REAL INSTITUTO elcano ROYAL INSTITUTE

NOVIEMBRE 2017
Nº 30

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 octubre 09

4 Herramientas del analista 10

5 Análisis de los ciberataques del mes de octubre 12

6 Recomendaciones

6.1 Libros y películas 19

6.2 Webs recomendadas 21

6.3 Cuentas de Twitter.....21

7 Eventos.....22

1 COMENTARIO CIBERELCANO:
La ciberguerra de Trump (III)

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

Participantes durante el ejercicio Cyber Guard 2016. Fuente: *www.defence.gov*

En abril de 2015, el secretario de Defensa Ashton Carter presentaba *la estrategia cibernética del Departamento de Defensa de los Estados Unidos.* Dicha estrategia enunciaba cinco objetivos y un conjunto de planes que debían implementar para alcanzarlos. Uno de estos objetivos era la creación de una ciberfuerza bajo el mando del U.S Cyber Command, que recientemente ha adquirido la categoría de *Mando Combatiente Unificado.* Esta ciberfuerza deberá estar operativa en 2018 y dispondrá de un total de 6.200 profesionales integrados en 133 equipos "Cyber Mission" repartidos de la siguiente manera:

- 13 equipos "National Mission" que tienen como objetivo la defensa de los intereses de los Estados Unidos ante ciberataques a gran escala.
- 68 equipos "Cyber Protection" que tienen como objetivo la protección de los sistemas de información y comunicaciones del Departamento de Defensa.
- 27 equipos "Combat Mission" que tienen como objetivo apoyar a los diferentes Mandos Combatientes mediante la generación de "efectos" en el ciberespacio para el apoyo a las operaciones en curso.

· 25 equipos “Support “ que tienen como objetivo apoyar a los “National Mission” and “Combat Mission” en sus tareas.

El 21 de octubre de 2016, el *Pentágono anunciaba que los 133 equipos habían alcanzado la Initial Operational Capability (IOC)*, es decir, todas las unidades disponían de las capacidades mínimas necesarias para desempeñar buena parte de las tareas que tenían asignadas. El pasado 2 de noviembre, la U.S Navy y el U.S Army anunciaban que sus equipos “Cyber Mission” – con un año de antelación según el calendario previsto- habían alcanzado la Full Operational Capability (FOC), es decir, disponían ya de todas las capacidades y el personal formado y entrenado, según los criterios marcados por el U.S Cyber Command, para ejercer con garantías todas las tareas encomendadas. En los próximos meses se espera que los equipos integrados en el U.S Marine Corps y U.S Air Force alcancen la FOC.

Uno de los principales retos a los que se deberá enfrentar el Pentágono será mantener una ciberfuerza operativa, formada y entrenada con las capacidades necesarias para hacer frente a los múltiples retos que un dominio tan mutante como el ciberespacio impone. Para ello, el desarrollo de *capacidades Cyber Range* y Cyber Lab serán imprescindibles. Además, la nueva política de contratación del Departamento de Defensa posibilitara incentivar la captación y retención del talento necesario para luchar en el ciberespacio.

En definitiva, la Administración Trump apuesta por la creación de una ciberfuerza que garantice la seguridad y defensa del país, cada vez más dependiente del dominio cibernético. En los próximos años veremos cómo crecen las inversiones no solo para la adquisición de cibercapacidades (defensivas, ofensivas y de inteligencia) sino para la captación, retención, formación y entrenamiento de la ciberfuerza del país.

“La Administración Trump apuesta por la creación de una ciberfuerza que garantice la seguridad y defensa del país, cada vez más dependiente del dominio cibernético.”

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Maksim, uno de los atacantes más prolíficos para Android, aumenta su actividad maliciosa

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

No es nuevo que la circulación de malware ha crecido de forma sustancial en los últimos años. Según estudios realizados por Nokia, se estima que se ha logrado elevar las cifras de infección en un 400% durante 2016, en donde el 86% de los equipos infectados son dispositivos móviles. En este sentido, según las bases de datos de amenazas de las que dispone *ElevenPaths*, a partir de mayo de 2016, comenzó a detectarse una amenaza que afectaba a dispositivos Android de la que, según la Figura 1, se pudo identificar un repunte de conexiones activas el pasado mes de marzo.

Número de las sesiones activas de las piezas de malware vinculadas al arsenal de Maksim.

El actor llamado Maksim descargaba aplicaciones legítimas y populares, las desempaquetaba e introducía el código malicioso para luego distribuirlas troyanizadas a través de webs de aplicaciones, la gran mayoría de juegos. Gran parte de las infecciones se realizaron a través de la navegación web, además de haberse detectado que las industrias más afectadas por esta amenaza han sido la industria al por mayor y la destinada a la alta tecnología. Asimismo, la amenaza procedería de países como Rusia, Alemania y Holanda con un mayor impacto en Estados Unidos y Armenia.

"El actor llamado Maksim descargaba aplicaciones legítimas y populares, las desempaquetaba e introducía el código malicioso para luego distribuirlas troyanizadas a través de webs de aplicaciones, la gran mayoría de juegos."

