REAL INSTITUTO elcano ROYAL INSTITUTE

DICIEMBRE 2017
Nº 31

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 Análisis de actualidad internacional 04

2 Ciberpolítica: análisis de actualidad 07

3 Informes y análisis sobre ciberseguridad publicados en noviembre 10

4 Herramientas del analista 10

5 Análisis de los ciberataques del mes de noviembre 11

6 Recomendaciones

6.1 Libros y películas 19

6.2 Webs recomendadas 21

6.3 Cuentas de Twitter 21

7 Eventos 22

1 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Analizando los archivos personales del último escondite de Bin Laden

AUTORES: Laboratorio de innovación de ElevenPaths

La Agencia Central de Inteligencia (CIA) hizo pública el pasado 1 de noviembre de 2017, la información recuperada en la operación ejecutada el 2 de mayo de 2011 en el complejo vinculado a Bin Laden en Abbottabad, Pakistán. Sin embargo, horas después de hacer pública la información en bruto de los discos duros extraídos de, al menos, tres equipos encontrados allí, la CIA eliminó el contenido argumentando "problemas técnicos". Ocho días más tarde volvieron a publicar la información, pero, en esta ocasión, modificada.

¿POR QUÉ TANTA PRISA EN RETIRAR LA INFORMACIÓN?

Este extremo es prácticamente imposible saberlo, sin embargo, a la hora de publicar la nueva información llegaron a dejar sus propios metadatos. Además, según informan, eliminaron algún fichero que contenía malware. Al verificar esos ficheros contra Virustotal obtuvimos el siguiente resultado: muestras no encontradas (524), con cero positivos (146) y con algún positivo (145). Aparentemente, muchos de los ficheros parecen no estar infectados. Sin embargo, por algún motivo, fueron eliminados por ser clasificados específicamente como "malware" o peligrosos.

```
MAL-000132    ./2011-1234/000201007/9B4429A8B0B5491FBC0302D5F595E9F3_212.zip/âŒÃ‘Î©Æ'Ã¿ Ã¡â^©Î´â^Ž
MAL-000133    ./2011-1234/000201007/A07894D63F9ABB7C8097936D4679BBF8_380.zip/Î©Ã±Î˜Âº 3.doc
MAL-000134    ./2011-1234/000201007/A1072D3F08C0115C6951FAE267265C38_294.zip/Æ'Î˜Â¼âŒâ^©Î€Ã.doc
MAL-000135    ./2011-1234/000201007/A31FFE7667FFD0CAC24E9394AB396895_WindowsUpdate.log
MAL-000136    ./2011-1234/000201007/ACE997C30A4678FA26D7EE53466433EF_55.zip/MOJLD6-1.DOC
MAL-000137    ./2011-1234/000201007/ACE997C30A4678FA26D7EE53466433EF_55.zip/MOJLD6-2.DOC
MAL-000138    ./2011-1234/000201007/ACE997C30A4678FA26D7EE53466433EF_55.zip/MOJLD6-3.DOC
MAL-000139    ./2011-1234/000201007/B741595C5C034E0E2557F1639B797CB4_353.zip/ÎƒÃ³Æ'Î†Îµ Î©Î˜Ã‘Î„Ã/
```

Ficheros .log (texto) catalogados por la CIA como malware.

Después de analizar la *primera publicación* realizada por la CIA, se verificó que (intencionalmente o no), se habían compartido archivos críticos del sistema. Los ficheros hiberfil.sys en Windows son un volcado de la memoria en sí y los pagefile.sys son el archivo de intercambio de memoria o "swap", por lo que se han podido ver ciertos trozos de "recuerdos" en memoria de diferentes procesos para conocer las direcciones URL a las que accedían desde ese ordenador, los proxies que utilizaban, además de identificarse algún indicador de compromiso (IOC, por sus siglas en inglés) como evidencia de la existencia de malware en la memoria del equipo. Como curiosidad, el antivirus que mantenían instalados los equipos incautados era una versión pirateada de ESET32, puesto que ejecutaban el servicio asociado. El análisis también parecía mostrar archivos pertenecientes al antivirus AVG e incluso algunas claves de software de Kasperksy, también pirateado.

ANÁLISIS DE LOS ARCHIVOS DE REGISTRO

Además de los ficheros de memoria, detectamos archivos de registro. Pudimos analizar todo tipo de archivos de sistema, incluidos no solo los ficheros HIVE, sino también SAM y SYSTEM. Con algunos ficheros HIVE y SYSTEM, pudimos saber qué programas se encontraban ejecutados al arrancar el sistema. Muchos de éstos eran un indicador de un equipo infectado. Por otro lado, también pudimos conocer no solo sus contraseñas sino también sus hábitos (cuándo generalmente iniciaban sesión o los usuarios con los que accedían a los equipos, así como cuándo fue el último login que se realizó). Respecto al último login realizado fue fechado el 1 de mayo de madrugada, justo un día antes de la operación de la CIA.

Name	Command line	Location
Msn Messsenger	C:\WINDOWS\system32\regsvr.exe	Run
Yahoo Messengger	C:\WINDOWS\system32\scvhost.exe	Run
cdoosoft	C:\WINDOWS\system32\olhrwef.exe	Run
ctfmon.exe	C:\WINDOWS\system32\ctfmon.exe	Run

Ejemplo de programas que arrancaban dos de los equipos.

