REAL INSTITUTO elcano ROYAL INSTITUTE

OCTUBRE 2017
Nº 29

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 septiembre 09

4 Herramientas del analista 10

5 Análisis de los ciberataques del mes de septiembre 11

6 Recomendaciones

6.1 Libros y películas 16

6.2 Webs recomendadas 18

6.3 Cuentas de Twitter.....18

7 Eventos.....19

1 COMENTARIO CIBERELCANO:
Hacia la construcción de un ciberespacio europeo seguro

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

Fuente: Military Times

El pasado 13 de Septiembre, la Comisión Europea presentaba el *Cybersecurity Package*, un marco de referencia a través del cual Bruselas pretende articular la construcción de la ciberseguridad y ciberdefensa europea.

El creciente impacto -económico, político y social- de los ciberataques constituye una de las principales preocupaciones para la inmensa mayoría de los dirigentes europeos. Es por ello que Bruselas implementará un conjunto de medidas con el objetivo de mejorar la seguridad y resiliencia del ciberespacio común europeo. Entre las medidas propuestas destacan: una reforma de la Agencia Europea para la Seguridad TIC (*ENISA*), otorgándole un mayor número de competencias y estrechando sus relaciones con las agencias de seguridad y defensa de la Unión Europea; la creación de un mercado único europeo en el ámbito de la ciberseguridad, cimentado este sobre un modelo de certificación a nivel europeo; la implantación efectiva de la *directiva NIS*, que debería producirse a mediados de 2018; la mejora de las capacidades de defensa, inteligencia y respuesta, que en la actualidad se han demostrado insuficientes; la creación de

un conjunto de redes de Excelencia en materia de ciberseguridad integrados en un gran Centro Europeo para la Investigación en el ámbito de la ciberseguridad; así como la promoción de la *formación, el entrenamiento y la concienciación en el ámbito de la ciberseguridad*, máxime cuando se estima que hay un déficit de más de 500.000 profesionales de la ciberseguridad en Europa.

Identificar a los actores que menoscaban la seguridad del ciberespacio del viejo continente, mejorar las capacidades de respuesta e investigación de las agencias europeas de seguridad y de las Fuerzas y Cuerpos de Seguridad de los estados miembros de la Unión Europea o fomentar la colaboración público-privada en el ámbito de la ciberseguridad, son algunas de las medidas con las que Bruselas pretende disuadir desde el ciberespacio.

A pesar del paso adelante que supone el CyberSecurity Package, Europa necesita disponer de una industria de ciberseguridad europea solvente, que proporcione aquellas capacidades que permitan poner en marcha de manera real y efectiva la seguridad y defensa del ciberespacio común europeo. En la actualidad, la seguridad y defensa del ciberespacio europea es altamente dependiente de las cibercapacidades provenientes de Estados Unidos, Israel, e incluso, Rusia.

En definitiva, no cabe duda de que la seguridad y defensa del ciberespacio constituyen una prioridad política para la Unión Europea. La creación de una industria de ciberseguridad europea innovadora y competitiva debe ser una prioridad para Bruselas, aunque no debemos olvidar que muchos de los estados miembros son reacios a compartir sus cibercapacidades destinadas a la defensa de sus ciberespacios nacionales.

"la seguridad y defensa del ciberespacio europea es altamente dependiente de las cibercapacidades provenientes de Estados Unidos, Israel, e incluso, Rusia."

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Injerencias en el proceso electoral alemán

