REAL INSTITUTO elcano ROYAL INSTITUTE

ENERO 2017
Nº 21

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 Xavier Serrano 10

4 Informes y análisis sobre ciberseguridad publicados en diciembre de 2016 ... 15

5 Herramientas del analista 16

6 Análisis de los ciberataques del mes de diciembre de 2016 18

7 Recomendaciones

7.1 Libros y películas 24

7.2 Webs recomendadas 26

7.3 Cuentas de Twitter.....26

8 Eventos.....27

1 COMENTARIO CIBERELCANO:
La ciberguerra de Trump

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

Fuente: : New York Times

A principios de 2013, el General *Valery Gerasimov* –Jefe del Estado Mayor de las Fuerzas Armadas de Rusia y viceministro de Defensa –argumentaba en los siguientes términos la im-portancia del uso del ciberespacio en *la nueva estrategia diseñada por el gobierno de Moscú para hacer la guerra*: *"Luchar una guerra sin lucharla: uso de la información, redes sociales virtuales, campañas de desinformación y engaño".*

A finales de 2016, el FBI y el DHS hacían público un *informe donde acusaban al Kremlin* de haber ordenado y ejecutado la ex filtración de los correos electrónicos de la candidata demócrata Hillary Clinton y otros miembros de su partido, así como su posterior publicación durante la carrera electoral hacia la Casa Blanca. Haciendo uso de algunas de las técnicas descritas por Gerasimov, el objetivo de Moscú -tal y como ha *concluido el Presidente Obama* - era influir en el resultado de las pasadas elecciones estadounidense. En este sentido, el presidente electo Donald Trump ha mostrado su airado desacuerdo con las conclusiones de las agencias de inteligencia del país las cuales considerada interesadas.

Sin embargo, no cabe duda de que durante la administración Trump la seguridad y defensa en el ciberespacio seguirán ocupando un lugar importante en la agenda política de Washington. En este sentido, el *vicepresidente electo Mike Pence* ha asegurado que Trump ejecutara durante los primeros días de su mandato *"un conjunto de acciones para luchar contra los ciberataques*

y proteger a los ciudadanos estadounidense de las amenazas cibernéticas". No será fácil pero Washington deberá afrontar una nueva etapa en la *ciberguerra que se libra* desde hace décadas ya que son cada vez más los actores –estatales y no estatales- que disponen de cibercapacidades de primer nivel. En este sentido, *el senador John McCain se ha mostrado muy crítico con la administración Obama* acusándola, al igual que Trump, de improvisar ante los diferentes ciberincidentes – *filtraciones de Snowden, ciberespionaje chino, ciberataques desde Iran, etc…*- que han acontecido durante los dos mandatos del demócrata. Es por ello que McCain reclama una nueva Estrategia Nacional de Ciberseguridad, acompañada de un conjunto de políticas, que permitan mejorar la seguridad y defensa del ciberespacio estadounidense. La reestructuración del U.S Cyber Command y su posible desvinculación de la NSA, la mejora en la coordinación cibernética entre las diferentes agencias de inteligencia del país y el *progreso de la colaboración público - privada en materia de ciberseguridad* son algunos de los desafíos a los que deberá enfrentar la administración Trump.

En definitiva, ahora más que nunca los estadounidenses son conscientes de que el ciberespacio es una dimensión configurada para ejercer poder. El presidente Trump tiene ante sí el reto de consolidar un sistema nacional de ciberseguridad con el objetivo de preparar al país para la ciberguerra del futuro.

"Luchar una guerra sin lucharla: uso de la información, redes sociales virtuales, campañas de desinformación y engaño"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

La guerra en Siria como pretexto para infectar a usuarios con ransomware

AUTOR: Yaiza Rubio, Analista de THIBER, the cybersecurity Think Tank. Analista de inteligencia de ElevenPaths.

Las cifras de 2016 sobre el número de infecciones por *ransomware* son alarmantes. Según un informe publicado por *Kaspersky Lab*, se estima que la frecuencia de infección por este tipo de *malware* en empresas es de una cada 40 segundos, convirtiéndose la educación, las telecomunicaciones y el entretenimiento los sectores más afectados. Sin embargo, el ratio de infección de usuarios individuales es todavía más impactante: uno cada diez segundos.

