REAL INSTITUTO elcano ROYAL INSTITUTE

JULIO 2017
Nº 27

CIBERelcano

Informe mensual de ciberseguridad

Desarrollado por: THIBER

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Copyright y derechos:

Informe editado en Madrid.

Más información:

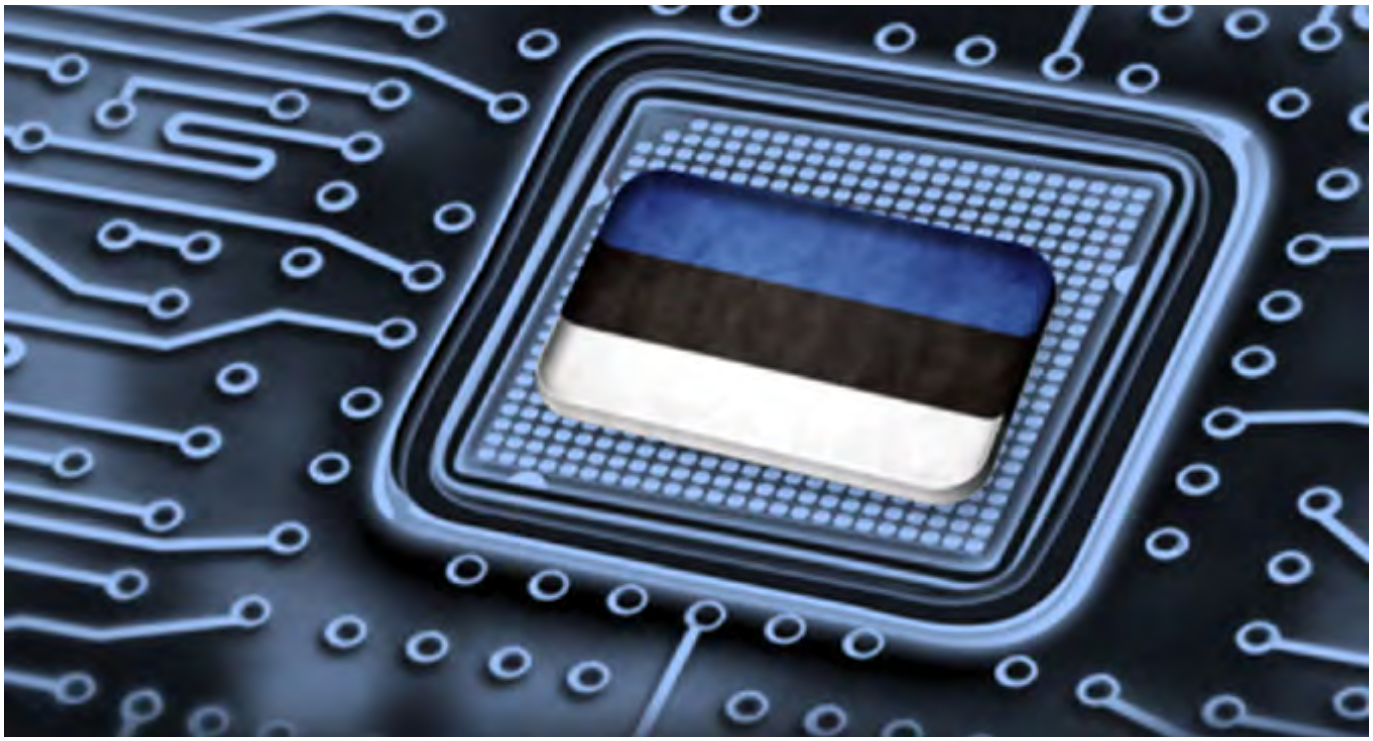
Fundación Real Instituto Elcano de Estudios Internacionales y Estratégicos.

THIBER, The Cyber Security Think Tank.

Índice

1 COMENTARIO CIBERELCANO:
Estonia y las embajadas de datos

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



Fuente: Estonian World

Unos días antes del comienzo de la presidencia estonia de la Unión Europea, el presidente de esta pequeña república báltica Juri Ratas anunciaba la apertura, a principios de 2018, de la *primera embajada de datos de su país en Luxemburgo.*

La creciente amenaza cibernética, en especial la proveniente de Moscú, ha provocado que el gobierno estonio haya acelerado sus planes –que comenzaron a diseñar a principios de 2014- para la creación de las primeras *embajadas de datos* alrededor del mundo. Estas embajadas serán centros de datos -localizadas fundamentalmente en infraestructuras nacionales en el exterior, principalmente en embajadas físicas en las capitales de sus principales aliados, entre los que además de Luxemburgo se barajan Reino Unido, Finlandia, los Países Bajos, Estados Unidos o Japón- que albergarán una réplica de los sistemas TIC y las bases de datos críticas necesarias para garantizar el funcionamiento del país en caso de invasión, ciberataque, desastre natural o cualquier otro tipo de contingencia.

La abrupta adaptación de la inmensa mayoría de las sociedades y gobiernos frente a los riesgos del ciberespacio les está llevando a dotarse de nuevas capacidades e instrumentos de ciberseguridad y ciberdefensa que hasta hace unos años parecían de ciencia ficción. El riesgo –real y factible– que corren los sistemas de informa-

ción públicos en el interior de los países está llevando a reforzar sus infraestructuras de tecnologías de la información y las comunicaciones, pero también a pensar en nuevos instrumentos como la replicación de esos sistemas en el exterior para diversificar los riesgos y potenciar la resiliencia frente a ellos. Las *embajadas de datos* se constituyen en una opción de respuesta ante futuras –y cada vez más frecuentes- crisis cibernéticas.

No cabe dudad de que lo que convierte a las embajadas de datos en algo revolucionario no es ni mucho menos su vertiente técnica, puesto que el almacenamiento de información en servidores externos o en la "nube" es algo que se ha normalizado en los últimos años en el ámbito empresarial y gubernamental, sino que lo realmente novedoso es que sea un gobierno quien replique buena parte de su información, incluida la sensible y clasificada, en diversas localizaciones físicas fuera del territorio nacional, bien sea en terceros países dentro de instalaciones sujetas al derecho diplomático y consular o en servidores privados.

En definitiva, las embajadas de datos son una opción que se debe sopesar porque su réplica no está exenta de riesgos, tanto por aquellos relacionados con la inherente vulnerabilidad de las TIC así como por los condicionantes físicos, técnicos, económicos y políticos que conllevan y dificultan su generalización en el medio plazo. Por tanto, la experiencia estoniana resultará esencial para determinar la forma en la que se podrían articular si se consideran interesantes para la política exterior y la ciberseguridad de un país y de la comunidad internacional.

"la experiencia estoniana resultará esencial para determinar la forma en la que las embajadas de datos se podrían articular si se consideran interesantes para la política exterior y la ciberseguridad de un país y de la comunidad internacional"

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

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.

