REAL INSTITUTO elcano ROYAL INSTITUTE

ABRIL 2017
Nº 24

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 Entrevista a Silvia Barrera 10

4 Informes y análisis sobre ciberseguridad publicados en marzo de 2017 13

5 Herramientas del analista 14

6 Análisis de los ciberataques del mes de marzo de 2017 16

7 Recomendaciones

7.1 Libros y películas 21

7.2 Webs recomendadas 24

7.3 Cuentas de Twitter.....24

8 Eventos.....25

1 COMENTARIO CIBERELCANO:
Formar ciberguerreros (II)

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

Fuente: International Business Times

La capacitación de los profesionales de la ciberseguridad y la ciberdefensa es esencial para disponer de una ciberfuerza que permita establecer las medidas de seguridad apropiadas de los ciberespacios nacionales y garantizar la operatividad de las Fuerzas Armadas modernas. Esta formación no debe solo circunscribirse a un ámbito tecnológico sino también al estratégico. Los mandos militares no solo deberán comprender la importancia estratégica de las tecnologías del ciberespacio y su aplicación en la planificación y conducción de las operaciones militares, sino también deberán saber relacionarse con la industria civil para comunicar sus crecientes necesidades en el nuevo dominio.

En este sentido, la inmensa mayoría de nuestros socios y aliados están definiendo planes de formación y entrenamiento cibernético. Estos planes están poniendo de manifiesto la necesidad de promover profundos cambios culturales que posibiliten integrar a una nueva generación de ciberguerreros en una estructura organizativa y operativa que no está preparada para maximizar las ventajas que el dominio cibernético puede proporcionar.

La Alianza Atlántica ha promovido -liderado por Portugal- el *Multi National Cyber Defence Education and Training Project* (*MN CD &ET*) - englobado este dentro de los proyectos de

Defensa Inteligente de la OTAN- para proporcionar una formación y entrenamiento en el ambito ciber a los miembros de las Fuerzas Armadas de las naciones miembro de la OTAN.

Estados Unidos dispone de múltiples iniciativas en este sentido: centros de excelencia de ciberdefensa en el ámbito de sus ejércitos y la armada; planes de formación obligatorios para todo el personal militar, como los promovidos por la U.S Navy o el U.S Air Force; modificación de los planes de estudio de las Academias Militares para potenciar la enseñanza de los futuros líderes de la ciberdefensa estadounidense; o programas formativos mixtos entre la industria y las Fuerzas Armadas.

España dispone de un Plan de Formación en Ciberdefensa (Plan FORCIBE) que contempla diferentes currículos formativos en el ámbito ciber.

El *gap generacional* hará necesario que en las Academias Militares los futuros oficiales y suboficiales no solo sean adiestrados en la vertiente más tecnológica de este ámbito sino también en el modo de exponer a sus superiores, menos familiarizados con este nuevo dominio, las ventajas inherentes al uso de capacidades cibernéticas en futuras operaciones militares.

En definitiva, el adiestramiento en materia de ciberdefensa del personal de las Fuerzas Armadas no deberá circunscribirse únicamente a una formación tecnológica sino deberá servir como palanca de cambio para integrar de manera efectiva el dominio ciber en las operaciones militares.

"Será necesario promover profundos cambios culturales que posibiliten integrar a una nueva generación de ciberguerreros en una estructura organizativa y operativa que no está preparada para maximizar las ventajas que el dominio cibernético puede proporcionar"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Desprotegidos por defecto

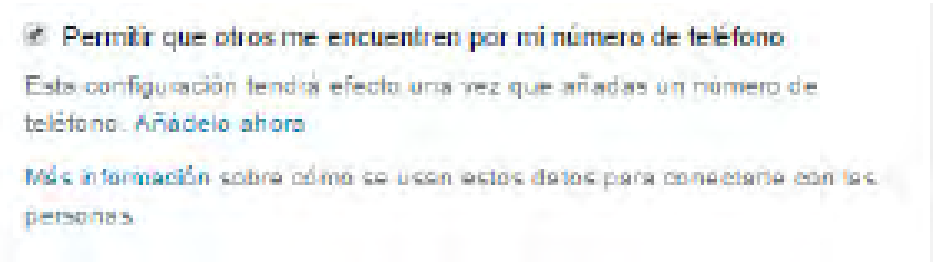
AUTOR: Yaiza Rubio y Félix Brezo, Analistas de THIBER, the cybersecurity Think Tank. Analistas de inteligencia de ElevenPaths.

El *Reglamento General de Protección de Datos* (GDPR, por sus siglas en inglés), destinado a proporcionar a los ciudadanos de la Unión Europea un mayor control sobre sus datos personales, introduce un nuevo concepto que deberán adaptar tanto fabricantes de tecnología como desarrolladores de aplicaciones y redes sociales: la privacidad por defecto.

Con este principio se pretende proporcionar privacidad tanto en el contenido como en los metadatos obtenidos del usuario (por ejemplo, localización y tiempo de la llamada) y que necesitarán encontrarse anonimizados o borrados si el usuario no ha dado su consentimiento. A pesar de que el GDPR define el término consentimiento como «un acto afirmativo claro que refleje la voluntad del interesado de aceptar el tratamiento», en la actualidad nos encontramos ante servicios que, por defecto, habilitan casillas ya marcadas de las que el usuario no es consciente.

Las opciones que más se repiten en las redes sociales son las siguientes:

· *Permitir que terceros puedan encontrar a otros usuarios*. Esta casilla permitiría a terceros encontrar a otros usuarios de la red social en base al correo electrónico o el número de teléfono. Incluso, en Twitter, el uso de esta opción le estaría proporcionando información al usuario objetivo a través de la sección *A quién seguir* de qué perfil le habría buscado.

