REAL INSTITUTO elcano ROYAL INSTITUTE

MAYO 2017
Nº 25

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 Antonio Ramos 10

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

5 Herramientas del analista 14

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

7 Recomendaciones

7.1 Libros y películas 22

7.2 Webs recomendadas 25

7.3 Cuentas de Twitter.....25

8 Eventos.....26

1 COMENTARIO CIBERELCANO:
Hackear el Pentágono

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

Fuente: Notebookspec.com

En Marzo de 2016, inspirándose en programas similares llevados a cabo por grandes compañías tecnológicas de los Estados Unidos, el Pentágono anunciaba la convocatoria del primer *Bug Bounty* en la historia de la administración del país. Bajo el elocuente título de *"Hack the Pentagon"*, el entonces Secretario de Defensa Ash Carter retaba a los hackers estadounidenses a reportar los fallos de seguridad que detectasen en los sitios webs dependientes del Departamento de Defensa.

Durante 20 días, 1.400 hackers – entre los que se encontraban profesionales de las TIC, profesores universitarios e incluso estudiantes de bachillerato- siguieron las *reglas impuestas por el Departamento de Defensa* para testar la seguridad de parte del ciberespacio militar estadounidense. Cientos de bugs fueron reportados – el primero de ellos a los 13 minutos de comenzar el reto -y más de 75.000 dólares repartidos entre los expertos que reportaron fallos de seguridad relevantes.

Ante el éxito de esta iniciativa, el Pentágono organizó otras actividades similares como el programa *"Hack the Army"* y en los próximos meses patrocinará el reto "Hack the Air Force", que se convertirá en el mayor evento de este tipo organizado hasta la fecha y al cual han sido

invitados a participar hackers procedentes de Australia, Nueva Zelanda, Canadá y Reino Unido, países que junto a Estados Unidos forman la *Alianza Five Eyes.*

Este tipo de eventos están posibilitando que el Pentágono integre profesionales, procesos y tecnologías innovadoras en la seguridad y defensa de su ciberespacio específico.

Del mismo modo, el Secretario de Defensa James Mattis ha decidido ampliar el ámbito de estas iniciativas y para ello ha contado con un grupo reducido de hackers con el objetivo de testear los sistemas internos del Pentágono, algunos de ellos críticos para su actividad diaria. Para ello, los expertos del Departamento de Defensa han replicado ciertos sistemas de información y comunicaciones militares en sus *Cyber Ranges*, entornos virtuales donde los hackers pueden testar la seguridad de los citados sistemas sin necesidad de tener acceso a los entornos de producción.

No cabe duda de que la ciberseguridad y la ciberdefensa son una prioridad política y operativa para el Pentágono, tal y como demuestra el sustancial incremento en el presupuesto destinado a ciberoperaciones así como la prórroga del programa de *contratación de personal civil* del DoD que potenciará la contratación de especialistas para el desarrollo, operación y mantenimiento de las capacidades cibernéticas del Pentágono. Algunos de estos especialistas serán reclutados tras la realización de este tipo de retos.

En definitiva, iniciativas como "Hack the Pentagon" no solo posibilitan la resolución de incidentes de seguridad en parte del ciberespacio militar estadounidense, sino que además permite identificar y captar talento en el ámbito de la ciberdefensa nacional; siendo una excelente oportunidad para reclutar expertos cualificados que formen parte de los "red teams" destinados a mantener la operatividad de las Fuerzas Armadas del país, cada vez más dependiente del ámbito ciber.