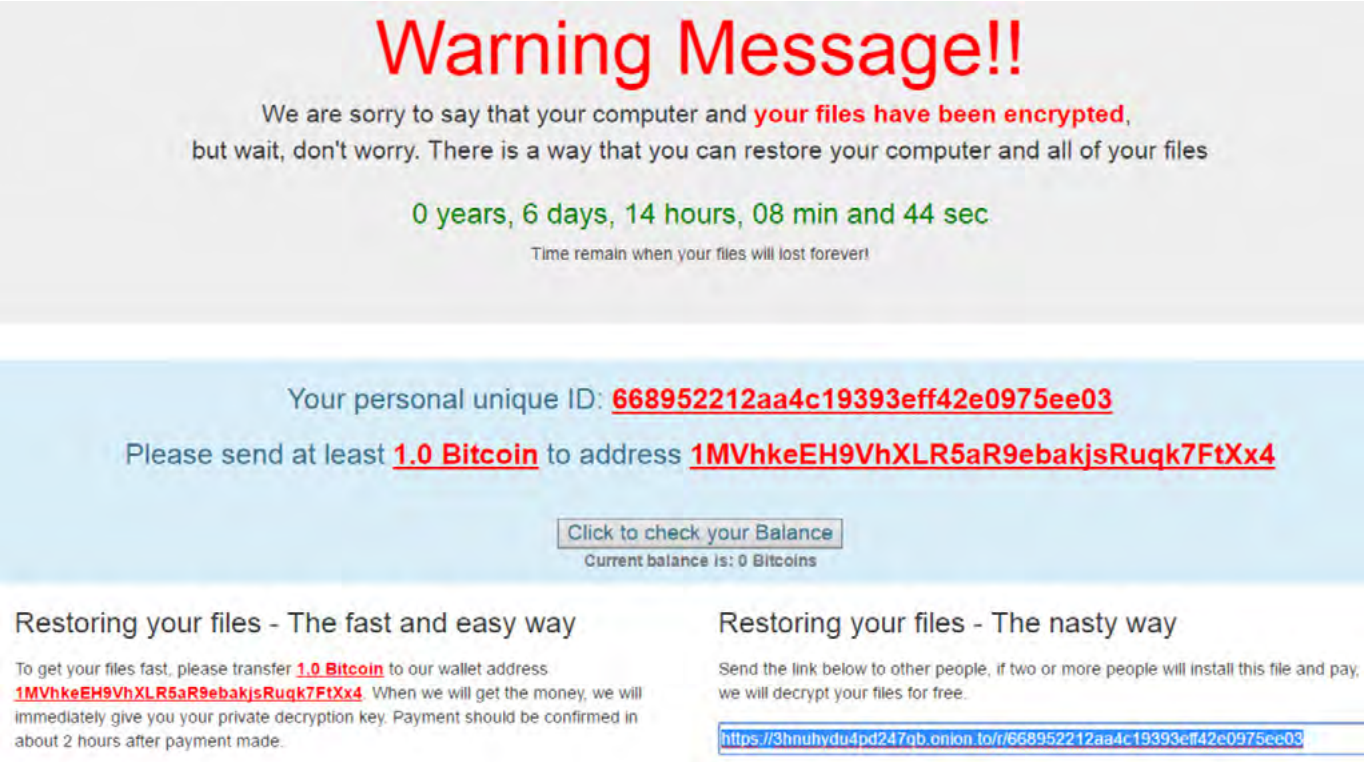
También es preocupante la cantidad de nuevas familias y modificaciones de *ransomware* que se han detectado a lo largo de este año. Llegó la primavera con la aparición de *Cerber* y *Locky*, que utilizaban correos electrónicos spam con archivos adjuntos para su propagación, mientras que otras como *CTB-Locker*, *CryptoWall* y *Shade* seguían su respectiva evolución. En cambio, se dijo adiós a otras variantes como T*eslacrypt, Encryptor RaaS* y *Wildfire*. La aparición de tantos tipos de familias ha dado lugar a que en ocasiones se hayan podido identificar versiones no del todo profesionalizadas.

Esto es lo que ha ocurrido con el *ransomware* denominado *Popcorn Time*. Después de que *Malware Hunter Team* publicara a principios del mes de diciembre el descubrimiento de este nuevo *ransomware*, analistas de *ElevenPaths*, descargaron y analizaron nuevas versiones de éste hasta llegar a identificar ciertos descuidos por parte de los propios desarrolladores del *malware*.

Un *ransomware* con visión de extorsión piramidal.

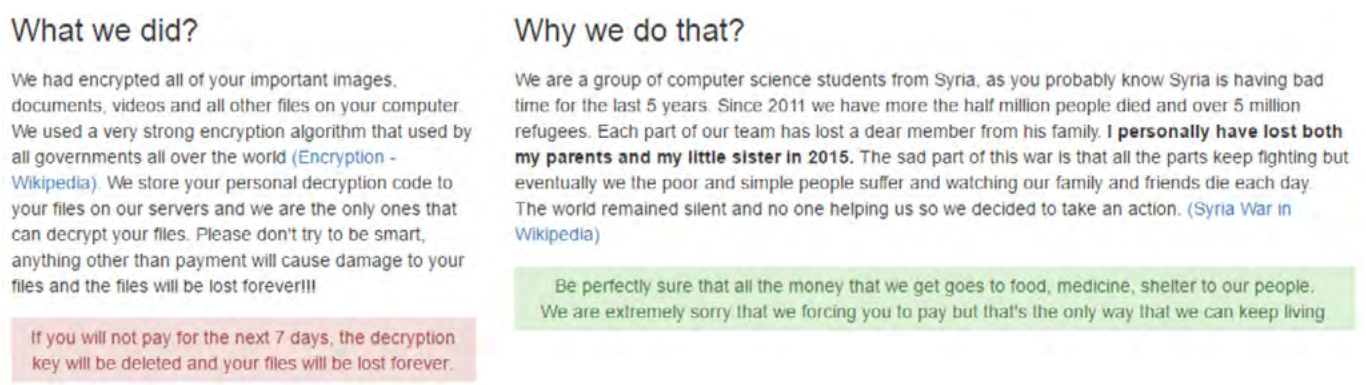
Este *ransomware* utiliza un nuevo sistema para aumentar el número de infecciones convirtiendo a las víctimas en atacantes. A cualquier

usuario infectado por el *malware* Popcorn Time (cuyo nombre es heredado de la aplicación para la visualización de películas en *streaming*) se le ofrece la posibilidad de desbloquear sus archivos con el pago generalmente de un *bitcoin*. La novedad es que también existe una segunda opción descrita por los desarrolladores como «the nasty way» (modo sucio, en español) que consiste en que el usuario forme parte de la infección ofreciéndole la posibilidad de descifrar sus ficheros de forma gratuita si consigue infectar y que paguen otras dos personas más.



Tipos de opciones para recuperar la información cifrada.