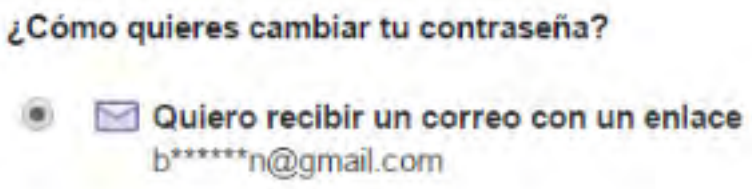


Opción de visibilidad de Twitter

· *Personas que quizá conozcas.* Esta opción proporcionaría a los usuarios de la red social poder contactar con otras personas en función de datos personales entregados, las redes de la que formas parte o de la actividad realizada. Sin embargo, no es sólo Facebook el único en emplear términos demasiado ambiguos que no permitirían saber con claridad a los usuarios qué información estarían cruzando.

Opción de privacidad de Facebook

· *Recuperación de contraseñas.* La recuperación de contraseñas sin que se notifique al usuario (imaginemos que lo hiciera un tercero en el contexto de un potencial ataque) podría suponer una reducción de su privacidad si tras anonimizar su dirección de correo todavía se consigue intuir la información mostrada.



Recuperación de contraseñas en Facebook

· *Recepción de anuncios.* El usuario recibirá anuncios personalizados basados en la información compartida con terceros si no deshabilita la casilla de contenido promocionado, tal y como ocurre en Twitter. En este caso, un tercero cedería su información a esta red social, obtenida por ejemplo a través de la suscripción de su boletín, con el objetivo de encontrar usuarios potencialmente interesados y mostrar así el contenido promocionado.

Esto le permite a Twitter mostrar anuncios sobre temas en los que hayas mostrado interés. Más información sobre cómo funciona esto y sobre tus controles de privacidad adicionales.

Funcionamiento del contenido promocionado en Twitter

· *No rastrear (Do Not Track o DNT).* Al tener desactivada la opción de DNT en el navegador del usuario (es recomendable revisarlo también en el dispositivo móvil, ya que suele encontrarse deshabilitada), la red social ofrecerá anuncios o sugerencias personalizadas.

Send a "Do Not Track" request with your browsing traffic

Opción Do Not Track en Chrome

· *Configuración de privacidad solamente a través de la instalación de aplicación.* Algunas redes sociales solamente permiten la configuración de privacidad a través de su aplicación móvil, como Instagram y ask.fm.

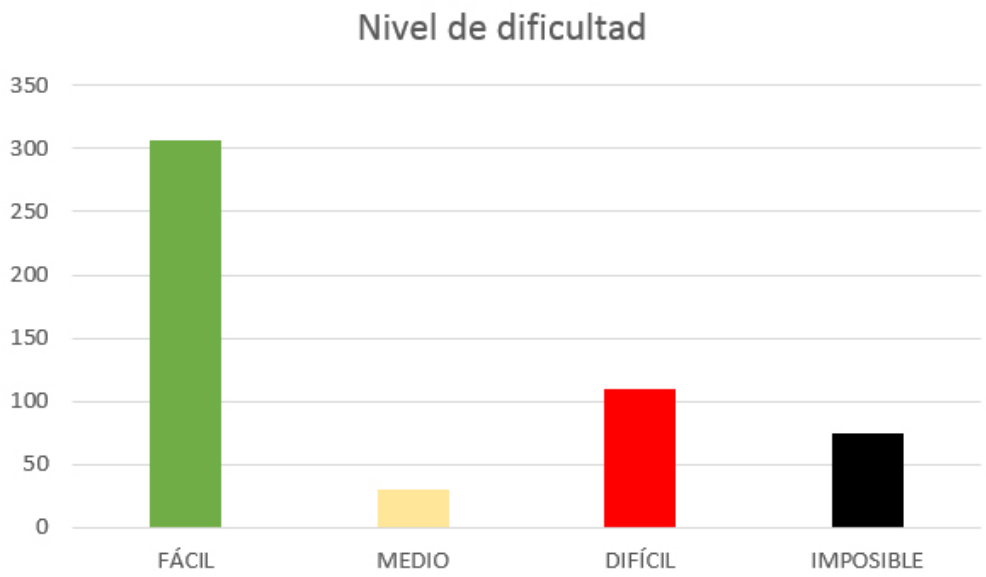
¿Cómo configuro mis fotos y vídeos como privados para que solo puedan verlos los seguidores aprobados?

De forma predeterminada, cualquiera puede ver tu perfil y tus publicaciones en Instagram. Puedes hacer que tus publicaciones sean privadas, de manera que solo las vean los seguidores aprobados. Si las publicaciones están configuradas como privadas, tus seguidores aprobados serán los únicos que podrán verlas en la pestaña "Fotos" de "Buscar y explorar" y en las páginas de hashtags o de ubicación. Las publicaciones no se pueden configurar como privadas desde un ordenador.

