segmentos de 20 minutos si la compañía no pagaba el cuantioso rescate solicitado en bitcoins.

Si bien la autoría es desconocida, es necesario destacar que un actor criminal conocido como TheDarkOverlord recientemente llevó a cabo una actividad de extorsión similar dirigida Netflix. En ese momento, TheDarkOverlord alegó haber accedido a los títulos asociados con otras compañías prominentes del sector audiovisual norteamericano, haciendo posible que el mismo actor sea responsable de esta última amenaza a Disney.

CIBERESPIONAJE

A principios del mes de mayo, *la Oficina del Primer Ministro israelí* dijo que la Autoridad de Defensa Cibernética del país bloqueó un ataque importante contra las redes de computadoras del país en esa semana. En un anuncio, la Oficina del Primer Ministro afirmó que diversos correos electrónicos de phishing que parecían ser de una institución académica y una compañía privada fueron enviados a 120 instituciones, individuos y oficinas gubernamentales de Israel. Los archivos adjuntos eran documentos Word que contenían una vulnerabilidad 0 day.

Los ataques han sido identificados como llevados a cabo por un grupo de hackers conocido como OilRig, que diversos expertos en seguridad han vinculado en el pasado a Irán.

La Oficina del Primer Ministro ha estado tratando recientemente de otorgar amplios poderes a la Autoridad de Defensa Cibernética, una medida que ha sido controvertida en algunas partes del establishment de defensa en Israel.

El CERT israelí identificó públicamente dicha campaña dirigida a múltiples entidades israelíes con documentos que explotaban la vulnerabi-

lidad CVE-2017-0199. Esta campaña también incluía el uso del malware POWBAT. Se cree que esta actividad es consistente con la actividad de espionaje cibernético desarrollada por Irán en el pasado que utilizó anteriormente la familia de malware POWBAT dirigida a una amplia gama de organizaciones, incluyendo entidades gubernamentales, sector financiero, energía, telecomunicaciones, química, aviación civil y tecnología de la información.

Los actores asociados con el malware POWBAT han dirigido constantemente sus ataques contra entidades en Oriente Medio, con especial énfasis en Israel, Arabia Saudí, Emiratos Árabes Unidos y Qatar. Además, diversos análisis indican que la infraestructura relacionada con las muestras del malware POWBAT se superponen con los dominios asociados con la actividad del malware SEAWEED (Remexi) y CACHEMONEY (WinDollar) que se cree empleado por los servicios de inteligencia iraníes.

El primer ministro Benjamin Netanyahu en la conferencia Cyber Tech en enero.

También a principios de mayo el presidente de la agencia alemana de inteligencia, Hans-Georg Maasen, *indicó que el grupo ruso de hackers APT28* ha reunido "grandes cantidades de datos" durante una campaña de ciberespionaje lanzada en mayo del 2015 contra el Bundestag y que era decisión del Kremlin decidir si dichos datos serían utilizados para realizar operaciones de información y desestabilización durante las elecciones de septiembre en Alemania.

Maassen reiteró su convicción de que Rusia estaba aumentando las campañas de propaganda, ataques cibernéticos y otras acciones para desestabilizar la sociedad alemana. También dijo que ataques similares atacaron diversos cuerpos legislativos alemanes, a la canciller Angela Merkel, a la Unión Demócrata Cristiana (CDU) ya otras organizaciones. El gobierno alemán mostraba su preocupación ante una inundación de noticias falsas de origen ruso sobre el electorado alemán días antes de los comicios de septiembre.