Otra particularidad de este *ransomware* es su intención de apelar al corazón de los afectados. Los autores se hacen pasar por estudiantes de informática en Siria y explican que han tomado la determinación de realizar esta acción porque nadie les ayuda. En concreto, el escritor del comunicado comenta que debido a la guerra «él personalmente ha perdido a sus padres y a su hermana pequeña en 2016».



Descripción de qué han hecho y por qué.

Sin embargo, aunque aparentemente ha sido desarrollado de forma ingeniosa, no sigue el patrón habitual del *ransomware* profesional. Tras un análisis pormenorizado, se ha evidenciado el método utilizado para la generación de las claves de cifrado utilizadas por cada muestra para secuestrar los ficheros. De hecho, se han identificado versiones anteriores en las que las contraseñas eran “123456”.

Funcionalidades nuevas de este *ransomware*.

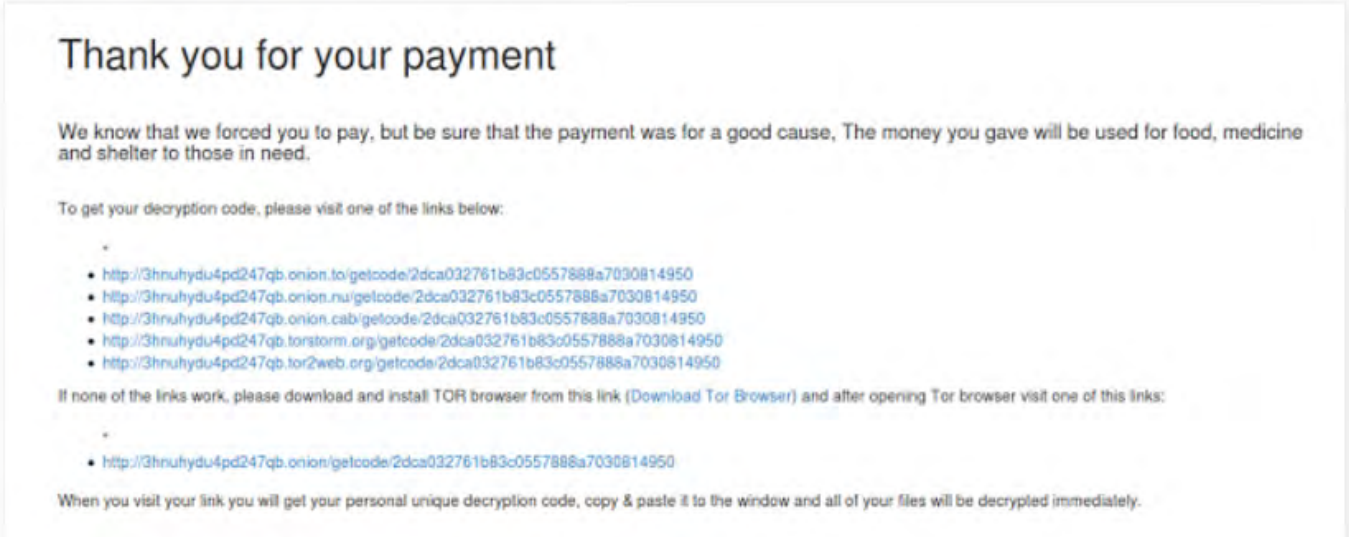
Pagar el rescate no es una medida garantista para recuperar los ficheros cifrados. No hay manera de saber si el ciberdelincuente cumplirá su parte del trato, así como tampoco de si el equipo infectado mostrará en un futuro alguna actividad sospechosa. Se estima que una de cada cinco empresas pequeñas y medianas que pagaron el rescate en 2016 nunca recuperaron su información.

En el caso de Popcorn Time, si se analiza el código HTML, nunca llega a realizar la validación del pago contra la plataforma de blockchain.info. Se desconoce si se trata por un error en la implementación ya que la dirección de Bitcoin propiedad del atacante aparece entrecomillada, o de si dicho error constituye parte del engaño ya que la plataforma nunca actualizará el valor de la cadena de bloques en el caso de efectuarse el pago.

```
function check(){$.get("https://blockchain.info/q/addressbalance/"12S9xb85GaVtrHrrh9MoMDHT2KZsndJ8C9"?confirmations=3",
function (data){data=data / 100000000; if (data >="1.0"){$("#paid").removeClass("hide"); $("#notpaid").addClass("hide");
$("#notpaid1").addClass("hide");}else{$("#balance").html("Current balance is: " + data + " Bitcoins");}
});}$("#chkbalance").on("click", function (){check();});
$(function (){check(); $('#clock').countdown({date: "Dec 19, 2016 13:42:15"});}); </script> </body></html>
```

Volumen de credenciales filtradas por país. Fuente: ElevenPaths.

De hecho, despliegan un servicio en la red anónima Tor donde se supone que dan acceso al código de descifrado. Al acceder a ellas, ya sea mediante intermediarios como onion.to o la descarga del navegador Tor, no fue posible obtener ninguna clave. Es por ello que podría deducirse que se encuentran aún en fase de pruebas.



Thank you for your payment

We know that we forced you to pay, but be sure that the payment was for a good cause, The money you gave will be used for food, medicine and shelter to those in need.