Uno de los objetivos más importantes de la investigación fue encontrar contraseñas usadas para proteger las comunicaciones entre terroristas. En este sentido, encontramos una dirección de correo insertada en un documento Word, sin embargo, el contexto del archivo era mucho más interesante. Se trataba de una carta donde el remitente recomendaba que, debido a que Internet es tan inseguro, su comunicación debía ser comprimida y protegida con contraseña en los archivos que se fueran a enviar entre ellos. La contraseña significaba en inglés algo similar a: “No tengo objeción a lo que di, y él es de mente abierta”.

árabe español inglés árabe - detectado

inglés español francés Traducir

18- Then I asked you for special e-mails that are between us and you for direct correspondence, so we dispense with the mediator, and the mediator is for backup communications or you need to convert large files (attachments transferred via intermediaries) and because we are close to us, the Internet is very weak, But we can send messages and attached files of small size, and we have brothers engaged in communication and correspondence faithful, have experience, and use proxies and ways to go and disappear, thank God in general good things, but because of the weakness of the net, as I told you , So the file T large volume on the broker you transmit normally as you do, because we have another arrangement to her, but we want to put a password between us, so any attached files are compressed and you send a closed password, and the password is the complement between the two lines of the following two

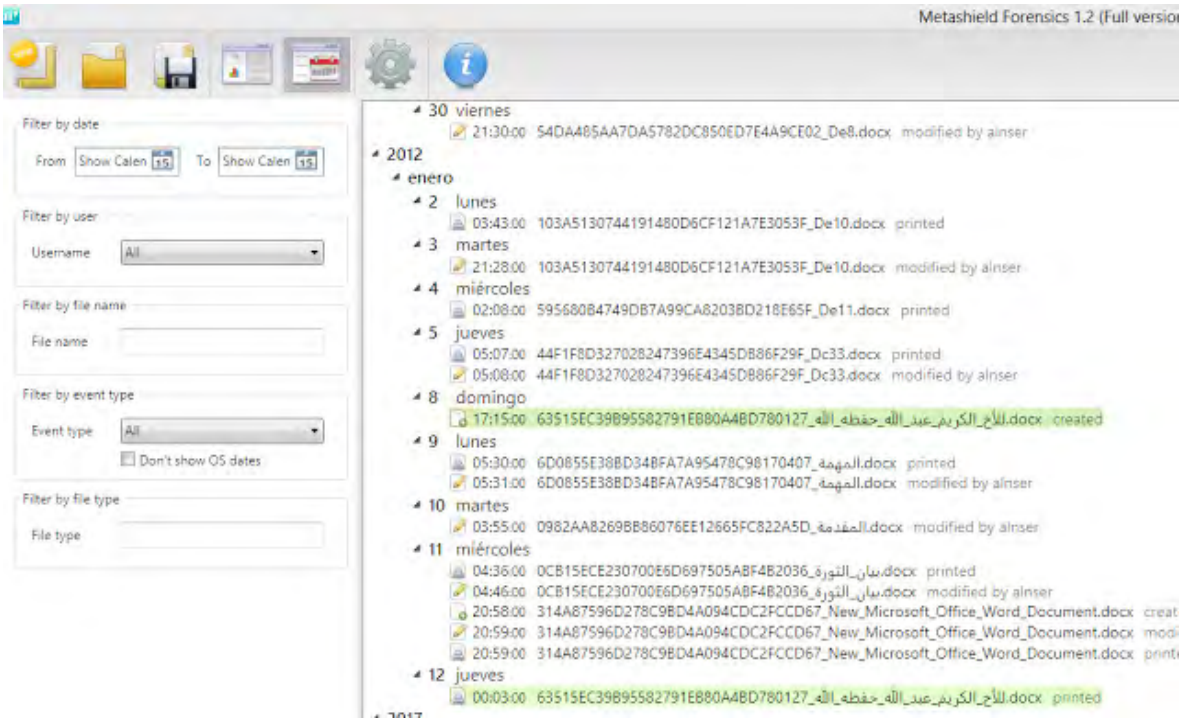
I have no objection to what I gave, and he is the open-minded

Then I will start and give you Emilela, we will be sent to him on the blessing of God which is:
fidaa22@yahoo.com

[Note: For more encryption and backup, please notify the responsible members of the transmission from you that they can change the extension of the attached files they send (which are encoded in the secrets program) to any audio or video extension such as: MP3, Love, and call them names do not indicate the body, and this is optional]

En estas carta se envían las instrucciones para ejecutar una comunicación “segura”

Tras analizar los metadatos de los ficheros, también pudimos encontrar uno de los últimos documentos escritos desde esos equipos. La fecha se establece en enero de 2012 (o incluso más adelante), es decir, después de la operación. Sin poder establecer otro motivo, suponemos que la fecha de algunos equipos se encontraba configurada incorrectamente.



Ciclo de vida de algunos de los documentos.

Por último, también guardaban en sus discos duros un libro de hacking. Este libro fue creado por el conocido “Terrorista 007” y se trataba de una guía básica sobre seguridad ofensiva, creado probablemente en 2006, con trucos y hacks comunes.