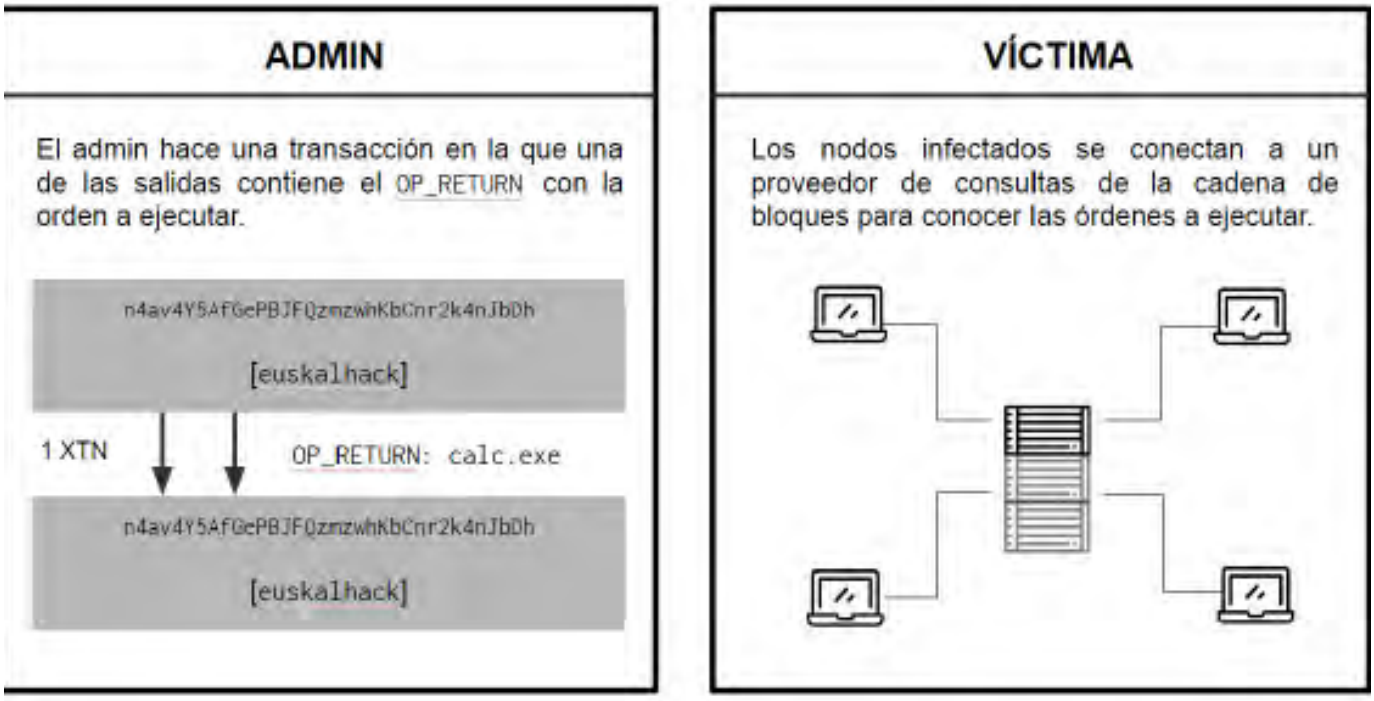
La tecnología Blockchain ha venido para quedarse. Desde enero de 2009, cuando se registró la primera operación en la cadena de bloques de Bitcoin, han surgido cada vez más aplicaciones que hacen uso de esta tecnología más allá de utilizarla como un registro de operaciones de pago. Sin embargo, no existen demasiadas publicaciones que se hayan atrevido a analizar en detalle esta tecnología para identificar sus potenciales usos maliciosos. Con este objetivo fue presentada en la conferencia de ciberseguridad EuskalHack la charla *Make This Last Forever: Blockchain-based C&C.*

Antes de la aparición de Blockchain, los desarrolladores de aplicaciones maliciosas debían buscar diferentes mecanismos para que los servidores de mando y control (C&C por sus siglas en inglés) estuvieran siempre accesible con el objetivo de que los equipos infectados de las víctimas supieran dónde encontrar las órdenes a ejecutar. Han pasado de utilizar chats en IRC y servidores web a redes sociales para ocultar la comunicación del C&C en un bosque de información legítima existente enviada por usuarios legítimos. En este sentido, a principio del mes de junio la empresa de seguridad *ESET* descubrió

que el grupo Turla utilizaba el perfil de Britney Spears para la publicación del C&C aprovechando que damos por hecho que este tipo de redes sociales siempre permanecerán accesibles.

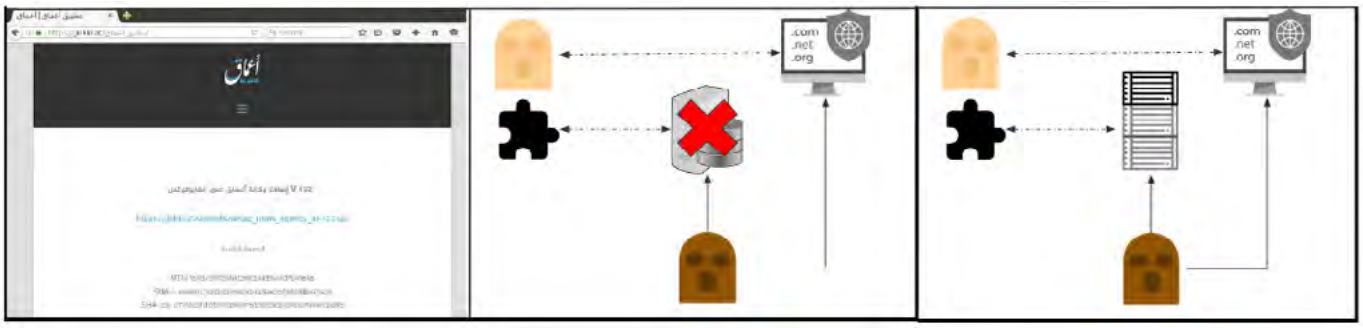
Pero Blockchain ya habría solucionado (sin querer) el objetivo de la perpetuidad de la comunicación que estarían buscando los administradores de una *botnet* con sus víctimas. En 2013, fue incorporada la funcionalidad del OP_RETURN en donde se puede almacenar una pequeña parte de información (hasta 80 bytes) en la cadena de bloques.

La *prueba de concepto* presentada para ilustrar la charla tendría dos fases. La primera, una aplicación que permitiría al administrador hacer una transacción incluyendo la orden a ejecutar en el campo OP_RETURN. La segunda, dos clientes destinados a ejecutar las órdenes almacenadas en la cadena de bloques que, en esta prueba de concepto serían consultadas por las víctimas a través de plataformas de terceros que facilitan dicha información como, por ejemplo, *blockexplorer.com*. De esta manera, y dado que la información una vez anclada en la blockchain es muy difícil de eliminar, el administrador podría actualizar el listado de órdenes de forma recurrente.