To get your decryption code, please visit one of the links below:

- http://3hnuhydu4pd247qb.onion.to/getcode/2dca032761b83c0557888a7030814950
- http://3hnuhydu4pd247qb.onion.nu/getcode/2dca032761b83c0557888a7030814950
- http://3hnuhydu4pd247qb.onion.cab/getcode/2dca032761b83c0557888a7030814950
- http://3hnuhydu4pd247qb.torstorm.org/getcode/2dca032761b83c0557888a7030814950
- http://3hnuhydu4pd247qb.tor2web.org/getcode/2dca032761b83c0557888a7030814950

If none of the links work, please download and install TOR browser from this link (Download Tor Browser) and after opening Tor browser visit one of this links:

- http://3hnuhydu4pd247qb.onion/getcode/2dca032761b83c0557888a7030814950

When you visit your link you will get your personal unique decryption code, copy & paste it to the window and all of your files will be decrypted immediately.

Servicio de Tor donde se encuentra la clave de descifrado.

Por su parte, el método «the nasty way» es novedoso entre las funcionalidades de propagación identificadas con anterioridad. Los analistas tras analizar el código observaron que no contiene ninguna instrucción que compruebe las futuras infecciones a otros usuarios de forma automática, por lo que existe una alta probabilidad de que se trate de un simple bulo para propagar el *malware*.

No hay duda que los cibercriminales cada día son más profesionales. Se han llegado a ver casos en donde ofrecen a las víctimas soporte técnico para la compra de *bitcoins* o incluso configuran ataques cada vez más dirigidos hacia personalidades importantes para construir una imagen de marca sobre el *ransomware*.

Mientras evolucionan las herramientas de detección contra esta amenaza, los usuarios debemos recordar siempre la siguiente máxima: el sentido común también debe estar presente en internet.

"Mientras evolucionan las herramientas de detección contra esta amenaza, los usuarios debemos recordar siempre la siguiente máxima: el sentido común también debe estar presente en internet."

3 Entrevista a Xavier Serrano.
Chief Information Security Officer (CISO) de Grupo Banco Sabadell

1. Como responsable de seguridad de la información de Banco Sabadell, ¿podría indicarnos cuáles son las principales competencias dentro de su área? ¿Cuál es su rol en la implementación de la estrategia corporativa? ¿Existe una cultura corporativa de protección de los activos digitales en la compañía?

Mis competencias son las del CISO Global del Grupo, siendo responsable de la seguridad de la información global para todos los países, desde la perspectiva de la segunda línea de defensa (identificación de riesgos y tendencias, análisis de riesgos y determinación de políticas, especificación de controles a implementar, medición del cumplimiento y efectividad de dichos controles, Reporting hacia la Dirección y reguladores y mejora continua volviendo al inicio del ciclo). Desde esa perspectiva global, mi equipo coordina a los diferentes equipos CISO locales de cada país, a quienes también se prestan servicios centralizados de seguridad a través de la filial tecnológica del Grupo.

Dentro de la estrategia corporativa, mi contribución está orientada a la protección del funcionamiento de los procesos críticos del Grupo, así como a facilitar la transformación digital en la que está inmersa el Grupo. Dentro de la estrategia de transformación digital, asegurar la seguridad de la información es fundamental e imprescindible para que dicha estrategia se pueda sustentar.

Existe una cultura corporativa de protección de los activos digitales y un apoyo desde la Dirección, que ve la creciente importancia que está cobrando la seguridad de la información como sustento del negocio tradicional y especialmente el digital, donde no tener incidentes significativos es algo imprescindible para nuestros directivos, nuestros clientes y empleados, reguladores y stakeholders en general.

2. El proceso de internacionalización que se está ejecutando, con la adquisición de algunas entidades extranjeras como el TSB ¿Expone al banco a nuevos vectores de ataque al aumentar su superficie digital? Dichas amenazas ¿se focalizan contra sus propios activos digitales o contra sus clientes?

El Grupo está creciendo y operando en nuevos países como México o UK. Ello, efectivamente, aumenta el nivel de exposición por incremento de superficie digital y también nos enfrenta a nuevos vectores propios de los nuevos países en los que operamos. Para compensar esta situación, nos hemos dotado de una nueva organización, incorporando a nuevos profesionales cualificados, cambiando, industrializando y automatizando nuestros procesos internos y acompañando lo anterior con inversiones en tecnología.

Las amenazas se focalizaron en los inicios de Internet hacia los activos digitales de las empresas, posteriormente (y en concreto en el caso de las entidades financieras) los delincuentes digitales observaron que les podía ser más sencillo intentar engañar a los clientes y hacia allí focalizaron su esfuerzo. Pero posteriormente fueron ganando experiencia y hoy en día se focalizan tanto en los activos de las empresas como de los clientes, por lo que la protección la debemos aplicar en ambos puntos (proteger nuestros activos y entregar servicios a nuestros clientes que sean a prueba de las amenazas que les puedan crear terceros malintencionados).

3. Como trabajador de una empresa con alcance multinacional ¿los profesionales del sector nacional se encuentran igualmente reconocidos y valorados fuera de las fronteras? ¿existe diferencia entre las capacidades nacionales y las internacionales en los proveedores de servicio de ciberseguridad?

Siempre hemos tenido la percepción de que en España se cuenta con muy buenos profesionales dentro del ámbito de la seguridad de la información. El proceso de incorporación de nuevos profesionales para trabajar en este entorno internacional en el que nos encontramos nos lo ha corroborado. El perfil que hemos incorporado se corresponde con profesionales que cuentan con experiencia trabajando en el extranjero y acostumbrados a los estándares internacionales. Estamos viendo que su valor es reconocido desde los diferentes países en los que trabajamos.

