REAL INSTITUTO elcano ROYAL INSTITUTE

SEPTIEMBRE 2017
Nº 28

CIBERelcano

Informe mensual de ciberseguridad

Desarrollado por: THIBER

Copyright y derechos:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos-THIBER, the Cyber Security Think Tank

Todos los derechos de esta Obra están reservados a Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos y a THIBER, the Cyber Security Think Tank. Los titulares reconocen el derecho a utilizar la Obra en el ámbito de la propia actividad profesional con las siguientes condiciones:

a) Que se reconozca la propiedad de la Obra indicando expresamente los titulares del Copyright.
b) No se utilice con fines comerciales.
c) No se creen obras derivadas por alteración, trasformación y/o desarrollo de esta Obra.

Los titulares del Copyright no garantizan que la Obra esté ausente de errores. En los límites de lo posible se procederá a corregir en las ediciones sucesivas los errores señalados.

Eventuales denominaciones de productos y/o empresas y/o marcas y/o signos distintivos citados en la Obra son de propiedad exclusiva de los titulares correspondientes.

Informe editado en Madrid.

Más información:

Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank.

Índice

1 Comentario Ciberelcano 04

2 Análisis de actualidad internacional 06

3 Informes y análisis sobre ciberseguridad publicados en agosto 09

4 Herramientas del analista 10

5 Análisis de los ciberataques del mes de agosto 12

6 Recomendaciones

7.1 Libros y películas 19

7.2 Webs recomendadas 21

7.3 Cuentas de Twitter.....21

7 Eventos.....22

1 COMENTARIO CIBERELCANO:
Preparándose para la guerra del ciberespacio

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

Fuente: Military Times

La indudable importancia estratégica que las operaciones cibernéticas tienen para el Pentágono ha propiciado que el presidente Trump haya elevado el status del U.S Cyber Command a *Mando Combatiente Unificado*.

Aunque esta decisión no supone una sorpresa ya que durante la administración Obama se convirtió en un debate recurrente, no ha sido hasta la llegada del Secretario de Defensa James Mattis cuando se ha materializado. Esta decisión permitirá centralizar el mando y control de las operaciones en y a través del ciberespacio así como garantizar que el Pentágono dedica los recursos necesarios para hacer y ganar la "guerra del ciberespacio", aumentando el presupuesto para la adquisición de capacidades destinadas a ciber-operaciones y a la *formación y el entrenamiento de los futuros cibersoldados.* Del mismo modo, esta decisión garantizará la comunicación directa entre el Comandante del U.S Cyber Command y el Secretario de Defensa, algo que por otra parte ya ocurría en tiempos de Panetta, Hagel y Carter, a pesar de la subordinación del cibercomando al U.S Strategic Command (USSTRATCOM).

Además, esta decisión también acaba con otro de los debates estrella de la última década: el Comandante del U.S Cyber Command se desvincula de la Agencia Nacional de Seguridad (NSA), del que también era director. Es por ello

que ahora Mattis deberá decidir cuál es el futuro del Almirante Rogers, actual responsable de la NSA y U.S Cyber Command.

Sea como fuere, el Pentágono vislumbra un campo de batalla en continua transformación donde la superioridad tecnológica es determinante. En este sentido, resulta evidente que la industria de defensa estadounidense empieza a comprender que las necesidades del Pentágono solo son alcanzables si abandonan el enfoque tradicional en el que estaba instalada e implantan un proceso continuo de transformación que requiere, entre otros aspectos, la atracción de mucho talento, invertir en I+D+i e incorporar a las PYMES en el modelo productivo. Por otro lado, el Pentágono ha comprendido que debe trabajar en la atracción de la industria tecnología del país que hasta ahora ha sido ajena – y en muchos casos reticente- al mundo militar. El Pentágono, ***a través de DIUX***, se ha instalado en Silicon Valley, Boston y Austin para embarcar en su proyecto a los principales talentos tecnológicos del país. A pesar de que DIUX es una iniciativa impulsada por Ashton Carter el secretario Mattis ha sabido reconocer el valor e importancia de la misma otorgándole un apoyo explícito: personal, presupuesto y agilidad en los procesos de contratación. En el ámbito puramente cibernético, la generación de cibercapacidades no está siendo una tarea sencilla, lo que supone un reto existencial para el Pentágono que busca disponer de capacidades que le procuren una conciencia situacional que les permita ejercer un mando y control efectivo en el ciberespacio, lo que a día de hoy no es posible. En este sentido, la mediación del DIUX será determinante.

En definitiva, prepararse para la guerra del ciberespacio es una tarea difícil que requiere disponer de nuevas estructuras organizativas dentro de las Fuerzas Armadas, personal altamente cualificado, capacidades de última generación y el apoyo a inequívoco a la industria nacional.