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

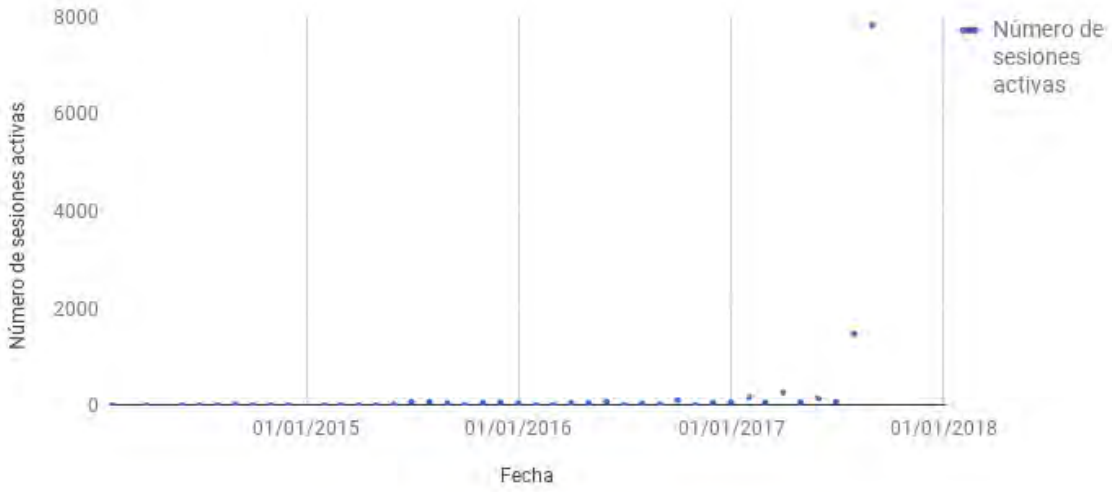
Una vez concluidas las elecciones en Alemania, la red social Facebook publicó el pasado 27 de septiembre un comunicado en su *blog* en donde confirmaba que habrían "eliminado decenas de miles de cuentas falsas en Alemania". Sin embargo, antes de las elecciones, también se habrían detectado operaciones de propaganda y desinformación procedentes de medios de comunicación rusos similares a los identificados en las elecciones de Estados Unidos y de Francia. De hecho, el grupo de trabajo East StratCom de la Unión Europea, creado en 2015 para combatir las campañas de desinformación del gobierno ruso, descubrió que la canciller Angela Merkel estaba siendo objetivo constante de este tipo de ataques debido a su *política hacia los refugiados*. Y, otro caso relacionado, son los correos electrónicos enviados a medios de comunicación sobre el *«Caso Lisa»* en donde soldados alemanes habrían sido acusados de violación durante su estacionamiento en Lituania como parte de las fuerzas militares de la OTAN.

"antes de las elecciones, también se habrían detectado operaciones de propaganda y desinformación procedentes de medios de comunicación rusos"

ELECCIONES SIN FUGA DE INFORMACIÓN

Sin embargo, parece que los ataques perpetrados y confirmados por el BSI por parte de APT28 a diversas infraestructuras políticas alemanas como el Bundestag o el partido político Unión Demócrata Cristiana no habrían llegado consumar ningún tipo de robo de información, ya que días previos no se presenció ninguna fuga de información referente a ningún partido político.

De todas formas, según las bases de datos de amenazas de las que dispone Eleven Paths, se habría identificado en los meses de agosto y septiembre de 2017 un repunte de sesiones activas de equipos infectados por la suite de *malware* utilizada por APT28.



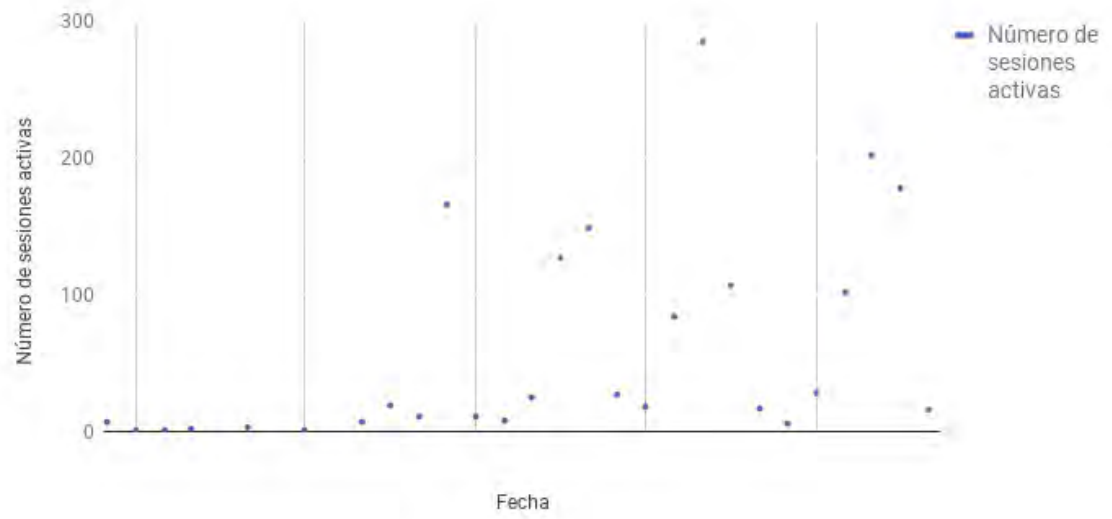
Número de sesiones activas de la suite de malware de APT28.