En cuanto a los proveedores nacionales y su comparación con los internacionales, podemos concluir que no existe mucha diferencia, pero sí que podemos decir que existen pocos proveedores de origen nacional que hayan desarrollado

productos de seguridad nacionales con resultados suficientes como para ser reconocidos a nivel internacional. Existen muchos más proveedores nacionales dedicados a los servicios de seguridad de la información que al desarrollo de software de seguridad que perdure con éxito en el tiempo, esa parece una asignatura pendiente.

4. Bajo la óptica de una entidad financiera, ¿qué medidas de control o de coordinación echa en falta por parte de la Administración con el objetivo de mejorar la respuesta ante ciberincidentes? ¿Qué medidas de control o de coordinación ante incidentes a nivel empresarial y gubernamental propondría?

En España existen servicios de apoyo en materia de ciberseguridad proporcionados por la Administración para las empresas privadas que están catalogadas como infraestructura crítica o como infraestructura estratégica. No voy a desvelar estos servicios ni estos mecanismos de coordinación, pero me parecen adecuados en su estado actual.

Como punto de mejora y ya más centrados en el ámbito financiero, sería de utilidad disponer de mecanismos de la Administración para la monitorización y respuesta rápida ante incidentes que afecten al ámbito financiero. Lo anterior, junto con una regulación adicional sobre la apertura de cuentas en las entidades, serían un buen complemento a las medidas adoptadas por cada entidad y ayudarían a que el crimen organizado buscara objetivos en otros países.

"Existe una cultura corporativa de protección de los activos digitales y un apoyo desde la Dirección, que ve la creciente importancia que está cobrando la seguridad de la información como sustento del negocio tradicional y especialmente el digital."

5. Con la proliferación del concepto de omnicanalidad, los servicios financieros se han vuelto más globales, móviles, digitales y basados en la nube. ¿Qué significan estas tendencias desde el punto de vista de la ciberseguridad y la gestión de riesgos tecnológicos para el sector financiero? Como consecuencia ¿a que amenazas se encuentra expuesta una entidad como Banco Sabadell?

Estas tendencias incrementan la exposición y la tipología de riesgos, situación que implica una necesidad de incrementar las inversiones y los recursos humanos dedicados a la protección de los nuevos canales, servicios y aplicaciones. En el contexto de tipos de interés y márgenes bajos y alta regulación en que se mueven las entidades financieras, los incrementos de inversión y gasto en protección deben obtenerse por reducción de costes o incremento de ingresos como consecuencia de esta nueva omnicanalidad.

Las amenazas son las tradicionales, pero se incrementa muy notablemente la exposición, por lo que se hace fundamental diseñar de forma segura los nuevos desarrollos y los cambios que se realizan, y validarlos antes de entregarlos al entorno productivo definitivo.

6. Los proyectos de transformación digital en las entidades financieras están acercando tecnologías muy ligadas a la seguridad de la información como las criptodivisas o el blockchain. ¿se están abordando iniciativas en este sentido en la entidad? ¿cuál cree que será su futuro?

Se están abordando desde el departamento de Innovación, y nuestro departamento está participando en ello, como en todo proyecto significativo.

Aunque veo muy clara la desaparición de la moneda tradicional, en favor del dinero en formato electrónico (pagos mediante instrumentos como tarjetas, el teléfono móvil y otros medios de pago como la banca a distancia), no veo claro que vayan a ser las criptodivisas no reguladas las que vayan a substituir el dinero tradicional o los medios de pago electrónicos más conocidos. Blockchain tiene unas características que lo hacen útil para una serie de funciones, pero no acabo de ver que entre ellas tengan que estar necesariamente los servicios de criptodivisa.

7. Ante la proliferación de los servicios de información de amenazas existente ¿considera que las entidades financieras se encuentran en grado de llevar a cabo procesos de ciberinteligencia?

Considero que hay muchísimo camino por recorrer todavía en cuanto a información sobre amenazas y sobre inteligencia, y sobre su inte-

gración automática con los sistemas de seguridad que nos protegen. En el momento actual creo que existe un exceso de información al respecto, mucha de ella redundante, sin que ello implique obtener más calidad en las deducciones y en la inteligencia obtenida.

Es por ello que creo que irán apareciendo fuentes de información especializadas en sectores verticales concretos y mayor calidad en la información proporcionada por estas fuentes.

En el momento actual las entidades financieras pueden y deben disponer de procesos de ciberinteligencia, para ir madurándolos continuamente. El uso adecuado de toda esta información marca hoy en día la diferencia en cuanto a estar protegido en mayor o menor grado.

8. Desde un punto de vista prospectivo ¿cuál cree que será el panorama de ciberamenazas futuras ante las que deberá estar preparada una empresa como Banco Sabadell de cierto tamaño y con creciente exposición digital?

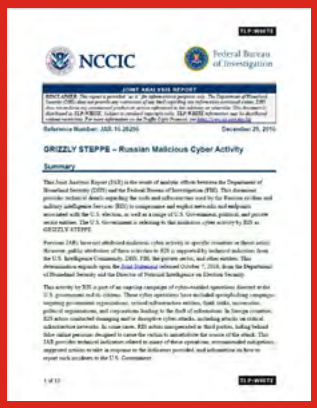
A las amenazas a las que ya están expuestas otras entidades de mayor tamaño: intentos de acceso, engaño, extorsión, robo y sabotaje de servicios prácticamente continuados, situación que obliga al entrenamiento y a la gestión de incidentes continuada, así como a la colaboración muy estrecha con otras entidades y con las fuerzas y cuerpos de seguridad. Y al uso de anchos de banda muy elevados, pues los sistemas conectados (IoT mal configurados) podrán ser fuente automática para la realización de ataques sofisticados.