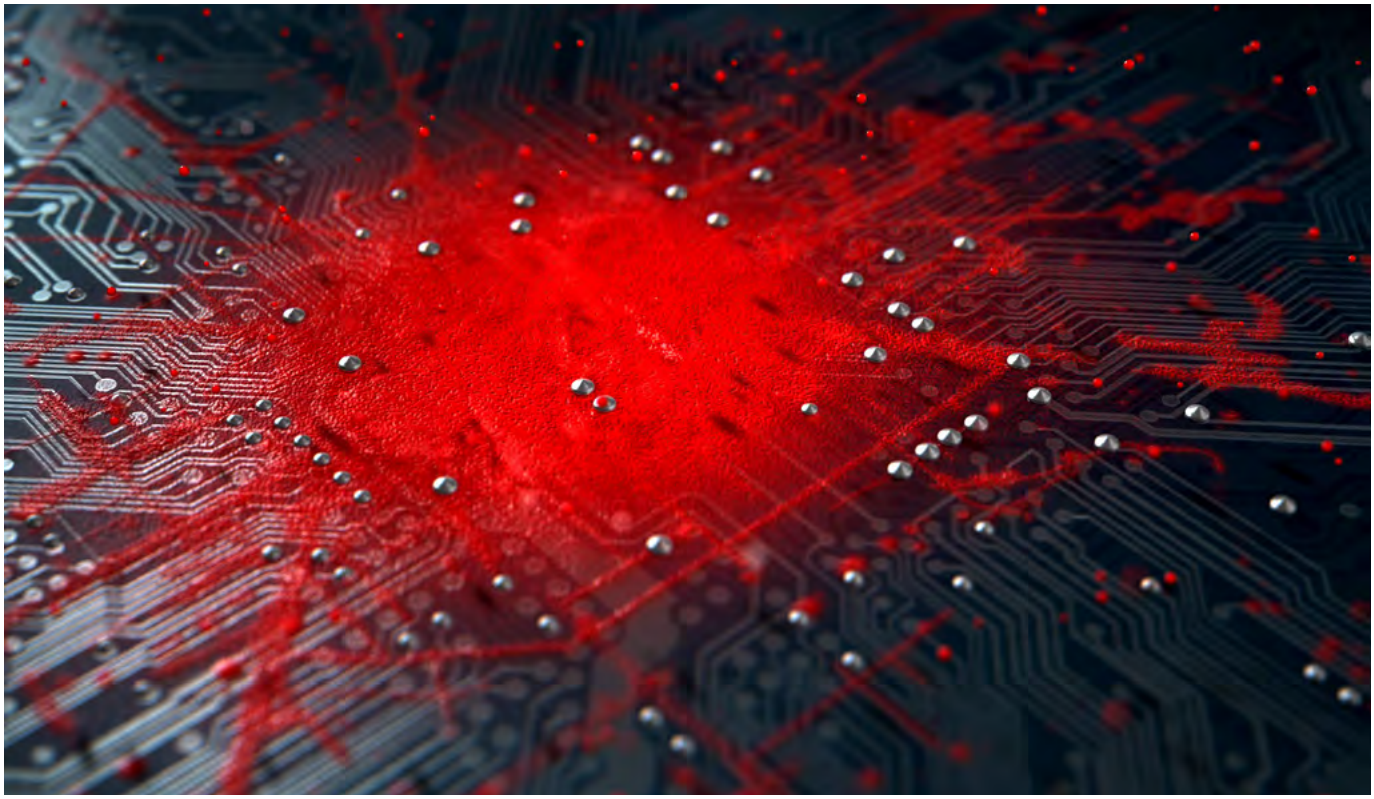
"Hack-The-Pentagon ha posibilitado que el Pentágono integre profesionales, procesos y tecnologías innovadoras en la seguridad y defensa del ciberespacio militar estadounidense"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Estrategias de defensa para la lucha contra las amenazas avanzadas

AUTORES: Miguel Ángel de Castro Simón. Senior Cybersecurity Analyst at ElevenPaths.
Nikolaos Tsouroulas. Head of Cybersecurity Product Managemet at ElevenPaths.

Los avances tecnológicos, intereses económicos, sociales y políticos han generado un nuevo contexto de amenazas avanzadas que nunca antes se habían presentado. Estas nuevas amenazas son mucho más sofisticadas tecnológicamente, disponen de más recursos y no son detectadas por las soluciones y servicios tradicionales de seguridad. Esta problemática afecta hoy en día tanto a pequeñas como a grandes organizaciones y organismos públicos convirtiéndose todos ellos en un potencial objetivo dado que las soluciones de seguridad tradicionales (AV, firewall, IDS, DLP, etc.) no han sido capaces de dar respuesta de forma efectiva.

En este sentido, una protección efectiva frente a este nuevo tipo de amenazas debe combinar medidas de seguridad de infraestructura y perímetro tradicionales, junto con sistemas específicos para la detección de amenazas avanzadas con el fin de dificultar la intrusión inicial, reducir la posibilidad de escalada de privilegios, limitar el daño y detectar cualquier tipo de actividad sospechosa de forma temprana. Adicionalmente tras la materialización de una amenaza, debe ser posible recopilar la información que precisan los investigadores forenses para determinar el daño provocado, cuándo se ha producido y quién es el causante.



DIVERSIDAD DE ENFOQUES EN LA INDUSTRIA

Como respuesta al escenario actual, la industria está evolucionando ante las nuevas amenazas desarrollando soluciones, tanto ubicadas en la red como en el *endpoint*, para tratar de cubrir el espectro más amplio posible y así hacer frente a las diferentes variantes y particularidades que las caracterizan.

Centrando nuestra atención en las soluciones basadas en *endpoint*, las cuales se denominan como *Endpoint, Detection and Response* (EDR, por sus siglas en inglés), pueden categorizarse en dos grandes grupos: aquellas que disponen de mayores capacidades de detección preventiva, es decir, aquellas que detienen la amenaza antes de que sea ejecutada, o en aquellas basadas en detección analítica, es decir, las que monitorizan el comportamiento de todos los eventos del sistema en busca de patrones anómalos que indiquen un posible compromiso.

"...la mayoría de estas soluciones se basan en detección mediante firmas y no nos protegen de estas amenazas más avanzadas."

Otra de las visiones que los fabricantes han implementado en las soluciones parte de la premisa de que no existe riesgo cero, por lo que aportan funcionalidades de respuesta que centran su atención en ofrecer características forenses a los analistas para actuar tras la materialización de una amenaza. Si bien por sí mismas, las capacidades de respuesta no ofrecen protección ante amenazas avanzadas, sí suponen un complemento que habitualmente incorporan las soluciones basadas en prevención o en detección.

Tras estudiar el problema, se considera que la protección en el *endpoint* es clave teniendo en cuenta los siguientes aspectos. En primer lugar, utilizar elementos de red resulta ineficaz, dada la movilidad, el uso de sistemas *cloud* y el crecimiento del uso de canales cifrados de los propios *endpoints*. En segundo lugar, los usuarios finales son los que interactúan con los sistemas de información, incluso en algunas ocasiones con permisos de administración o con acceso a información muy sensible, por lo que no debe descartarse que de forma intencionada o no los usuarios sean uno de los principales riesgos a tener en cuenta.