Uno de los libros de hacking encontrado en uno de los ordenadores de Bin Laden

2 CIBERPOLÍTICA: ANÁLISIS DE ACTUALIDAD

La Unión Europea descarta legislar el uso del cifrado

AUTORES: Javier Alonso Lecuit. Miembro Grupo de Trabajo sobre Ciberpolítica del Real Instituto Elcano

En diciembre de 2016, el Consejo Europeo de Ministros de Interior y Justicia solicitó a la Comisión Europea que defiera una posición sobre el uso del cifrado y otros mecanismos de anonimización en el contexto de las investigaciones policiales y judiciales contra el crimen organizado y el terrorismo.

El perímetro de análisis incluía el uso de cifrado en terminales de usuario y otros dispositivos TIC, estructuras de datos, espacios de almacenamiento en servidores, cloud, aplicaciones de comunicaciones y redes sociales (Skype, Whatsapp, Telegram, etc), páginas online o redes de comunicaciones, así como otros mecanismos de anonimización en *darknet.*

En su *Comunicación de octubre de 2017*, la Comisión reafirmó su firme apoyo al uso de técnicas de cifrado robustas para asegurar la economía digital, en línea con el Reglamento General para la Protección de Datos de Carácter Personal (art. 32) y la opinión de *ENISA* en diciembre de 2016. Básicamente, la Comisión interpreta que el uso de cifrado en Europa deriva del derecho fundamental a la privacidad de las personas físicas y jurídicas, por lo que:

- descarta legislar o limitar el uso de técnicas de cifrado
- excluye legalizar el uso de puertas traseras en redes, aplicaciones y dispositivos
- requiere a las autoridades que el descifrado u otras soluciones alternativas para el acceso a la información cifrada sea proporcional, no afecte de forma indiscriminada a grandes grupos de usuarios, ni debilite o se ponga en riesgo la protección de una determinada red, servicio o dispositivo.

Como estas tres condiciones de partida, a pesar de su enorme relevancia, no dan respuesta al problema inicial planteado, es decir, neutralizar los mecanismos de cifrado utilizados por el crimen organizado y el terrorismo en el contexto de las investigaciones policiales y judiciales; la Comisión expone varias medidas técnicas y operativas encaminadas a reforzar las actuales capacidades de las autoridades nacionales:

- El EC3 (Europol European Cybercrime Centre) ofrecerá a las autoridades de los estados apoyo técnico para el descifrado o la aplicación de técnicas alternativas que faciliten la información cifrada de los sujetos investigados, sin por ello exponer a riesgos adicionales de seguridad al conjunto de los usuarios del servicio afectado
- Promoverá entre los estados la compartición de un conjunto de técnicas (toolbox) alternativas al descifrado y utilizadas para el acceso a información cifrada en el curso de las investigaciones

- Alentará la colaboración con la industria tecnológica, proveedores de comunicaciones y proveedores de Internet, en particular aquellos que han incorporado el cifrado en sus servicios o tienen capacidad para interceptar los datos o metadatos de las comunicaciones.

- Creará una red de expertos europea al servicio de las fuerzas de seguridad y autoridades judiciales de los estados.

- Establecerá programas para la formación en este ámbito de fuerzas de seguridad y autoridades judiciales en colaboración con el ECTEG (European Cybercrime Training and Education Group) y CEPOL (EU Agency for Law Enforcement Training).

- En colaboración con el EC3 y Eurojust, el EJCN (European Judicial Cybercrime Centre) realizará un seguimiento de mejores prácticas y monitorizará los métodos de cifrado empleados por las organizaciones criminales y terroristas.

Estas medidas tácticas se verán complementadas en 2018 con el Plan de Cibeseguridad presentado en septiembre de 2017 al Parlamento y Consejo de Europa *(The Cybersecurity Act)* con propuestas tales como el anuncio de una Directiva para el acceso de las autoridades policiales y judiciales a pruebas digitales - en particular aquellas que se encuentren cifradas - (Directiva *e-evidence)* o diversas actuaciones encaminadas a fortalecer la cooperación transfronteriza entre las autoridades nacionales mediante la creación de una plataforma de comunicación o la armonización de los mecanismos para la cooperación judicial, entre otras.

En este contexto es significativo el creciente apremio de las autoridades comunitarias y nacionales sobre los principales proveedores de aplicaciones Internet (Apple, Google, Facebook o Microsoft, etc.) y los operadores de telecomunicaciones para la interceptación y entrega en claro de datos y metadatos de las comunicaciones, tanto desde el plano de la colaboración como en cumplimiento de nuevas obligaciones legislativas que se han incorporado en las leyes de seguridad nacional, por ejemplo del Reino Unido o Francia.

Sin embargo, las autoridades y la industria tecnológica se enfrentan a dificultades que son en ocasiones prácticamente insalvables en tiempo, forma y coste como claves solo accesibles por el usuario final o prácticamente imposibles de descifrar aplicando los medios y plazos disponibles, así como limitaciones a la obligación de colaboración de los incriminados en aplicación del derecho de no incriminación reconocido en determinados países, entre otros.

En consecuencia, las autoridades debaten con el sector tecnológico alternativas tales como obligar a los proveedores de internet a conocer y verificar la identidad del usuario si ofrecen aplicaciones cifradas o establecer la obligación a los usuarios y organizaciones titulares de los datos cifrados de facilitar el acceso a las autoridades. Estas alternativas desplazarían el foco sobre el descifrado hacia nuevos ámbitos como por ejemplo la responsabilidad del proveedor de la aplicación de Internet en validar la identidad del usuario al tiempo de asegurar su privacidad y anonimato frente a terceros en la red.