"En el contexto de tipos de interés y márgenes bajos y alta regulación en que se mueven las entidades financieras, los incrementos de inversión y gasto en protección deben obtenerse por reducción de costes o incremento de ingresos como consecuencia de esta nueva omnicanalidad."

4 Informes y análisis sobre ciberseguridad publicados en diciembre de 2016

Securing Smart Airports (ENISA)

Grizzly Steppe- Russian Malicious Cyber Activity (FBI & NCCIC)



CyberSecurity Regulation and Incentives Review (UK HM Office)

PETs controls matrix - A systematic approach for assessing online and mobile privacy tools (ENISA)

Smart Grid CyberSecurity (Eurelectric)

Cyber Flash: A spotlight on cyber and privacy trends (Deloitte)

Cyber Threat Analysis for 2017 (Booz Allen Hamilton)

Trends 2017: Security held ramson (ESET)

5 HERRAMIENTAS DEL ANALISTA:
Crits

Ante el aumento en la sofisticación de los ciberataques, las organizaciones deben mejorar constantemente sus capacidades defensivas. Así pues, se hace necesario contar con una plataforma para almacenar información técnica con alto nivel de detalle sobre cada amenaza individual. También es necesario realizar análisis profundos sobre estos datos para generar inteligencia operativa y accionable. Además, es necesario contar con la capacidad de compartir esta información entre los miembros del equipo de respuesta a incidentes en tiempo real, no únicamente tras el evento.

Originalmente desarrollado a partir de los investigadores encargados de proteger los propios sistemas de MITRE, CRITs -Collaborative Research Into Threats- reúne información de ciberamenazas obtenidas de ataques individuales y a menudo dispares, y representa estos datos en formatos estandarizados para facilitar el análisis y el intercambio de información que podrá ser utilizada después para proteger la red de una organización de futuros ataques. MITRE publicó su plataforma de código abierto en 2014, disponible desde GitHub.

CRITs facilita la agregación, el análisis y el intercambio de niveles de información técnica sobre ciberamenazas. Gestiona enormes cantidades de datos obtenidos de ataques individuales, a menudo dispares, y realiza análisis para descubrir patrones en los objetivos, las herramientas y las técnicas de un adversario. CRITs además ensambla estas piezas de un rompecabezas aparentemente desconectadas en una imagen cohesionada de una amenaza cibernética. Utilizando un vocabulario común, CRITs puede compartir inmediatamente esta "imagen de datos" con otros equipos de analistas cibernéticos para ayudarles a prevenir futuros ataques.

La plataforma CRITs puede soportar diferentes tipos de usuarios, desde analistas de malware e inteligencia a expertos en ingeniería inversa. La profundidad y la diversidad de la información compartida entre estos múltiples especialistas puede ayudar a mejorar de forma continua la herramienta.

Pestaña de funciones de análisis

Configuración de servicios

6 Análisis de los Ciberataques del mes de diciembre de 2016

AUTOR: Adolfo Hernández, subdirector de THIBER, the cybersecurity think tank.
Cybersecurity advisor, Telefonica/ElevenPaths.

CIBERCRIMEN

A comienzos de mes, *el Banco Central ruso confirmó que, recientemente, unos atacantes desconocidos robaron 2.000 millones de ru-blos*, equivalentes a 31millones de dólares, de cuentas del Banco Central. Para ello, usaron credenciales suplantando a un cliente del banco.

Sus planes fueron en parte frustrados por el banco, que fue capaz de reducir el daño en alrededor de 26 millones de dólares. Algunos de esos fondos habían sido colocados en nuevas cuentas mulas creadas por los hackers durante el ataque. El banco logró congelar las cuentas antes que se ejecutasen las órdenes de transferencia.

Banco Central ruso

Por otra parte, la primera semana del mes *se hizo público el robo de millones de cuentas asociadas a la web Dailymotion*, una de las mayores plataformas de video del mundo.

Aparentemente, un atacante desconocido extrajo 85,2 millones de direcciones de correo electrónico únicas y nombres de usuario de los sistemas de la compañía, pero casi una de cada cinco cuentas sustraídas, aproximadamente 18,3 millones, tenía además la contraseñas asociada, que se mezclaban con la función hash bcrypt.

El hack se cree que se llevó a cabo el 20 de octubre por un atacante, cuya identidad aun es desconocida, según LeakedSource.

El 3 de diciembre, *el fabricante japonés de cosméticos Shiseido Co. emitió* un comunicado público relativo a un suceso ocurrido en su portal de tienda online, dirigida por la filial IPSA Co., ya que había sufrido un acceso ilegítimo y, como resultado, la información personal de unos 420.000 clientes ha sido expuesta.

Los datos filtrados incluyen los nombres y direcciones de los clientes, pero también la información del medio de pago (tarjeta de crédito) de hasta 56.000 de esos clientes. La información de la tarjeta de crédito de los usuarios que hicieron compras online entre el 14 de diciembre de 2011 y el 4 de noviembre de este año puede haber sido filtrada.

La compañía ya ha denunciado el caso a la policía y el Ministerio de Economía, Comercio e Industria del país nipón. Así mismo, la tienda online ha permanecido cerrada durante varios días como medida cautelar.

Los ciberataques en el sector financiero, tras unos meses muy activos, especialmente tras el ataque al Banco Central de Bangladesh, no ce-san. Los ataques dirigidos contra el sistema de transferencia bancaria mundial (SWIFT) siguen siendo lucrativos.

A comienzos de mes, SWIFT lo comunicaba a las entidades financieras ante la creciente amenaza sobre sus sistemas informáticos. Los ataques y las nuevas tácticas de hacking subrayan la vulnerabilidad existente en la red de mensajería SWIFT, que maneja billones de dólares en transferencias de fondos diariamente.