"La importancia estratégica de las ciberoperaciones ha propiciado que el presidente Trump haya elevado el status del U.S Cyber Command a Mando Combatiente Unificado."

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:

Asedio al anonimato en la batalla por el control de la red

AUTORES:
Félix Brezo. Analista de THIBER, the cybersecurity think tank. Analista de inteligencia en ElevenPaths.
Yaiza Rubio. Analista de THIBER, the cybersecurity think tank. Analista de inteligencia en ElevenPaths.

A finales de agosto, la Oficina Nacional de Información de Internet del gobierno chino publicaba un *nuevo reglamento* orientado a la clarificación de los criterios de publicación de contenidos en internet. En dicho documento, cuya entrada en vigor quedaba fijada para el 1 de octubre, la Administración del Ciberespacio de China ha puesto en marcha un reglamento que pretende asegurar que los usuarios de internet que operen en plataformas del país estén plenamente identificados relegando el anonimato en la red a un plano puramente clandestino.

Para materializar estos objetivos, la iniciativa, que consta de apenas 13 artículos, apuesta por ejercer una mayor presión sobre los administradores de foros y plataformas de internet para que sean estos quienes asuman su obligación de verificar la identidad real de los usuarios que acceden a sus contenidos. Entre las obligaciones de las plataformas, eso sí, se incluirá la de tomar las medidas oportunas para brindar una protección adecuada a los datos recabados mientras aseguran la no divulgación de los datos facilitados por los usuarios ni su uso para otros fines diferentes de la mera identificación de los usuarios.

La iniciativa de la administración china es la más reciente pero no será la última. A finales de julio el presidente ruso *Vladimir Putin firmó una ley* que prohibirá el uso de VPN (redes privadas virtuales), *proxies* y otras tecnologías orientadas a navegar por internet de forma anónima a partir del próximo 1 de noviembre.

La propia red Tor, que ha visto cómo las descargas de Tor Browser se han disparado *hasta los 17,5 millones de descargas* en el primer semestre del año, no ha sido ajena a este debate. Los administradores del proyecto han publicado este verano *una nota reivindicativa* en la que la comunidad de desarrolladores rescata los valores la estricta defensa de la privacidad que viene ejerciendo el proyecto desde 2001 a raíz de la polémica migración a un servicio oculto de un conocido sitio web de carácter supremacista. Lo cierto es que el dilema moral que subyace sobre el mal uso que algunos puedan hacer de la tecnología no tiene fácil respuesta. Tomar la decisión sobre qué contenidos son reprobables y cuáles no puede resultar una tarea extremadamente compleja cuando las realidades de unos y otros chocan o incluso son antagónicas. El papel de la tecnología como facilitadora del intercambio de comunicación puede resultar incluso una cuestión colateral en el marco de un debate mucho más amplio sobre cuáles son los verdaderos límites de la libertad de expresión y el derecho a la intimidad cuando ambos se ejercen a escala global y, especialmente, cuando resulta una tarea técnicamente compleja determinar orígenes, destinatarios e incluso mensajes intercambiados.

"Vladimir Putin firmó una ley que prohibirá el uso de VPN, proxies y otras tecnologías a partir del próximo 1 de noviembre."

En cualquier caso, la forma tradicional en que concebimos la forma de conectarnos hoy en día hace uso de la infraestructura tecnológica que ponen a nuestro servicio los grandes proveedores de servicios de internet cuyo gobierno y regulación está extendido. Sin embargo, las *mesh networks* ya ofrecen mecanismos de conexión alternativos en formas de redes privadas establecidas entre los propios dispositivos de los usuarios. Seguramente el caso de éxito más *reconocido es el del uso de Firechat* con motivo de una serie de protestas que tuvieron lugar a finales del mes de septiembre en Hong Kong en 2014. En un contexto en el que el acceso a internet se mostró cuanto menos inestable, el uso de este tipo de redes permitió a los manifestantes permanecer en contacto y organizados incluso en el caso de que las redes de comunicaciones fueran intervenidas o incluso desconectadas.

Desde *Serval Mesh* y *Commotion* hasta *Briar Project* o *B.A.T.M.A.N.*, son varios los proyectos de *software libre* que ya hoy implementan aproximaciones funcionales de un fenómeno que es más presente que futuro. Sin embargo, el proceso democratizador del concepto de conectividad no es un fenómeno aislado. La puesta en funcionamiento de proyectos de generación de energía y de autoabastecimiento que se apoyan en tecnologías que facilitan su intercambio entre particulares pueden ser solo el principio de un futuro próximo en el que los servicios que hoy tenemos interiorizados como centralizados empiecen a dotar al ciudadano de una verdadera autonomía e independencia tecnológica.