HERRAMIENTAS

Se le ha podido atribuir numerosas aplicaciones maliciosas a través de la correlación de los apk disponibles en las webs manejadas por el atacante. Además, son muchas y variadas las funcionalidades detectadas en las aplicaciones que utiliza en su arsenal, entre las que se encuentran las siguientes:

- **Inyecta troyanos en aplicaciones legítimas** cuyo objetivo era entregar publicidad a las víctimas, enviar SMS e incluso obtener el control administrativo y remoto del dispositivo. Otro de los troyanos utilizados incorporaba sistemas legítimos para protegerse del análisis y la detección del mismo. Adicionalmente, mostraba un alto nivel de sofisticación al ser capaces de omitir el sistema de aviso de carga, utilizado para notificar a los usuarios el precio de un servicio Premium y requerir la autorización del usuario.

- **Incorpora librerías de Adware** en aplicaciones legítimas para obtener información de los dispositivos como las aplicaciones instaladas o ejecutándose, el operador y la geolocalización entre otra información para ser enviada al servidor *command and control* (C&C). Algunas de estas librerías usan el método ClassLoader clásico que permite cargar y ejecutar código dinámicamente.

- **Usa familias de malware** con capacidad de enviar información del dispositivo a un servidor de *command and control.* En este sentido, enviaba SMS a instituciones financieras para consultar saldos de cuenta, cargaba cualquier SMS entrante (incluidos los resultados de la consulta de saldo) en el servidor C2, envía SMS a números de teléfono de los contactos de la víctima y reenvía las llamadas entrantes para interceptar la autenticación en dos pasos basadas en voz.

- **Utiliza troyanos SMS** con amplias funcionalidades como pueden ser el envío de mensajes de texto Premium a un número específico o el envío de mensajes de texto generalmente con un enlace a una web manejada por sí mismo o a una amenaza diferente. Usualmente obtiene la lista de contactos y los mensajes de texto del dispositivo de la víctima o incluso borra los mensajes de texto entrantes que cumplan con los criterios establecidos por el C&C.

- **Utiliza *ransomware*** específicamente diseñado para Android, el cual bloquea la pantalla y no sólo cifra los archivos existentes, sino que también infecta los ejecutables, actuando así como un virus parásito

TÉCNICAS

Maksim utiliza diversas técnicas para la distribución del malware. La más utilizada consiste en registrar dominios y publicar aplicaciones legítimas con código malicioso inyectado. Sin embargo, en otra de sus campañas, se han identificado una serie de subdominios maliciosos registrados bajo un dominio legítimo perteneciente a un conocido proveedor de servicios de alojamiento compartido en Rusia.

En este sentido, para atraer a las víctimas a que descargaran el malware, en ocasiones, realizaba un ataque de phishing por SMS en el que se incluía una URL maliciosa. De esta manera, al hacer click, el dispositivo de la víctima quedaría infectado. Y, por último, otra de las técnicas comunes usadas por este threat actor es el uso de instaladores que aparentemente parecen de otras aplicaciones.

Este es un ejemplo de la necesidad de reforzar la seguridad en los dispositivos móviles. Sin embargo, los usuarios también deben tener en cuenta, como se ha podido ver en este ejemplo, cuáles son los riesgos de descargar aplicaciones desde markets no oficiales.

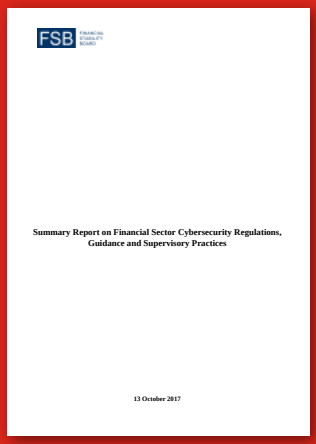
"Este es un ejemplo de la necesidad de reforzar la seguridad en los dispositivos móviles. Los usuarios también deben tener en cuenta, cuáles son los riesgos de descargar aplicaciones desde markets no oficiales."

3 Informes y análisis sobre ciberseguridad publicados en octubre de 2017

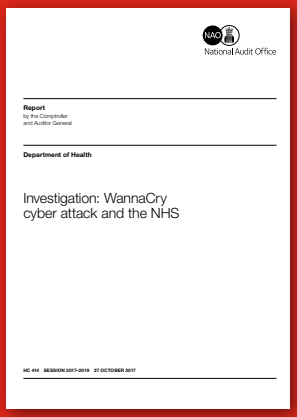
Cyber Threat-Scape Report (Accenture)

The healthy approach to cyber security (KPMG)

Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices (Financial Stability Board)



Investigation: WannaCry cyber attack and the NHS (UK National Audit Office)



Cyber Security: Small Business Guide (UK National Cyber Security Centre)

Empty Threat or Serious Danger? Assessing North Korea's Risk to the Homeland (The George Washington University)

Política Nacional de Ciberseguridad en Chile (Derechos Digitales)

The Cybridisation of EU Defence (ETH Zurich)

4 HERRAMIENTAS DEL ANALISTA:
Threat Intelligence Hunter

Threat Intelligence Hunter es una herramienta opensource de inteligencia que permite buscar indicadores de compromiso (IoCs) en múltiples fuentes de seguridad disponibles gratuitamente y algunos servicios a través de API. La idea detrás de la herramienta es facilitar la búsqueda y el almacenamiento de IoCs agregados frecuentemente para crear su propia base de datos local de indicadores.