Esquema de comunicación del admin con las víctimas

Otro caso que podría darse es el uso de Blockchain para la resolución de dominios. Tal y como se publicó en el *blog* de *ElevenPaths* a principios de año, la agencia de noticias AMAQ de Estado Islámico habría utilizado extensiones de navegador para facilitar a sus seguidores el acceso a sus páginas web. En el caso de que se quisiera evadir cualquier tipo de censura, el campo OP_RETURN podría utilizarse en el caso de que se quisiera que los seguidores supieran en todo momento a qué webs deberían conectarse. En el caso de que dicho servidor dejara de estar disponible, el administrador únicamente tendría que realizar una nueva transacción que añadir a la cadena de bloques donde se publicara a través de OP_RETURN la nueva URL a la que conectarse.



Esquema de comunicación del administrador con sus seguidores.

Sin embargo, existen otros proyectos menos conocidos por el gran público, que también podrían utilizarse con un objetivo similar. En concreto, ***Namecoin*** cuya cadena de bloques puede almacenar hasta 520 bytes de información, o ***Ethereum*** que es una plataforma de computación distribuida que implementa funciones de contratos inteligentes de forma nativa ampliando los casos de uso de la tecnología, o incluso ***Bitmessage*** como protocolo de comunicación descentralizado y cifrado.

Lo que sí que parece claro es que la tecnología ofrece posibilidades interesantes. Es cuestión de tiempo que un *threat actor* llegue a implementar este tipo de comunicación a sabiendas que existe poco margen para su detección. En muchos casos, la aspiración pasaría por identificar peticiones a proveedores de información de la cadena de bloques, compartir información sobre direcciones vinculadas a muestras de *malware* vistas en el pasado o, del mismo modo que Coinsecrets, monitorizar la información expuesta mediante la funcionalidad del OP_RETURN.

"Es cuestión de tiempo que un threat actor llegue a implementar este tipo de comunicación a sabiendas que existe poco margen para su detección."

3 Informes y análisis sobre ciberseguridad publicados en junio de 2017

Global CyberSecurity Index 2017 (ITU)

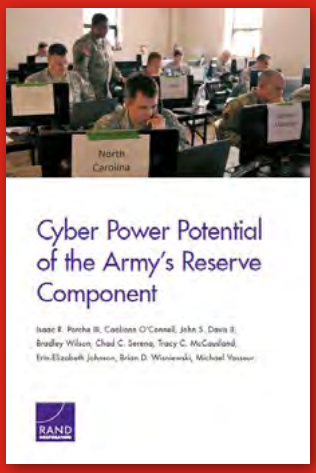
Cyber Europe 2016: After Action Report (ENISA)

Study on CSIRT Maturity (ENISA)

Realizing the potential of Blockchain (World Economic Forum)

Reflection paper on the future of the European Defence (European Commission)

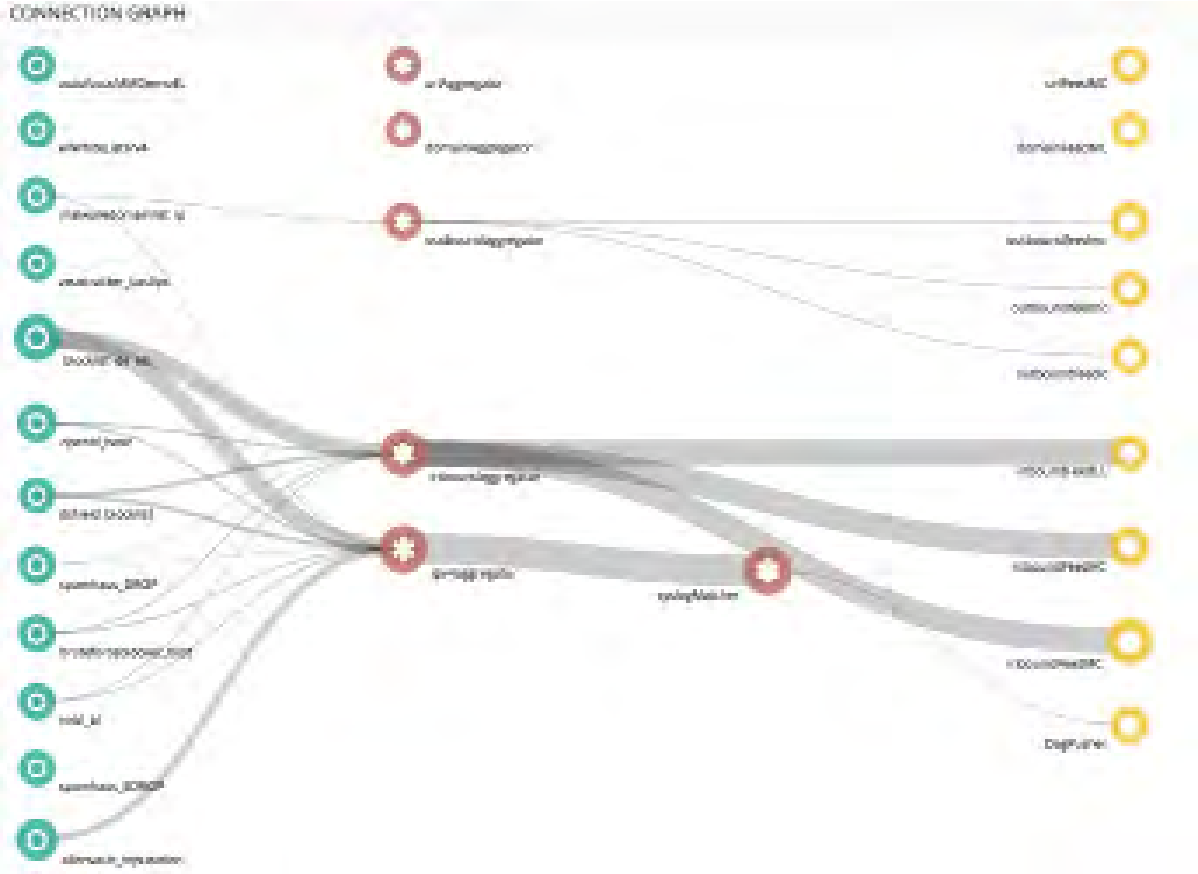
Cyber Power Potential of the Army´s Reserve Component (RAND)



Cyber Operations: Defending Political-IT Infrastructures (Stiftung)

Countering the proliferation of malware (HARVARD Kennedy School)

4 HERRAMIENTAS DEL ANALISTA:
MineMeld



MineMeld es un marco de procesamiento extensible de inteligencia de amenazas desarrollado por Palo Alto Networks, siendo una herramienta de código abierto apoyada por la comunidad para manipular lista de indicadores de compromiso y transformarlos o agregarlos para el consumo por parte de distintos elementos de la infraestructura de seguridad de cualquier organización.

MineMeld tiene muchos casos de uso y puede extenderse fácilmente para cumplir muchos más. Aquí están algunos ejemplos:

- Conectarse al Spamhaus DROP feed y transformarlo para su cumplimiento por Palo Alto Networks EDL Objects (Lista Dinámica Externa).
- Mine Office 365 proporciona direcciones IP proporcionadas por Microsoft y crea dinámicamente una lista EDL para su uso en una política de seguridad de Palo Alto Networks para restringir aún más el tráfico.
- Agregar CERTs e ISACs a las alertas de Inteligencia de amenazas, eliminando duplicados, expirando entradas y consolidando las direcciones de ataque y los niveles de confianza luego hacer esta lista disponible para su aplicación por parte de terceros herramientas.
- Extraer los indicadores de los mensajes syslog y agregarlos con indicadores procedentes de fuentes de terceros.