No podemos perder de vista que fenómenos similares ya han tenido lugar, por ejemplo, en el ámbito de los medios de comunicación. Las grandes cadenas de radio y televisión y los grupos de presión han visto como su hegemonía como creadores de opinión es ya cuestionada por la inmediatez e independencia con la que todos opinamos, contamos o difundimos artículos de blog, *podcasts* o canales en Youtube. Si las telcos y energéticas pasarán o no por un proceso de revolución similar puede que al final sea solo cuestión de tiempo. Y quizás no sean las últimas.

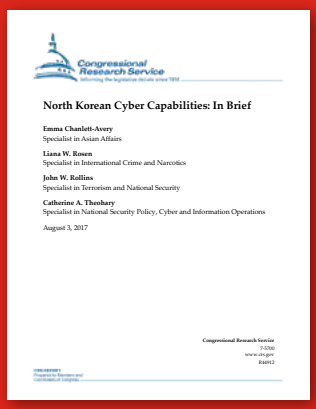
"las mesh networks ya ofrecen mecanismos de conexión alternativos en formas de redes privadas establecidas entre los propios dispositivos de los usuarios."

3 Informes y análisis sobre ciberseguridad publicados en junio de 2017

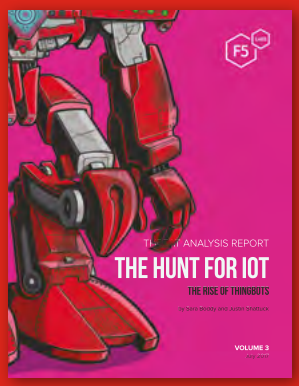
Ramsonware 2017 (Symantec)

Threat Landscape Report Q2 2017 (Fireye)

North Korean Cyber Capabilities (U.S Congress Research Service)

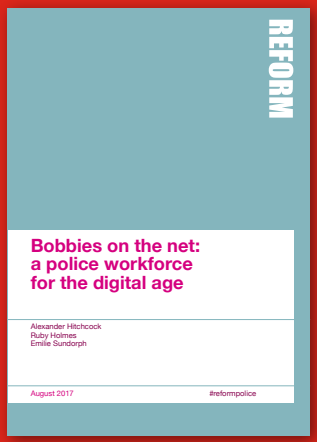


The hunt for IoT (F5 Labs)

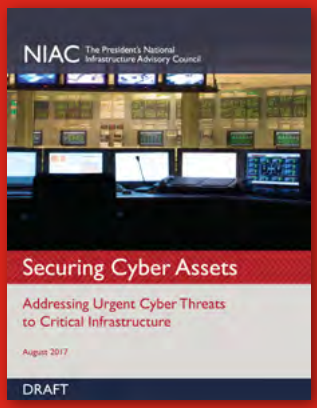


2017 U.S State and Federal Government Cybersecurity Report (Security Scorecard)

Bobbies on the net: a police workforce for the digital age (REFORM)



Securing Cyber Assets (NIAC)



Cyber Threat Data sharing needs refinement (Lexington Institute)

4 HERRAMIENTAS DEL ANALISTA:
Cuckoo Sandbox

Cuckoo Sandbox es un sistema de análisis de malware ampliamente utilizado en el entorno de análisis de seguridad.

Permite analizar cualquier archivo cualquier archivo sospechoso en él y en cuestión de segundos Cuckoo le proporcionará algunos resultados detallados esbozar lo que dicho archivo hizo cuando se ejecutó dentro de un entorno aislado.

En estos tiempos en evolución, la detección y eliminación de artefactos maliciosos no es suficiente: es de vital importancia entender cómo funcionan para entender el contexto, las motivaciones y los objetivos de un ataque, para proteger mejor en el futuro el entorno afectado.

Así pues, Cuckoo Sandbox es un software gratuito que automatiza la tarea de analizar cualquier archivo malicioso bajo Windows, OS X, Linux y Android.

Cuckoo Sandbox es un sistema avanzado, extremadamente modular y 100% de código abierto orientado al análisis de malware con cientos de casos de uso reales. Por defecto es capaz de:

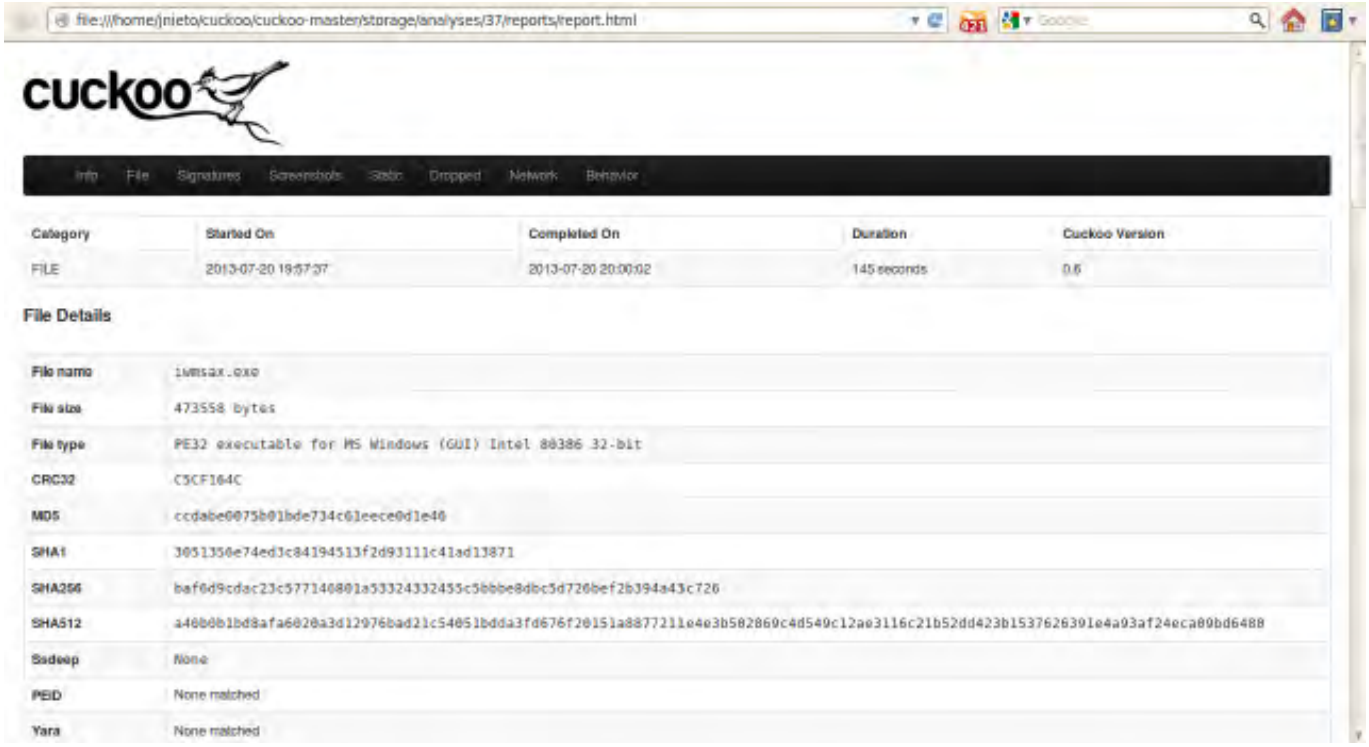
- Analiza muchos archivos maliciosos diferentes (ejecutables, exploits de documentos, applets Java), así como sitios web maliciosos, en entornos virtualizados Windows, OS X, Linux y Android.

- Trazar llamadas API y comportamiento general de un archivo.

- Volcar y analizar el tráfico de red, incluso cuando está cifrado.

- Realizar análisis avanzados de memoria del sistema virtualizado infectado con soporte integrado para Volatility.

Aún más interesante, gracias al amplio diseño modular de Cuckoo, se puede personalizar tanto el proceso como las etapas de elaboración de informes. Cuckoo ofrece todos los requisitos para integrar fácilmente el sandbox en estructuras y entornos de análisis y almacenes de datos existentes con los datos deseados, en el formato seleccionado.