Desarrollada en el ámbito del Proyecto ThreatHunting, la herramienta está focalizada para falicitar un tipo de *hunting* de indicadores analítico, que implica escribir código para filtrar y procesar grandes cantidades de datos y descubrir los posibles vectores de ataques sobre la infraestructura tecnológica. La solución está sustentada en herramientas de búsqueda desarrolladas en Python y Jupyter.

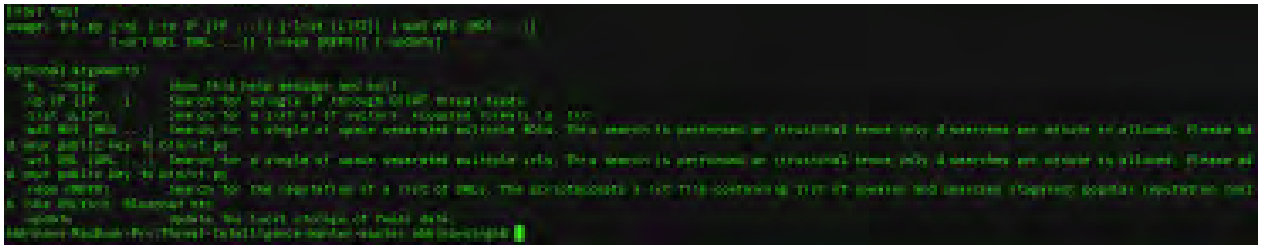
Sin embargo, uno de los obstáculos con los que suele afrontar un *hunter* o un analista de inteligencia nuevo es descubrir cuál será su *stack* de análisis y luego hacer que todas las piezas trabajen juntas. Para hacer esto un poco más fácil, esta herramienta de análisis de datos basado en Python, Pandas, PySpark y Jupyter Notebook permite facilitar dichas tareas. Hunter empaqueta herramientas de análisis de Big Data de alto rendimiento que pueden ejecutarse en un PC. Para ayudar a que sea lo más fácil posible poner la pila de herramientas en funcionamiento, han sido desplegadas en un contenedor Docker para que pueda instalar y ejecutar el sistema con un solo comando.

Las siguientes herramientas están incluidas en la solución:

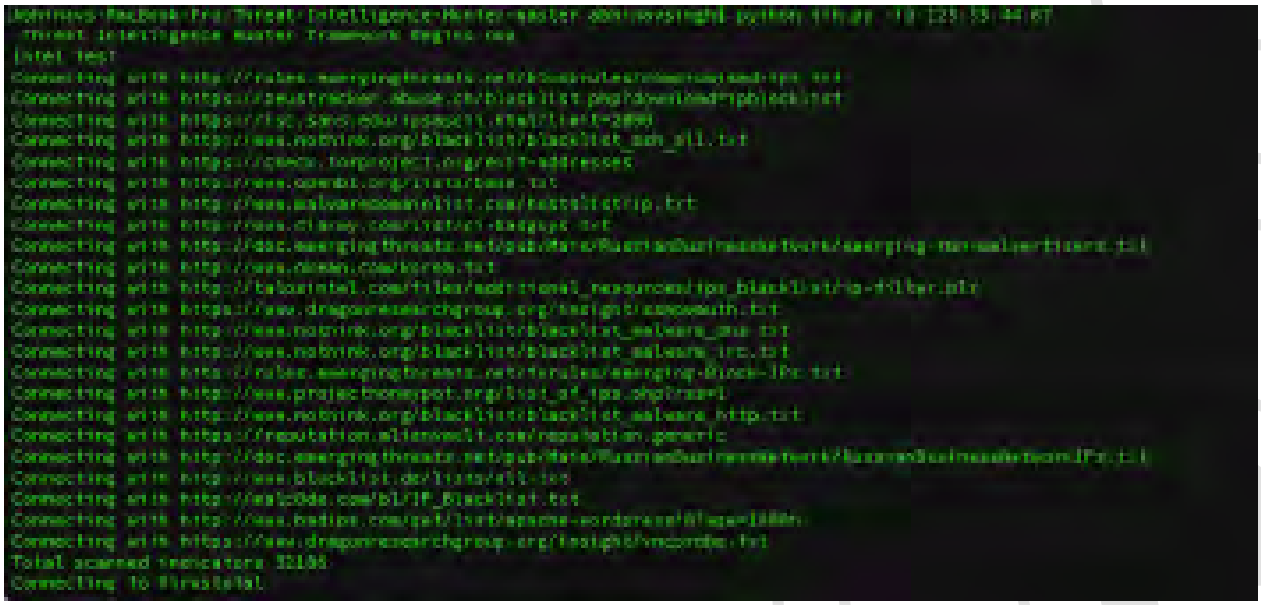
· Python 2 & 3
· Apache Spark 2.0 with PySpark
· Jupyter Notebook
· seaborn
· matplotlib
· Plotly (módulo Python para crear gráficos y visualizaciones)
· pandas
· numpy
· scikit-learn
· Módulos elasticsearch y elasticsearch-dsl (high-level ES client)
· Splunk SDK for Python

Las características principales son:

· Almacenamiento local de amenazas: permite actualizar periódicamente su almacenamiento local desde los feeds listados en el script feeds.py., pudiendo agregar una lista propia.