Configuración de privacidad en Instagram

Por otro lado, seguro que nos hemos encontrado en alguna ocasión ante la dificultad de darnos de baja de un servicio de internet determinado. En este sentido, están surgiendo proyectos como *Just Delete* que proporciona las direcciones URL exactas de al menos 520 plata-

formas para poder darse de baja directamente, así como un indicador de su dificultad e información que el usuario necesita conocer sobre dicho proceso. Según los servicios que tiene registrados, la categorización de todas ellas en función del indicador de dificultad para la eliminación de sus datos sería el siguiente:



Nivel de dificultad para darse de baja de las plataformas

Hasta que llegue el 25 de mayo de 2018, fecha establecida para la aplicación obligatoria del GDPR en cada Estado miembro de la Unión Europea, esperemos que los aspectos relativos a la privacidad de los usuarios en los servicios online no sean tan costosos de leer y comprender como los Términos y Condiciones del *Servicio Kindle de Amazon*, porque... ¿quién tiene ocho horas para leerlos? Y, más aun, ¿de verdad somos capaces de comprender las implicaciones de lo que leemos?

"El Reglamento General de Protección de Datos introduce un nuevo concepto que deberán adaptar tanto fabricantes de tecnología como desarrolladores de aplicaciones y redes sociales: la privacidad por defecto."

3 Entrevista a Silvia Barrera.

Inspectora de la Unidad de Investigación Tecnológica del Cuerpo Nacional de Policía

1. Como Inspectora de la Unidad de Investigación Tecnológica (UIT) del Cuerpo Nacional de Policía, ¿podría indicarnos cuáles son las principales competencias de su área?

Soy la Jefa de la Sección Técnica, la sección encargada de extraer las evidencias digitales en los operativos policiales más importantes y de especial complejidad técnica de la Policía, no solo de la UIT. El trabajo de mi sección es crucial para obtener las pruebas necesarias procedentes de todos los dispositivos informáticos que se incautan durante las entradas y registros.

2. ¿Cómo se incardina la UIT en la actividad de la CNP?

La UIT no solo lleva a cabo las investigaciones con implicación tecnológica sino que, con frecuencia, participamos y coordinamos en otras investigaciones en las que existe un componente tecnológico como seguimientos en redes sociales, forenses en dispositivos informáticos, etc. Vamos, que no nos aburrimos ;)

3. ¿En qué consiste el día a día de la UIT?

No solo tenemos presencia en las investigaciones tecnológicas sino que cada vez recibimos más requerimientos para participar en grupos de trabajo internacionales, reuniones de coordinación de las investigaciones en EUROPOL e INTERPOL, diseño y participación en actividades y foros sobre ciberseguridad, buscar soluciones tecnológicas y aplicaciones prácticas de las nuevas medidas judiciales como el agente encubierto o las monedas virtuales. Cada vez tenemos más trabajo, de mayor especialización y complejidad.

4. ¿Podría indicarnos qué tipos delictivos son los que mayor crecimiento presentan en España?

Los fraudes son los más frecuentes, con un 60% de incidencia, pero los ciberataques, intrusiones, fugas de información y los delitos cometidos a través o con implicación de las redes sociales. En todo caso, existe una elevada cifra negra de hechos que son denunciados. No saber que se está siendo víctima de un delito, de qué forma se puede denunciar, sentimiento de culpabilidad por pensar que uno tiene la culpa de lo que ha sucedido o pensar que la denuncia sirve de poco, son algunos de los motivos.

5. En su opinión, ¿están alineados los procesos de investigación policial con los procesos procesales y judiciales en España? ¿se encuentran los cuerpos policiales con cortapisas a la hora de realizar investigaciones efectivas en el ciberespacio?

No. Lo que se denuncia, se investiga. Otra cosa es que la Ley de Enjuiciamiento Criminal o la del Poder Judicial no concrete ni delimite competencias y no se ajuste a la realidad de este tipo de hechos. O agilizamos y concretamos los procesos, o se quedarán muchas denuncias y procedimientos sin investigar.

6. Dada su amplia experiencia en el campo de la investigación operativa ¿cree que la tipificación penal de los delitos tecnológicos es lo suficientemente amplia para recoger y amparar las actuaciones ilegítimas en el ciberespacio o, por el contrario, los delincuentes cuentan con cierto margen de indefinición que les favorece?

No, no hace falta incluir más delitos sino agilizar los procedimientos. El ciberespacio tiene otras normas y demanda procedimientos más ágiles. Desde luego, la investigación y las medidas procesales tradicionales no sirven.

7. Pregunta obligada ¿existen mecanismos ágiles de coordinación con otros cuerpos con competencias de delitos informáticos como Guardia Civil, policías autonómicas y locales? Y en el plano internacional ¿qué tal funciona la coordinación con Europol, Interpol y otros cuerpos policiales?

Si, a nivel estatal existen mecanismos de coordinación con otras policías pero hay tanto trabajo que rara es la vez que se cruzan las investigaciones. A nivel internacional, EUROPOL e INTERPOL realizan una labor clave, no solo participando en la coordinación de los dispositivos, sino que si es necesario, agentes de estas instituciones participan directamente en nuestros dispositivos aportando su experiencia y sus medios. Sin la existencia de estas agencias, sería imposible llevar a cabo las investigaciones.

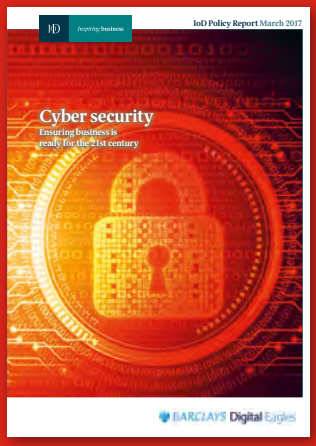
8. ¿Cuentan las fuerzas y cuerpos de seguridad del Estado con los recursos humanos y tecnológicos necesarios para hacer frente a un perfil criminal cada vez más sofisticado y profesionalizado? Si pudiese pedir ¿qué pediría?

