REAL INSTITUTO elcano ROYAL INSTITUTE

NOVIEMBRE 2016
Nº 19

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 Simon Roses 10

4 Informes y análisis sobre ciberseguridad publicados en octubre de 2016 13

5 Herramientas del analista 14

6 Análisis de los ciberataques del mes de octubre de 2016.....16

7 Recomendaciones

7.1 Libros y películas 23

7.2 Webs recomendadas 25

7.3 Cuentas de Twitter.....25

8 Eventos.....26

1 COMENTARIO CIBERELCANO:
La dimensión cibernética en el ámbito de las Fuerzas Armadas

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

Fuente: Diginomica

Aunque las campañas militares recientes podrían sugerir que la integración y explotación de la dimensión cibernética en el ámbito militar es algo novedoso, la realidad es que sus orígenes se sitúan a comienzos de la década de 1960 mientras que los primeros intentos de integrar en red las distintas capacidades de los ejércitos datan de mediados de los años setenta. En la actualidad, no sólo el elemento cibernético se ha consolidado como una dimensión esencial para la optimización del planeamiento y la conducción de las operaciones, sino que todos los sistemas, armas, plataformas y procesos se fundamentan en el poder de la red para llevar a cabo sus funciones.

Aunque las Tecnologías de la Información y las Comunicaciones se han integrado en el conjunto de las fuerzas armadas para mejorar su gestión y funcionamiento, su mayor beneficio e s u na capacidad sin precedentes para obtener, procesar, filtrar e interpretar incalculables volúmenes de información de interés militar; compartirla a todos los usuarios que la puedan necesitar de manera casi instantánea y neutralizar cualquier posible amenaza con rapidez, precisión, eficacia y sin la necesidad de exponer innecesariamente las fuerzas propias al fuego enemigo.

Y a pesar de que las tecnologías de la información y las comunicaciones – y podríamos añadir la robótica y la inteligencia artificial en ge-

neral– se han integrado en nuevas plataformas (furtivas y no-tripuladas); sensores (C4 e ISTAR) y armas (de precisión e inteligentes) para proporcionar importantes mejoras en la forma de concebir, plantear y conducir las operaciones; lo realmente relevante es que este conjunto de sistemas puedan trabajar y operar en red, permitiendo que cualquier soldado pueda conocer y controlar todo lo que sucede a su alrededor, bien sea reconociendo el terreno, identificando las amenazas, designando los objetivos o atacando los blancos en función de su situación, riesgo o disponibilidad.

Ésta es la premisa sobre la que se fundamenta el sistema de sistemas - como base para la Operación en Red- basado en la capacidad de la integración en red de todos los elementos de las fuerzas armadas para acumular una inmensa cantidad de información sobre el área de operaciones, convertirla en inteligencia útil para las fuerzas que operan sobre el terreno y aprovecharla de inmediato para derrotar al adversario.

Aunque todo lo expuesto con anterioridad pudiesen parecer los argumentos del guión de una prometedora película de ciencia-ficción, la realidad es que las principales potencias mundiales disponen de las capacidades mencionadas arriba y no conciben una operación militar ni mucho menos la obtención de la supremacía en el campo de batalla sin la dimensión cibernética.

"el elemento cibernético se ha consolidado como una dimensión esencial para la optimización del planeamiento y la conducción de las operaciones militares"

2 ANÁLISIS DE ACTUALIDAD INTERNACIONAL:
Wikileaks y el malware avanzado del AKP turco

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

El pasado 19 de julio a las 23:00 horas de Ankara, WikiLeaks filtraba los primeros correos electrónicos sustraídos al partido AKP de Turquía. Este hecho tuvo repercusión en el mundo de la seguridad ya que la organización liderada por Julian Assange, siendo fiel a su política de publicación de documentos secretos, difundió el contenido tal y como se lo facilitó su fuente original distribuyendo también el *malware* que contenía. Sin embargo, todavía se desconocían numerosos aspectos y el alcance del software malicioso, como refleja el siguiente *informe* publicado recientemente en el que se analizan las muestras de *malware* propagadas en la filtración incluyendo el propio contenido malicioso.