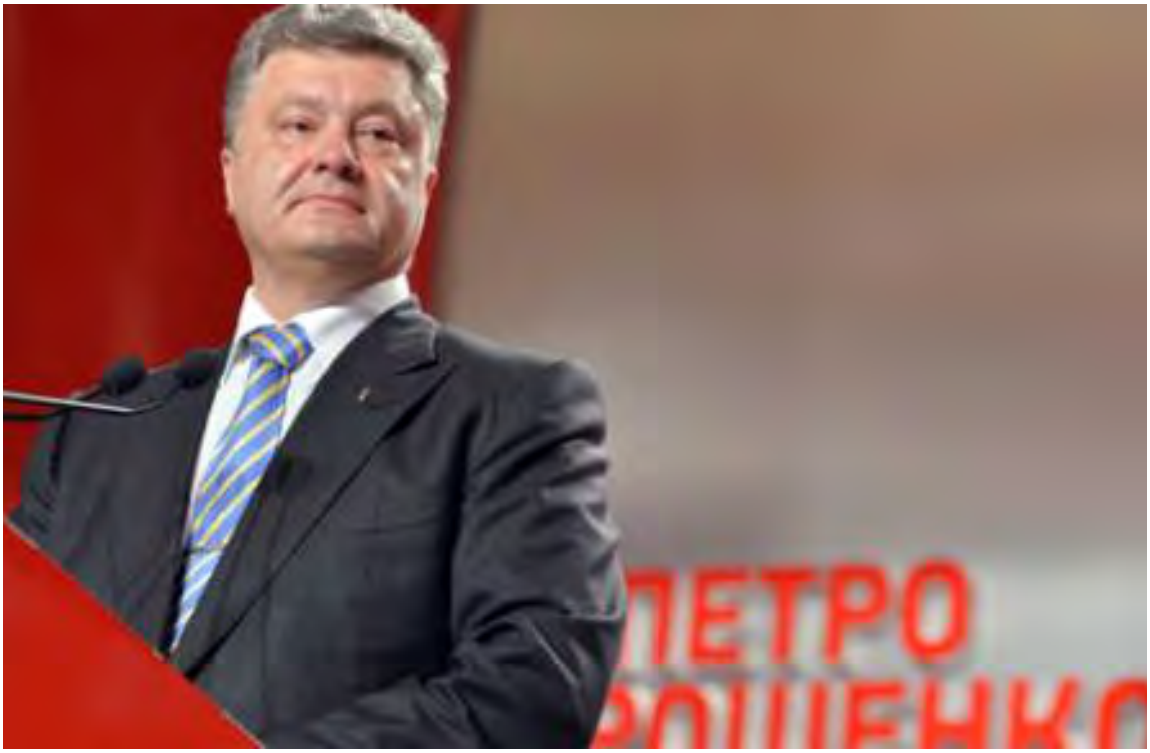
Ya con anterioridad, con una supuesta atribución rusa, diversos actores atacaron instituciones democráticas de Estados Unidos antes de las elecciones presidenciales con el mismo objetivo. Del mismo modo, la evaluación de Maassen de que el APT28 (conocido también como equipo zar) exfiltraba grandes cantidades de datos sería coherente con la actividad previamente identificada por este actor. Es plausible que estos actores pudieran utilizar fugas estratégicamente cronometradas, incluyendo materiales potencialmente alterados o totalmente fabricados, surgiendo antes de las elecciones alemanas con la intención de desacreditar a la canciller Merkel y Martin Schulz, dos de los candidatos menos alineados con los intereses del Kremlin. Se ha observado anteriormente la actividad de influencia rusa en Europa y en Alemania, promoviendo principalmente narrativas destinadas a debilitar la Unión Europea y la OTAN, e incitar a la ansiedad entre las poblaciones europeas con respecto a la crisis de los inmigrantes y refugiados sirios.

Hans-Georg Maassen, jefe de la Oficina Federal Alemana para la Protección de la Constitución (Bundesamt fuer Verfassungsschutz) en una foto de archivo.

El 16 de mayo, *Ucrania acusó a Rusia* de dirigir un ataque organizado contra la web del presidente Petro Poroshenko en respuesta a la imposición de sanciones por parte de Kiev contra múltiples negocios online y redes sociales rusas. Las sanciones se aplicaron ese mismo martes contra varios servicios online rusos, incluyendo Yandex, la mayor empresa online rusa, y los activos financieros de la empresa en Ucrania fueron congelados. Ahora hay más de 400 firmas rusas en la lista negra de Kiev desde la anexión rusa de Crimea en 2014. La portavoz del Ministerio de Relaciones Exteriores de Rusia, Maria Zakharova, calificó las sanciones de “clara manifestación de censura con motivación política”.

En una declaración en la página de Facebook de la administración presidencial, Dmytro Shymkiv, subjefe de la administración presidencial, especificó que el sitio web del presidente de Ucrania fue atacado por un ataque DDoS desde “recursos web de Yandex y VK”, dos entidades

que fueron prohibidas en las recientes sanciones contra empresas rusas. Aunque no está claro si estos recursos web se refieren a IPs utilizados para atacar el sitio web del presidente, los ataques DDoS pueden ser extremadamente difíciles de atribuir ya que la fuente del tráfico es fácilmente falsificable. Por lo tanto, a pesar del momento del ataque que sugiere que fue en represalia por las mencionadas sanciones, esta información por sí sola no es suficiente para atribuir el ataque a los actores patrocinados por el Estado ruso. Sin embargo, este ataque DDoS sigue patrones similares de ataques anteriores dirigidos a naciones tradicionalmente en la esfera de influencia rusa para prevenir o socavar las políticas antirusas percibidas, como los ataques DDoS contra los medios de comunicación en Montenegro tras las acusaciones de posible participación rusa en un reciente intento de golpe de Estado.