Pediría que el cibercrimen, su magnitud real, la especialización tecnológica y la importancia de nuestro trabajo pasen a ser una preocupación y una prioridad real para el Estado. Todo lo que falta, vendría después.

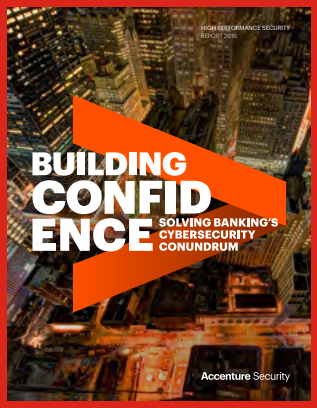
"Pediría que el cibercrimen, su magnitud real, la especialización tecnológica y la importancia de nuestro trabajo pasen a ser una preocupación y una prioridad real para el Estado."

4 Informes y análisis sobre ciberseguridad publicados en marzo de 2017

Cyber Security: Ensuring business is ready for 21st century (Barclays)



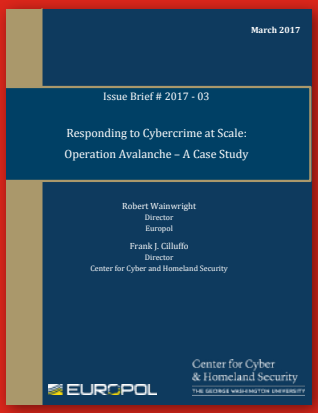
Building confidence: Solving banking´s cybersecurity conundrum (Accenture)



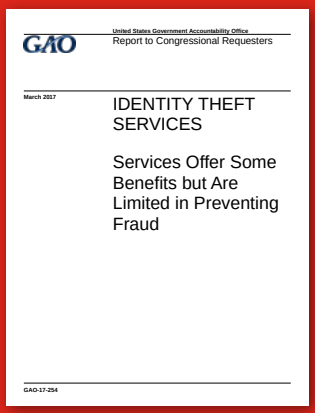
New Zealand´s Cybersecurity Strategy (New Zealand Government)

Women in Cybersecurity (EWF & (ISC)2)

Operation Avalanche – A Case Study (EUROPOL & George Washington University)



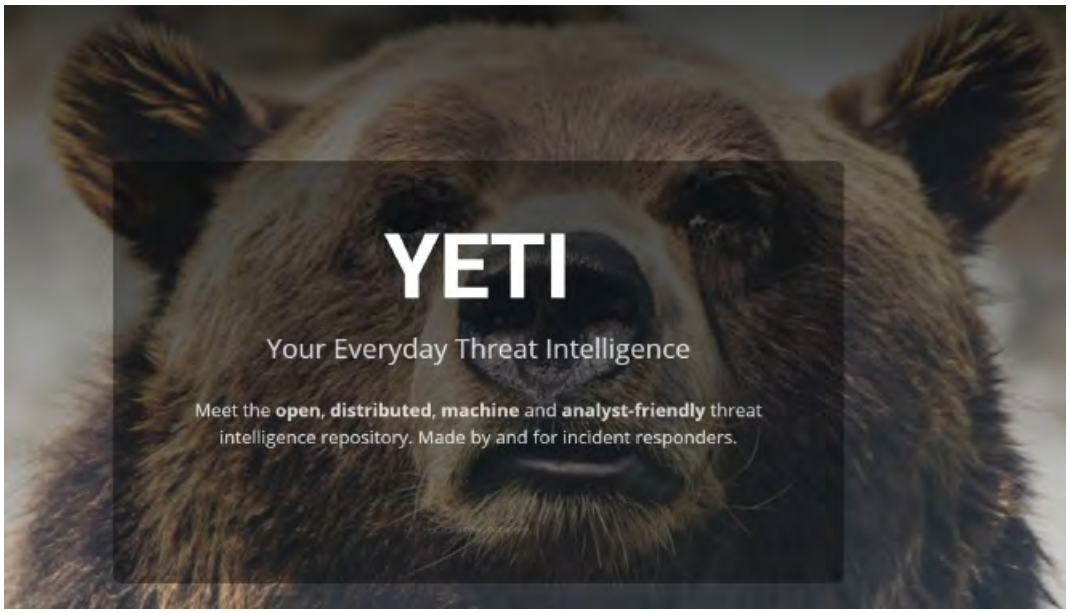
Identity Theft Services (U.S GAO)



Perspective on cyber risks 2017 (MinteEllison)

The U.S Army robotics and autonomous systems strategy (U.S Army)

5 HERRAMIENTAS DEL ANALISTA:
Yeti



Yeti es una plataforma destinada a organizar observables, indicadores de compromiso, TTPs (tácticas, técnicas y procedimientos) y conocimientos sobre ciberamenazas en un único repositorio unificado. Yeti también enriquecerá automáticamente los observables (por ejemplo, resolviendo dominios o geolocalizando IPs) para que no tenga que hacerlo el analista. Yeti proporciona además una interfaz web para los analistas (interfaz de usuario basada en Bootstrap) y otra para integraciones (API web) para que otras herramientas puedan interactuar con la solución.

Yeti nació de la frustración de tener que responder a la pregunta "¿dónde he visto este artefacto de inteligencia antes?" o buscar objetivos específicos para vincularlos a una familia de malware concreta. Aunque originalmente era un proyecto independiente, Yeti no podría haber existido sin el equipo de CERT Société Générale, que realizó innumerables horas de pruebas de la herramienta y orientó el desarrollo para adaptarse mejor a sus necesidades.