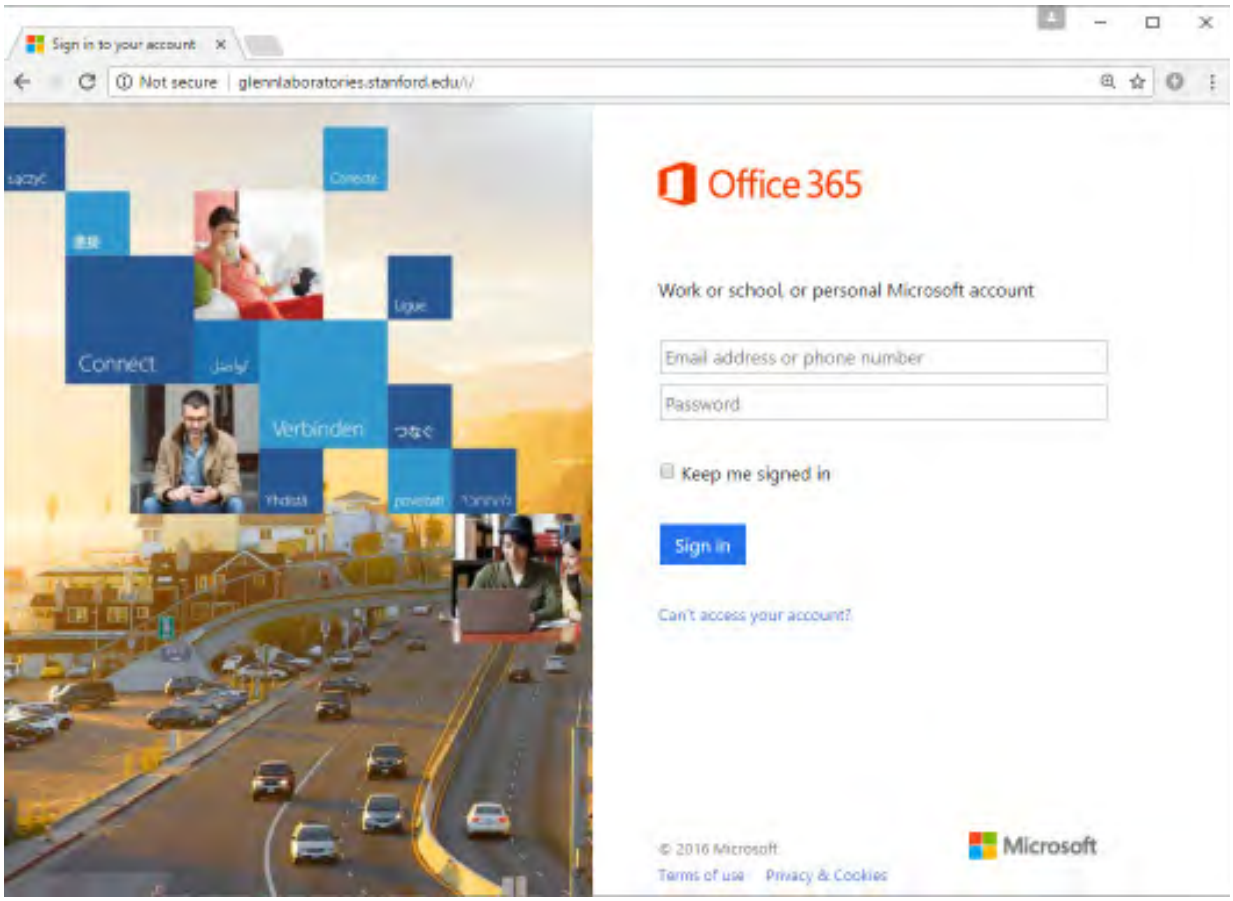
5 Análisis de los Ciberataques del mes de junio de 2017

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

CIBERCRIMEN

A comienzos del mes de junio, un subdominio perteneciente a la Universidad de Stanford ha estado albergando y distribuyendo malware durante los últimos cuatro meses, siendo además utilizado por los atacantes para lanzar ataques de phishing y spam. Los investigadores de Netcraft *notificaron dicha actividad maliciosa a los administradores de Stanford*, ya que el subdominio empleado pertenecía al Centro Paul F. Glenn para la Biología del Envejecimiento de dicha universidad. Según las marcas temporales, la actividad maliciosa comenzó el 31 de enero de 2017, cuando un solo actor subió una web shell simple. Una vez que el sitio fue comprometido, otros actores acudieron al servidor vulnerable.

Es común que los atacantes comprometan sitios web legítimos como plataforma para sus operaciones. Este tipo de explotación puede utilizarse para distribuir malware a los visitantes de una web determinada, crear y servir webs de phishing u otro contenido malintencionado a través de medios tales como anuncios maliciosos, iframes o spam.



Phishing de Office 365 albergada en un subdominio de Stanford.

El grupo de cibercriminales conocidos como FIN10, ejecutó a mediados de mes una operación de extorsión contra objetivos principalmente en Norteamérica, según indican *investigadores de FireEye*. Los atacantes comprometieron la infraestructura de red de las organizaciones objetivo, obteniendo datos valiosos y amenazando con hacerlos públicos a menos que se les pagase una cantidad determinada.

Para algunas víctimas que no respondieron a la demanda, FIN10 intensificó su operación y destruyó sistemas de producción críticos y filtró datos robados a periodistas en un intento por aumentar la visibilidad del ataque y obligar a las víctimas a pagar. La mayoría de las víctimas han sido compañías mineras y casinos canadienses. La actividad, en algunos casos, comenzó con el lanzamiento de correos electrónicos de phishing y se cree que se inició en 2013. Se dice a las víctimas que paguen un rescate de entre 100 y 500 bitcoins.