Distribución realizada para la infección

Para materializar una infección, un atacante necesita proveerse de una infraestructura tecnológica que le permita mantener el control del equipo infectado sin ser detectado. En este caso, tras analizar las direcciones origen de los correos electrónicos comprometidos se pudo comprobar que estos aprovechaban ciertas configuraciones vulnerables en los servidores de correo para maximizar sus posibilidades de éxito. En este contexto, pudieron llevar a cabo hasta tres técnicas de ingeniería social a través de vectores de ataque que algunos analistas han

considerado spear phishing, con el objetivo de garantizar que el destinatario abriera finalmente los ad-juntos maliciosos:

- Mediante la suplantación de direcciones de correo del propio partido político con el dominio akparti.org.tr.

```
1  Received: from user01-PC ([113.174.25.205])
2          by mail.akparti.org.tr (IceWarp 10.0.7) with ESMTP id VXX02800
3          for <milletvekilleriak@akparti.org.tr>; Thu, 07 Jul 2016 19:42:00 +0300
4  Content-Type: multipart/mixed; boundary=Apple-Mail-C43C69CE-2B43-F202-DEBC-3A1B8DA0BE5E
5  Content-Transfer-Encoding: 7bit
6  From: <milletvekilleriak@akparti.org.tr>
7  Mime-Version: 1.0 (1.0)
8  Date: Thu, 07 Jul 2016 23:26:06 +0700
9  Subject: [Spam] 2718C81F9CF7FBE4
10 Message-Id: <FDB7D463-C01B-D8AF-7CDC-1CC29812277A@akparti.org.tr>
11 To: huseyincelik@akparti.org.tr
12 X-Mailer: iPhone Mail (13F69)
13 X-Spam-Checker-Version: SpamAssassin 3.2.5 (1.1) on mail.akparti.org.tr
14 X-Spam-Flag: YES
15 X-Spam-Level: ****
16 X-Spam-Status: "Yes, hits=4,11 required=3,00 tests=RCVD_IN_PBL=0,91,SUBJ_ALL_CAPS=1,00,RAT
17
18 --Apple-Mail-C43C69CE-2B43-F202-DEBC-3A1B8DA0BE5E
19 Content-Type: text/plain;
20     charset=us-ascii
21 Content-Transfer-Encoding: 7bit
22
23 --Apple-Mail-C43C69CE-2B43-F202-DEBC-3A1B8DA0BE5E
24 Content-Type: application/vnd.ms-word.document.macroEnabled.12;
25     name=2718C81F9CF7FBE4.docm;
26     x-apple-part-url=06943163-CF29-044C-FDF6-FBBB339EC98F
27 Content-Disposition: attachment;
28     filename=2718C81F9CF7FBE4.docm
29 Content-Transfer-Encoding: base64
```

- Mediante la utilización de nombres de usuario de administración de la organización como support, scan, reception, printer, operator, helpdesk, administrator y admin.

```
1  Received: from 127.34.72.115.in-addr.arpa ([115.72.34.127])
2          by mail.akparti.org.tr (IceWarp 10.0.7) with SMTP id UKG01609
3          for <mehmetcakir@akparti.org.tr>; Wed, 06 Jul 2016 06:00:09 +0300
4  Mime-Version: 1.0
5  X-Mailer: Internet FAX, MGCS
6  Content-Type: multipart/mixed; boundary="+-+-+-+-MGCS-+-+-+-+"
7  Date: Wed, 06 Jul 2016 09:44:19 +0700
8  Message-Id: <17918226877081880387.C5919AE9@akparti.org.tr>
9  From: <support60@akparti.org.tr>
10 Subject: Scanned image
11 To: mehmetcakir@akparti.org.tr
12 X-Spam-Checker-Version: SpamAssassin 3.2.5 (1.1) on mail.akparti.org.tr
13 X-Spam-Level: *
14 X-Spam-Status: "No, hits=1,21 required=3,00 tests=RATWARE_RCVD_BONUS_SPC=1,00,BAYES_50=0,00,MR_NOT_ATTRIBUTED_IP=0,20,NO_RDNSZ=0,01 autolearn=No
   version=3.2.5"
15
16 --+-+-+-+-MGCS-+-+-+-+
17 Content-Type: text/plain; charset=iso-8859-1
18 Content-Transfer-Encoding: Quoted-Printable
19 Content-X-CIAJWNETFAX: IGNORE
20
21 Image data has been attached to this email.
22
23 --+-+-+-+-MGCS-+-+-+-+
24 Content-Type: application/vnd.ms-word.document.macroEnabled.12; name="05-07-2016_448150.docm"
25 Content-Transfer-Encoding: base64
26 Content-Disposition: attachment; filename="05-07-2016_448150.docm"
27 Content-Description: 05-07-2016_448150.docm
```