En pocas palabras, Yeti permite:

- Presentar observables y obtener una conjetura de calidad sobre la naturaleza de la amenaza.
- A la inversa, centrándose en una amenaza, permite listar rápidamente todos los TTPs, observables y malware asociado.
- Permite que los analistas se enfoquen en la adición de inteligencia en lugar de preocuparse por los formatos de exportación compatibles con otros sistemas.
- Visualizar gráficos de relación entre diferentes amenazas.

Esto se ejecuta a través de:

- Recopilación y procesamiento de observables desde una amplia gama de fuentes diferentes (instancias MISP, rastreadores de malware, feeds XML, feeds JSON ...)

- Una API web para automatizar las consultas (pensando en la integración con una plataforma de gestión de incidentes) y el enriquecimiento (sandbox de malware).

- Exportación de los datos en formatos definidos por el usuario para que puedan ser ingeridos por aplicaciones de terceros (listas de bloqueo, SIEM, etc.).

Yeti está fundamentalmente programado en Python y JavaScript, si bien integra otros proyectos de código abierto como:

- MongoDB: un almacén de datos orientado a documentos.

- Redis: un almacenamiento de valores clave (utilizado por Celery para la programación).

- Apio: un programador (utiliza Redis).

6 Análisis de los Ciberataques del mes de marzo de 2017

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

CIBERCRIMEN

Múltiples expertos en seguridad ponen en duda *las afirmaciones de un actor con nombre en clave Turkish Crime Family*, que afirmó a comienzos de mes estar en posesión de cientos de millones de credenciales del servicio iCloud de Apple. El grupo afirmó tener una base de datos de 750 millones de credenciales de iCloud.com, mac.com y me.com, pero Apple dijo que no hubo violaciones de los sistemas de Apple, incluyendo Apple ID e iCloud. El actor, potencialmente turco, afirmo que haría públicas las credenciales a menos que recibiera $75.000 USD en criptodivisas o $ 100.000 USD en vales de iTunes. Aunque un análisis de 54 muestras proporcionadas parece legítimo, un portavoz de Shape Security dijo que sospecha que el actor puede haber empleado ataques de relleno de credenciales utilizando datos de incumplimientos anteriores para tener acceso a un pequeño número de cuentas de iCloud. Adicionalmente, el actor ha sido inconsistente con sus demandas, en un comunicado afirmó que tenía 200 millones de credenciales y en otro más de 750 millones.

Apple alega que las direcciones de correo electrónico y las contraseñas probablemente se obtuvieron de servicios de terceros previamente comprometidos. Si bien la legitimidad de los actores es incierta, como medida de precaución, se ha sugerido a los usuarios que cambien sus contraseñas de forma preventiva.

CIBERESPIONAJE

El Departamento de Seguridad Nacional de los Estados Unidos (DHS, por sus siglas en inglés) *ha estado investigando durante este mes comportamientos sospechosos procedentes de múltiples torres de telefonía móvil pertenecientes a un operador móvil estadounidense en Washingon DC*. El Programa de Vigilancia de la ESD basado en Las Vegas dice que una gran cantidad de datos están siendo recogidos por un tercero y se desconocen los motivos y actores implicados. La compañía ha detectado torres de telefonía falsas, que son a menudo utilizados por los ciberdelincuentes. Una fuente dijo al Washington Post que la actividad se observó por primera vez en el área del DC, pero fue observada posteriormente en otros sensores a través de los EE.UU. Un sensor estaba cercando a la Casa Blanca y al Pentágono.

Esta no es la primera vez que el Programa de Vigilancia de ESD ha informado sobre la existencia de torres de telefonía móvil falsas en la región de Washington DC. En 2014, la compañía lanzó una declaración indicando que sus ingenieros y algunos clientes habían descubierto una docena de torres telefónicas móviles, conocidas como receptores IMSI, alrededor de Washington, DC y otras partes de los Estados Unidos. Los números de identificación internacional de suscriptores móviles (IMSI) se utilizan para identificar a un abonado específico en una red móvil y se almacenan en las tarjetas SIM de los usuarios. Un catcher IMSI es una estación base que engaña a los usuarios de teléfonos celulares cercanos para que se conecten a ella en vez de a la estación base legítima de una red de telefonía móvil. Los receptores IMSI tienen el potencial de causar un daño significativo si son usados por un actor malicioso. Una vez que un dispositivo móvil es interceptado por un IMSI, el operador del interceptor es capaz de realizar una serie de tareas, incluyendo espionaje en llamadas o mensajes de texto, y en algunos casos, instalar software malicioso en el dispositivo. La ubicación de los receptores IMSI reportados en los medios de comunicación es preocupante, ya que conduce a preguntas sobre quién aprovecha esta capacidad.

Una gran cantidad de datos móviles en Washington DC está siendo interceptada por un tercero desconocido utilizando falsas estaciones base móviles situadas cerca de la Casa Blanca y el Pentágono

Un portavoz de la Oficina Federal Alemana para la Seguridad de la Información (BSI) dijo que el gobierno ha tenido éxito en la gestión de dos ciberataques del grupo de espionaje APT28, también conocido como Fancy Bear. El presidente de la BSI, Arne Schoenbohm, comunicó que el primer intento tuvo lugar en mayo de 2016, cuando el grupo intentó establecer un dominio de Internet para el partido de la Unión Demócrata Cristiana (CDU) de Angela Merkel en la región del Báltico. El segundo ataque ocurrió meses después, cuando se lanzó una campaña de phishing dirigida a los partidos alemanes en la cámara baja del parlamento. Según diversos informes, esa campaña utilizó un nombre de dominio OTAN en un esfuerzo por inyectar malware.