· Verificar una IP contra los feeds de amenazas existentes y la base de datos local
· Verificar la lista de direcciones IP en bloque (en un archivo de texto)
· Comprobar si hay hash MD5
· Verificar la presencia URL en una lista negra
· Comprobar la reputación de IPs y/o URLs (Actualmente admite URLVoid y Virustotal)



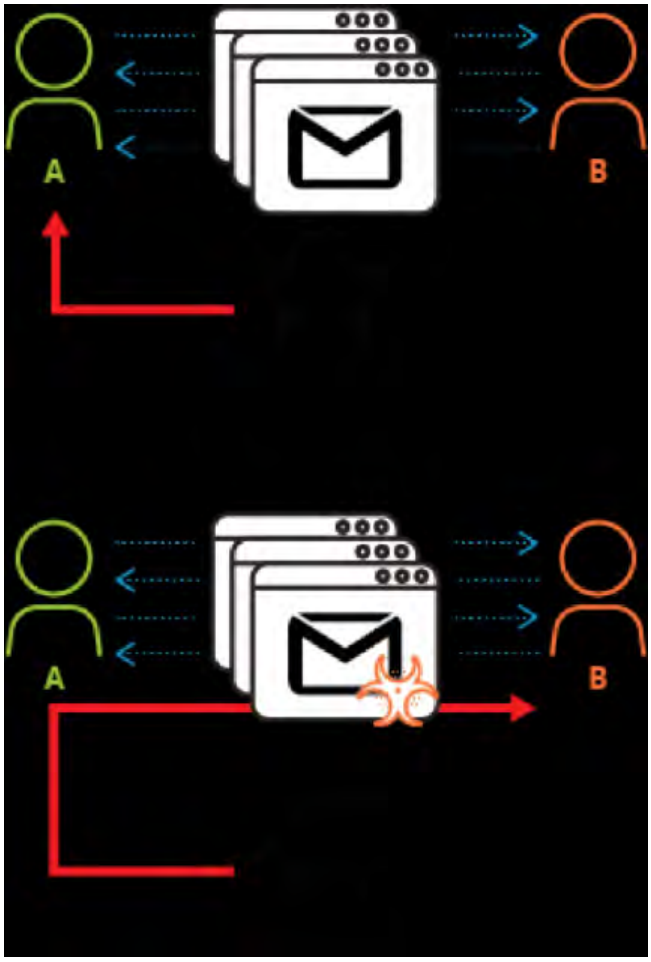
5 Análisis de los Ciberataques del mes de octubre de 2017

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

CIBERCRIMEN

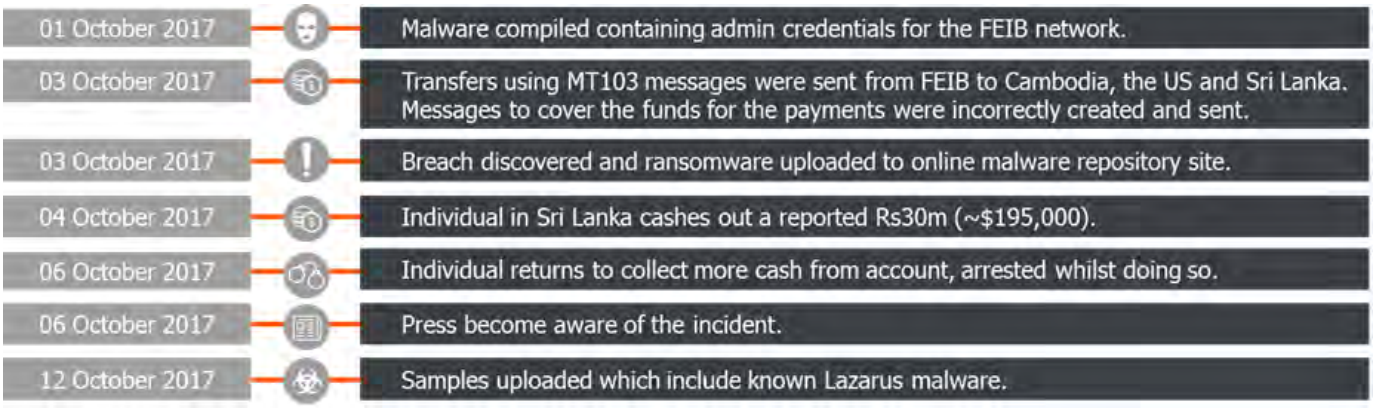
El día 7 de octubre *investigadores de Palo Alto* publicaron una investigación en la que se analizaba una nueva campaña de spear-phishing en la que los atacantes interceptaban una conversación continua a través de correo electrónico, se hacían pasar por uno de los participantes y engañaban a la otra parte para que descargase malware. La campaña, llamada FreeMilk, aprovecha una vulnerabilidad de ejecución remota de código de Microsoft (CVE-2017-0199) y personaliza el contenido señuelo para cada objetivo. Los atacantes primero interceptan una conversación por correo electrónico, haciendo que el objetivo crea que todavía está conversando con la persona original. Luego envían archivos adjuntos maliciosos a través de emails de phishing que contienen dos malware llamados PoohMilk y Freenki. La función de PoohMilk es ejecutar el downloader Freenki, mientras que Freenki recopila información sobre el sistema objetivo, incluida la dirección MAC, el nombre de usuario, el nombre de la máquina y los procesos que se ejecutan en dicho sistema. Freenki también puede tomar capturas de pantalla y enviarlas a un servidor de mando y control (C&C) para que los atacantes puedan explotar y descargar software malicioso adicional.