Entre todas estas muestras de *malware*, se detectó un *downloade*r llamado Coreshell con impacto en organizaciones gubernamentales en Alemania. Coreshell descarga en una segunda fase un *backdoor* desde un *command and control.*

OTRAS AMENAZAS GENÉRICAS

Desde otro punto de vista, también se han identificado otras familias de *malware genérico* y no asociado a grupos conocidos o al menos no atribuidos a APT28 como parte de su arsenal de herramientas actual. Entre ellas se han encontrado distintos tipos de *malware* con capacidades de robo de información, control de los sistemas infectados y diferentes implementaciones para atacar plataformas Windows, Mac y Android.

El rango temporal en la que se sitúan estas amenazas es desde enero del 2015 hasta las más recientes detectadas durante el desarrollo de esta investigación en septiembre de 2017. Por su parte, los vectores de infección han sido el correo electrónico, la navegación web, Flash, FTP, Ownclod y Mediafire.



Número de sesiones activas de muestras genéricas con impacto en instituciones gubernamentales.

Durante 2017 hemos visto diferentes técnicas que hacían uso de la red con el objetivo de modificar el rumbo de unas elecciones. Sin embargo, todavía nos queda calendario electoral con fechas señaladas en países como las de Tailandia, Chile o Corea del Sur donde seguro que tanto fabricantes de seguridad como plataformas de redes sociales estarán implementando ciertas medidas con el objetivo de presenciar unas elecciones lo más democráticas posible.

"Durante 2017 hemos visto diferentes técnicas que hacían uso de la red con el objetivo de modificar el rumbo de unas elecciones"

3 Informes y análisis sobre ciberseguridad publicados en septiembre de 2017

Proposal for ENISA regulation (European Commission)

Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (European Commission)

Cracking down on digital piracy (FACT UK)

2017 Cost of Cybercrime Study (Accenture)

The SME Cyber Market: How your business can benefit (Supply UK)

Outlook for fifty cyber security controls (TAG Cyber)

Riesgos de uso de Telegram (CCN CERT)

Digital vision for CyberSecurity (ATOS)

4 HERRAMIENTAS DEL ANALISTA:
Cyber Security GeoIP Attack Map Visualization

Este visualizador de ciberataques a través de un mapa con geoposicionamiento fue desarrollado para mostrar ataques en la red de una organización en tiempo real. *Es un proyecto opensource* desarrollado Matthew Clark fundamentalmente usando Python y JavaScript.

Para su correcto funcionamiento, el servidor de datos lee los datos de entrada de un archivo syslog y analiza la IP de origen, la IP de destino, el puerto de origen y el puerto de destino. Los protocolos se determinan a través de puertos comunes y las visualizaciones varían en color según el tipo de protocolo. En el siguiente *enlace* se puede visualizar un vídeo demostrativo. Este proyecto reutiliza funcionalidades de un visualizador de tráfico desarrollado por Sam Cappella en 2015 para el Palmetto Cyber Defense Competition.

Este programa se basa totalmente en syslog, y debido a que todos los dispositivos forman registros de forma diferente, es necesario personalizar la función de análisis de registros (llamado parseador). Si su organización utiliza un sistema de información de seguridad y de gestión de eventos (SIEM), probablemente puede normalizar los registros para ahorrarle tiempo escribiendo expresiones regulares.

Así pues, el mecanismo recomendado de funcionamiento sería:

- Enviar todo el syslog al SIEM.
- Utilizar el SIEM para normalizar los registros.
- Enviar los registros normalizados al cuadro de mandos (cualquier máquina Linux que ejecute syslog-ng funcionará) ejecutando este software para que el servidor de datos pueda analizarlos.

5 Análisis de los Ciberataques del mes de septiembre de 2017

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

CIBERCRIMEN

Un nuevo *informe de Symantec* publicado a comienzos de mes ha revelado que un grupo de atacantes autodenominados Dragonfly 2.0 realizó una campaña de ciberataques dirigido a decenas de compañías eléctricas estadounidenses en la primavera y el verano de este año.