No es la primera vez que entidades gubernamentales y políticas alemanas reciben campañas de ataques dirigidos atribuidos al gupo APT28 (conocidos también como Tsar Team). Al menos desde abril de 2016, el grupo APT28 está apuntando activamente a organizaciones gubernamentales, diplomáticas y militares de Europa en sus esfuerzos por recopilar información estratégica que respalde las prioridades de seguridad nacional de Rusia. Concretamente, APT28 se dirigió a la CDU de la canciller alemana Angela Merkel, utilizando un servidor de correo corporativo de la CDU falsificado para robar credenciales y facilitar futuras operaciones y movimientos laterales. Además, en 2015, los actores de APT28 se dirigieron al Bundestag utilizando el malware conocido como XTunnel. APT28 ha demostrado durante mucho tiempo un gran interés en los asuntos del gobierno alemán, e históricamente se dirige a las entidades gubernamentales y de defensa en apoyo a cuestiones geopolíticas y regionales de interés para el Gobierno ruso.

A mediados de mes, *diversos investigadores de seguridad confirmaron que se encontró malware preinstalado en 38 dispositivos móviles Android* pertenecientes a dos grandes organizaciones. Investigadores de Check Point dicen que el malware estaba presente en los dispositivos antes de que fueran entregados a los usuarios, aunque no fuera parte de la ROM preinstalada por el proveedor. Esto indicaría que el malware se instaló en algún lugar a lo largo

de la cadena de suministro. No está claro si las infecciones fueron parte de un ataque dirigido contra las dos compañías, una de las cuales era una compañía de tecnología multinacional y la otra una gran compañía de telecomunicaciones. La mayor parte del malware era adware, aunque también se encontró información maliciosa de Loki.

HACKTIVISMO

Durante el mes de marzo, la web del Ministerio de Relaciones Exteriores de Corea del Sur *ha sufrido varios ataques distribuidos de denegación de servicio* (DDoS, por sus siglas en inglés) provenientes de direcciones IP chinas. Estos intentos se producen durante una época de tensión por el despliegue de un sistema de defensa antimisiles estadounidense en Corea del Sur. El mes pasado se produjeron ataques similares contra las versiones chinas de las webs del retailer surcoreano Lotte cuya consecuencia fueron periodos prolongados de inactividad, conllevando una fuerte pérdida de ingresos.

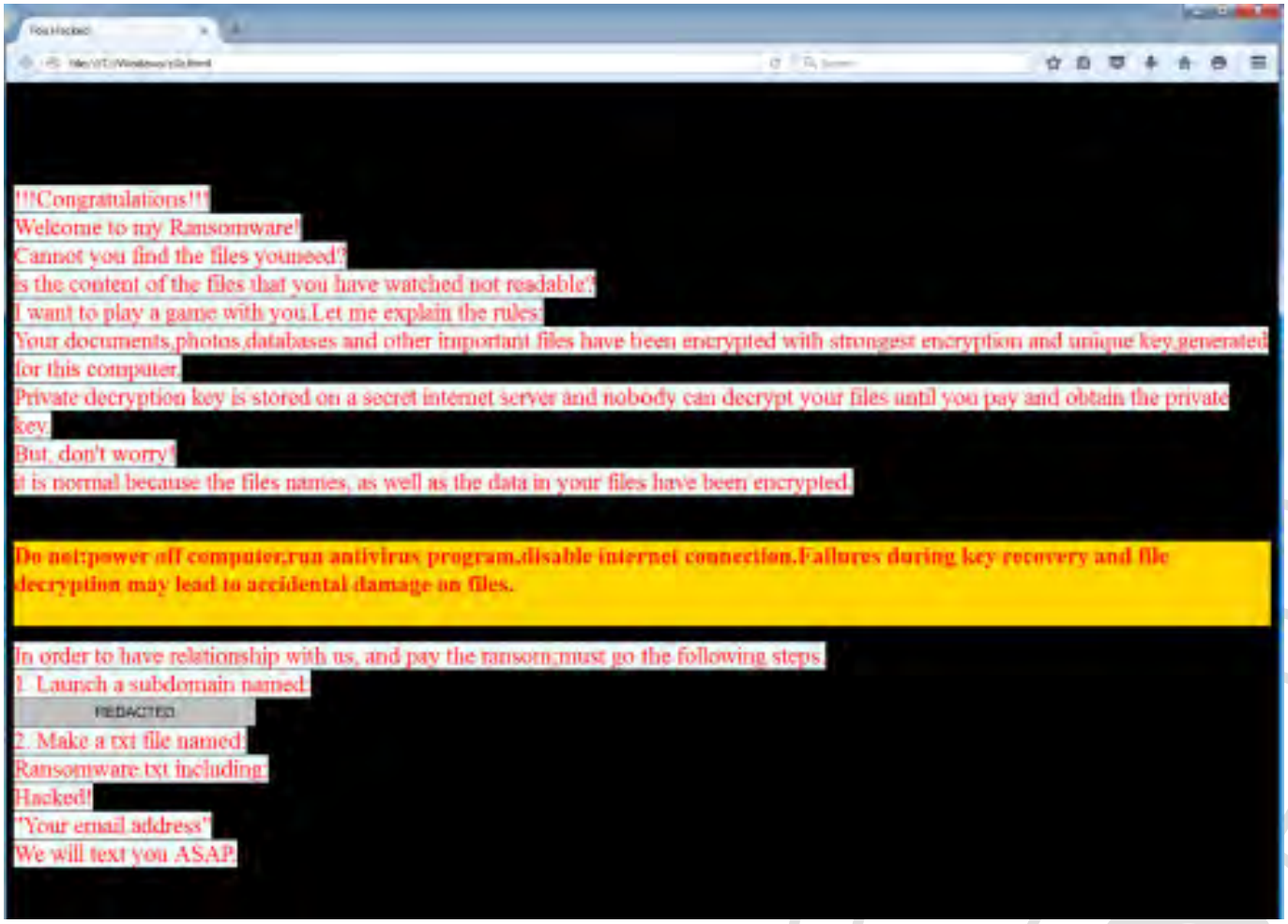
Debido a las actuales tensiones entre Corea del Sur y China, se espera que este tipo de ataques contra el gobierno de Corea del Sur y entidades privadas de la región se sigan sucediendo. Varios grupos hacktivistas pro-China han declarado públicamente su intención de atacar webs surcoreanas con DDoS y fugas de datos. Sin embargo, no se ha observado ningún actor reclamando la responsabilidad de los mencionados ataques contra el Ministerio de Relaciones Exteriores. Aunque algunos medios de comunicación atribuyen estos ataques DDoS al grupo hacktivista pro-China Red Union, el grupo negó su participación en cualquier actividad contra Corea del Sur para el despliegue del sistema de defensa antimisiles THAAD. Es posible que estos ataques fueran llevados a cabo por criminales, hacktivistas o actores hacktivistas de falsa bandera bajo el nombre de “Honker”, un término hacktivista chino común para el hacker pro-China Red Hat.