- Mediante cuentas de correo que usaban dominios que parecían provenir de organizaciones confiables como grandes empresas de hosting, operadoras o servicios de correo.

```
1  Received: from static.vnpt.vn ([14.161.18.50])
2          by mail.akparti.org.tr (IceWarp 10.0.7) with ESMTP id EVM08938
3          for <huseyincelik@akparti.org.tr>; Mon, 16 May 2016 19:22:38 +0300
4  From: "Amazon.com" <auto-shipping@amazon.com>
5  Reply-To: "auto-shipping@amazon.com" <auto-shipping@amazon.com>
6  Message-ID: <252B7A103B67B4D9139C2DBCC36F2698C7010C0E7BF2F6797419004 51@amazon.com>
7  Subject: [Spam] Your Amazon.com order has dispatched (#193-8689801-1900803)
8  To: huseyincelik@akparti.org.tr
9  MIME-Version: 1.0
10 Content-Transfer-Encoding: 7bit
11 Content-Type: multipart/mixed; charset=us-ascii; boundary="DbMail-MIME-Boundary-98529"
12 X-Spam-Checker-Version: SpamAssassin 3.2.5 (1.1) on mail.akparti.org.tr
13 X-Spam-Level: **
14 X-Spam-Status: "No, hits=2,76 required=3,00 tests=RATWARE_RCVD_BONUS_SPC=1,00,BAYES_50=0,00,BLANKBODY_ATT_SPAM=1,00,SARE_FROM_SPAM_WORDS=0,75,
15
16 This is a multipart MIME message
17 DbMail-MIME-Boundary-98529
18 Content-Type: text/plain; charset=us-ascii
19
20 Dear Customer,
21
22 Greetings from Amazon.com,
23
24 We are writing to let you know that the following item has been sent using  Royal Mail.
25
26 For more information about delivery estimates and any open orders, please visit: http://www.amazon.com/your-account
27
28 Your order #193-8689801-1900803 (received April 26, 2016)
29
```

Asimismo, se identificaron 2067 direcciones IP distintas distribuidas a nivel mundial como origen de los correos maliciosos, entre los que se han encontrado servidores web, ADSL residenciales y servidores de correo. La utilización de medios tan diversos no solo facilitó el envío de correos maliciosos sino que garantizó el anonimato de los atacantes.

Tipo de malware utilizado

Entre el *malware* más descargado por los destinatarios se encontraron diferentes familias de *ransomware* y de troyanos bancarios. Este tipo de *software* malicioso suele proceder de campañas con proyección mundial que utiliza la ciberdelincuencia organizada con fines puramente monetarios. Sin embargo, lo más destacable en la investigación fue la identificación del uso de troyanos tipo *backdoor*, que suelen estar asociados a robos de información y a ataques con el objetivo de realizar movimientos laterales en el seno de una organización u otro tipo de técnicas asociadas a ataques persistentes avanzados (APT, por sus siglas en inglés).

"...lo más destacable en la investigación fue la identificación del uso de troyanos tipo backdoor, que suelen estar asociados a robos de información y a ataques dirigidos..."

Después de analizar los correos adjuntos asociados a este tipo de troyano, se reconocieron como objetivo a personalidades relevantes dentro del gobierno turco como Bekir Bozdağ (Ministro de Justicia), Ömer Çelik (Ministro de relaciones con la Unión Europea), Nurettin Canikli (Primer Ministro de Turquía) y Hüseyin Çelik quien tam-bién ha ocupado diferentes cargos destacados dentro del gobierno.

Críticas al full-disclosure de WikiLeaks

Tras la publicación de los primeros correos del AKP, WikiLeaks fue objetivo de duras críticas por parte de diversas asociaciones en defensa de los derechos de la mujer por no tomar las cautelas mínimas para proteger y filtrar determinados datos de carácter personal.

Algunas figuras relevantes de los mencionados movimientos, como la *norteamericana de origen turco Zeynep Tufekci*, afirman que entre los emails publicados se encuentran datos personales de todas las votantes de 79 de las 81 provincias que conforman el territorio turco, exponiendo a dichas mujeres a los grupos radicales islamistas de la zona que se declaran en contra del sufragio femenino en la región.