A pesar de las soluciones que se adopten, y aunque aumenten las obligaciones sobre la industria y mejoren las capacidades técnicas de interceptación de comunicaciones cifradas de uso masivo en Internet, será difícil evitar que la delincuencia organizada y las organizaciones terroristas utilicen aplicaciones de cifrado end-to-end específicas o mecanismos de anonimización avanzados.

3 Informes y análisis sobre ciberseguridad publicados en noviembre de 2017

Estrategia de Seguridad Nacional 2017 (Departamento Seguridad Nacional)

Security recommendations for IoT (ENISA)

Making your company cyber resilient (Accenture)

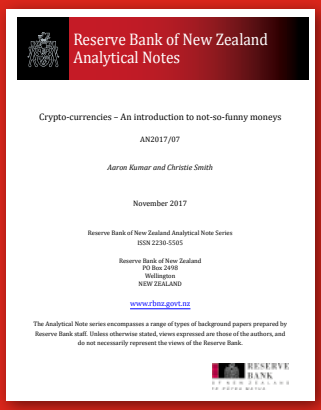
Commonality of risk assessment language in cyber insurance (ENISA)

Principios y recomendaciones basicas en ciberseguridad (CCN-CERT)

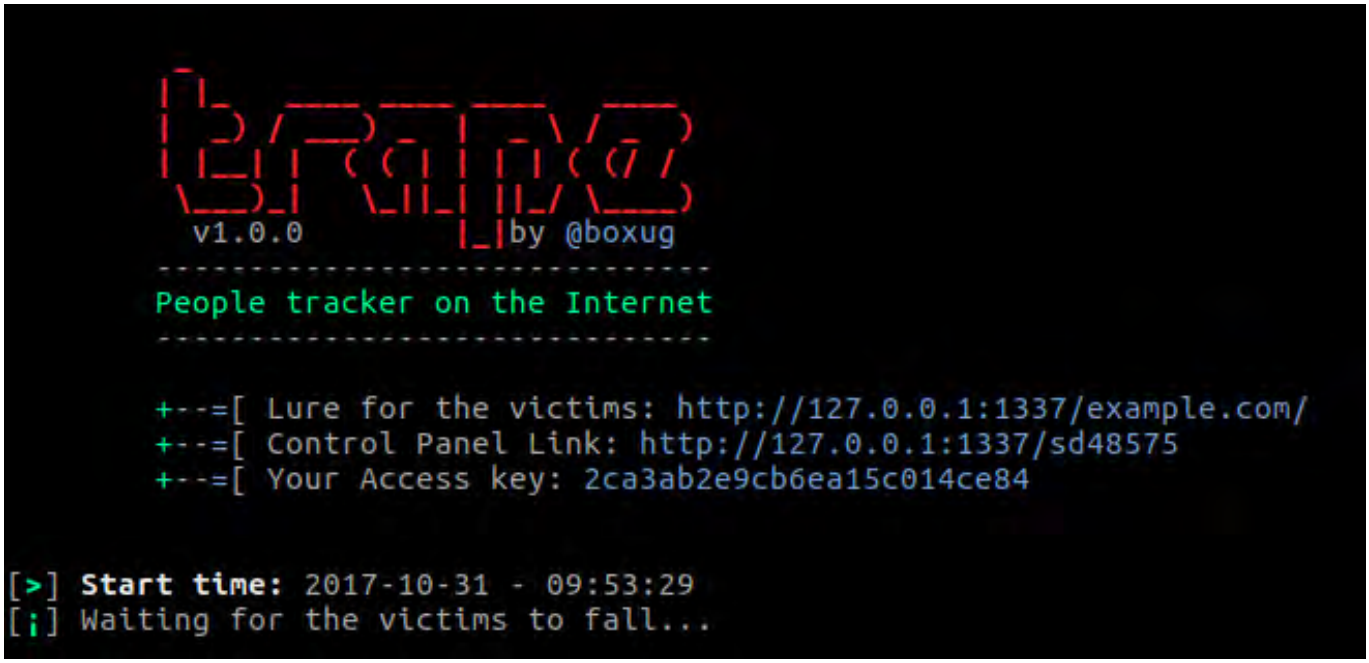
Entendiendo los ciberataques (Panda Security)

Annual Incident Analysis Report for the Trust Service Providers (ENISA)

Crypto-currencies: An Introduction to not-so funny moneys (Reserve Bank of New Zealand)



4 HERRAMIENTAS DEL ANALISTA:
Trape, people tracker on the Internet



Trape es una herramienta de reconocimiento gratuita de código abiertos que permite a los analistas rastrear sujetos en Internet, siendo la información que se puede obtener muy detallada. Como indican sus desarrolladores, esta herramienta se ha publicado con fines educativos a fin de mostrar cómo un usuario malintencionado podría rastrear, monitorizar u obtener información de credenciales de usuarios, desde un punto de vista de awareness y concienciación.