En más de 20 casos, los atacantes accedieron con éxito a las redes de las empresas objetivo. El informe reveló algo aún más preocupante: en algunos casos los hackers obtuvieron "acceso operativo" o control de los interfaces que usan los ingenieros para enviar comandos a equipos como disyuntores, dando así a los atacantes la capacidad de detener el flujo de electricidad en los hogares y negocios de los Estados Unidos.

Es necesario destacar que hay una diferencia entre estar a un paso de provocar el sabotaje y estar realmente en una posición para ejecutarlo. Ahora estamos hablando de evidencia técnica sobre el terreno de lo que podría suceder en Estados Unidos. Los únicos ataques conocidos para explotar capacidades similares fueron los ciberataques contra la red de energía ucraniana en 2015. Empresas de seguridad, incluyendo FireEye, han atribuido esos ataques al actor estatal ruso Sandworm Team.

La vinculación de Symantec de la actividad dirigida al sector energético (denominada Equipo Koala) con la reciente focalización en el sector energético (tildada como TEMP.Isotope) es plausible. La actividad TEMP.Isotope más antigua conocida coincide con las últimas intrusiones observadas del Equipo Koala, y tienen un enfoque superpuesto en el sector energético. El interés específico de Koala Team en los sistemas ICS del sector energético sugiere que su actividad es la preparación para un ataque disruptivo, y cualquier conexión entre los dos actores refuerza la probabilidad de que TEMP.Isotopo estuviera realizando una labor de reconocimiento sobre sistemas críticos.

Equifax, una importante agencia estadounidense de informes de crédito sobre los consumidores que recopila y agrega información sobre más de 800 millones de consumidores individuales y más de 88 millones de empresas en todo el mundo, informó que *unos actores maliciosos obtuvieron acceso no autorizado* a información de consumidores.

Los atacantes accedieron principalmente a "nombres, números de Seguridad Social, fechas de nacimiento, direcciones y, en algunos casos, números de licencia de conducir", según las declaraciones públicas de la compañía. En algunos casos, los atacantes accedieron a otra información personal como los números de tarjeta de crédito.

El incidente afecta potencialmente a 143 millones de consumidores estadounidenses. Además, Equifax informó que los atacantes accedieron potencialmente a información sobre los clientes británicos y canadienses. Sin embargo, Equifax declaró que no identificó ninguna evidencia de que los atacantes accedieran a las bases de datos de informes de crédito de la compañía

Los cibercriminales con motivación económica se basan en este tipo de datos para ejecutar una amplia variedad de esquemas de ataque que suelen implican fraude de identidad.

CIBERESPIONAJE

Turla Team, un conocido equipo asociado a labores de ciberespionaje, con potencial vinculación al Kremlin, *ha lanzado este mes una nueva campaña dirigida al sureste de Europa,* sobre objetivos políticos que ya lo eran del antiguo bloque soviético. Según la firma de seguridad ESET, Turla está aprovechando una nueva puerta trasera de segunda fase en un vector de ataque con múltiples etapas.

La herramienta, llamada "Gazer", está vinculada a Turla a través de similitudes en el código y el uso de los mismos servidores intermedios que en la actividad previamente observada de Turla. Gazer utiliza la implementación de criptografía personalizada no observada en las herramientas anteriores utilizadas por Turla. ESET también señaló que, si bien la nueva herramienta tiene algunas capacidades adicionales, no ha reemplazado por completo a otras puertas traseras de segunda etapa utilizadas por el grupo.

Los actores estatales con vinculación rusa representan a algunos de los adversarios más sofisticados en el panorama actual. Los grupos más importantes, incluyendo APT28 y Turla Team, mantienen múltiples líneas de herramientas para ejecutar diversas etapas de explotación, y frecuentemente se descubren nuevas herramientas a medida que continúan desarrollando y mejorando sus capacidades. Gazer o WHITEBEAR parecen ser "loaders" de segunda fase desplegados después de que una de sus herramientas de primera etapa inicialmente compromete la máquina objetivo.