Los investigadores dicen que la campaña FreeMilk está en curso y está siendo dirigida a una amplia gama de víctimas en varias regiones del mundo como Egipto, Japón, Vietnam y Corea del Sur, así como a los objetivos relacionados con el Comité Olímpico Internacional y los grupos de derechos humanos vinculados a Naciones Unidas.



Esquema del secuestro de conversaciones para distribuir malware.

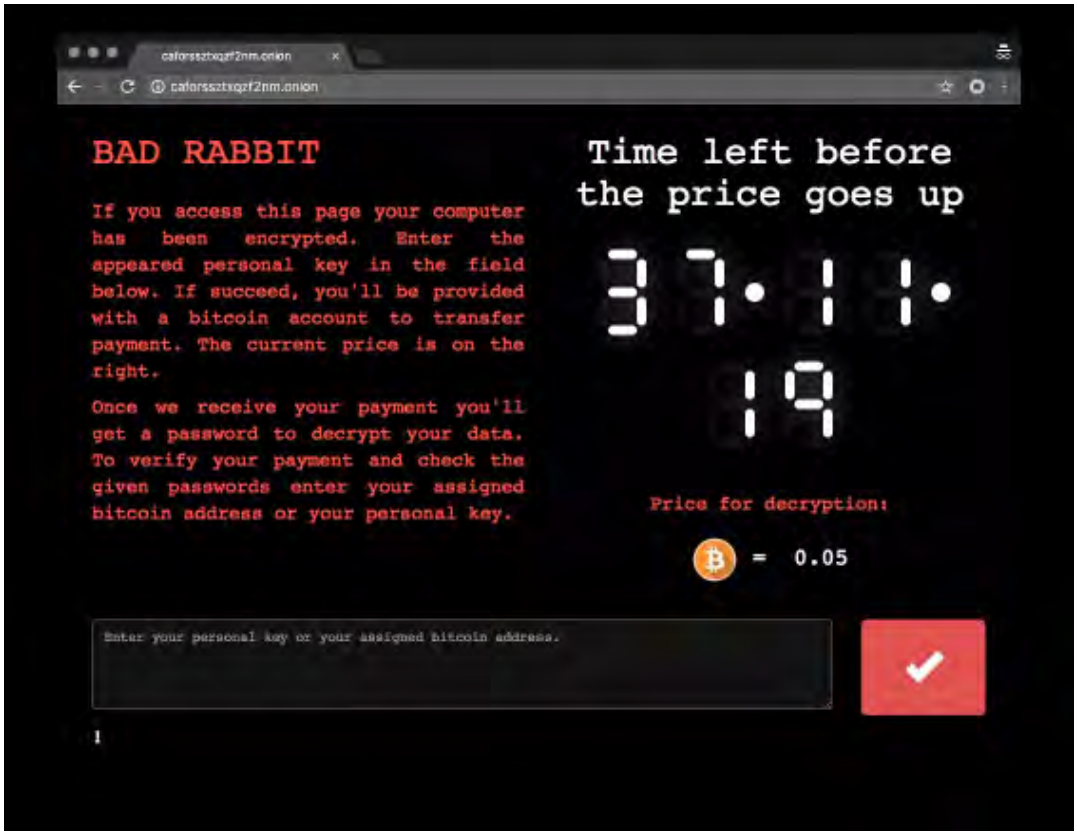
A principios de mes, *se hizo público el ciberataque sufrido por el Far Eastern International Bank,* atribuido a Corea del Norte. El ataque al banco taiwanés explotó con éxito un vector sobre la red financiera global SWIFT para robar aproximadamente 60 millones de dólares. Los fondos se transfirieron del banco a cuentas en varios países, incluidos Sri Lanka, Camboya y los Estados Unidos. Dos personas fueron detenidas en Sri Lanka varios días después del ataque por su papel en la operación. Los investigadores de *BAE Systems* han identificado las herramientas utilizadas en el ataque, identificando patrones comunes a las empleadas por Lazarus Group, actor asociado a Corea del Norte. Parte del malware descubierto por BAE fue utilizado por Lazarus en ataques dirigidos a organizaciones financieras en Polonia y México. El malware incluye mensajes escritos en ruso, actuando como *false flags.*



Timeline del ataque sobre el Far Eastern International Bank (FEIB)

Ya a finales de mes, una nueva campaña *global de ransomware denominado "BadRabbit"* infectó activos en diversas entidades y redes de Europa del Este y Rusia. El ataque infectó rápidamente a diversos operadores de infraestructuras críticas en Ucrania, incluido el aeropuerto de Odessa y el sistema de metro de Kiev. Más de la mitad de las víctimas están ubicadas en Rusia, incluida la agencia de noticias Interfax, seguida de Ucrania, Bulgaria, Turquía y Japón, según indicaron los investigadores de ESET.