RECOMENDACIONES PARA SELECCIONAR UNA SOLUCIÓN

En primer lugar, la organización debería preguntarse si necesita una solución de nueva generación para protegerse de las amenazas avanzadas. Partiendo de la premisa de que dispone de alguna solución tradicional, debemos ser conscientes de que la mayoría de estas soluciones se basan en detección mediante firmas y no nos protegen de estas amenazas más avanzadas. Es necesario destacar que cualquier tipo de compañía, independientemente de su tamaño o sector es susceptible de sufrir un ataque avanzado, teniendo en cuenta que la información que albergan es la principal variable que definirá la estrategia de

diseño ante amenazas avanzadas. Asimismo, a medida que las empresas más grandes y más maduras incrementan su capacidad de defensa, los cibercriminales ponen su punto de mira en empresas más pequeñas que colaboran con su objetivo final, como puerta de entrada más fácil de abrir.

La segunda consideración de la que tendríamos que partir es que no existen soluciones que cubran todo el espectro y que protejan de las amenazas avanzadas. En este sentido, existen diferentes aproximaciones que atienden diferentes necesidades, con ventajas e inconvenientes, pero que ninguna solución por sí sola ha ofrecido un resultado satisfactorio del 100% de las pruebas llevadas a cabo.

Para definir nuestra estrategia de protección, en primer lugar, debemos conocer el perfil de riesgo de nuestra organización. Este indicador vendrá definido tanto por la información de que se dispone como por el impacto producido tras un incidente. De la misma manera también debemos conocer para qué tipo de actores somos potenciales objetivos. Finalmente es importante añadir en la ecuación el presupuesto y la capacidad de operación interna, dado que no todas las soluciones tendrán el mismo impacto en términos de coste y de complejidad de operación. Como resultado, se muestra a continuación una tabla a alto nivel que relaciona el riesgo a sufrir un tipo de amenaza según la sensibilidad de información que se maneja, asociado con la capacidad de operación interna y los posibles atacantes.

Tabla. Riesgo asociado a las organizaciones.

SENSIBILIDAD INFORMACIÓN	CAPACIDAD OPERATIVA	AGENTE AMENAZA	TIPO AMENAZA	RIESGO
BAJA/MEDIA	BAJA/MEDIA	CIBERCRIMEN HACKTIVISTAS	COMMODITY	ALTO
			AVANZADA	MEDIO
			APT	BAJO
MEDIA/ALTA	MEDIA/ALTA	CIBERCRIMEN HACKTIVISTAS ESPÍA/INSIDER	COMMODITY	ALTO
			AVANZADA	ALTO
			APT	MEDIO
ALTA/MUY ALTA	ALTA	CIBERCRIMEN HACKTIVISTAS ESPÍA/INSIDER CIBEREJERCITO	COMMODITY	ALTO
			AVANZADA	MUY ALTO
			APT	ALTO

Como conclusión, si se dispone de una capacidad de operación reducida y no se almacena información extremadamente sensible podrían desplegarse soluciones basadas en prevención o detección, teniendo en cuenta que la mayoría de estas soluciones incorporan ambas funcionalidades en mayor o menor medida. Por el contrario, si la capacidad de operación es alta y se maneja información de alta sensibilidad se recomienda de forma adicional a los sistemas de prevención o detección, soluciones basadas en respuesta. En ocasiones, también se puede considerar la incorporación de sistemas UEBA (User and Entity Behavior Analytics), ante un riesgo especial contra *insider threats*.

"...cualquier tipo de compañía, independientemente de su tamaño o sector es susceptible de sufrir un ataque avanzado..."

3 Entrevista a Antonio Ramos.
Socio fundador de Leet Security

1. Como socio fundador de Leet Security ¿podría indicarnos cuáles son las principales líneas de actuación y servicios de su compañía?

En LEET Security, dado su rol como Agencia de calificación de seguridad, circunscribimos nuestra actividad a servicios relacionados con las evaluaciones de seguridad. Tradicionalmente, la calificación de seguridad de servicios y, en breve, también comenzaremos a certificar el cumplimiento con el Esquema Nacional de Seguridad, dadas las sinergias existentes entre ambos procesos. En relación a la calificación, tenemos dos líneas principales: para los usuarios de servicios, les ayudamos a identificar los niveles de calificación a solicitar en función de la criticidad de los servicios a externalizar y, para los proveedores de los servicios, realizamos propiamente la evaluación del nivel de capacidades en ciberseguridad del servicio que ofrecen, lo que incluye, además del sello con el nivel de calificación obtenido, un dictamen de calificación con las pautas a seguir para mejorar dicho nivel acorde a la metodología de evaluación que hemos desarrollado en la Agencia.

2. ¿En qué consiste un servicio de calificación o rating de seguridad para empresas? ¿Se encuentra el mercado maduro para este tipo de servicios?

La calificación es un servicio que permite conocer el nivel de capacidades en materia de ciberseguridad de un servicio concreto (ya sea

un servicio tecnológico, o un servicio basado en tecnología, es decir, que suponga un acceso del proveedor a sistemas de sus clientes o la gestión de información del cliente en sistemas del proveedor) asegurando que durante la vigencia del mismo, el nivel de capacidades es el expuesto en el sello publicado por el proveedor, gracias a que no se limita a una auditoría inicial, sino que incluye actividades de monitorización continua y revisiones periódicas (es decir, va mucho más allá de las típicas certificaciones de SGSI (sistemas de gestión de seguridad de la información) que solo evalúan mecanismos de gestión, pero que no permiten conocer el nivel de protección real de un servicio, algo que sí proporciona el nivel de calificación).