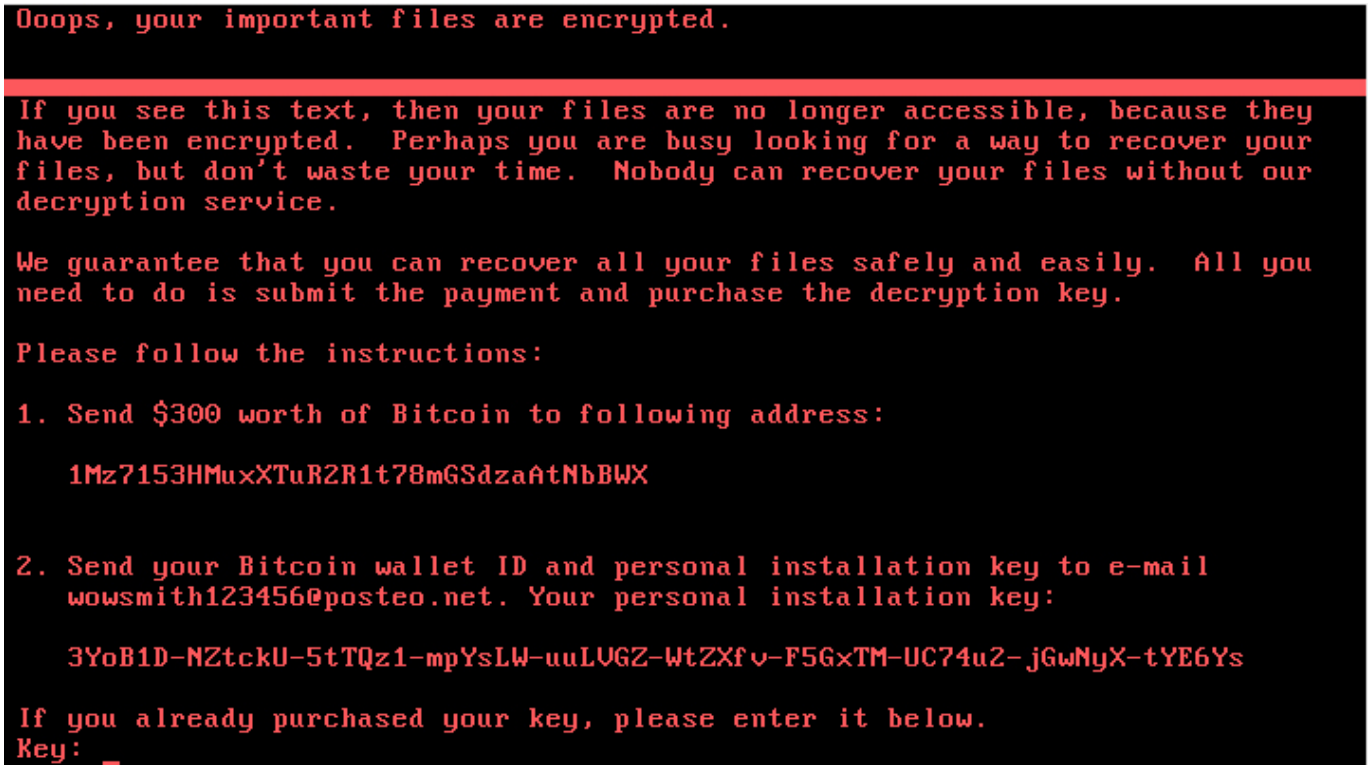
Finalmente, durante la última semana del mes, se vivió un nuevo episodio de un ataque a gran escala combinando un gusano con un malware de tipo ransomware llamado Petya. *Varios investigadores creen que los creadores del* ransomware Petya/NotPetya que se propagaron en Ucrania y se extendieron globalmente el último martes de junio pueden tener otras motivaciones que el delito cibernético. El malware es similar al Petya ransomware que apareció por primera vez en marzo de 2016, pero utiliza una implementación de algoritmo de cifrado diferente, apunta a diferentes tipos de archivos y aprovecha la misma vulnerabilidad EternalBlue SMB utilizada por el malware WannaCry, por lo que Kaspersky ha denominado al malware “NotPetya”.

El país más afectado fue Ucrania, a pesar de que se registraron víctimas en otros 65 países. Microsoft afirma que más de 12.500 equipos informáticos en Ucrania fueron infectadas. Todavía existe cierto desacuerdo sobre el vector de infección inicial. Microsoft y Cisco concluyen que pudo ser el proceso legítimo de actualización del software de contabilidad de

impuestos M.E.Doc, siendo comprometido y usado para distribuir el malware, pero la empresa ucraniana que desarrolló ese software niega públicamente este punto. Además, Bitdefender dice que ha observado infecciones en organizaciones que no utilizan dicho software. La firma Kryptos cree que la velocidad de la infección sugiere que una vulnerabilidad de día cero pudo haber sido empleada.

Cabe destacar que el malware tarda hasta una hora en lanzar el proceso de cifrado y reiniciar el sistema, algo poco común para un ransomware. Al reiniciar, se informa al usuario de que el disco está siendo verificado para detectar errores. En cuanto al pago, dado que el proveedor del servicio de correo electrónico Posteo bloqueó el acceso a la dirección de correo electrónico utilizada por el atacante, es imposible pagar el rescate y obtener la clave de descifrado. Bitdefender cree que la campaña podría no haber sido la intención de robar dinero, sino más bien destruir datos porque inicialmente se dirigía a empresas específicas y sus creadores no pusieron énfasis en el método de pago de rescate y descifrado. Recorded Future afirma que existen indicios de que el ladrón de información de Lokibot puede haber sido usado como payload secundario, lo que significa que el robo de datos podría ser el propósito de la campaña.

Análisis recientes de este ataque revelaron que el malware se elimina antes de cifrar y propagar si su nombre de archivo sin la extensión está presente en la ruta C:/Windows. También se han identificado pruebas adicionales de que el software M.E.Doc se utilizó como un vector de infección en esta campaña en territorio ucraniano.



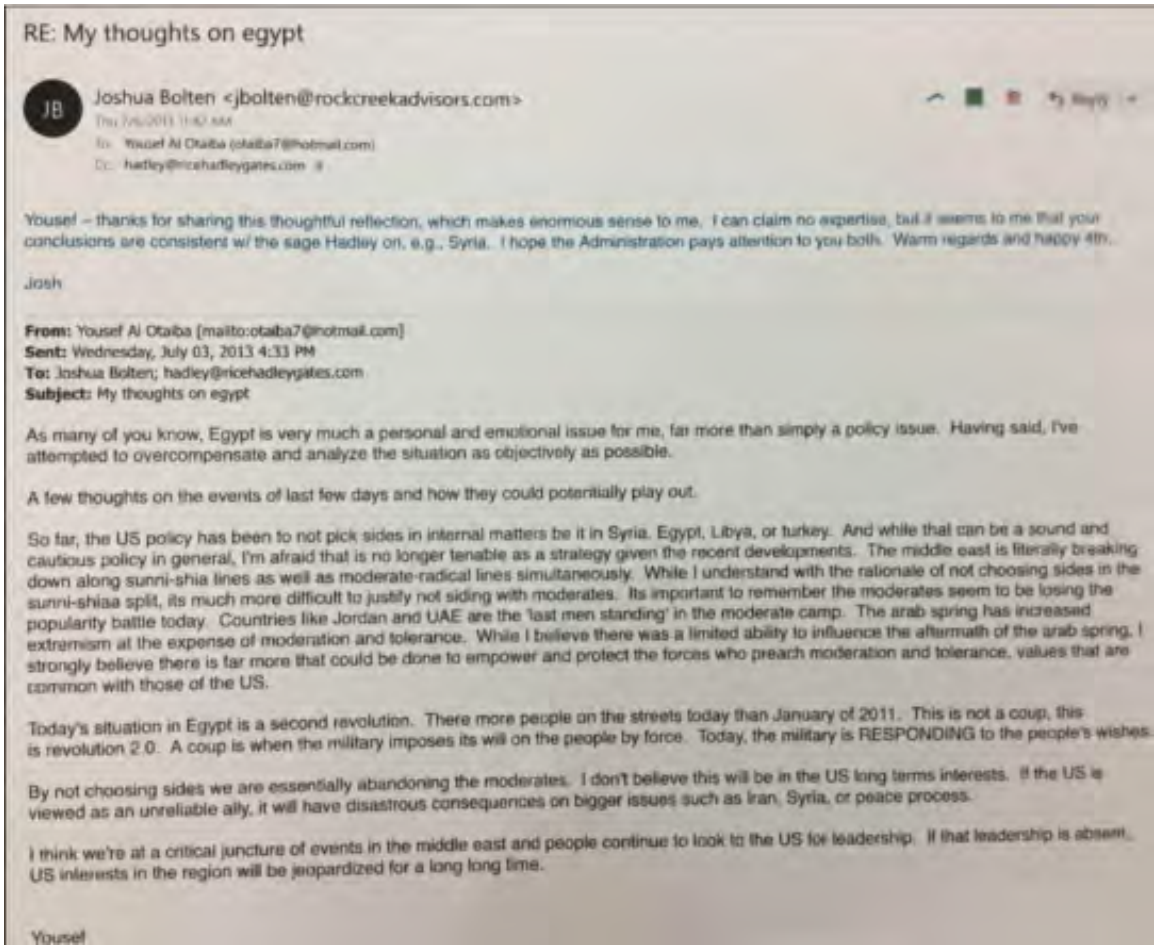
Phishing de Office 365 albergada en un subdominio de Stanford.