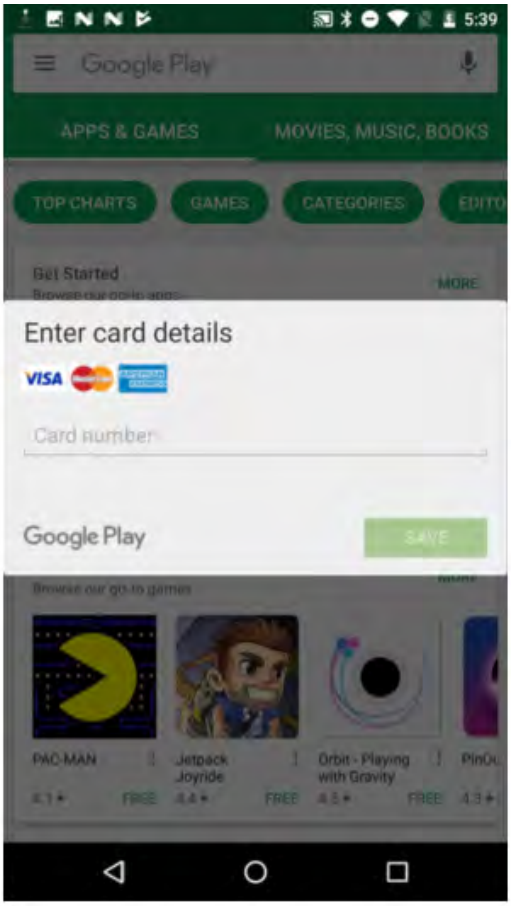


5 Análisis de los Ciberataques del mes de agosto de 2017

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

CIBERCRIMEN

A comienzos de mes, el grupo de ciberdelincuentes responsables del troyano bancario *Svpeng han sido observados* de nuevo usando un nuevo keylogger que explota una función diseñada para ayudar a las personas con discapacidades a acceder a sus *smartphones*. El malware se instala desde sitios web maliciosos oculto como un falso reproductor de Flash. Una vez instalado, el malware pide permiso para utilizar los servicios de accesibilidad, otorgando derechos de administrador sobre el dispositivo y bloqueando cualquier intento de eliminar dichos privilegios. Con acceso al servicio de accesibilidad, un atacante puede acceder a la interfaz de usuario de todas las demás aplicaciones instaladas en el dispositivo y robar datos de ellas. El malware también permite a los atacantes enviar y recibir textos, hacer llamadas y leer contactos. Una característica única es su capacidad de tomar *screenshots* cada vez que un usuario introduce una contraseña. Con el acceso a las aplicaciones bancarias y este mecanismo de captura de pantalla, las víctimas corren el riesgo de que sus credenciales bancarias se vean comprometidas.



Una pantalla de phishing como la empleada por Svpeng

Por otra parte, el archiconocido grupo Carbanak (también conocido como FIN7) ha añadido algunas nuevas armas a su kit de herramientas ofensivas y de filtración de información. El prolífico grupo de hackers existe desde al menos 2015 y se cree que ha atacado a más de 100 bancos, conllevando para el grupo unos beneficios estimados de 1.000 millones de dólares. *Investigadores de Proofpoint observaron recientemente* el grupo que aprovechaba una nueva macro de documentos ofimáticos y una puerta trasera Javascript conocida como Bateleur. Ambas herramientas tienen sofisticadas funciones anti-sandbox y antidetección y se han actualizado varias veces desde junio. El vector de ataque implica el envío de un correo electrónico que contiene un documento adjunto con la macro. Un señuelo que coincida con la cuenta de correo electrónico de envío (es decir, Outlook, Gmail) afirma que el documento está cifrado por el servicio de protección del servidor de correo. Cuando la víctima intenta descifrar, el documento habilitado ejecuta la macro. Esta última campaña se ha observado dirigida a cadenas de restaurantes en Estados Unidos.

También durante el mes de agosto, *Check Point identificó a un hacker nigeriano solitario* que logró infiltrarse en más de 4.000 organizaciones con técnicas "técnicamente simples" que incluían correos electrónicos de spam obvios y fáciles de identificar y herramientas anticuadas. El éxito del atacante revela el mal estado de la concienciación en ciberseguridad en muchas organizaciones. Los ataques comenzaron con un correo electrónico muy genérico dirigido a la dirección de correo electrónico principal de una compañía. Usando una dirección de correo electrónico de Yahoo y haciéndose pasar por un empleado del gigante petrolífero saudí Aramco, el hacker solicitaba información de contacto a los empleados del

departamento financiero para tratar de engañarlos para que revelasen información bancaria o le enviasen dinero.

El hacker también intentó entregar malware antiguo y fácilmente detectable a través de archivos adjuntos infectados. El malware incluía keyloggers y herramientas antiguas de acceso remoto (RATs). Mientras que este hacker en particular logró infiltrarse en miles de organizaciones, fue descuidado con su propia seguridad operativa y permitió a expertos en seguridad identificarlo y localizarlo en Lagos, Nigeria

CIBERESPIONAJE

En el plano del ciberespionaje, *se ha identificado a un grupo de seguridad ofensiva* patrocinados por el gobierno iraní que forman parte del conocido grupo de Cobalt Gypsy, lanzando una campaña de engaño a través de *honeypots* o señuelos diseñados para atrapar a hombres que trabajan en industrias estratégicas para los intereses de Irán.

Han empleado una ciberidentidad de una mujer llamada “Mia Ash” , que ha estado activa en Facebook, LinkedIn, WhatsApp y otros sitios de redes sociales desde abril de 2016 pretendiendo ser una mujer atractiva de unos veinticinco años, con una fotografía sugerente y que aspira a ser modelo. La campaña incluye la distribución de malware disfrazado de encuesta de fotografía. El malware, conocido como PupyRAT, coincide con el malware enviado en el pasado por Cobalt Gypsy y, cuando se descarga, puede dar a un atacante el control completo de un equipo infectado. La campaña se dirigió principalmente a hombres de mediana edad que trabajan como técnicos e ingenieros en empresas de petróleo y gas, aeroespacial y de telecomunicaciones.