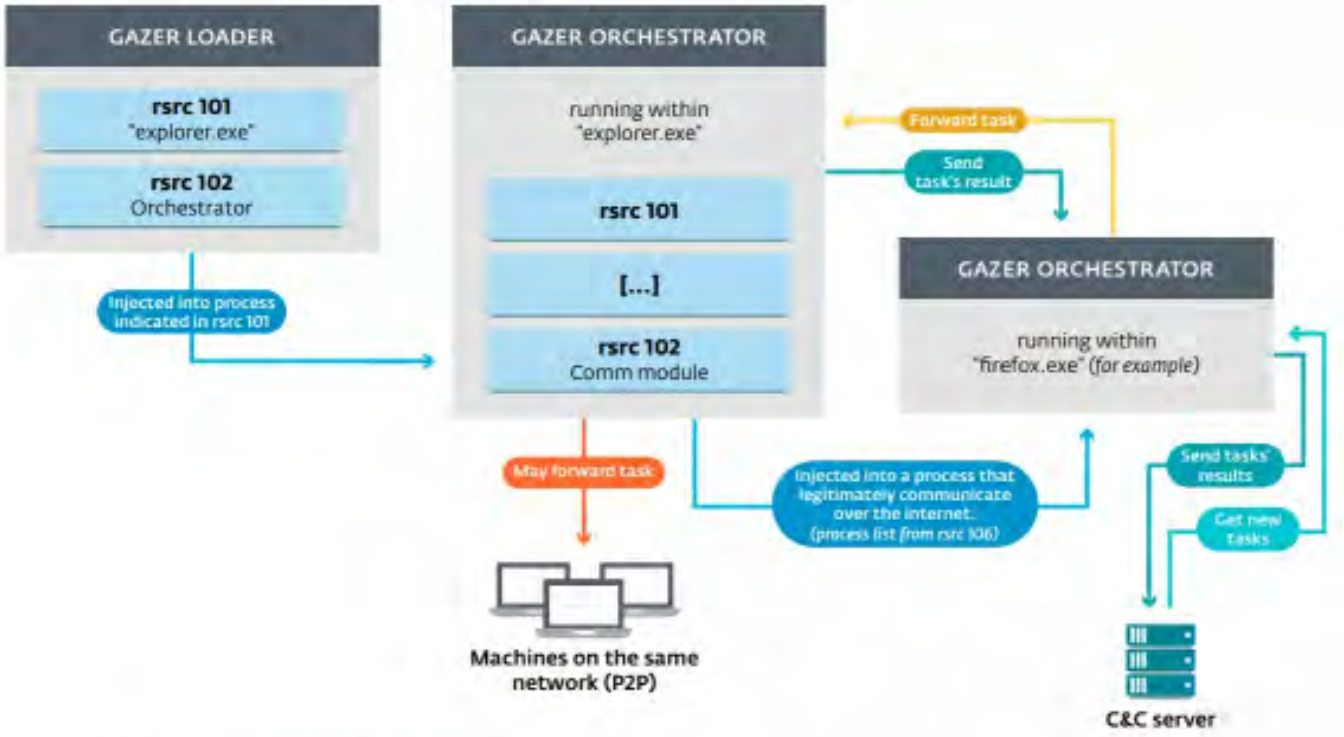


Figure 2. **Gazer architecture**

A comienzos de mes, el parlamento del estado alemán de Sajonia-Anhalt ha sido *paralizado por un aparente ataque de ransomware.* El ataque comenzó cuando un empleado abrió un archivo adjunto a un correo electrónico malicioso. Actualmente no hay indicadores sobre si el ataque era dirigido o formaba parte de una campaña más amplia no dirigida específicamente al gobierno. En cualquier caso, el gobierno alemán no es ajeno a los ataques cibernéticos. A principios de este año, el Parlamento alemán fue víctima de una campaña de *malvertising* y en 2015 el Bundestag soportó un ataque de troyanos perpetrado durante seis meses, atribuido al presunto grupo de espionaje ruso APT28 (Fancy Bear).

No se dispone de ningún indicador de que este ataque esté relacionado con la actividad de un actor estatal y el ransomware es más comúnmente usado en ataques con motivación económica. Sin embargo, los recientes ataques de Petya sugieren que los actores estatales pueden encontrar valor en el uso de un rescate para obligar o castigar a los adversarios estatales, o perjudicar los intereses económicos de sus adversarios. Al obligar al parlamento alemán a apagar sus equipos informáticos hasta que se resuelva la infección, el ataque de ransomware funciona como una interrupción de servicio.