CIBERESPIONAJE

A comienzos de mes, *Corea del Sur denunciaba un ciberataque sobre el mando cibernético basado en Seúl.* Aparentemente, las primeras investigaciones apuntan a que el servidor de la intranet del cibercomando surcoreano ha sido contaminado con malware, verificando que algunos documentos militares, incluyendo información confidencial, han sido filtrados según un comunicado de un funcionario del Ministerio de Defensa Nacional. La misma fuente acusaba a Corea del Norte de estar detrás de las últimas campañas contra objetivos digitales surcoreanos.

En cuanto a las campañas contra el sector industrial, *ThyssenKrupp anunciaba que diversos atacantes externos habían operado contra su división de Soluciones Industriales*, específicamente contra la unidad que se especializa en la construcción de grandes plantas industriales. Las sucursales en los Estados Unidos, Europa, Asia y Argentina fueron afectadas por el incidente. La dirección general de la compañía ha comunicado que los atacantes fueron capaces de filtrar "registros de datos de varias unidades de negocios antes de que su actividad fuera descubierta y detenida".

Que el sector industrial y, específicamente, ThyssenKrupp sea objetivo de ciberataques no es sorprendente. Con ingresos anuales que el año pasado superaron los 45.000 millones de dólares y operaciones que abarcan desde la construcción naval hasta la fabricación de ascensores y la logística global, es fácil ver por qué atacantes externos, patrocinados por Estados o no, se interesen en acceder a sus entornos informáticos corporativos.

Se cree que los atacantes están basados en el sudeste asiático. ThyssenKrupp ha presentado una denuncia penal y está trabajando con las autoridades alemanas para seguir investigando los ataques.

La agencia de inteligencia alemana informó el 8 de diciembre de un aumento sorprendente de campañas rusas de propaganda y desinformación en la red destinadas a desestabilizar la sociedad alemana, detectándose diversos ciberataques contra partidos políticos germanos de origen ruso.

El jefe de la agencia de inteligencia alemanada (BfV), Hans-Georg Maassen, comunicaba la detección de un "número creciente de campañas agresivas de espionaje cibernético y ciberoperaciones que podrían poner en peligro a los funcionarios del gobierno alemán, miembros del parlamento y empleados de partidos democráticos".

Maassen, quien planteó preocupaciones similares sobre los esfuerzos rusos para interferir en las elecciones alemanas el pasado mes de noviembre, referenció lo que denominó "evidencia creciente" sobre tales esfuerzos rusos y dijo que se esperaban nuevos ataques cibernéticos.

La canciller Angel Merkel y el presidente de la Agencia Federal de inteligencia alemana

En el plano norteamericano, *la agencia estadounidense encargada de asegurar que las máquinas de votación cumplan con las normas de seguridad, fue atacada por un actor desconocido tras las elecciones de noviembre.*

La empresa de seguridad, Recorded Future, monitorizando los mercados *underground* donde los ciberdelincuentes compran y venden artículos, descubrieron a algunos usuarios que ofrecían credenciales de acceso para los sistemas en la Comisión de Asistencia Electoral de Estados Unidos. Haciéndose pasar como compradores, los analistas de la compañía participaron en una conversación con el vendedor, descubriendo que el hacker era de habla rusa y que había obtenido las credenciales de más de 100 personas en la comisión electoral tras explotar una vulnerabilidad de base de datos bastante común.

En Ucrania, los mismos atacantes que hace casi un año produjeron un apagón en gran parte del territorio, *han estado ejecutando ataques contra los bancos del mismo país en los últimos meses.*

La empresa de seguridad ESET informa que el grupo de autores que han hecho uso del malware TeleBots contra los bancos ucranianos en las últimas semanas, comparte una serie de similitudes con el grupo BlackEnergy, que llevó a cabo ataques contra la industria energética en Ucrania en diciembre de 2015 y enero de 2016. ESET cree que el equipo de BlackEnergy ha evolucionado en lo que denominan grupo TeleBots.

Al igual que con las campañas atribuidas al grupo de BlackEnergy, los atacantes usaron mensajes de correo electrónico fraudulento (phishing) con documentos de Microsoft Excel que contenían macros maliciosas como principal medio de propagación de la infección. Una vez que una víctima hace clic en el botón "Habilitar contenido", Excel ejecuta la macro maliciosa.

Infografía de BlackEnergy

HACKTIVISMO

En el plano del activismo cibernético, el *Ministerio de Defensa de Ucrania comunicó a mediados de mes* que su sitio web fue víctima de diversos ataques que buscaban hacer inaccesible la web, impidiendo que el gobierno diese actualizaciones sobre el conflicto separatista pro-ruso en las regiones orientales. El sitio web fue atacado regularmente por ataques de denegación de servicio, pero no todos lograron afectar sus operaciones.

Del mismo modo, el Ministerio de Finanzas de Ucrania y los sitios web del Tesoro del Estado también fueron atacados. En estos casos, al acceder a la web legítima, redireccionaba a la dirección *https://www.whoismrrobot.com/*

7 Recomendaciones

7.1 Libros y películas

Película:
ZERO DAYS

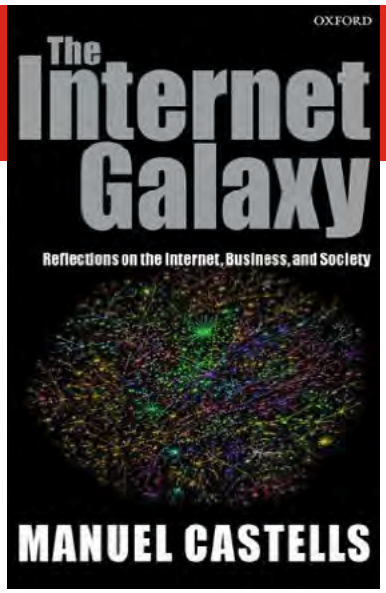
Sinopsis: 'Zero Days' es un documental norteamericano que se centra en Stuxnet, un malware supuestamente creado por Estados Unidos e Israel para intentar menoscabar el programa nuclear iraní.