Adicionalmente, los datos, aparentemente aportados a WikiLeaks por un actor externo con acceso al servidor de correo de AKP, fueron publicados demasiado rápido, exponiendo así al atacante que seguía manteniendo acceso al servidor del partido político.

No es la primera vez que WikiLeaks publica ficheros que contienen *malware*. En septiembre de 2015,el investigador independiente Josh Wie-

der, encontró *malware alojado en la sección The Global Intelligence Files* del sitio web de la organización. Es por esto que se recomienda a periodistas y analistas que consulten dichos documentos con cautela a fin de no resultar infectados.

La seguridad tradicional no es suficiente

Las soluciones de seguridad tradicionales no son suficientes ante muestras de *malware* aún no identificadas y que podrían estar asociadas a ataques dirigidos. A pesar de que la seguridad en términos absolutos no existe, las tecnologías de defensa contra *malware* avanzado podrían convertirse en la solución ante unas amenazas que presentan una probabilidad muy alta de materializarse.

Si parafraseamos a Eugene H. Spafford, experto en seguridad de la información, el único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aun así, ni el propio experto apostaría su vida por él. Sin duda una visión muy escéptica pero muy ilustrativa de por qué es importante mantenernos siempre alerta en lo que se refiere a nuestros sistemas de defensa.

"A pesar de que la seguridad en términos absolutos no existe, las tecnologías de defensa contra malware avanzado podrían convertirse en la solución ante unas amenazas que presentan una probabilidad muy alta de materializarse"

3 Entrevista a Simon Roses.
Fundador y CEO de VULNEX

1. Simón, ¿cómo surgió VULNEX?

VULNEX surgió ante la necesidad de crear en España una empresa altamente especializada en materia de ciberseguridad que combinara servicios avanzados, formación de calidad e innovadora y desarrollase productos killer. En definitiva, una empresa creada por hackers para hackers con una visión global.

Desde 2012 hemos ido alcanzado importantes hitos: ganamos un proyecto de I+D para DARPA y fuimos invitados al Pentágono en mayo de 2014 para presentar nuestro trabajo. Además, hemos impartido numerosas conferencias en los principales congresos nacionales e internacionales de ciberseguridad (Black Hat, DEF CON, RSA, OWASP o HITB).

2. Y, ¿cuales son las principales líneas de actividad de VULNEX?

Desde sus inicios, VULNEX es una empresa que ofrece servicios de alto valor añadido y especializados tales como Hacking Ético, Seguridad en el Desarrollo de software así como Servicios Avanzados en Ciberseguridad. También contamos con una formación de primer nivel en Hacking Ético, Análisis de Malware, Hacking Móviles, *Open Source Intelligence (*OSINT) y *Security Data Science*, que hemos tenido el placer de impartir en varios países y a FCSE de distintas nacionalidades.

En la actualidad, estamos apostando por el desarrollo de productos. BinSecSweeper, nuestro primer producto, ha sido desarrollado con la beca de I+D del DARPA. Se trata de una plataforma en la nube que combina análisis estático, análisis dinámico y análisis Big Data para identificar riesgos en todo tipo de ficheros, documentos, aplicaciones móviles, etc. Tiene diversas características que lo convierten en un producto único en el mercado.

3. En su opinión, ¿cuáles son los principales retos en materia de ciberseguridad a los que se enfrentan gobiernos, empresas y ciudadanos?

Los tiempos han cambiado y la mayoría de gobiernos y empresas no lo han comprendido todavía. Los días donde los hackers entraban en

sistemas ajenos por el simple afán de superación han quedado atrás. Hoy en día los criminales, que no hackers, se han profesionalizado y son capaces de lanzar miles de ataques al día a un coste muy bajo. Es por ello que para defenderse se requiere una cierta inversión que muchos gobiernos y empresas no están realizando.

Estamos rodeados de información en ordenadores, tablets, móviles, redes sociales, Internet de las Cosas, etc., y es vital que se tomen las medidas necesarias en seguridad y privacidad para proteger toda esta información. Cualquier información es o puede ser valiosa en cualquier momento para alguien.

4. ¿Qué diagnóstico haces del estado de la ciberseguridad nacional?

El mercado español lo resumo como mucho ruido y pocas nueces. Últimamente se habla mucho de ciberseguridad, pero la realidad es que se invierte muy poco. En el fondo, la seguridad se percibe como un gasto cuando realmente es una inversión.