El ministro de Asuntos Exteriores surcoreano Cho June-hyuck

La compañía de seguridad PaloAlto ha identificado durante el mes de marzo un *nuevo tipo de ransomware, aparentemente diseñado para fines políticos.* El ransomware es generalmente utilizado por los ciberdelincuentes para obtener ganancias monetarias, cifrando los datos de la víctima y obligando a los usuarios infectados a pagar un rescate económico para descifrar sus archivos.

Sin embargo, en este caso, la campaña de ransomware 'RanRan' exigió una declaración política a cambio de la clave de cifrado. Se suponía que la víctima crearía un subdominio en su propio sitio web con un nombre difamatorio relacionado con un líder político y anunciaría que habían sido hackeados.

PaloAlto no proporciona detalles del actor responsable, pero observa varios errores en el código de rescate, así como la reutilización de código fuente disponible públicamente. Es importante destacar que el ransomware no alcanzó su objetivo en este caso, en el sentido de que las demandas de rescate no parecen haber sido cumplidas. Esto representa un nuevo uso de ransomware y una evolución interesante de la amenaza. Aunque esta iteración no tuvo éxito, es posible que estos actores busquen desarrollar maneras más sofisticadas de lograr fines políticos a través de un ransomware.



7 Recomendaciones

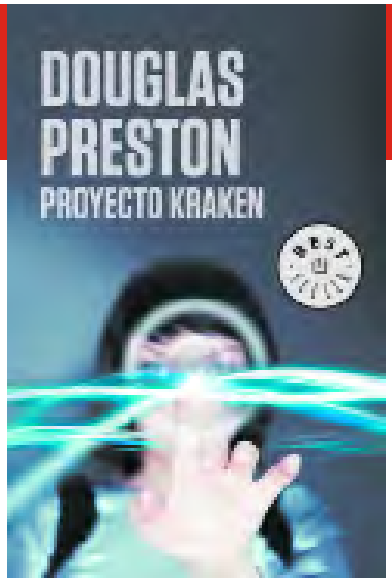
7.1 Libros y películas

Película:
GHOST IN THE SHELL

Sinopsis: Basada en la internacionalmente aclamada saga de ciencia ficción, 'Ghost in the Shell' narra la historia de Major, un híbrido cyborg-humano femenino único en su especie, que dirige un grupo operativo de élite llamado Sección 9. Consagrada a detener a los extremistas y criminales más peligrosos, la Sección 9 se enfrenta a un enemigo cuyo objetivo principal consiste en anular los avances de Hanka Robotic en el campo de la ciber-tecnología.

Libro:
UNA AL DÍA

Autor: Sergio de los Santos
Num. Páginas: 328
Editorial: 0xWORD
Año: 2015
Precio: 22.00 Euros
Sinopsis: Las casi dos décadas de "Una al día" sirven de excusa para un libro que está compuesto por material nuevo, revisado y redactado desde la perspectiva del tiempo. Además, incluye entrevistas exclusivas a los personajes relevantes de cada momento en el mundo de la seguridad: Bruce Schneier, Eugene Kaspersky, Cuartango, Mikel Urizarbarrena, Jorge Ramió, Johannes Ullrich...



Cómic:
PROYECTO KRAKEN

Autor: Dougas Preston
Num. Páginas: 384
Editorial: Punto de Lectura
Año: 2016
Precio: 9.95 Euros
Sinopsis: Melissa Shepherd lidera el equipo de la NASA que ha lanzado un vehículo de pruebas en el llamado mar de Kraken, uno de los lagos de Titán, la luna más grande del planeta Saturno. La nave posee un software de inteligencia artificial capaz de operar como una criatura autónoma, a la que Melissa ha bautizado con el nombre de Dorothy. Cuando en la central de la NASA desde donde se monitoriza el experimento se produce una explosión y mueren varios científicos, Dorothy despierta en un entorno hostil para el que no está preparada. Se siente traicionada, responsabiliza a su creadora y decide rebelarse y destruirla a ella y a su mundo.