Facebook y LinkedIn han eliminado el perfil de Mia Ash desde que Dell SecureWorks comenzó a investigar el perfil falso. Si bien las campañas asociadas a actores estatales iranís se caracterizan por su sofisticación y el uso de vulnerabilidades de “día 0”, algunos grupos emplean en sus campañas ingeniería social con diverso nivel de sofisticación.

En el plano de operaciones de información, *los esfuerzos de propaganda rusa han estado inundando las plataformas de medios sociales durante al menos un año* en un intento de promover candidatos occidentales preferidos en las elecciones y erosionar la reputación de sus oponentes. Twitter y Facebook han sido inundados con millones perfiles gestionados por bots que promueven y transmiten mensajes pro-rusos para ampliar su efecto. Sin embargo, los esfuerzos de propaganda en LinkedIn han pasado casi inadvertidos. Esta presión se ha dirigido principalmente a los miembros con antecedentes en inteligencia de los EE.UU. o la política de Rusia. Muchos de estos miembros, con largas y distinguidas carreras gubernamentales, se han quejado de un rastreo activo pro ruso y de falsas acusaciones de comportamiento criminal y desviado. Algunos incluso han sido baneados permanentemente debido a quejas sin fundamento hechas por presuntos miembros pro-rusos de las diversas redes sociales. Además de los esfuerzos de *trolling* que están desarrollando, las redes sociales y LinkedIn concretamente es supuestamente terreno fértil para que agentes de inteligencia rusos recopilen información de inteligencia y antecedentes profesionales sobre objetivos de reclutamiento potencial o chantaje.

En el pasado se ha monitorizado con mayor foco las campañas de desinformación predominantemente en Twitter y Facebook, dada la facilidad con la que las narrativas pueden amplificarse en esas plataformas. Por el contrario, LinkedIn, menos utilizado para la transmisión de mensajes, es improbable que sirva como una plataforma para la propagación de narrativas, pero puede ser apalancado por actores estatales pro-rusos como una herramienta eficaz para la recolección de inteligencia y posicionamiento de señuelos.

Durante el mes de Agosto se detectó también *una campaña de espionaje de origen ruso que ha utilizado las redes Wi-Fi de los hoteles* para espiar a los huéspedes usando una herramienta de hacking de la NSA (publicada por ShadowBrokers) para ejecutar los ataques. Desde al menos el otoño pasado, APT 28 (también conocido como Fancy Bear), ha atacado a las víctimas a través de redes Wi-Fi de hoteles según un nuevo informe de FireEye. Según el informe, el grupo ha comenzado a utilizar la herramienta EternalBlue utilizada anteriormente en el ransomware de WannaCry. Estos ataques sirven como recordatorio de que las redes de hoteles no son seguras para los usuarios con información sensible.

También durante este último mes han llegado informes de buques que se desvían de su curso en el Mar Negro, lo que ha llevado a algunos expertos a teorizar sobre un *ciberataque de autoría rusa que es capaz de falsificar la señal de GPS.* Desde el pasado mes de junio, por lo menos 20 buques de la ciudad rusa de Novorossiysk se encontraron a 32 kilómetros de distancia desde donde su GPS de navegación por satélite los había localizado. Diversos analistas de seguridad han estado advirtiendo durante años de la posibilidad de suplantar la señal GPS, incluyendo indicios de que Rusia ya tenía dicha capacidad desarrollada. En los últimos meses, algunos expertos han afirmado que la tecnología y la experiencia están ampliamente disponibles y que las capacidades de *spoofing* de GPS podrían ser descargadas de Internet en un hardware comercial convencional.

Finalmente, los investigadores de Proofpoint han descubierto una *nueva campaña de ciberespionaje dirigida a participantes e individuos con interés en el G20.* La campaña surgió a mediados de julio y está aprovechando una nueva vulnerabilidad en JavaScript para desplegar el *backdoor* KopiLuwak, una herramienta empleada por el grupo Turla. Turla ha operado durante muchos años y es ampliamente conocida su vinculación al gobierno ruso. El artefacto ha sido observado en un documento distribuido a través de un phishing que decía ser una invitación a una reunión del grupo de trabajo del G20 de octubre. Se cree que el documento original es auténtico y, por lo tanto, probablemente robado a alguien que ya estaba comprometido. El documento señuelo instala la puerta trasera KopiLuwak cuando se hace clic sobre él y establece la persistencia de modo que es difícil de eliminar.