CIBERESPIONAJE

Ya en el plano del ciberespionaje y del robo de información, a comienzos de junio *se comunicó públicamente el ataque contra la cuenta de correo electrónico perteneciente al embajador de los Emiratos Árabes Unidos en los Estados Unidos,* Yousef al-Otaiba, viéndose comprometida, con mensajes filtrados a múltiples medios de comunicación, incluyendo The Intercept, The Daily Beast y el Huffington Post.

El atacante empleó una dirección de correo electrónico con dominio.ru y se refirió a sí mismo como GlobalLeaks. También mostró su adhesión a DCLeaks, identificado por diversos investigadores como un sitio web operado por actores rusos. Según los informes, los correos electrónicos muestran la cooperación entre los Emiratos Árabes Unidos y la Fundación para la Defensa de las Democracias (FDD) pro-israelí y neoconservadora.

Los correos electrónicos filtrados parecen mostrar al embajador de los Emiratos Árabes Unidos involucrando a individuos, incluyendo ex-funcionarios del gobierno de Estados Unidos y miembros de diversos think tank en discusiones sobre el supuesto apoyo financiero de Qatar a organizaciones terroristas. La naturaleza de este contenido parece corroborar la afirmación del gobierno de Qatar relativa a la existencia de "una corriente de influencia orquestada por opiniones y noticias liberadas por organizaciones anti-Qatar" antes de la visita de Trump a Oriente Medio y la falsificación de noticias de QNA.



RE: My thoughts on egypt

JB Joshua Bolten <jbolten@rockcreekadvisors.com>

Yousef – thanks for sharing this thoughtful reflection, which makes enormous sense to me. I can claim no expertise, but it seems to me that your conclusions are consistent w/ the sage Hadley on, e.g., Syria. I hope the Administration pays attention to you both. Warm regards and happy 4th.

Josh

From: Yousef Al Otaiba [mailto:otaiba7@hotmail.com]
Sent: Wednesday, July 03, 2013 4:33 PM
To: Joshua Bolten; hadley@ricehadleygates.com
Subject: My thoughts on egypt

As many of you know, Egypt is very much a personal and emotional issue for me, far more than simply a policy issue. Having said, I've attempted to overcompensate and analyze the situation as objectively as possible.

A few thoughts on the events of last few days and how they could potentially play out.

So far, the US policy has been to not pick sides in internal matters be it in Syria, Egypt, Libya, or turkey. And while that can be a sound and cautious policy in general, I'm afraid that is no longer tenable as a strategy given the recent developments. The middle east is literally breaking down along sunni-shia lines as well as moderate-radical lines simultaneously. While I understand with the rationale of not choosing sides in the sunni-shiaa split, its much more difficult to justify not siding with moderates. Its important to remember the moderates seem to be losing the popularity battle today. Countries like Jordan and UAE are the 'last men standing' in the moderate camp. The arab spring has increased extremism at the expense of moderation and tolerance. While I believe there was a limited ability to influence the aftermath of the arab spring, I strongly believe there is far more that could be done to empower and protect the forces who preach moderation and tolerance, values that are common with those of the US.

Today's situation in Egypt is a second revolution. There more people on the streets today than January of 2011. This is not a coup, this is revolution 2.0. A coup is when the military imposes its will on the people by force. Today, the military is RESPONDING to the people's wishes.

By not choosing sides we are essentially abandoning the moderates. I don't believe this will be in the US long terms interests. If the US is viewed as an unreliable ally, it will have disastrous consequences on bigger issues such as Iran, Syria, or peace process.

I think we're at a critical juncture of events in the middle east and people continue to look to the US for leadership. If that leadership is absent, US interests in the region will be jeopardized for a long long time.

Yousef

Extracto de un potencial email filtrado al embajador de EAU en EEUU

Durante la segunda quincena del mes, *investigadores de FireEye hicieron público* que el grupo ruso denominado APT28 ha estado atacando a Montenegro, potencialmente como respuesta a la adhesión del país a la Organización del Tratado del Atlántico Norte (OTAN) el 5 de junio. A principios de este año, la compañía recuperó muestras de malware de un ataque de phishing, tratando de emplear como gancho documentos relacionados con la OTAN y la visita de una unidad del ejército europeo al país. La expansión de la OTAN es a menudo vista como una amenaza a la seguridad por parte de la Federación de Rusia, y la candidatura de la adhesión de Montenegro fue fuertemente discutida por Rusia y los partidos políticos pro-rusos en Montenegro.

Rusia se ha opuesto firmemente al proceso de adhesión de Montenegro a la OTAN desde el inicio y es probable que continúe utilizando sus capacidades ciber para socavar la integración de Montenegro en la Alianza. Se cree que el grupo APT28 estuvo detrás de la actividad porque el malware utilizado, denominado GAMEFISH, sólo ha sido utilizado por el grupo en el pasado y porque el grupo se ha dirigido previamente a los países miembros de la OTAN.

El secretario general de la OTAN, Jens Stoltenberg (dcha.), junto a Igor Luksic, ministro de Exteriores de Montenegro

Por otra parte, a lo largo de este mes, *muestras de malware utilizado por el equipo de ciberespionaje ruso Turla* han sido observadas mediante en comentarios de Instagram para comunicar la dirección de su servidor de mando y control a los hosts infectados. El grupo Turla ha estado activo desde, al menos, 2007. La empresa de seguridad ESET observó recientemente a Turla usando ataques de watering hole para entregar un javascript para realizar un perfilado de sus víctimas. En uno de esos ataques, observaron una extensión de Firefox que actuaba como una puerta trasera y que permitía a los atacantes cargar, descargar y ejecutar archivos y realizar reconocimientos de las máquinas infectadas. Lo destacable de este backdoor es el

método de obtención de la dirección IP del servidor de mando y control – buscando la URK un comentario específico en la cuenta de Instagram de Britney Spears.