Por tanto, a diferencia de otros mecanismos (tipo certificación), el objetivo no es hacer lo mínimo para conseguir cumplir los criterios para pasar el examen, sino conocer y exhibir el ni-

vel de capacidades implementadas a través de un examen riguroso de las mismas. Este enfoque, que en ocasiones se denomina como de construcción de capacidades, permite además simplificar los procesos de demostración de cumplimiento con distintas normativas, gracias a los mapeos entre los requisitos de los distintos niveles con los referenciales más relevantes en esta materia; es decir, en un proceso de auditoría se pueden obtener diferentes "sellos", lo que supone una mejora de eficiencia muy relevante para los proveedores de los servicios.

Respecto al mercado, pienso que está en el momento oportuno. De hecho, según un estudio que acabamos de realizar, el 78% de las empresas valora positivamente disponer de este tipo de calificaciones. De hecho, permite simplificar la situación actual en la que cada cliente envía cuestionarios de seguridad diferentes a todos sus proveedores y los proveedores responden a múltiples tipos de cuestionarios, todos ellos muy parecidos, aportando un lenguaje común entre las dos partes: los niveles de calificación.

3. En un mercado nacional cuya existencia muchos expertos fijan como condición necesaria para un correcto desarrollo de las cibercapacidades de un país ¿Es difícil emprender? ¿Existe algún tipo de política incentivadora para este tipo de compañías a nivel nacional?

En mi caso, no puedo decir que haya sido difícil emprender, lo que es difícil es hacer que tu proyecto se materialice en una empresa viable, que sea sostenible y que pueda desarrollarse a futuro.

Y respecto a los incentivos, creo que los mediterráneos, a nivel personal, somos innovadores por naturaleza pero, sin embargo, por muchos esfuerzos que hagamos, a nivel corporativo, no existen esos incentivos: penalizamos los fracasos, envidiamos los éxitos del vecino, potenciamos la cultura organizativa orientada a no correr riesgos y, en definitiva, valoramos mucho más lo que viene de fuera. Un solo ejemplo, si queremos favorecer el emprendimiento, ¿cómo puede ser que, ni la Administración ni las grandes empresas, se reserven un presupuesto anual para contratar y probar a proyectos empresariales innovadores? Y no estoy hablando de subvenciones, como dice un buen amigo, "las subvenciones enganchan más que el tabaco", estoy hablando de contratar

y “arriesgar” con esos proyectos innovadores.

4. Dada su experiencia, ¿considera que las empresas nacionales del sector se encuentran bien posicionadas y reconocidas fuera de nuestras fronteras?

Yo distinguiría entre posicionamiento y reconocimiento. Empezando por el final, los profesionales españoles gozan de un gran prestigio a nivel internacional, de hecho, los podemos encontrar por todo el mundo. Otra cosa, es el posicionamiento de las compañías españolas. Evidentemente, hay compañías que lo están haciendo muy bien a nivel internacional, pero son las menos. Por norma general, el mercado español está muy fragmentado, con empresas muy locales y con una dimensión que no nos permite competir en el mercado internacional (parece que seguimos siendo un poco Quijotes). Una vez dicho esto, también creo que, en los últimos años, estamos haciendo un esfuerzo por dotarnos de esas capacidades, pero la fragmentación del mercado “único” europeo, tampoco es que ayude, pero desde luego, todos aspiramos a tener esa dimensión internacional.

5. La aproximación a los riesgos digitales ha cambiado, ¿considera que el mercado de tecnologías y servicios de seguridad se ha adaptado adecuadamente para dar respuesta a las nuevas necesidades? En caso negativo, ¿qué nos falta?

En mi opinión, toda la industria de seguridad o ciberseguridad, si preferimos este término, estamos también en un proceso de adaptación como ponen de manifiesto los nuevos productos que se están lanzando, no solo en el ámbito de la evaluación de la seguridad, como es el caso de nuestra Agencia de Calificación, sino también en el de la detección temprana, con sistemas para gestionar los programas de descubrimiento de vulnerabilidades o sistemas de contra-inteligencia o de la respuesta rápida, con metodologías para integrar la seguridad en DevOps que, por otra parte, creo que son punteros a nivel internacional.

6. Desde la experiencia del camino recorrido ¿qué recomendaciones daría a las startups españolas del mercado de la ciberseguridad?

No me considero nadie para dar consejos, pero si empezara de nuevo sí que habría elementos que desde luego tendría en cuenta: (i) tener claro desde el comienzo la dimensión internacional; (ii) validar cuánto antes con potenciales clientes si la idea que tenemos puede dar lugar a una empresa (de hecho, intentaría tener un cliente incluso antes de tener terminado el producto); y (iii) diseñar una empresa acorde a la magnitud del proyecto.

“...los profesionales españoles gozan de un gran prestigio a nivel internacional...”