Si bien hasta el momento no se han informado interrupciones importantes en EEUU, el Departamento de Seguridad Nacional (DHS, por sus siglas en inglés) emitió una advertencia sobre BadRabbit en el que se aconseja a las víctimas que se pongan en contacto con el FBI y que no paguen el rescate solicitado. En base a las similitudes con el patrón de ataque de EternalPetya de este pasado verano, es plausible que el Sandworm team sea el autor de esta nueva campaña, pero no se ha establecido ninguna atribución clara todavía. A diferencia de EternalPetya, que se diseñó para afectar exclusivamente a Ucrania, BadRabbit ha tenido una propagación indiscriminada, afectando a diversas agencias de medios rusos y entidades de Turquía, Japón y Bulgaria, después de afectar inicialmente al aeropuerto de Odessa.



Pantalla del ransomware BadRabbit

CIBERESPIONAJE

En el plano del ciberespionaje, *durante la primera semana de mes se verificó la existencia de un disidente chino afincado en Nueva York que parece estar en el centro de una serie de misteriosos ciberataques acaecidos en las últimas semanas.*

Los ataques fueron focalizados contra el Hudson Institute, un think tank político; y contra la firma de abogados Clark Hill. En ambos casos, parecen girar en torno a la campaña de China contra el disidente Guo Wengui (alias Miles Kwok) que actualmente está buscando asilo político en los Estados Unidos.

Hace tres semanas, se detectó un ataque de denegación de servicio distribuido (DDoS) contra el Hudson Institute que conllevó a la cancelación de un evento que encabezaba Guo Wengui. El instituto señaló que tenían pruebas de que el ataque se originó en Shanghai. El segundo ataque, contra la firma Clark Hill, llevó a la compañía a retirar misteriosamente su representación de Wengui, tras haber presentado el reclamo de asilo en su nombre.

Wengui es un multimillonario inmobiliario buscado en China por cargos de corrupción. Wengui respondió a esas acusaciones llamando a China una cleptocracia y generando documentos que, según él, muestran la actividad de espías chinos en territorio estadounidense. China calificó los documentos de falsificaciones y también negó la responsabilidad de los ciberataques contra el Hudson Institute y Clark Hill.

Miles Kwok, a principios de 2017 acusó al gobierno chino de utilizar los recursos de compañías chinas privadas para vigilar a ciudadanos chinos en el exterior. Los ataques contra Kwok

y las organizaciones asociadas con él, aunque actualmente no están atribuidos, se pueden ver como parte de una tendencia más amplia de la actividad llevada a cabo por gobiernos autoritarios y hacktivistas patrióticos utilizados para intimidar a los disidentes.

Guo Wengui

De nuevo en la región asiática, el gobierno surcoreano *acusó a mediados de mes a Corea del Norte* de haber robado un gran número de documentos militares del Ministerio de Defensa de Corea del Sur. El legislador surcoreano dijo que se robaron cerca de 235 gigabytes de documentos militares del Defense Integrated Data Center. El Ministerio de Defensa no ha realizado comentarios sobre las acusaciones. La supuesta información robada incluye planes de contingencia durante la guerra elaborados por EEUU y Corea del Sur, planes para operaciones de las Fuerzas Especiales e información sobre instalaciones militares y centrales eléctricas. El robo supuestamente tuvo lugar hace un año, pero según el legislador, el 80% de los documentos robados aún no se han identificado.

Ya hace un año, algunos analistas informaron sobre el incidente de septiembre de 2016 en el que se dice diversas campañas de ciberespionaje norcoreano accedieron al plan de guerra de EEUU y Corea del Sur conocido como OPlan 5027. Esta no es la primera vez que OPlan 5027 ha sido atacado. Ya en 2009, el Servicio de Inteligencia Nacional y el Comando de Seguridad de Corea del Sur informaron del robo de OPlan 5027 por parte de Corea del Norte.

Finalmente, los profesionales de ciberseguridad interesados en la próxima conferencia de la OTAN están siendo blanco de una campaña de phishing. Según los investigadores de Talos (Cisco), el conocido grupo APT28 vinculado con el Kremlin (también conocido como Fancy Bear) es responsable de la operación. Aparentemente, los atacantes crearon documentos maliciosos utilizando información copiada directamente del sitio web de la conferencia de CyCon en EEUU. CyCon está organizado por el Centro de Excelencia de Ciberdefensa de la OTAN (CCDCOE) en colaboración con el Army Cyber Institute en West Point y tendrá lugar del 7 al 8 de noviembre en Washington, DC. Mientras APT28 aprovechó una vulnerabilidad 0-day de Adobe en varias operaciones, esta campaña utiliza un documento de Office que contiene un script en visual basic.