El presidente ucraniano, Petro Poroshenko, en el momento de las declaraciones

HACKTIVISMO

El 3 de mayo a las 7:00 pm CEST, dos horas antes del inicio del debate presidencial francés, un *actor anónimo envió dos documentos cuestionables* al foro 4chan, alegando que los documentos demuestran los vínculos entre Macron y una compañía en las Bahamas, mostrando que Macron había ocultado estos activos al gobierno.

Diversos analistas realizaron un seguimiento de la propagación inicial de los documentos y las reclamaciones asociadas identificándose principalmente sujetos de habla inglesa de la comunidad de ultra derecha alt-right que en Twitter diseminó reclamaciones y enlaces a los documentos con el objetivo declarado de ayudar a Le Pen ganar las elecciones.

A las 9:00 pm CEST, la noticia de la existencia de los documentos se circuló en sitios de noticias marginales; el 4 de mayo, los medios de comunicación internacionales habían recogido el suceso.

Anteriormente se había observado que los partidarios de Le Pen de alt-right se coordinaron para promover la propaganda política en redes sociales, incluso en francés, aunque con un impacto limitado. Los actores, potencialmente incluyendo agentes de gobiernos extranjeros, podrían hacerse pasar como miembros de estas comunidades y aprovechar un gran número de participantes en medios sociales para difundir rápidamente su propaganda anti Macron.

Nicolas Vanderbiest, colaborador de France Culture, escribió en Twitter: "Así que la falsa noticia sobre la cuenta de Macron en las Bahamas, podemos decir sin ser engañosa, que es de origen ruso".

Antes de la elección de Emmanuel Macron como presidente francés, la comisión electoral del país *advirtió a los medios de comunicación franceses que no publicaran el contenido de los correos electrónicos hackeados.* La comisión advirtió que cualquier persona que circulase la dicha información podría estar cometiendo un crimen.

El 5 de mayo, la campaña de Macron fue víctima de un "ataque de hacking masivo", resultando en cientos de documentos internos publicados online. Un usuario anónimo publicó enlaces a unos 9 GB de datos en un post de Pastebin titulado "EMLEAKS" que coincide con el inicio de una moratoria a nivel nacional sobre la cobertura de medios relacionados con las

elecciones. La campaña de Macron dijo que los datos incluían documentos inocuos normales junto con documentos falsos insertados como medidas de contrainteligencia.

La descarga de EMLEAKS parece haber sido programada estratégicamente para influir en el discurso político durante el fin de semana electoral y socavar el llamamiento electoral de Macron. Esta actividad también es consistente con el reciente enfoque de los presuntos actores agresivos en medios sociales rusos que intentan promover narrativas anti-Macron y pro-Marine Le Pen en el contexto de las elecciones francesas.

Tweet de Wikileaks haciéndose eco de los EMLeaks

A finales del mes de mayo, *el gobierno de Qatar comunicó* que diversos ciberatacantes consiguieron acceder a la página web de su agencia de noticias estatal, Qatar News Agency (QNA), publicando supuestamente falsas declaraciones del Emir que han sido polémicas.

La historia hizo que Arabia Saudí y los Emiratos Árabes Unidos bloquearan los medios de comunicación de Qatar, incluyendo Al-Jazeera. En el artículo creado por los atacantes, el actual Emir, el jeque Tamim bin Hamad Al Thani, hacía comentarios polémicos con respecto a Israel e Irán.

El telegrama del informativo nocturno de la televisión estatal de Qatar mostró comentarios falsos, llamando a Hamas "el representante legítimo del pueblo palestino", y dijo que Qatar tenía "fuertes relaciones" con los Estados Unidos e Irán. "Irán representa un poder regional e islámico que no puede ser ignorado y es imprudente enfrentarse a él", dijo el comunicado. "Es una gran potencia en la estabilización de la región".

Según los informes, los atacantes también se hicieron con el control de la cuenta de Twitter de la agencia de noticias y publicaron falsas citas del ministro de Relaciones Exteriores de Qatar afirmando que existía un complot contra el país por otras naciones árabes. Los tweets fueron eliminados rápidamente. El director de la oficina de comunicaciones del gobierno de Qatar emitió un

comunicado diciendo que las declaraciones eran falsas, pero no explicó cómo ocurrió.

El artículo y los tweets de QNA incluyen declaraciones que son perjudiciales para los intereses nacionales de Qatar, dando crédito a las demandas de QNA que fueron falsificadas. Por ejemplo, el artículo incluye declaraciones destinadas a inflamar las divisiones entre Qatar y sus vecinos; declaraciones polémicas sobre Irán, el terrorismo y el proceso de paz palestino-israelí.