HACKTIVISMO

Raila Odinga, candidato de la oposición a las elecciones presidenciales de Kenia, ha afirmado que los resultados de los últimos comicios, fueron hackeados, arrojando al país a la violencia y al caos postelectorales.

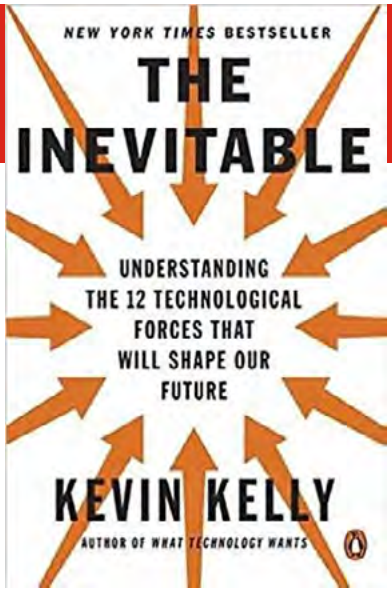
Aunque las elecciones del martes fueron en gran parte pacíficas, los primeros resultados que indican una ventaja significativa para el actual titular Uhuru Kenyatta han sido cuestionados por la oposición y las organizaciones de derechos humanos. Odinga dijo que el ataque ocurrió entre las 12:37 p.m. y 4:00 p.m. el martes. Afirmó que los hackers utilizaron las credenciales de un ex funcionario de alto rango para votar los resultados de las mesas electorales. “Ellos cargaron un algoritmo que es una fórmula para crear una brecha porcentual de 11 % entre nuestros números”, dijo Odinga, agregando que la cifra era “una función de una fórmula.” Ezra Chiloba, director electoral

en Kenia, negó el ataque, afirmando que los sistemas de la Comisión Electoral Independiente y de Límites (IEBC) estaban seguros.

El 9 de agosto, Odinga publicó imágenes de lo que decía ser capturas de pantalla de los registros de la base de datos de IEBC revelando señales de manipulación. IEBC ha reconocido los intentos de acceso al sistema, pero afirma que los registros no proporcionan evidencia de un compromiso exitoso. Los factores anteriores que contribuyeron a un ambiente de duda sobre la integridad del proceso electoral 2017 incluyen: el asesinato de Christopher Msando, alto funcionario del IEBC que supervisa la tecnología electoral, nueve días antes de las elecciones; importantes problemas técnicos con la tecnología electoral en las elecciones de 2013; informes de discrepancias entre los recuentos de votos registrados en los centros de votación y las cifras reportadas por IEBC; y las persistentes advertencias de Odinga durante la campaña de que los resultados electorales podrían ser manipulados. Ejemplos destacados de este tipo de actividades incluyen la actividad de Guccifer 2.0 y DC Leaks alrededor de las elecciones de 2016 en los EE.UU. y la afirmación infundada de CyberBerkut de haber comprometido a la Comisión Electoral Central de Ucrania durante las elecciones parlamentarias ucranianas de octubre de 2014.

6 Recomendaciones

6.1 Libros y películas



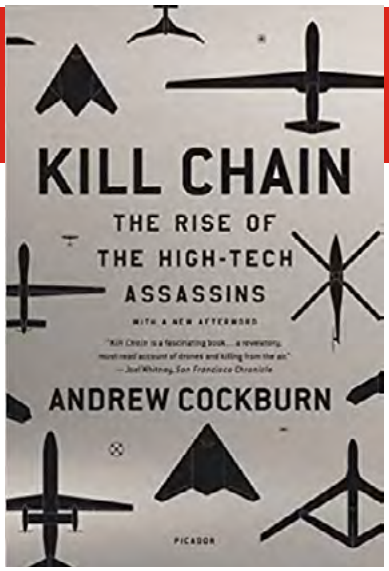
Cómic:
THE INEVITABLE

Autor: Kevin Kelly
Editorial: VIKING PRESS
Año: 2016
Sinopsis: El que fuera editor de WIRED y autor de clásicos como "WHAT TECHNOLOGY WANTS" (Ed. Viking Press, 2011) describe las fuerzas tecnológicas que van a marcar el desarrollo económico y social en los próximos treinta años. Con tono divulgativo, Kelly pasa por la economía colaborativa y subraya un importante cambio al que asistimos cada día, relativo a la mayor trascendencia práctica de la accesibilidad a las cosas y su uso en perjuicio de la propiedad de las mismas *("Access is so superior to ownership in many ways that is driving the frontiers of the economy").*

Hace hincapié en el IoT aunque no lo nombra como tal en todas las ocasiones que debería (las alusiones a la *"cognified laundry"* resultan cómicas) y acierta al resaltar cómo añadir algo de tecnología y conocimiento nuevo a procesos antiguos cambia el modo en que éstos solucionan los problemas reales.