El objetivo es entregar Seduploader, un malware utilizado por el grupo en ataques anteriores relacionados con la OTAN. Seduploader es un malware de reconocimiento capaz de realizar capturas de pantalla, recolectar y filtrar información del sistema, ejecutar código y descargar archivos. Esta campaña subraya el interés continuo de APT28 en el ámbito diplomático y, en particular, su enfoque en CyCon, sugiere un interés específico en seleccionar personas involucradas en la defensa y la industria de seguridad cibernética.

Alerta del CCDCOE sobre la campaña de phishing del CyCon

HACKTIVISMO

Desde el pasado domingo 1 de octubre, como resultado del referéndum catalán vinculado al proceso de independencia, el ciberespacio ha actuado, una vez más, como un espejo de la situación social y política. Más allá del uso masivo de las redes sociales para apoyar los procesos de influencia y propaganda de ambas partes, se han detectado diversas campañas de ciberataques de forma continuada durante todo el mes.

Los hacktivistas que apoyaban el proceso de independencia, justificándose por la protesta en Cataluña contra la intervención policial, han lanzado varios ciberataques contra *Banca March*, la Dirección General de Protección Civil y Emergencias, la Universidad de A Coruña, la *Universidad de Barcelona*, la Universidad Politécnica de Valencia, la *Universidad de Alicante*, la empresa *Canal Postal*, las firmas de telecomunicaciones *Flexinet* y *Telitec*, el *Ayuntamiento de Guadarrama* (Madrid), la Junta de Andalucía, la *Congrega-*

ción de los Sagrados Corazones, la *Fundación Francisco Franco*, la web de la Comisión Nacional del Mercado de Valores (CNMV), la web del Tribunal Constitucional entre otros objetivos. Algunos de los ataques fueron revindicados por *LulzSec*, Anonymous y *AnonPlus.*

Al mismo tiempo, diversos hacktivista contrarios al proceso de independencia también ha atacado varias páginas web de ayuntamientos catalanes que apoyan el proceso de independencia. Como resultado, los datos han sido filtrados y publicados en diversos sites. En ambos contextos, los vectores de ataque mayoritarios fueron los ataques de denegación de servicio distribuido (DDoS) y las inyecciones SQL.

En cualquier caso, el Gobierno de Cataluña no ha informado formalmente de ningún ataque cibernético específico mientras se celebraba el referéndum (1 de octubre). Sin embargo, en septiembre se detectó un pico de ciberataques en la estructura de la web del Gobierno de Cataluña, justo después de que se anunciara el referéndum, siguiendo la información facilitada por Jordi Puigneró, Secretario de Telecomunicaciones, Ciberseguridad y Sociedad Digital de Cataluña. Sin embargo, esas cifras no han podido verificarse públicamente. El presidente de Cataluña, Carles Puigdemont, también denunció que se detectaron algunos ataques en su cuenta personal de Twitter, tratando de robar sus credenciales mediante fuerza bruta.

En relación con los potenciales bots sociales u otros desarrollos similares coordinados y específicos, se ha podido comprobar que las cuentas de Twitter del líder de WikiLeaks Julian Assange y el ex contratista de NSA Edward Snowden representaron alrededor de un tercio del tráfico de Twitter bajo el hashtag #Catalonia . Es importante señalar que el hashtag #Catalonia generó más de 150.279 tweets y retweets. Alrededor de 40.000 de esas interacciones vinieron de la cuenta de Twitter de Julian Assange, mientras que 8.198 tweets y retweets surgieron de la cuenta de Edward Snowden.

Mediante el uso de la herramienta TwitterAudit, un análisis detallado de cerca de 5.000 seguidores de Assange en su perfil reveló que cerca del 59% son perfiles falsos, programados simplemente para reproducir automáticamente mensajes específicos. Julian Assange, así como Edward Snowden, Wikileaks y Russia Today en menor medida, han estado apoyando el movimiento independentista catalán, sacando provecho de la narrativa pro separatista, twitteando informaciones que distorsionaban o exageraban lo sucedido en España, poniendo en duda la legitimidad del sistema político español y, desde el 1 de octubre (cuando se realizó el referéndum) acusando a las autoridades españolas de represión política y violencia. Aunque podría decirse que Assange se ha convertido en el principal defensor internacional y portavoz informal del movimiento independentista, su impacto en la arena política española ha sido muy limitado, solo apoyado por los separatistas.

Así pues, parece evidente que ha habido operaciones de influencia en torno al referéndum y también hemos visto que las cuentas de Twitter favorables al Kremlin han aumentado en un 2.000% sus menciones a la crisis catalana (detectada por la herramienta *Hamilton 68*), mediante el uso del hashtag #Catalan en dichas cuentas. También hemos visto que los canales de comunicación con lazos directos con el gobierno ruso como RT o Sputnik han aumentado su cobertura de la situación catalana, difundiendo historias sobre el referéndum o comparando la independencia catalana con las acciones de Crimea en 2014.

6 Recomendaciones

6.1 Libros y películas

Película:
ASHLEY MADISON: SEX, LIES & CYBER ATTACKS

Sinopsis: Disponible en plataformas como Netflix, "Ashley Madison: Sex, Lies & Cyber Attacks" (2016) explica en 46 minutos la génesis del proyecto, en qué consiste la temática y las consecuencias del hackeo que expuso al escrutinio público la intimidad de millones de personas de todo el mundo.