El grupo Turla asociado al gobierno ruso, y que históricamente se ha dirigido contra entidades diplomáticas, gubernamentales y de defensa en Europa, Asia Central, Oriente Medio y Estados Unidos, ha vuelto a mostrar actividad este mes. Típicamente, los miembros del grupo Turla comprometen a las víctimas utilizando métodos avanzados y altamente específicos, como el spearphishing y watering holes. Esta última campaña utilizó una nueva técnica de inyección en los watering holes, llamada DARKVENOM, un bloque de javascript malicioso que se inyecta en sitios web comprometidos. Al cargar DARKVENOM, el navegador de la víctima decodifica un bloque de configuración codificado dentro del script que se utiliza para dirigir el navegador a Instagram donde se encuentran las directivas codificadas (contenidas dentro de los comentarios). Cuando se identifican directivas mediante una expresión regular, el navegador de la víctima se dirige a una URL arbitraria para cargar el contenido dinámicamente.

Ya a finales de mes, *una base de datos que contenía 198 millones de registros de votantes estadounidenses en todo el espectro político fue encontrada almacenada en un servidor de almacenamiento Amazon S3, propiedad de la firma Deep Root Analytics.* Se cree que es la mayor exposición conocida de los datos de los votantes. El investigador Chris Vickery, que descubrió los datos filtrados, notificó a la compañía y no hizo pública la información hasta que se obtuvieron los datos. Los datos incluyeron nombres, fechas de nacimiento, domicilio, números de teléfono, registro de votantes, etnia, información religiosa y más.

Estos registros de votantes expuestos podrían ser de valor para una variedad de actores maliciosos, incluyendo ciberdelincuentes que buscan monetizar información personal identificable (PII) y actores estatales involucrados en operaciones de espionaje o influencia contra Estados Unidos.

También a finales de mes, *el parlamento británico sufrió un intento "sostenido y decidido" de penetrar en su red de correo electrónico durante más de 12 horas*, cuando atacantes desconocidos atacaron las cuentas de políticos y personal de administración que utilizan contraseñas de acceso débiles. El evento conllevó la exposición de más de 9.000 usuarios con cuentas de correo electrónico en la red del Parlamento, aunque oficialmente, funcionarios del parlamento confirmaron que sólo se vieron comprometidas 90 cuentas de correo. Los diputados no pudieron acceder al correo electrónico, ya que los sistemas fueron desconectados.

Dado que los ataques de fuerza bruta empleados a menudo sólo requieren una sofisticación técnica baja y que las herramientas de fuerza bruta están disponibles públicamente en internet, los autores materiales, aunque posiblemente puedan ser actores estatales de alguna nación extranjera, también podrían incluir hacktivistas de baja sofisticación y actores con motivaciones financieras.

HACKTIVISMO

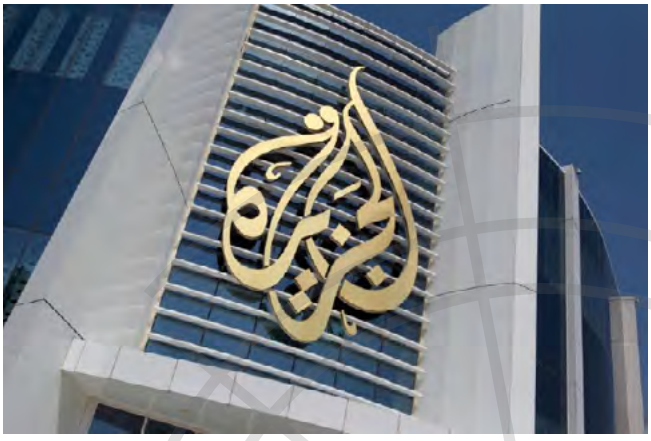
En el plano hacktivista, la cuenta de Twitter del ministro de Relaciones Exteriores de Bahrein, el jeque Khalid bin Ahmed Al Khalifa, *fue secuestrada por actores pro-chiítas el primer sábado del mes de junio*, quienes dejaron amenazas e imágenes hostiles hacia la familia real como "Vamos a pintar el suelo con tu sangre". Algunos de los mensajes incluyeron el logotipo del Saraya al-Mukhtar, un grupo chiíta que ha reclamado múltiples ataques contra las fuerzas de seguridad de Bahrein. El actor o los actores se hicieron cargo de la cuenta alrededor de las 5:30 de la mañana hora local y publicaron declaraciones e imágenes durante cuatro horas, incluyendo los mensajes retuiteados de Nimour al-Hurriya, otro grupo chiíta.

El Ministerio del Interior de Bahrein anunció el 4 de junio que su investigación sobre el compromiso de la cuenta de Twitter identificó a un sospechoso que anteriormente había sido buscado por las autoridades de Bahrein por cargos de terrorismo; sin embargo, no se observaron declaraciones recla-

mando la autoría en los perfiles de redes sociales de Saraya al-Mukhtar. Esto sugiere que el compromiso pudo haber sido conducido por un partidario o miembro del grupo, pero no fue sancionado oficialmente. Además de las declaraciones amenazadoras dirigidas contra la familia real de Bahrein, la cuenta comprometida amenazó también a la familia real saudí y criticó las recientes redadas policiales en las comunidades mayoritarias chiítas de Diraz en Bahrein y al-Awamiya en Arabia Saudita. Aunque el compromiso coincide con un período de intensas tensiones regionales, este incidente no parece estar directamente relacionado con la falsificación de noticias de la agencia de noticias Qatar del 24 de mayo.

La cuenta de Twitter del Ministro de Relaciones Exteriores de Bahrein, Sheikh Khaled bin Ahmed al-Khalifa, fue hackeada

Para finalizar, la entidad de noticias *Al Jazeera informó que ha estado combatiendo un ataque cibernético a gran escala en su plataforma de medios*, aunque los recursos de la web siguen operativos. El 8 de junio, la red twitteó que estaba "bajo ataque cibernético en todos los sistemas, sitios web y plataformas de medios sociales". Los ataques distribuidos de denegación de servicio (DDoS) son supuestamente uno de los tipos de ataque que han afectado al sitio web de Al Jazeera en ese periodo.



Basándonos en las descripciones de Al-Jazeera de la actividad de la amenaza y los efectos observados, es posible que al menos una parte del incidente ocurrido el 8 de junio tomase la forma de ataques DDoS. Es probable que el ataque esté relacionado con la crisis diplomática que ha aislado a Qatar, que también ha implicado una actividad maliciosa relevante contra la Qatar News Agency (QNA).

6 Recomendaciones

6.1 Libros y películas

Película:
RISK

Sinopsis: El documental gira en torno a Julian Assange, el fundador de WikiLeaks. Assange ha sido protagonista de inmunerables noticias, y la más reciente está relacionada con las elecciones presidenciales de Estados Unidos en 2016. WikiLeaks ha sido el responsable de dañar la imagen pública de la candidata demócrata Hillary Clinton al hacker su cuenta de correo y publicar el contenido.