Libro:
BITCOIN

Autor: Félix Brezo y Yaiza Rubio
Editorial: 0xWORD
Año: 2017
Sinopsis: El subtítulo del libro, la tecnología Blockchain y su investigación, resume perfectamente lo que hay en su interior y cuál es el enfoque que se aplica. A una brillante síntesis descriptiva sobre la historia y el estado actual de las criptodivisas sigue una aún más recomendable lista de conceptos teóricos sobre tecnología de bloques y su significado en la parte de Bitcoin (minería, pruebas de trabajo, carteras ...). En este apartado de conceptos básicos, en el capítulo del proceso de investigación ante la presencia de criptodivisas y, sobre todo, en el magnífico trabajo de notas y referencias bibliográficas (que pone la parte más académica donde debe estar) es donde se encuentra el mayor valor de esta obra, muy reseñable en su conjunto.



Libro:
KILL CHAIN. THE RISE OF THE HIGH-TECH ASSASINS.

Autor: Andrew Cockburn
Editorial: Henry Holt
Año: 2015
Sinopsis: Haciendo un destacable recorrido histórico que incluye los años de la guerra de Vietnam, los de Kosovo, y la ya larga guerra contra el terror yihadista, el libro sigue un hilo que explica los orígenes del uso militar de las tecnologías que han derivado en las operaciones de ataque selectivo contra personas y lugares calificados como target por agencias de información o ejércitos. Pero no se queda en el relato de los costosísimos programas de investigación y desarrollo de UAVs sino que, a través de la voz de expertos como el oficial del Pentágono Tom Christie, describe aspectos del uso de los PREDATOR que generalmente no conoce el público. Si se deja de lado la parte de crítica política, el libro aporta enorme cantidad de información tanto técnica como estratégica del uso de los drones en operaciones nunca exentas de polémica.

6.2 Webs recomendadas

http://icitech.org/
Sitio web del Insititute for Critical Infrastructure Technology, un think tank estadounidense dedicado al análisis y estudio de la ciberseguridad.

https://www.cio.gov/
Sitio web de la oficina del CIO del gobierno federal de los Estados Unidos.

https://www.incibe.es/ventures
Sitio web de la aceladora internacional de start-ups en ciberseguridad promovida por INCIBE.

https://warontherocks.com/
Sitio web de Web on the Rocks, una plataforma compuesta por analistas que diseccionan la actualidad geopolítica.

https://www.cyberwatching.eu/
Sitio web del observatorio europeo para la investigación y la innovación en el ámbito de la ciberseguridad y la privacidad.

http://nias2017.com/
Sitio web del Nato Infomation Assurance Symposium.

6.3 Cuentas de Twitter

@Isaiz

@NICPnews

@CyberReadyIndex

@ICITorg

@NATO_ACT

7 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1 Septiembre	Amsterdam	BSIDES	BSIDES Amsterdam	http://www.bsidesams.nl/
4-5 septiembre	Praga	WASET	19th International Conference on Cyber Intelligence and Cyber Terrorism	https://waset.org/conference/2017/09/prague/ICCICT/home
5-7 Septiembre	Bucarest	10Times	Cyber Intelligence Europe	https://10times.com/cyber-intelligence-europe-bucharest
6- 9 septiembre	Barcelona	Radare	r2con	http://rada.re/con/2017/
13- 15 Septiembre	Londres	44CON	44CON	https://44con.com/
14 septiembre	Madrid	ISACA	Los Jueves de ISACA: Emprendimiento en el mundo de la ciberseguridad.	http://isacamadrid.fikket.com/event/juevesisaca-14-s
15- 16 septiembre	Valencia	Rooted	Rooted Valencia	https://www.rootedcon.com/rootedvlc4
16- 17 septiembre	Bogota	DragonJAR	DragonJAR	https://www.dragonjarcon.org/
21 septiembre	Madrid	ISACA	Los Jueves de ISACA	http://isacamadrid.fikket.com/event/juevesisaca-21-s
27 septiembre	Madrid	ISMS Forum	VI Foro de la Ciberseguridad	https://www.ismsforum.es/evento/647/vi-foro-de-la-ciberseguridad-del-cyber-security-center-de-isms-forum/
26 septiembre	Londres	DC4420	DC4420	http://dc4420.org/

Patrocinadores

Consejo Asesor Empresarial

www.realinstitutoelcano.org

www.blog.rielcano.org

www.globalpresence.realinstitutoelcano.org

www.thiber.org

twitter.com/thiber_esp

www.linkedin.com/groups/7404269