4 Informes y análisis sobre ciberseguridad publicados en abril de 2017

The (R)Evolution will be tweeted (THIBER)

Operation Cloud Hopper (PWC)

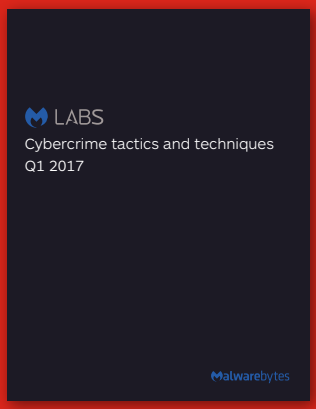
10 steps to Cyber Security (CESG)

Cybersecurity planning guide (Federal Communications Commission)

Cyber Security breaches Survey 2017 (UK Government)

CyberCrime: Undestanding the online business model (UK National Cyber Security Centre)

Cybercrime tactics and techniques 2017 (MalwareBytes)



Tactical Cyber (RAND)

5 HERRAMIENTAS DEL ANALISTA:
Unfetter

Unfetter es un proyecto de código abierto gratuito diseñado para ayudar a analistas de ciberinteligencia, profesionales de ciberseguridad y los responsables de toma de decisiones en materia ciber a identificar y analizar los problemas de seguridad y vulnerabilidades de una manera más escalable, repetible e industrializable.

El proyecto Unfetter es un proyecto conjunto desarrollado entre The MITRE Corporation y la Agencia de Seguridad Nacional de Estados Unidos (NSA).

Unfetter se basa en el modelo de Amenazas, Tácticas Adversarias, Técnicas y Conocimiento Común (ATT & CK) de MITRE, el Repositorio de Análisis Cibernético (CAR) asociado al mismo y una interfaz gráfica de usuario conocida como la Herramienta de Exploración del Repositorio Cibernético (CARET) que conecta CAR y ATT & CK.

Cuando se identifica una ciberamenaza, los profesionales de seguridad que trabajan en el plano táctico, operacional y estratégico deben trabajar juntos de forma rápida y eficaz para permitir desde una estrategia común de ciberseguridad proteger los activos contra el adversario. La capacidad de hacerlo de una manera repetible y escalable depende de la agilidad de una organización para descubrir las lagunas en su postura de seguridad, entender las tácticas del adversario y proponer acciones defensivas a tomar.

Unfetter mejora las metodologías de evaluación de seguridad actuales ayudando a averiguar qué hacer a continuación centrándose en las relaciones entre los datos. Unfetter desplaza el enfoque más allá de los indicadores de compromiso (IoCs) a una metodología basada en el comportamiento que permite a una compañía avanzar en su postura de seguridad de una manera mensurable y significativa.

APROVECHANDO LA COMUNIDAD

Unfetter facilita la puesta en marcha de un proceso de ciberinteligencia y aprovecha los modelos de amenazas comunes como ATT & CK ™ de MITRE. Los profesionales de seguridad pueden usar Unfetter para establecer una postura de seguridad base, explorar las relaciones entre sucesos para identificar las lagunas y experimentar con cursos defensivos de acción antes de que la amenaza se llegue a producir.

ANÁLISIS EN CONTEXTO

El prototipo inicial, conocido como Unfetter | Analytic, es una implementación de referencia de una plataforma diseñada para ayudar a los desarrolladores y analistas a experimentar y familiarizarse con el marco de ATT & CK ™ como un medio para medir la efectividad de los procesos de análisis.

DESCUBRIENDO DEBILIDADES

El segundo prototipo, Unfetter | Discover, está dirigido a ayudar al usuario a explorar las debilidades en su postura de seguridad defensiva y experimentar con las acciones a tomar. El enfoque inicial es el mapeo de las mitigaciones y los controles de seguridad de ATT & CK ™ y la demostración de cómo explorar, aprender y comunicarse entre los niveles táctico, operativo y estratégico de operación.

6 Análisis de los Ciberataques del mes de abril de 2017

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

CIBERCRIMEN

A mediados de abril, *Interpol presentó una investigación* conjunta entre diversas entidades del sector público y privado en el sudeste de asiático y, como resultado, se han identificado cerca de 9.000 servidores de comando y control empleados en malware de origen criminal y cientos de sitios web comprometidos. La operación fue dirigida por la Interpol Global Complex for Innovation (IGCI) con el apoyo del Gobierno chino, así como Kaspersky Labs, el Cyber Defense Institute, Trend Micro, British Telecom, Booz Allen Hamilton, Palo Alto Networks y Fortinet. Entre los 270 sitios explotados por el malware se encontraban varios sites gubernamentales que contenían datos personales de ciudadanos. Los servidores de C & C estaban ubicados en ocho países y la investigación aun está en curso.

Según la declaración de Interpol, los servidores C & C fueron utilizados por varias familias de malware, orientados fundamentalmente al robo de credenciales, DDoS, ransomware y distribución de spam. Estas categorías son las más comunes en los países de la ASEAN.

Por otra parte, analistas de la firma de *seguridad FireEye han verificado un incremento de los ataques atribuidos a actores estatales chinos* estando cada vez más dirigidos a las redes del gobierno, el ejército y la industria de la defensa de Corea del Sur para mostrar su desaprobación por el despliegue del sistema estadounidense de defensa aérea de gran altitud (THAAD). Aparentemente, lo que suscita la preocupación de China es que los sensores sensibles del radar del sistema de misiles antibalísticos podrían ser utilizados para realizar campañas de espionaje. Los analistas de FireEye han detectado un aumento en esa actividad desde febrero, cuando Corea del Sur anunció públicamente que desplegaría los sistemas. Esta actividad ha incluido ataques de *spear phishing* y *watering hole*, siendo ejecutados por los grupos conocidos como Team Tonto y APT10 (también conocido como Menupass).