Libro:
COMUNICACIÓN DE CRISIS

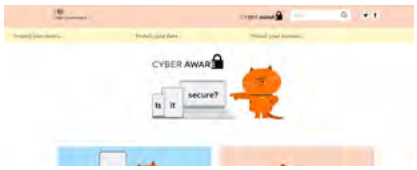
Autor: Antonio Castilla y Damián Ponce
Num. Páginas: 200
Editorial: Fragua
Año: 2015
Precio: 15.00 Euros
Sinopsis: A través del estudio académico y su confrontación con el universo laboral y especializado, se desarrollan diversas observaciones que se plasman en esta obra. Cómo el ciberespacio, el mundo digital ha modificado los paradigmas, creando nuevos horizontes en los que el comunicador profesional debe saber desenvolverse, ser proactivo, monitorizar a las audiencias y ser capaz de realizar estrategias comunicativas ante la hostilidad de los intervinientes en la Conversación. Empresa y profesionales deben ser conscientes de las nuevas reglas a aplicar en el mundo de la comunicación corporativa y de crisis en Internet, en el tenue horizonte del 2.0 que tiene sus propias normas y peligros comunicacionales.

Libro:
LA DIGITALIZACIÓN DEL OTRO

Autor: Carlos Ruiz
Num. Páginas: 152
Editorial: Milenio
Año: 2016
Precio: 15.00 Euros
Sinopsis: El Prometeo tecnológico del siglo XXI nos ha entregado el fuego artificial y nos ha convertido en pequeños demiurgos. Hemos despertado de un sueño milenario y se han abierto las puertas de la tierra prometida de la interactividad. Prometeo nos ha dado el poder simbólico y estamos ebrios de nosotros mismos. Somos hijos de un mesianismo tecnológico y estamos convencidos de que el único límite de la acción humana estriba en aquello que (todavía) no puede hacer la tecnología. El resto, es posible. Y deseable. Somos, como diría Ortega y Gasset, unos niños mimados. Vivimos en una sociedad acelerada, seducida por la tecnología y, sin darnos cuenta, a golpes de clics, renunciamos a nuestra vida privada y a nuestras libertades mientras nos entretenemos en Internet. No somos conscientes de que la nueva soberanía que tenemos en el ciberespacio pone en riesgo la propia democracia.

7.2 Webs recomendadas

http://www.cyberaware.gov.uk/
Sito web de la campaña del gobierno británico para la concienciación de PYMES y ciudadanos en materia de ciberseguridad.



https://www.cybercareers.gov/
Sitio web de la iniciativa Cyber Careers, la cual surge como resultado del desarrollo de la estrategia de la administración estadounidense para el reclutamiento personal que deberá velar por su ciberseguridad.

https://www.getcybersafe.gc.ca/index-en.aspx
Sitio web creado por el gobierno canadiense para la concienciación en materia de ciberseguridad de todos los sectores del país.

https://www.staysmartonline.gov.au/
Sitio web de la iniciativa del gobierno australiano destinada a la concienciación de sus ciudadanos sobre los riesgos asociados al uso de Internet.

http://iofthings.org/
Sitio web de IoT Things, la asociación de compañías dedicadas al desarrollo de tecnologías asociadas al Internet de las Cosas.

https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
Sitio web de la Interpol dedicado a la lucha contra el cibercrimen.

7.3 Cuentas de Twitter

@TRADOC

@sbarrera0

@fwhibbit_blog

@RadioHacking

@siteintelgroup

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
2- 6 abril	St. Maarten, Holanda	Kaspersky	Kaspersky SAS	https://sas.kaspersky.com/
3- 7 abril	Malta	International Financial Cryptography Association	Financial Cryptography and Data Security 2017	http://fc17.ifca.ai/
4-5 abril	Manchester	Industry 4.0 Summit	Industry 4.0 Summit	http://www.industry40summit.com/
4- 6 abril	Praga	EBC-Slovakia	CyberCentral	http://cybercentral.eu/
6 abril	Utrecht	DCWC Dutch Cyber Warfare Community	15th Dutch CyberWarfare Roundtable	https://www.eventbrite.nl/e/dcwc-roundtable-15-tickets-32599065683
7 abril	Edinburgo	BSIDES	Bsides Edinburgh	https://www.bsidesedinburgh.org.uk/
9 Abril	Dubai, UAE	ICS Cyber Security Forum	2nd Annual GCC ICS Cyber Security Forum	http://www.icssecurityforum.com/
18 - 19 abril	Riyadh	Fleming	Kingdom Cyber Security	https://fleming.events/en/events/security/kingdom-cyber-security-conference
21 abril	Paris	dotConferences	Dot Security	https://www.dotsecurity.io/
24 abril	Hamburgo	we.CONECT GLOBAL LEADERS	Rethink! IT Security 2017	http://rethink-it-security.de/de/
25- 27 abril	Mexico DF	infosecurity Group	Infosecurity Mexico	http://www.infosecuritymexico.com/en/About-InfosecurityMexico/About-Infosecurity-Mexico/
26- 27 abril	Londres	IQPC	ICS Cyber Security	https://icscybersecurity.iqpc.co.uk/
26- 28 abril	Paris	IEEE	2nd IEEE European Symposium on Security and Privacy	http://www.ieee-security.org/TC/EuroSP2017/
27- 28 abril	Gdynia, Polonia	x33fcon	x33fcon	https://www.x33fcon.com/#!index.md

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