Los investigadores de Symantec han identificado una campaña de ciberespionaje persistente dirigida tanto a India como a Pakistán, que creen que se remonta a octubre de 2016. La campaña es el trabajo de varios grupos independientes que comparten tácticas, técnicas y procedimientos (TTPs), lo que parece tener soporte estatal.

Los investigadores no han mencionado que un actor estatal pudiera estar detrás de los ataques, pero señalaron que los gobiernos y los militares con operaciones en el sur de Asia y con intereses en seguridad regional podrían estar en riesgo. La campaña aprovecha una puerta trasera llamada "Ehdoor" para acceder a los archivos en los equipos infectados.

En la campaña reciente dirigida contra objetivos en Qatar se emplearon puertas traseras similares. El malware, una vez instalado, permite a un atacante cargar y descargar archivos, ejecutar procesos, registrar pulsaciones de teclas, identificar la ubicación del objetivo, robar datos personales y tomar capturas de pantalla.

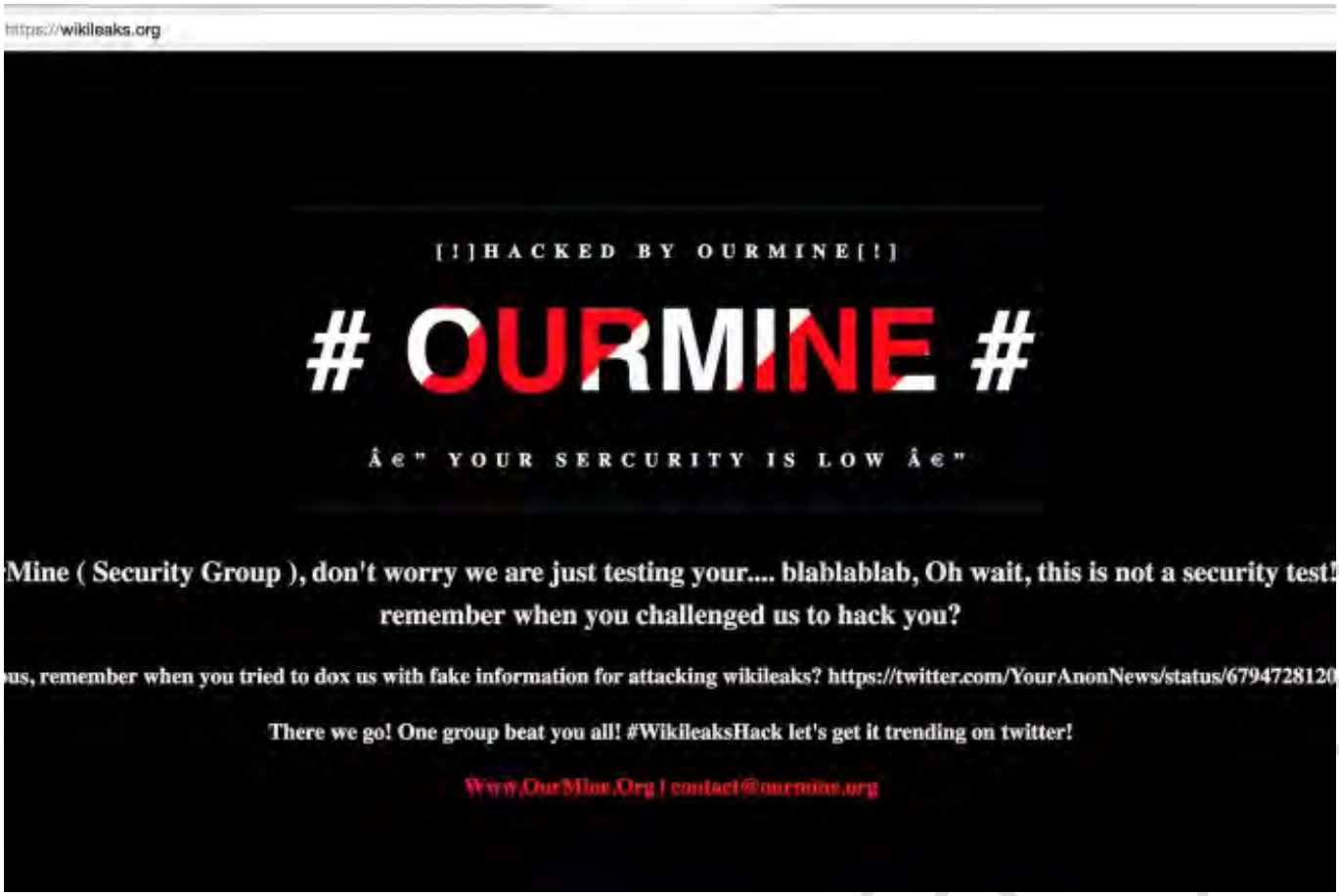
Las disputas fronterizas en el sur y el suroeste de Asia han proporcionado durante mucho tiempo oportunidades para una variedad de actividades de ciberespionaje, ya que la potencial crisis y el conflicto sostenido en curso ofrece una amplia oportunidad para captar contenido de interés.