En el pasado se observó que Tonto Team había dirigido sus ataques contra entidades de Corea del Sur. Durante el mes de marzo, los medios de comunicación surcoreanos informaron de un gran número de ataques de denegación de servicio distribuido (DDoS, por sus siglas en inglés), *defacements* e intentos de intrusión en entidades surcoreanas. Se consi-dera que esta actividad se está llevando a cabo como represalia por los hacktivistas chinos pro-gobierno contra la aprobación final de la instalación del sistema THAAD. En el pasado, el Gobierno chino ha denunciado continuamente el despliegue de THAAD en Corea del Sur. No es raro ver que este tipo de disputas diplomáticas resulten en ataques hacktivistas. Además, junto con estas actuaciones, también son comunes las campañas de ciberespionaje en este entor-no geopolítico. Estos actores a menudo buscan reunir información sobre intereses competitivos para obtener ventajas diplomáticas o militares.

Sistema THAAD

Finalmente, a comienzos de mes, *la empresa de préstamos británica Wonga advirtió a sus clientes que sus datos personales* podrían haberse robado en una fuga de datos en la compañía. La compañía expresó que estaba investigando el acceso ilegal y no autorizado sobre un total de unos 235.000 registros de clientes del Reino Unido y unos 25.000 más en Polonia. Entre los datos filtrados se encuentran nombre, dirección de correo electrónico, dirección postal, número de teléfono, los últimos cuatro dígitos del número de su tarjeta y el número de cuenta bancaria y código de clasificación.

CIBERESPIONAJE

El Centro para la Seguridad Cibernética de Dinamarca *emitió a mediados de mes un informe* acusando a Rusia del acceso ilícito en las cuentas de correo electrónico de su ministerio de Defensa en una acción que calificó de "ofensiva". "Esto es parte de una guerra continua rusa en este campo" dijo el ministro de Defensa, Claus Hjort Frederiksen, a la agencia de noticias danesa Ritzau. También comentó que la actividad ocurrió entre 2015 y 2016 y que se cree que fue llevada a cabo por el grupo de espionaje conocido como APT28 o Fancy Bear. Anteriormente, el grupo fue designado por el Departamento de Seguridad Interior de EEUU (DHS, por sus siglas en inglés) y la Oficina Federal de Investigaciones (FBI), por estar tras los ataques dirigidos contra organizaciones gubernamentales estadounidenses y partidos políticos.

La actividad de este grupo relacionado con el gobierno ruso ya ha sido identificada en el pasado, llevando a cabo acciones de desestabilización en territorio europeo y norteamericano. En 2015, APT28 lanzó un ataque al Bundestag alemán usando el malware llamado XTunnel. En 2016, se observaron trazas de su actividad dirigida a múltiples entidades gubernamentales estadounidenses y europeas, incluyendo organizaciones gubernamentales, diplomáticas y militares en Europa y cercanas a las elecciones presidenciales de Estados Unidos. Además, en el año 2016, también se identificó su modus operandi en el uso de avatares y perfiles en

redes sociales de usuarios hacktivistas rusos falsos, ejecutando filtraciones de información estratégicas y actividades de amplificación para potenciar las narrativas de las operaciones de influencia estatal en los contextos de las elecciones presidenciales de Estados Unidos, el conflicto sirio, las relaciones OTAN-Ucrania, así como en otros eventos internacionales.

El ministro de defensa danés Claus Hjort Frederiksen

A comienzos de mes, diversos analistas advirtieron que un *grupo de espionaje chino entró de forma no autorizada en los sistemas infor-máticos de un conglomerado comercial priva-do estadounidense* antes de la cumbre entre el presidente chino Xi Jinping y el presidente esta-dounidense, Donald Trump. El grupo insertó un enlace malicioso en las páginas web utilizadas por el Consejo Nacional de Comercio Exterior (NFTC) para registrar a los asistentes a la reunión, según confirmaron investigadores de Fidelis Cybersecu-rity. Al hacer clic en el vínculo se descargará una herramienta de vigilancia conocida como Scan-box, que registra el tipo y las versiones del sof-tware que se ejecutan en el equipo, acción que se realiza para posteriormente identificar si hay alguna vulnerabilidad conocida sin parchear. Fidelis afirmó que no tenía evidencia de que miembros de NFTC estuvieran infectados, y vinculó el incidente al actor APT10.

Por otra parte, el 13 de abril *se hizo pública la noticia* de que unos atacantes se dirigieron al Ministerio de Relaciones Exteriores del Reino Unido durante varios meses en 2016. El Centro Nacional de Seguridad Cibernética del Reino Unido no ha confirmado si se robaron datos o no. La firma de seguridad F-Secure afirmó que la oficina fue

el objetivo de una campaña de phishing aprovechando los dominios utilizados por el denominado Grupo Callisto, potencialmente relacionado con Rusia. Los correos electrónicos de phishing intentaron que las víctimas descargasen el malware desarrollado por primera vez por la compañía de software italiana Hacking Team.

HACKTIVISMO

Los hacktivistas del colectivo Anonymous *se comprometieron una vez más a lanzar un ataque dirigido* contra diversos sitios web militares, gubernamentales y de servicios financieros israelíes como parte de la campaña #OpIsrael el pasado 7 de abril. Iniciada en 2013, supuestamente fue concebida como un agravio contra el trato de Israel hacia los palestinos. La lista de objetivos para 2017 se publicó en Pastebin y se han publicado enlaces a herramientas de DDoS en YouTube. Le-jos de tener éxito, en los últimos años los ataques derivados de esta campaña periódica se han mi-tigado con éxito, sin más impacto que las inte-rrupciones de servicios en algunos sitios web. Así pues, la actividad de #OpIsrael volvió a satisfacer las expectativas de ataques de bajo impacto.