Entre las funcionalidades más destacables se encuentran:

- Reconocimiento remoto de sesiones: se puede saber dónde se ha conectado una persona, de forma remota. Esto ocurre a través de una derivación realizada en la misma política de origen (SOP).
- Actualmente se puede interactuar con la herramienta desde una interfaz web. (La consola, se convierte en una vista previa de los registros y acciones).
- El registro de las víctimas así como las solicitudes de datos, entre otros, se obtienen en tiempo real.
- Si se obtiene más información de una persona tras un equipo, se puede generar un ataque más directo y sofisticado. Trape fue utilizado en operaciones reales para rastrear criminales y conocer su comportamiento.
- Se pueden ejecutar ataques de phishing en tiempo real, ataques de hooking simples, mapping de usuarios, reconocimiento de objetivos, captura de credenciales e inteligencia de fuentes abiertas (OSINT).

Traper permite reconocer sesiones de los siguientes servicios:

1. Facebook
2. Twitter
3. VK
4. Reddit
5. Gmail
6. tumblr
7. Instagram
8. Github
9. Bitbucket
10. Dropbox
11. Spotify
12. PayPal
13. Amazon
14. Foursquare
15. Airbnb
16. Hackernews
17. Slack

El siguiente *enlace* contiene un video informativo en español sobre su funcionamiento.

5 Análisis de los Ciberataques del mes de noviembre de 2017

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

CIBERCRIMEN

A principios de mes, investigadores de Kaspersky descubrieron un *nuevo troyano bancario enfocado principalmente en atacar bancos en Rusia, Armenia y Malasia*. Los investigadores especulan que el troyano, conocido como Silence, puede ser el trabajo del conocido grupo criminal llamado Carbanak. Silence comienza su actividad maliciosa al obtener acceso a la cuenta de correo electrónico de un empleado del banco y utilizarla para enviar correos electrónicos de phishing a otros empleados.

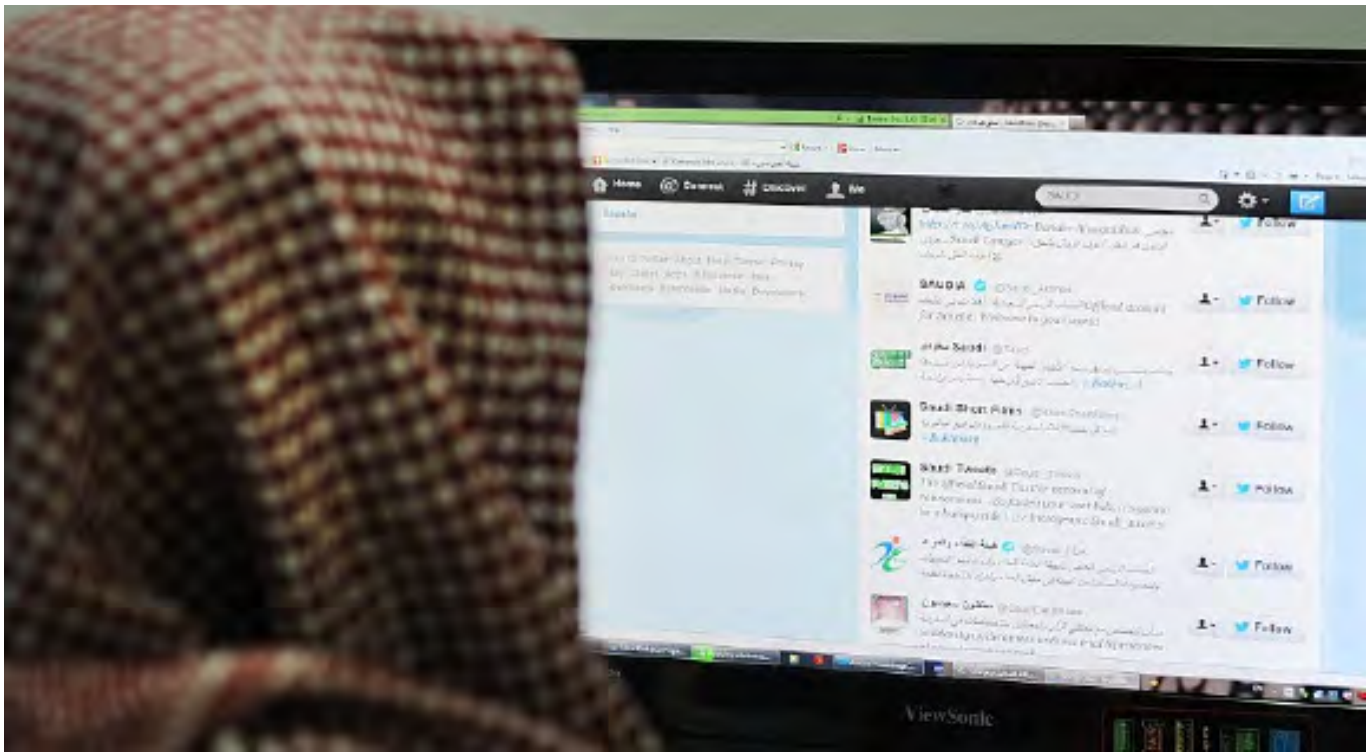
El correo electrónico de phishing instala un *dropper* que recopila datos en una máquina y envía la información a los servidores de comando y control de los atacantes (C&C). Cuando encuentran información útil, los atacantes despliegan un segundo *payload* malicioso que instala el malware Silence, que es capaz de realizar capturas de pantalla repetidas a intervalos rápidos, proporcionando un pseudo-video de la actividad de la víctima. Esa información puede ser utilizada por los atacantes en fases posteriores, como la identificación de URL para sistemas de administración financiera, aplicaciones locales que pueden ser explotadas u obtener una visión general de otros equipos en la red local.