HACKTIVISMO

El sitio web de Wikileaks fue modificado de forma maliciosa *(defacement)* a comienzos de mes por un grupo autodenominado OurMine. El grupo dejó el siguiente mensaje: "Hola, es OurMine (Grupo de Seguridad), no te preocupes, estamos probando tu ... blablablab, oh espera, esto no es una prueba de seguridad! Wikileaks, ¿recuerdas cuando nos desafiaste a hackearte? Anonymous, ¿recuerdas cuando intentaste *doxearnos* con información falsa para atacar a wikileaks [sic]?" El mensaje continua: "¡Ahí vamos! ¡Un grupo os golpeó a todos! #WikileaksHack será *trending topic* en twitter [sic]! "

OurMine se cree que ha estado relacionado también con ataques dirigidos a los CEOs de Google y Twitter en el pasado y sitios web como BuzzFeed y Variety.

La información existente sugiere que OurMine redirigió el tráfico del dominio controlado por WikiLeaks a una página modificada controlada por OurMine entre el 30 de agosto y el 31 de agosto de 2017. Aunque no se ha observado previamente esta táctica de OurMine, este incidente es consistente con las evaluaciones realizadas en el pasado de que OurMine está motivado por el reconocimiento público y el ego, así como un deseo de llamar la atención.



6 Recomendaciones

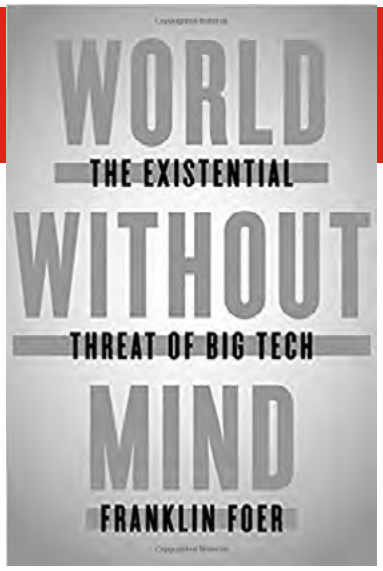
6.1 Libros y películas

Libro:
CYBERSECURITY FOR BEGINNERS

Autor: Raef Meeuwisse
Num. Páginas: 225
Editorial: Cyber Simplicity
Año: 2017
Precio: 16,00 Euros
Sinopsis: Raef Meeuwisse explica de manera sencilla e intuitiva los conceptos básicos que permiten comprender el mundo de la ciberseguridad así como las implicaciones que tiene el incremento del uso de internet por parte de criminales y terroristas.

Libro:
THE DARKENING WEB

Autor: Alexander Klimburg
Num. Páginas: 432
Editorial: Penguin Press
Año: 2017
Precio: 17,50 Euros
Sinopsis: El subtítulo del libro resume bien el contenido del mismo, la guerra por el ciberespacio. Alexander Klimburg, ahonda sobre las cibercapacidades que estan construyendo y utilizando las principales potencias mundiales con el objeto de ejercer una superioridad no solo tecnológica sino también en el control de la información con el objetivo de ejercer poder e influencia. Klimburg alerta de los peligros de minusvalorar el dominio cibernético y advierte de la pasividad de la inmensa mayoría de la comunidad internacional.