El rodaje ha durado seis años en los que su directora, Laura Poitras (Citizenfour), ha investigado la figura de Assange y todo lo que le rodea desde que lanzaron su primer ataque en el año 2007. WikiLeaks es una organización filtra información de comportamientos poco éticos por parte de los gobiernos y lo hace sin ánimo de lucro. El documental viene de la mano de Laura Poitras y está producido por Sam Esmail, creador de Mr. Robot. Risk cuenta con imágenes reales de los verdaderos protagonistas de la historia: Julian Assange, Sarah Harrison y Jacob Appelbaum, entre otros muchos.

Cómic:
DNI-E TECNOLOGÍA Y USOS

Autor: Rames Sarwat
Num. Páginas: 280
Editorial: 0xWORD
Año: 2017
Precio: 22.00 Euros
Sinopsis: El DNI-e electrónico está entre nosotros desde hace bastante tiempo pero, desgraciadamente, el uso del mismo en su faceta electrónica no ha despegado. Todavía son pocas las empresas y los particulares que sacan provecho de las funcionalidades que ofrece. En este libro Rames Sarwat, de la empresa SmartAccess, desgrana los fundamentos tecnológicos que están tras él y muestra como utilizar el DNI-e en entornos profesionales y particulares. Desde autenticarse en los sistemas informáticos de una empresa, hasta desarrollar aplicaciones que saquen partido del DNI-e.

Libro:
HACKING CON DRONES: LOVE IS IN THE AIR

Autor: David Meléndez
Num. Páginas: 280
Editorial: 0xWORD
Año: 2017
Precio: 22.00 Euros
Sinopsis: "Hacking con Drones" es un recorrido por los aspectos tecnológicos y técnicos más relevantes del mundo de los drones, y concretamente de los multicópteros, que abarca desde una visión general de las tecnologías subyacentes, hasta el montaje y programación de este tipo de aeronaves, así como su puesta a punto, pilotaje, y particularidades de cada caso, inspirado en la propia experiencia del autor para construir y programar desde cero su propio dron.

Libro:
LA REINVENCIÓN DE THE NEW YORK TIMES

Autor: Ismael Nafria
Num. Páginas: 492
Editorial: Amazon Media (Kindle)
Año: 2017
Precio: 6,00 Euros
Sinopsis: El objetivo principal de este libro es explicar el proceso de reinvención que ha vivido el diario más influyente del mundo, The New York Times, durante las dos últimas décadas para adaptarse a la nueva era digital y móvil. Los medios de comunicación, y de manera especial los periódicos, han visto como su sector se ha transformado radicalmente desde la aparición de internet. Tanto los modelos de negocio de los medios como los hábitos de consumo de información de los usuarios han sufrido profundos cambios. El caso del Times ofrece un buen número de lecciones que pueden ser muy útiles para otros medios con independencia de su tamaño o localización.

Libro:
EL SÍNDROME VIDAR

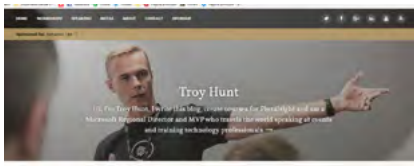
Autor: Jorge de la Cera
Num. Páginas: 293
Editorial: Independent
Año: 2017
Precio: 7,40 Euros
Sinopsis: Sebastián Lasarte, matemático y hacker ya en la cincuentena, revive recuerdos que creía enterrados al recibir una llamada inesperada. Se trata de Martina, antigua alumna de la facultad, que ahora ejerce como operadora de turbina en la central nuclear de North Anna. Allí están ocurriendo incidentes extraños, que escapan a cualquier explicación lógica. El descubrimiento de un antiguo casco, con una extraña inscripción, solo sirve para detonar las peores expectativas.

Sebas y Martina intentarán encontrar el patrón que se esconde detrás de la amenaza invisible que se cierne sobre la central. Descubrirán que nada es lo que parece.

6.2 Webs recomendadas

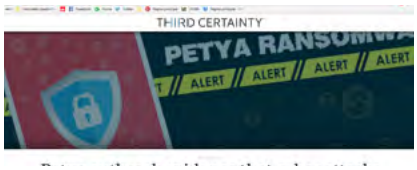
https://www.liquidmatrix.org/blog/
LiquidMatrix es un blog escrito por profesionales de la industria de la ciberseguridad y la ciberdefensa. Además de blogs, el sitio también ofrece podcasts para aquellos que prefieran escuchar las noticias en vez de leerlas.

https://www.troyhunt.com/
Troy Hunt es un ejecutivo de Microsoft que comparte sus pensamientos sobre el mundo de la ciberseguridad generando interesantes debates a través de su sitio web.



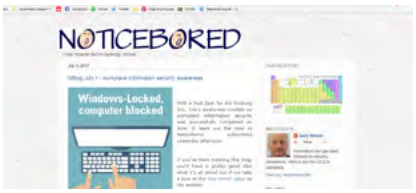
http://www.afcea.org/content/#
Sitio web de la revista online SIGNAL que trata sobre temas relacionados con la seguridad y defensa, especialmente aquellos relacionados con la ciberseguridad y la ciberdefensa.

http://thirdcertainty.com/
Sitio web editado por Byron Acohido donde se analizan las principales noticias del sector de la ciberseguridad y la ciberdefensa.



http://www.itsecurityguru.org/
Sitio web donde encontraras las ultimas noticias del sector de las TIC con análisis certeros de la actualidad del dominio cibernético.

http://blog.noticebored.com/
Interesante blog editado por Gary Hinson que comparte con los lectores su particular punto de vista sobre la actualidad del ciberespacio.



6.3 Cuentas de Twitter

@EUdefence

@RadioHacking

@KJScheid

@UKDefJournal

@cyber__affairs

7 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
4 Julio	Londres	Dods Group	The Cyber Security Summit	https://www.ruhrsec.de/2017/
4- 7 julio	Singapur	Interpol	INTERPOL World 2017	https://www.esetsecuritydays.com/es/
5- 7 julio	Barcelona	Pulse Conferences	CISO 360 Congress	https://paranoia.watchcom.no/
7- 8 Julio	Sheffield (UK)	Steelcon	Steelcon	http://www.ismsforum.es/evento/645/xix-jornada-internacional-de-seguridad-de-la-informacion-de-isms-forum/
18- 29 julio	León	INCIBE	Cybersecurity Summer BootCamp 2017	https://www.eiseverywhere.com/ehome/caro2017/448403/
22-27 julio	Las Vegas	UBM	Black Hat USA 2017	revolutionbanking.es
26- 28 julio	Madrid	IEEE	The 14th International Joint Conference on e-business and Telecommunications – ICETE 2017	http://2017.confidence.org.pl/
26- 28 julio	Singapur	RSA	RSA Conference 2017 Asia Pacific & Japan	http://www.e-crimecongress.org/event/france
27-30 Julio	Las Vegas	DEF CON Communications	DEF CON 25	http://www.cisoeurope.misti.com/

Con el patrocinio de

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 · gasNatural fenosa

Consejo Asesor Empresarial

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA · endesa

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