El 22 de noviembre, diversos funcionarios en Arabia Saudita comunicaron la detección de nuevos ciberataques que intentaban interrumpir e infectar las redes informáticas del gobierno.

Según el Centro Nacional de Seguridad Cibernética (NCSC), el ataque utilizó código Powershell para la infección, pero no mencionó el origen del ataque ni a qué entidades gubernamentales se dirigió. Sin embargo, dijeron

que sospechaban de un nuevo grupo avanzado realizando actividades a través de APTs distribuidos a través de *spearphishings*. Arabia Saudí tiene una historia de ciberataques avanzados, sobre todo tras el conocido Shamoon, un malware que eliminaba el contenido de discos duros y que fue utilizado contra el sector energético saudí en 2012.

Los saudíes han sido tradicionalmente atacados por grupos ubicados en Medio Oriente y el sur de Asia. El grupo con vinculación iraní APT33 y Newscaster Team son las amenazas avanzadas más frecuentes para Arabia Saudita, enfocándose, entre otros, hacia los sistemas de control industrial y otros objetivos del sector energético saudita.



CIBERESPIONAJE

En el plano de las operaciones de espionaje en el ciberespacio, *la investigación del abogado estadounidense Robert Mueller sobre los presuntos vínculos entre Rusia y la campaña presidencial de Donald Trump* ha revelado que potenciales atacantes de origen ruso intentaron acceder a las cuentas de correo electrónico de altas autoridades civiles y militares estadounidenses entre marzo de 2015 y mayo de 2017.

Concretamente, los atacantes accedieron los correos electrónicos del Secretario de Estado John Kerry, del ex secretario de Estado Colin Powell o de los Jefes del Mando Supremo Aliado en Europa, Philip Breedlove y Wesley Clark. También dirigieron los ataques a más de 130 personas que trabajaban para el Partido Demócrata, así como a otras del Partido Republicano. La investigación de Mueller entra en una nueva etapa ahora que el Departamento de Justicia anunció a mediados de mes que el ex asesor de campaña de Trump, George Papadopoulos, se declaró culpable de mentir a los agentes del FBI que investigaban la posible colusión entre la campaña de Trump y el gobierno ruso.

En los últimos meses, THIBER ha ido informando sobre diversas campañas de espionaje con nexos rusos dirigido a generales estadounidenses y personal de la OTAN desde el verano

de 2016 como parte de la campaña “DC Leaks” que, aparentemente, puede ser una campaña falsa de hacktivismo llevada a cabo por APT28, también conocido como Cozy Bear o Tzar Team. Estos esfuerzos reflejan esfuerzos sostenidos de largo alcance de Rusia para influir en las elecciones a nivel internacional, afectando a las naciones extranjeras y aumentando la posición relativa de Rusia a nivel global, bajo los objetivos de la doctrina de información del Kremlin. Si bien esta información no es nueva, es de esperar que eventos similares reciban un mayor escrutinio a medida que continúen las investigaciones sobre la campaña de influencia rusa de 2016 en las elecciones presidenciales de EEUU.

A comienzos de mes, *una investigación del Ministerio de Defensa de Corea del Sur sobre un ciberataque en Daewoo Shipping and Marine Engineering Company* determinó que la autoría de los mismos era atribuible a Corea del Norte. Según la legisladora surcoreana Kyung Dae-soo, los atacantes pudieron robar planos sensibles de buques de guerra y otros documentos clasificados en un ataque que tuvo lugar en abril del año pasado.

La compañía ha construido varios buques de guerra surcoreanos, incluidos un buque de clase Aegis y submarinos. Los investigadores pudieron atribuir el ataque a atacantes norcoreanos porque el patrón era idéntico a otros ataques conocidos con origen en Pyongyang.

Los esfuerzos ciber de Corea del Norte parecen haberse centrado principalmente en objetivos financieros durante el año pasado, con actividades que van desde campañas de ransomware hasta ataques al sistema financiero SWIFT y la explotación de criptomonedas.

Sin embargo, la selección de una empresa de construcción naval en Corea del Sur está alineada con los objetivos estratégicos del régimen de

Pyongyang. Sin embargo, no debería descartarse la vinculación de este ataque concreto con un actor estatal chino que, con frecuencia recopilan información sobre propiedad intelectual militar, investigación y diseño. Podrían estar interesados en obtener información naval relacionada con las disputas actuales en el Mar del Sur de China. Al no disponer más información detallada sobre las tácticas, técnicas y procedimientos utilizados en este ataque, no es posible evaluar con precisión la atribución.

Por otra parte, el *6 de noviembre fue detectada una campaña de ciberespionaje a gran escala por parte de la empresa de seguridad Volexity*, dirigida aparentemente contra la Asociación de Naciones del Sudeste Asiático (ASEAN) y otros grupos de la sociedad civil en Vietnam, Camboya y otros países.

Potencialmente, la atribución podría vincularse al grupo OceanLotus (también conocido como APT 32) de con nexos con el gobierno vietnamita, implantando spyware en la web principal de la ASEAN y en más de 80 webs, incluidos pequeños medios de comunicación, grupos de derechos humanos y de la sociedad civil e individuos críticos con el gobierno vietnamita.