Libro:
SINFONIER

Autor: Fco. Jesús Gómez, P. J. Martínez, E. Suárez, A. J. Sánchez
Num. Paginas: 208
Editorial: 0xWORD
Año: 2016
Precio: 22.00 Euros
Sinopsis: Este libro es un recorrido por el camino del procesamiento de datos de la mano del paradigma del procesamiento en tiempo real. El objetivo que los autores persiguen es comprender y utilizar, en parte gracias a las facilidades de Sinfonier, una tecnología tan compleja y potente como es Apache Storm.

Libro:
THE INTERNET IS NOT THE ANSWER

Autor: Andrew Keen
Num. Paginas: 304
Editorial: Atlantic Books
Año: 2015
Precio: 20.00 Euros
Sinopsis: Andrew Keen expone los resultados de sus investigaciones sobre los efectos nocivos que Internet tiene sobre la sociedad, economía y cultura de nuestros días. Interesantes reflexiones que ponen en contexto el "hype" de Internet



Libro:
LA GALAXIA INTERNET

Autor: Manuel Castells
Num. Paginas: 304
Editorial: Oxford University Press
Año: 2003
Precio: 30.00 Euros
Sinopsis: Internet es el medio de comunicación esencial en la era de la información. Ya ha influido profundamente en nuestra forma de trabajar, de informarnos, de relacionarnos, de aprender y de vivir. Pero ¿qué sabemos de los efectos de Internet sobre la sociedad, la empresa y la vida cotidiana? La investigación social ofrece un conocimiento objetivo del alcance real de Internet.

Libro:
COMPUTING: A CONCISE HISTORY

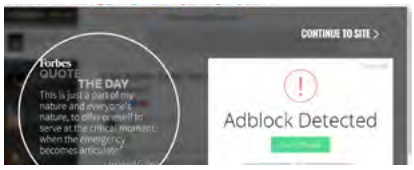
Autor: Paul E.Ceruzzi
Duracion: 4 Horas (audiobook)
Editorial: Gildam Media, LLC
Año: 2012
Precio: 12.00 Euros
Sinopsis: Un viaje por el mundo de la computación, desde el hardware al Internet de las Cosas pasando por el software e Internet. Imprescindible para comprender en 4 horas el cómo y porqué de la actual evolución de la tecnología.

7.2 Webs recomendadas

http://www.nytimes.com/pages/technology/index.html
Sitio web de la sección de tecnología del New York Times donde encontrarás interesantes análisis y enlaces a las principales noticias del sector de las nuevas tecnologías.

https://warontherocks.com/tag/cyber/
Sitio web donde encontraras los análisis sobre seguridad y defensa en el ciberespacio que se publican en el blog War on the Rocks.

http://www.forbes.com/security/
La sección de seguridad de la revista Forbes recopila los análisis de los principales expertos mundiales en el área de la ciberseguridad y la ciberdefensa.



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

https://www.ecs-org.eu/
Sitio web del European Cyber Security Organization (ECSO)

http://www.ted.com/search?q=cybersecurity
Enlace con las principales conferencias TED en el ámbito de la ciberseguridad y la ciberdefensa.

7.3 Cuentas de Twitter

@WarOnTheRocks

@ppperez

@ForensicFocus

@HackSysTeam

@nytimesbits

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
13 enero	Ginebra	Swiss Cybersecurity	Swiss CybeerSecurity	https://www.swiss-cybersecurity.ch/coming-events.php
13 -14 enero	Zurich	WASET	International Conference on Cyber-Physical Systems	https://www.waset.org/conference/2017/01/zurich/ICCPS
14 enero	Lucknow, India	Hackers Day	Hackers Day 2017	https://www.hackersday.org/
14 - 20 enero	Les Diablerets, Suiza	idQuantique	The 9th Annual Winter School on Quantum Cyber Security	http://www.idquantique.com/news-events/9th-winter-school-on-quantum-cyber-security/?doing_wp_cron=1483611160.0433330535888671875000
23 - 24 enero	Londres	IoT Tech	IoT Tech Expo Global 2017	http://www.iottechexpo.com/europe/
23 - 25 enero	Valencia	FIRST	50th TF-CSIRT meeting and FIRST Regional Symposium for Europe	https://www.first.org/events/symposium/valencia2017
24 - 25 enero	Lille, Francia	CEIS	Forum International de la cybersécurité	https://www.forum-fic.com/
26- 27 enero	Standford, California	Standford University	Blockchain Protocol and Security Engineering	https://cyber.stanford.edu/blockchainconf
30 enero - 1 Febrero	Tel Aviv	CyberTech Israel	CyberTech Israel 2017	http://www.cybertechisrael.com/
31 enero - 1 Febrero	Londres	IQPC Exchange	Cyber Security Exchange for Financial Services	https://cybersecurityexchange.iqpc.co.uk/

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

RED ELÉCTRICA DE ESPAÑA · renfe · REPSOL

Santander · Telefónica

Consejo Asesor Empresarial

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA · endesa

IBERIA · Fundación Cajasol

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269