El grupo de hackers *Shadow Brokers reapareció* la última semana del mes de abril dando a conocer las contraseña de los archivos que contenían las herramientas tecnológicas robadas meses atrás a la división TAO de la Agencia de Seguridad Nacional (NSA) que se cree que el grupo había intentado previamente vender. El grupo había anunciado anteriormente su retiro de la escena activa, pero confirmó en las redes su regreso como respuesta al ataque con misiles es-

tadounidenses en un aeródromo sirio. En enero, el grupo lanzó un paquete de herramientas que supuestamente fue utilizado por el gobierno de Estados Unidos para vigilar sistemas Windows. Mientras que muchos investigadores occidentales creen que el grupo es de origen ruso, Shadow Brokers lo negó nuevamente este mes, diciendo: "Si los shadowbrokers son rusos, ¿no crees que estaríamos en todos los informes del gobierno estadounidense sobre hacking ruso?"

La sincronización de la liberación de la contraseña en el contexto de las relaciones entre Es-tados Unidos y Rusia, junto con la existencia de docenas de cuentas de Twitter que participan en la promoción automatizada (mediante bots) de enlaces con el correo de Shadow Brokers del 8 de abril con mensajes idénticos de una manera similar a la promoción indirecta que ya se observó promoviendo la actividad de amenazas y anuncios de otros personajes hacktivistas falsos vinculados a Rusia, parece reforzar esta atribución.

Sede central de la NSA

7 Recomendaciones

7.1 Libros y películas

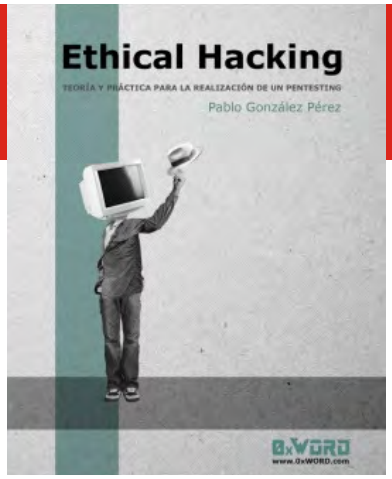
Película:
LIFE

Sinopsis: La tripulación de la Estación Espacial Internacional viaja a Marte con el objetivo de comprobar si las muestras recogidas en el planeta rojo presentan indicios de vida inteligente. Cuando uno de los científicos a bordo examina la única célula encontrada, todo el equipo presencia un hecho insólito: la prueba incuestionable de que hay vida extraterrestre.

Ante su asombro, deciden examinar y establecer el primer contacto con el organismo alienígena. Desgraciadamente, el grupo de astronautas descubrirá demasiado tarde que esta forma de vida es más inteligente de lo que esperaban, hasta tal punto que sus vidas podrían estar en grave peligro. Si ese ente microscópico llega a la Tierra podría poner en peligro toda existencia humana, ¿cuál es exactamente la amenaza a la que se enfrentan? ¿cómo le harán frente?

Cómic:
LA CUARTA REVOLUCIÓN INDUSTRIAL

Autor: Klaus Schwab
Num. Páginas: 189
Editorial: Debate
Año: 2016
Precio: 12,00 Euros
Sinopsis: En La Cuarta Revolución Industrial, Klaus Schwab, fundador del Foro Económico Mundial, describe las características clave de la nueva revolución tecnológica y resalta las oportunidades y dilemas que ésta plantea. Las nuevas formas de colaboración y gobernabilidad, acompañadas de una narrativa positiva y compartida, pueden moldear la cuarta revolución industrial para beneficio de todos. Si aceptamos la responsabilidad colectiva de crear un futuro en el que la innovación y la tecnología sirvan a las personas, podremos llevar a la humanidad a nuevos niveles de conciencia moral.

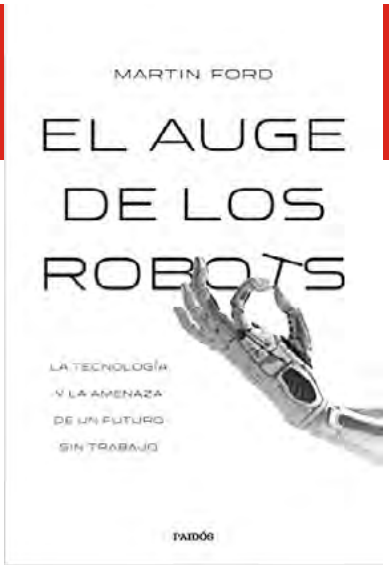


Libro:
ETHICAL HACKING

Autor: Pablo González Pérez
Num. Páginas: 240
Editorial: 0xWORD
Año: 2017
Precio: 22,00 Euros
Sinopsis: El hacking ético es el arte que permite llevar a cabo acciones maliciosas envueltas en la ética profesional de un hacker que ha sido contratado con el fin de encontrar los agujeros de seguridad de los sistemas de una organización. En el presente libro puedes encontrar procedimientos, procesos, vectores de ataque, técnicas de hacking, teoría y práctica de este arte.
El libro propone un enfoque distinto a lo común, en el cual se guiará al lector por un conjunto de pruebas a realizar en auditorías técnicas. La auditoría perimetral y auditoría interna son el foco común en este tipo de procesos. Además, se añaden pruebas modernas no tan comunes en los procesos de hacking ético. Los famosos APT, las pruebas de DDoS o las simulaciones de fugas de información desde dentro de la organización son algunos de los ejemplos que podrás encontrar en el libro.