El spyware permitió a los atacantes rastrear, perfilar y redirigir a los visitantes a dichos sitios web comprometidos mediante exploitkits.

Ya a mediados de mes, *se hizo público que un contratista desconocido del Pentágono dejó una gran cantidad de datos críticos militares* en un servicio público en internet. Los datos constan de más de 1.800 millones de publicaciones comprendiendo un periodo que abarca casi un marco temporal de ocho años. El contratista dejó los registros en tres contenedores (buckets) de Amazon Web Server S3 de acceso público en lo que parece ser una operación de recopilación de inteligencia patrocinada por militares estadounidenses, dirigida tanto a ciudadanos americanos como a otros. Las publicaciones provienen de una variedad de fuentes que incluyen Facebook, grupos de discusión de fútbol y foros de videojuegos. Los contenedores AWS se configuraron para permitir el acceso a cualquier persona con una cuenta AWS de libre acceso. Los expertos han expresado su preocupación no solo por la recopilación de información sobre ciudadanos estadounidenses, sino también porque la seguridad sobre los datos era increíblemente laxa.

HACKTIVISMO

En el plano del hacktivismo, un grupo de piratas informáticos que se cree *vinculado a Hamas, durante este mes ha comenzado a focalizarse sobre organizaciones en Medio Oriente y el Norte de África con algunas herramientas y técnicas nuevas.*

El grupo, conocido como Gaza Cybergang (también conocido como Molerats y el Equipo de Gaza Hackers Team), existe desde al menos desde 2012 y se cree que tiene motivaciones políticas. Históricamente, el grupo se ha enfocado en organizaciones gubernamentales, diplomáticos y políticos de países como Egipto, Emiratos Árabes Unidos, Yemen, Jordania, Libia, Irán e Israel.

Los investigadores afirman que el grupo ahora también está focalizado en una organización del sector petrolífero y gasístico de la región.

Se cree que los hackers pudieron poner en peligro la red de la empresa y robar información durante más de un año. Gaza Cybergang agregó un troyano Android a su arsenal descubierto por Kaspersky en abril de 2017. Si bien se encontraron rastros del malware móvil Android en algunos de los ataques del grupo, también ha utilizado el *downloader* Downeks y la suite Cobaltstrike para obtener acceso remoto para las capacidades de espionaje y exfiltración de datos sin ser detectados.

Finalmente, un grupo hacktivista musulmán conocido como *Di5s3nSi0N ha atacado el sitio web oficial de ISIS / ISIL (Daesh) y ha publicado una lista de casi 2.000 usuarios* suscritos al boletín informativo y a las actualizaciones por correo electrónico de dicha web. La web de Amaq, que también actúa como una agencia de noticias para la organización terrorista, afirmó recientemente que estaba haciendo frente a una oleada de ciberataques. Un día después del anuncio de Amaq de que podían "manejar ataques a través de correo electrónico o cualquier tipo de ataque", Di5s3nSi0N encontró un error en la web que le permitió robar la lista de suscriptores. Al tener la web bajo control, los atacantes enviaron correos electrónicos insultantes a los suscriptores desde la dirección oficial del sitio informándoles que su información se había visto comprometida.

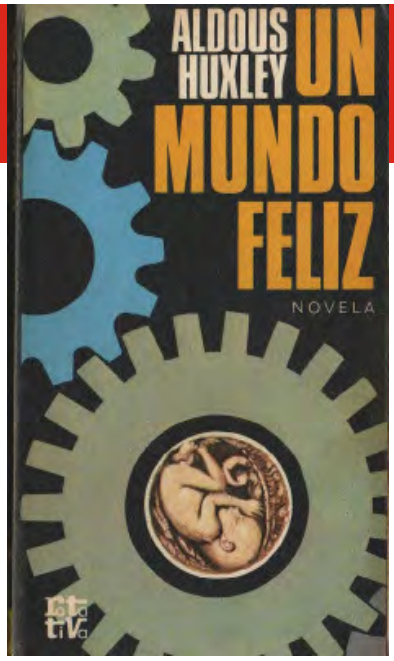
El contenido de dicho email era „Amaq ha sido #hackedo. Este es solo el comienzo #silencetheswords #amaq #daesh #OpISIS. „ Hemos observado que el usuario @Di5s3nSi0N__2 ha obtenido acceso a la lista de correo de Amaq de un miembro del grupo hacktivista pro-ISIS United Cyber Caliphate (UCC), que compartió capturas de pantalla del mismo mensaje de correo electrónico, presumiblemente enviado a la lista de correo de Amaq. Las publicaciones de @ Di5s3nSi0N__2 del 10 de noviembre parecen estar destinadas a publicitar este acceso públicamente, pero no indican que el actor haya llevado a cabo acciones adicionales con éxito, a pesar de afirmar la intención de hacerlo.