Publicar artículos de noticias o comunicados de prensa falsos en sitios web comprometidos no es una táctica novedosa. En junio de 2016, la agencia estatal jordana de medios de comunicación y el diario saudí Al-Watan sufrieron ataques similares en los que se distribuyeron falsos artículos que presuntamente citaban a miembros de la familia real saudí.

Un empleado de Qatar de canal de noticias de la lengua árabe de Al Jazeera camina más allá del logotipo de Al Jazeera en Doha, Qatar.

6 Recomendaciones

6.1 Libros y películas

Película:
EL CÍRCULO

Sinopsis: 'El Círculo' es la adaptación cinematográfica del best-seller de Dave Eggers. Mae Holland, una mujer que consigue la oportunidad de su vida al empezar a trabajar en el Círculo, la compañía tecnológica más influyente del mundo donde se involucra con un hombre misterioso. Este thriller muestra los peligros de la vida en la era digital. El Círculo rastrea las contraseñas de los usuarios para obtener los datos personales recogidos en su email, sus redes sociales y sus operaciones bancarias para utilizarlos posteriormente contra ellos empleando un innovador sistema operativo. Esto hace que la privacidad sea ahora un privilegio con el que muchos no pueden contar.

Libro:
MICROHISTORIAS: ANÉCDOTAS Y CURIOSIDADES DE LA INFORMÁTICA

Autor: Rafael Troncoso y Francisco José Ramírez
Num. Páginas: 280
Editorial: 0xWORD
Año: 2016
Precio: 22.00 Euros
Sinopsis: ¿Sabías que Steve Jobs le llevó en persona un ordenador Macintosh a Yoko Ono y también a Mick Jagger? ¿O que Steve Wozniak, después de crear el mítico ordenador Apple II dejó su querida empresa Apple para crear otra que fabricaba mandos a distancia? ¿Y que Jay Miner, el genio que creó el Amiga 1000 tenía una perrita que tomaba parte en algunas de las decisiones de diseño de este ordenador? ¿O que Xenix fue el sistema Unix más usado en los 80s en ordenadores personales y que éste era propiedad de Microsoft? Estas son sólo algunas de las historias y anécdotas que encontrarás en este libro de Microhistorias.

Libro:
CRIME INVESTIGATION

Autor: Felipe Colorado
Num. Páginas: 280
Editorial: 0xWORD
Año: 2016
Precio: 18.00 Euros
Sinopsis: ¿Un atentado en la Casa Blanca? La caída de Silk Road y Kickass Torrent. Un diputado en una oscura trama de chantaje desde la Deep Web. Espías rusos, grupos militares chinos, pistoleros yihadistas en California. Carders, el secretario general de Interpol, narcos, hacktivistas, servicios secretos…
El autor afila su pluma, en una intensa labor de recopilación y divulgación, desentrañando los más impactantes casos reales de Informática Forense y Hacking.

Libro:
BLOCKCHAIN: LA REVOLUCIÓN INDUSTRIAL DE INTERNET

Autor: Alexander Preukschates
Num. Páginas: 288
Editorial: EDICIONES GESTION 2000
Año: 2017
Precio: 11,00 Euros
Sinopsis: Alexander Preukschates asesor de empresas para la definición de estrategias y gestión de proyectos relacionados con Blockchain. En su vida profesional ha ejercido como consultor de estrategia y responsable de negocio de diversas startups.

La tecnología Blockchain tiene el potencial de revolucionar el mundo de la misma forma que el Internet de la Información a través del Internet del Valor que se basa en Blockchain. En este libro, expertos españoles en esta nueva tecnología, exploran las aplicaciones potenciales del Blockchain en diferentes industrias y sectores profundizando también en el entendimiento del movimiento de la descentralización y las bases de la tecnología que la hacen posible.

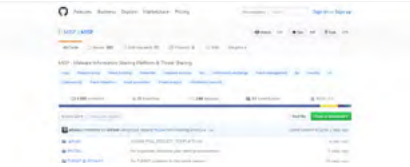
Libro:
CIBERSEGURIDAD: LA COOPERACIÓN PÚBLICO-PRIVADA

Autor: Varios
Num. Páginas: 367
Editorial: CESEDEN
Año: 2017
Precio: Gratuito
Sinopsis: Algunos de los expertos nacionales identifican las tendencias actuales y futuras de la ciberseguridad y estudian la oportunidad de colaboración público-privada realizando propuestas prácticas que permitan la consecución de los mayores beneficios al sector de la ciberseguridad.