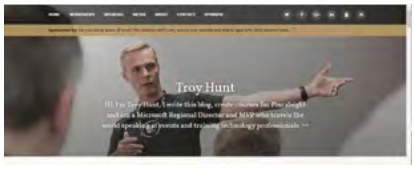
Libro:
WORLD WITHOUT MIND

Autor: Franklin Foer
Num. Paginas: 272
Editorial: Penguin Press
Año: 2017
Precio: 14,50 Euros
Sinopsis: Foer analiza de manera crítica la cara oculta de los avances tecnológicos y los objetivos ocultos de grandes compañías. Compramos a través de Amazon, nos relacionamos a través de Facebook, nos informamos a través de Google o trabajamos usando los productos de Microsoft o Apple. Pero, ¿cómo utilizan estas compañías el inmenso poder que le confiere el uso de su tecnología por buena parte de la humanidad?

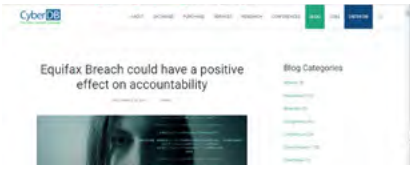
6.2 Webs recomendadas

https://www.welivesecurity.com/
Sitio web donde los profesionales de ESET nos proporcionan su visión sobre la seguridad TIC.

https://www.troyhunt.com/
Sitio web de Troy Hunt, MVP de Microsoft y experto en ciberseguridad.



https://www.cyberdb.co/blog/
Blog de CyberDB que proporciona información sobre noticias, investigaciones, productos y compañías del mundo de la ciberseguridad.



https://cybersec.buzz/
Sitio web que ofrece noticias y análisis de los principales expertos sobre la actualidad de la ciberseguridad y la ciberdefensa.

http://www.zonealarm.com/blog/
Blog de ciberseguridad donde los profesionales de CheckPoint analizan las últimas novedades del mundo de la seguridad TI.

https://security.googleblog.com/
Sitio web donde Google informa sobre las novedades más relevantes de sus investigaciones en mundo de la ciberseguridad.

6.3 Cuentas de Twitter

@jetapiador

@vxheaven.org

@kpoulsen

@cylab

@natashenka

7 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
2- 8 octubre	Praga	SANS	SANS DFIR Prague 2017	https://www.sans.org/security-training/by-location/all
3 y 4 de octubre	Estocolmo		CYBSEC 2017	https://infosec-conferences.com/events-in-2017/cybsec-2017/
3 Octubre	Madrid	ISACA	CiberTodos - La Ciberseguridad: Una Responsabilidad de Todos	http://www.isaca.org/chapters7/madrid/events/eventos/pages/mes-europeo-de-ciberseguridad.aspx
4 y 5 de octubre	Madrid	CCI	IX Congreso Internacional de Ciberseguridad Industrial en Europa	https://www.cci-es.org/web/cci/detalle-congreso/-/journal_content/56/10694/393798
4 y 5 de octubre	Londres	Cyber Security Europe	Cyber Security Europe	http://www.cybersecurity-europe.com/
4 - 6 de octubre	Madrid	Virus Bulletin International Conference	Virus Bulletin (VB2017)	https://www.virusbulletin.com/conference/vb2017/
11- 13 octubre	Glasgow	Sapphire	National Information Security Conference	http://www.sapphire.net/nisc/
16 - 19 Octunre	Luxemburgo	Hack.Lu	Hack.Lu	https://2017.hack.lu/
17 - 19 octubre	Madrid	AUI	Congreso Europeo sobre Privacidad y Protección de Datos	http://www.cdp2017.org/documentos/CdP2017-PresentacionCongreso.pdf
17 - 18 octubre	Madrid	CLOUD COMMUNITY EUROPE	ExpoCloud 2017	http://www.eurocloudspain.org/
23- 26 octubre	Madrid	IEEE	International Carnahan Conference on Security Technology	http://atvs.ii.uam.es/iccst2017/
24- 25 octubre	León	INCIBE	XI Edición ENISE	https://www.incibe.es/enise
26 - 27 de octubre	Valencia	ISACA	XI Congreso Isaca Valencia	http://www.isacavalencia.org/eventos/

Patrocinadores

Consejo Asesor Empresarial

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269