6 Recomendaciones

6.1 Libros y películas

Libro:
LA LOCURA DEL SOLUCIONISMO TECNOLÓGICO

Autor: Evgeny Morozov
Num. Páginas: 441
Editorial: KATZ
Año: 2015
Precio: 22,00 Euros
Sinopsis: Una advertencia sobre las trampas y los peligros de la fantasía, no tan lejana, de un mundo de eficiencia sin fisuras. Dentro de poco tiempo, la tecnología nos permitirá resolver problemas de maneras altamente originales, así como realizar sofisticadas intervenciones a gran escala en los ámbitos de la política, la cultura y la vida cotidiana. La tentación de la era digital es la de arreglar todo desde el crimen y la corrupción hasta la polución o la obesidad por medio de estrategias digitales de cuantificación. Sin embargo, una vez que los dilemas políticos y morales más profundos y persistentes se transformen en cuestiones no controvertidas y fácilmente manejables por medios tecnológicos, ¿qué resultados tendrá este"solucionismo"? ¿Sabemos acaso cómo nos afectará? Si cambiamos las motivaciones de nuestro comportamiento cívico y moral, es probable que cambiemos también la naturaleza misma de dicho comportamiento. Con el argumento de que necesitamos con suma urgencia una manera nueva de debatir las consecuencias morales de las tecnologías digitales, el libro nos advierte sobre las trampas y los peligros de la fantasía, no tan lejana, de un mundo de eficiencia sin fisuras.



Libro:
UN MUNDO FELIZ

Autor: Aldous Huxley
Num. Páginas: 256
Editorial: De Bolsillo
Año: 1932
Precio: 10,00 Euros
Sinopsis: La novela describe un mundo en el que finalmente se han cumplido los peores vaticinios: triunfan los dioses del consumo y la comodidad, y el orbe se organiza en diez zonas en apariencia seguras y estables. Sin embargo, este mundo ha sacrificado valores humanos esenciales, y sus habitantes son procreados in vitro a imagen y semejanza de una cadena de montaje.

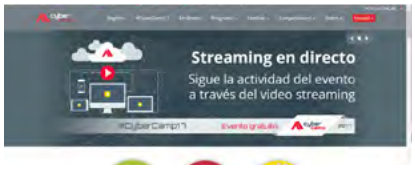
Libro:
LA SOCIEDAD DE COSTE MARGINAL CERO

Autor: Jeremy Rifkin
Num. Páginas: 464
Editorial: Paidós
Año: 2016
Precio: 28,00 Euros
Sinopsis: Jeremy Rifkin, el analista de tendencias económicas más importante de nuestro tiempo, nos acompaña en un viaje hacia un futuro que va más allá del sistema capitalista La sociedad de coste marginal cero confirma a Jeremy Rifkin como un visionario sin igual en el campo de las tendencias tecnológicas. Asistimos a la aparición de una nueva y extraordinaria infraestructura tecnológica–el Internet de las cosas–con el potencial de reducir a casi cero los costes marginales de grandes segmentos de la vida económica en los próximos años. Según Rifkin, este descenso de los costes marginales está dando lugar a una economía mixta–en parte mercado capitalista y en parte procomún colaborativo–que tiene repercusiones de gran alcance para la sociedad. En definitiva, Rifkin presenta una sociedad de coste marginal casi nulo que desencadenará en un nuevo paradigma económico.

6.2 Webs recomendadas

http://www.eulisa.europa.eu/Pages/default.aspx
Sitio web de la agencia europea para la gestión de grandes infraestructuras TIC.

https://cybercamp.es/
Sitio web donde podrás encontrar los videos y ponencias del evento CyberCamp 2017.



https://falsefriends.es/
Sitio web de False Friends, un colectivo de analistas e investigadores interesados en temas de seguridad.

https://www.state.gov/s/cyberissues/
Sitio web del Departamento de Defensa de los Estados Unidos responsable de la coordinación en materia relacionadas con el ciberespacio.

https://www.saferinternet.org.uk/
Sitio web del gobierno británico dedicado a la educación y concienciación en materia de ciberseguridad.

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

6.3 Cuentas de Twitter

@CybercampEs

@monivalle

@yrubiosec

@Bitcoin

@EULISA_agency

7 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
30 nov- 3 diciembre	Santander	INCIBE	CyberCamp 2017	https://cybercamp.es
1 diciembre	Amsterdam	akjassociates	7th e-Crime & Cybersecurity Europe Summit	http://www.e-crimecongress.org/event/europe
4-5 diciembre	Londres	Black Hat	Black Hat Europe 2017	https://www.blackhat.com/eu-17/
4-7 diciembre	Rennes, Francia	IEEE	IEEE International Workshop on Information Forensics and Security (WIFS)	http://wifs2017.org/
11-14 diciembre	Cambridge, UK	IEEE	The World Congress on Industrial Control Systems Security (SCADA/ ICS)	http://wcicss.org/
11-14 diciembre	Cambridge, UK	WorldCIS	World Congress on Internet Security (WorldCIS-2017)	http://www.worldcis.org/
13- 14 diciembre	Madrid	CCN-CERT	XI Jornadas STIC CCN-CERT	https://www.ccn-cert.cni.es/sobre-nosotros/jornadas-stic-ccn-cert/x-jornadas-stic-ccn-cert.html
29- 30 diciembre	Berlin	Hack4	Hack4	https://hack4.org/

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

gasNatural fenosa · Santander · Telefónica

Consejo Asesor Empresarial

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA · endesa · CEPSA

IBERIA · Fundación Cajasol · Escribano Mechanical & Engineering

Empresas Colaboradoras

CLH · European Climate Foundation · Aeroespacial y Defensa everis

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269