6.2 Webs recomendadas

https://www.govcert.admin.ch/
Sitio web del CERT gubernamental de Suiza.

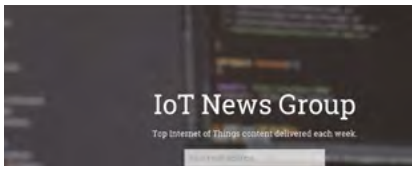
https://github.com/MISP/MISP
Github del proyecto Malware Information Sharing Platform (MISP).



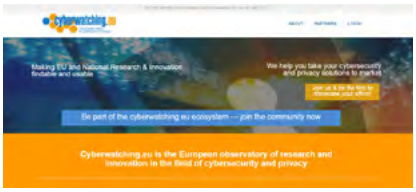
https://nccoe.nist.gov/
Sitio web del Centro Nacional de Ciberdefensa de los Estados Unidos.

https://ccdcoe.org/cycon-2017.html
Sitio web de la Cyber Security Conference organizada por el NATO Cyber Defence Centre of Excellence.

http://iotnewsletter.org/
Sitio web que agrega información relacionada con las tecnologías IoT.



http://www.cyberwatching.eu/
Sitio web del Observatorio Europeo de Ciberseguridad, para promover la innovación en Ciberseguridad y Privacidad.



6.3 Cuentas de Twitter

@dsn

@dlargacha

@CERTAFr

@CertUC3M

@GovCERT_CH

7 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
2 - 4 junio	Moscú	moscowc0n	moscowc0n	https://moscowc0n.com
1 Junio	Munich	e-Crime & Cybersecurity Germany	The 9th e-Crime & Cybersecurity	http://www.e-crimecongress.org/event/germany
5- 6 Junio	Lisboa	ISEG, University of Lisbon	2017 European Security Conference	http://secconf.iseg.ulisboa.pt/
6- 8 junio	Londres	InfoSecurity	Information Security Europe	http://www.infosecurityeurope.com/
7 junio	Barcelona	SegurInfo	Segurinfo España 2017	http://segurinfo.org/home.php
7-8 junio	Madrid	ISACA	High Level Conference 2017	http://www.isaca.org/chapters7/madrid/events/eventos/pages/high-level-conference.aspx
8 junio	Londres	RSA	RSA Conference Unplugged 2017: London	https://www.rsaconference.com/events/ldn17
12 - 13 junio	Berlín	Security of Things World	Security of Things World 2017	http://securityofthingsworld.com/en/
13 junio	Gibraltar	The Gibraltar Cyber Security Summit	Gibraltar Cyber Security Summit	https://www.gibcyber.com/
14 junio	Londres	Unlocked	Unlocked London	https://unlocked.events/
14 -15 junio	Kiev	GCS	Global Cybersecurity Summit 2017	https://gcs17.com/
19 - 23 junio	París	Hack in Paris	Hack in Paris	https://hackinparis.com/
22 junio	Madrid	Red Seguridad	IX Encuentro de la Seguridad Integral (Seg2)	http://www.redseguridad.com/eventos/agenda-del-sector/ix-encuentro-de-la-seguridad-integral-seg2
23 - 24 junio	Donostia	ASOCIACIÓN DE SEGURIDAD INFORMÁTICA EUSKALHACK	EuskalHack Security Congress	https://securitycongress.euskalhack.org/
25 - 29 junio	Tel Aviv	Ministry of Foreign Affairs of Israel	Cyber Week 2017 Israel	https://cyberweek.tau.ac.il/2017/index.php
27 junio	Alcobendas	Logitek	MATconference: Ciberseguridad en la Industria 4.0 e Infraestructuras críticas	http://www.meetandtalkevents.com/ciberseguridad-en-la-industria-4-0-e-infraestructuras-criticas/

Patrocinadores

GOBIERNO DE ESPAÑA — MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

GOBIERNO DE ESPAÑA — MINISTERIO DE DEFENSA

GOBIERNO DE ESPAÑA — MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

GOBIERNO DE ESPAÑA — MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

ACERINOX · AIRBUS GROUP · ATLANTIC COPPER · BBVA

enagas · IBERDROLA · IBM · INDITEX

indra · CaixaBank · MUTUAMADRILEÑA · OHL

tecnalia Inspiring Business · RED ELÉCTRICA DE ESPAÑA · renfe · REPSOL

Santander · Telefónica

Consejo Asesor Empresarial

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA · endesa · gasNatural fenosa

IBERIA · Fundación Cajasol · Escribano Mechanical & Engineering

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269