Libro:
THE FUTURE OF WAR: A HISTORY

Autor: Lawrence Freedman
Num. Páginas: 400
Editorial: Allen Lane
Año: 2017
Precio: 20,00 Euros
Sinopsis: El autor realiza un extraordinario análisis sobre la evolución del arte de la guerra durante las últimas décadas, analizando los grandes retos que suponen para la principales potencias mundiales las amenazas híbridas y la ciberguerra.

Libro:
ALTERNATIVE WAR

Autor: J.J. Patrick
Num. Páginas: 388
Editorial: Cynefin Road
Año: 2017
Precio: 17,50 Euros
Sinopsis: En el transcurso de una extensa investigación que abarca principalmente Europa y América del Norte, el autor ha reunido a expertos, informes de inteligencia clasificados, registros públicos y testimonios de testigos para construir la descripción más amplia y precisa del asalto de Vladimir Putin a los aliados de la OTAN hasta la fecha mediante la explotación del dominio cibernético.

Libro:
CYBER WAR: THE NEXT FRONTIER FOR NATO

Autor: U.S Naval Postgraduate School
Num. Páginas: 56
Editorial: U.S Naval Postgraduate School
Año: 2015
Precio: 5,50 Euros
Sinopsis: Definir y comprender qué constituye un ciberataque es una cuestión complicada, en gran parte debido al hecho de que aún no ha habido un ciberataque a gran escala contra ninguna nación. Con la ayuda del Manual de Tallin de Michael Schmitt, publicado en 2013, es posible comprender qué elementos deben cumplirse para que un ataque cibernético justifique una respuesta de la OTAN. Este libro analiza y explora la posición única en la que opera la OTAN y el deber de la OTAN de proteger a los miembros de su alianza y a los estados miembros para que se protejan unos a otros.

6.2 Webs recomendadas

http://www.cert.hr/
Sitio web del Centro de Respuesta ante Incidentes Informaticos del gobierno de Croacia.

https://www.cncs.gov.pt/en/
Sitio web del Centro Nacional de Ciberseguridad de Portugal.

https://www.cpni.gov.uk/
Sitio web del Centro Nacional de Protección de Infraestructuras Críticas del Reino Unido.

https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
Sitio web de la Comisión dedicado a la ciberseguridad y la ciberdefensa

https://securityledger.com/
Sitio web que publica diariamente información relacionada con la ciberseguridad y ciberdefensa.

https://www.ncsc.gov.uk/
Sitio web del Centro Nacional de Ciberseguridad del Reino Unido.

6.3 Cuentas de Twitter

@REjercitos

@CERTAFr

@HRCERT

@OBSAE

@CSIRTCV

7 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1-2 Noviembre	Utrecht	Infosecurity	Infosecurity Netherlands	http://prosecurityexpo.de/?lang=en
7-8 noviembre	Washington DC.	CCDCOE	CyCon U.S.	http://aci.cvent.com/events/2017-international-conference-on-cyber-conflict-cycon-u-s-/event-summary-004d598d31684f21ac82050a9000369f.aspx?p=10
7-8 noviembre	Abu Dhabi	RSA	RSA Conference 2017	https://www.rsaconference.com/events/ad17
7-8 noviembre	Munich	Qatalyst Global	Industrial IoT Europe	https://www.industrialiotseries.com/europe/
9 noviembre	Lisboa	Bsides	BSides Lisbon	https://www.bsideslisbon.org/
13 Noviembre	Airport City Avenue, Israel		ICS Cybersec 2017	https://ics-cybersec-2017.events.co.il/home
14 Noviembre	Madrid	CLOUD COMMUNITY EUROPE	ExpoCloud 2017	https://www.eurocloudspain.org/
13-14 Noviembre	Berlín	Management Circle AG	Global Cyber Security Leaders 2017	http://www.global-leaders-summits.com/summit/global-cyber-security-leaders
14-16 Noviembre	Barcelona	SmartCity	Smart City Expo World Congress	http://www.smartcityexpo.com/
16- 17 Noviembre	Moscú	ZeroNights	ZeroNights 2017	https://2017.zeronights.org/
16- 17 Noviembre	Viena	roots conference	ROOTS	http://www.roots-conference.org/
23 Noviembre	Madrid	akjassociates	3rd e-Crime and Cybersecurity Spain	http://www.e-crimecongress.org/event/spain
28 Noviembre	Madrid	CSA ES	Encuentro de Cloud Security Alliance	https://www.ismsforum.es/evento/649/vii-encuentro-de-cloud-security-alliance-espana/
30 Noviembre	Madrid	Red Seguridad	I Jornada de Inteligencia y Seguridad	http://www.seguritecnia.es/revistas/seg/eventos/I_INTELIGENCIA/I_inteligencia_programa.pdf
4-7 Diciembre	Londres	Black Hat	Black Hat Europe	https://www.blackhat.com/eu-17/

Patrocinadores

Consejo Asesor Empresarial

Empresas Colaboradoras

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269