Libro:
TRANSFORMACIÓN DIGITAL

Autor: Debora J. Slotnisky
Num. Páginas: 138
Editorial: Digital House
Año: 2016
Precio: 7,00 Euros
Sinopsis: Transformación Digital: cómo las personas y las empresas deben adaptarse a esta revolución es un libro que propone una lectura rápida debido a su lenguaje llano. Sin embargo, la obra obliga a repensar la actualidad y los nuevos escenarios organizacionales que se esperan para el corto plazo, con el objetivo de que CEOs, directores, ejecutivos y profesionales encaren con éxito esta nueva realidad.
De la misma manera, ofrece un panorama excepcional para que los jóvenes replanteen sus habilidades para ser competitivos en base a los conocimientos requeridos por el mundo laboral. Adicionalmente presenta herramientas y consejos para que los interesados se sumen rápidamente a este proceso, que es, para muchos, la nueva revolución industrial.



Libro:
EL AUGE DE LOS ROBOTS

Autor: Martin Ford
Num. Páginas: 304
Editorial: Paidós
Año: 2016
Precio: 19,95 Euros
Sinopsis: En El auge de los robots, Martin Ford, empresario de Silicon Valley, pronostica que, conforme la tecnología continúe su desarrollo acelerado y las máquinas comiencen a encargarse de ellas mismas, se necesitarán menos personas. La inteligencia artificial está ya en camino de volver obsoletos muchos empleos: asistentes jurídicos, periodistas, oficinistas e inclusive programadores están a punto de ser reemplazados por robots y software inteligente. El resultado podría ser un desempleo masivo y una mayor desigualdad, así como la implosión de la economía misma del consumidor. El auge de los robots es una lectura indispensable para cualquiera que desee comprender lo que significa la tecnología acelerada para sus propios prospectos económicos, sin mencionar los de sus hijos, así como a la sociedad como un todo.

7.2 Webs recomendadas

http://fifthdomain.com/
Sito web estadounidense dedicado a noticias del dominio ciber en el ámbito de la seguridad y la defensa.

https://e-estonia.com/
Sitio web promovido por el cluster TIC estonio para dar a conocer las noticias del ámbito ciber del país mas conectado del planeta.

http://www.mncdet-pt.net/
Sitio web del proyecto NATO Smart Defence dedicado a la formación y entrenamiento en materia de ciberdefensa.

https://www.eda.europa.eu/what-we-do/activities/activities-search/cyber-defence
Sitio web de la Agencia Europea de Defensa (EDA) dedicado a la ciberdefensa.

http://www.defenseone.com/
Portal especializado en noticias y análisis en el ámbito de la Seguridad y la Defensa

http://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber.html
Sitio web de la empresa Lockheed Martin dedicado a la ciberseguridad y ciberdefensa.

7.3 Cuentas de Twitter

@C4ISRNET

@theFifthDomain

@HECFBlog

@USDS

@e_estonia

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
2- 5 mayo	Bochum, Alemania	RuhrSec	RuhrSec	https://www.ruhrsec.de/2017/
10 mayo	Bilbao	ESET	ESET Security Day	https://www.esetsecuritydays.com/es/
10 mayo	Oslo	Watchcom Security Group	Paranoia 2017	https://paranoia.watchcom.no/
11 mayo	Madrid	ISMS Forum	XIX Jornada Internacional de Seguridad de la Información	http://www.ismsforum.es/evento/645/xix-jornada-internacional-de-seguridad-de-la-informacion-de-isms-forum/
11 mayo	Cracovia	ESET	CARO 2017	https://www.eiseverywhere.com/ehome/caro2017/448403/
11 mayo	Madrid	IKN	Revolution banking	revolutionbanking.es
18 mayo	Cracovia	CONFidence	CONFidence 2017	http://2017.confidence.org.pl/
18 mayo	Paris	AKJ	The 6th e-Crime Cybersecurity France	http://www.e-crimecongress.org/event/france
22- 24 mayo	La Haya	MISTI	14th Annual CISO Europe Summit & Roundtable 2017	http://www.cisoeurope.misti.com/
23- 24 mayo	Moscú	Positive Technologies	Positive Hack Days (Phd7)	https://www.phdays.com
24 mayo	Copenague	CCCC	Copenhagen Cybercrime Conference (CCCC)	http://www.cyberhagen.com/events/copenhagen-cybercrime-conference-2017/event-summary-660496cb491e4b3593aca2ff791c48bb.aspx
23- 25 mayo	Sao Paulo	Exposec	EXPOSEC	http://exposec.tmp.br/16/en/
29 - 31 mayo	Munich	ISACA	2017 Euro CACS	https://www.isaca.org/ecommerce/Pages/european-cacs-europe.aspx
30 mayo - 2 junio	Tallín	NATO Cooperative Cyber Defence Centre of Excellence	CyCon 2017	https://ccdcoe.org/cycon/
2 - 4 junio	Moscú	moscowc0n	moscowc0n	https://moscowc0n.com

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