España cuenta con estupendos profesionales que optan por irse al extranjero, donde existen proyectos más interesantes y están mejor pagados y valorados. Esto está afectando de forma negativa al mercado español, en el que la calidad y precios han bajado drásticamente. Tanto es así que empresas extranjeras están aprovechando para abrir oficinas en España con el único fin de reclutar el talento que las empresas nacionales no captan porque no pueden o no quieren competir.

Lo cierto es que los clientes deberían pagar precios más altos por lo que reciben para que las consultoras pudieran retribuir mejor a sus empleados y atraer talento. De esa forma, la calidad del mercado mejoraría considerablemente. Si no, la situación será cada vez peor para el mercado de la ciberseguridad en España: solo quedarán grandes empresas nacionales sin talento alguno y se recurrirá a empresas extranjeras con precios mucho más elevados. Ya estamos llegando al punto donde se paga gustosamente lo que piden las empresas extranjeras, pero si son nacionales, el cliente te impone el precio (por supuesto, ridículo y por debajo de coste), ¡y hasta te proponen que lo hagas gratis con la promesa

de futuros contratos! La empresa española debe salir del servicio del *bodyshopping* de una vez por todas.

5. ¿Qué medidas habría que tomar en el corto plazo para mejorar la ciberseguridad nacional?

El gobierno junto con el sector privado deben potenciar en serio la industria nacional de ciberseguridad en áreas como:

- Desarrollar verdaderos centros de I+D en ciberseguridad en las universidades
- Incrementar los precios por servicios y formación para poder mejorar salarios
- Promover la concienciación en seguridad y privacidad a todos los niveles
- Potenciar la inversión en startups de ciberseguridad: hablamos de dinero real y no de pequeñas cantidades que no permiten crear nada.
- Mejorar la seguridad y privacidad en el software, móviles, Internet de las Cosas, etc.
- Crear una industria fuerte basada en productos innovadores

"El mercado español de ciberseguridad se resume en: mucho ruido y pocas nueces"

En definitiva, invertir en ciberseguridad. Es cierto que desde el gobierno y la industria privada están saliendo diferentes iniciativas pero se quedan en eso, iniciativas. Es hora de coger el toro por los cuernos en una industria con un altísimo potencial de crecimiento en el mercado mundial.

6. Por último, ¿qué medidas adoptarías para la captación y proyección del talento nacional en materia de ciberseguridad?

Tres medidas: mejorar salarios, planes de formación continua y proyectos interesantes. El mercado español en ciberseguridad es inmaduro comparado con Alemania o los países anglosajones donde retribuyen más adecuadamente y se solicitan servicios y formación más avanzados. Ahora mismo el profesional de ciberseguridad en España está quemado y desilusionado.

En España existe talento y la captación pasa por invertir en ciberseguridad para crear centros de excelencia en I+D donde estas personas puedan recibir formación continua para estar en la vanguardia, creen productos de valor y realicen servicios de calidad.

4 Informes y análisis sobre ciberseguridad publicados en octubre de 2016

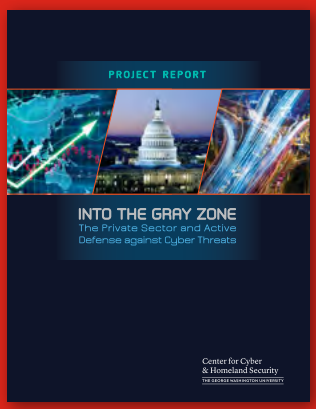
National CyberSecurity Strategy (UK Government)

Principales riesgos en el uso de Whatsapp (CCN-CERT)

Moving forward with cybersecurity and privacy (PWC)

Cyber Risk Report 2016 (HP)

Into the gray zone (George Washington University)



Guide to Cyber Threat Information Sharing (NIST)

Singapore´s CyberSecurity Strategy (Singapore Government)

The state of Cyber Security Professional Career (ISSA)

5 HERRAMIENTAS DEL ANALISTA:
Malice

El objetivo de *Malice* es convertirse en una alternativa de código abierto del conocido servicio VirusTotal, de forma que cualquier profesional de seguridad, desde una gran compañía a un investigador individual, puede disponer de un sistema antivirus multi fabricante y offline en el que poder procesar sus muestras de ficheros en busca de software malicioso.

Malice es una aplicación que permite interactuar con su servicio a través de una API, habilitando multitud de integraciones posibles con software externo.

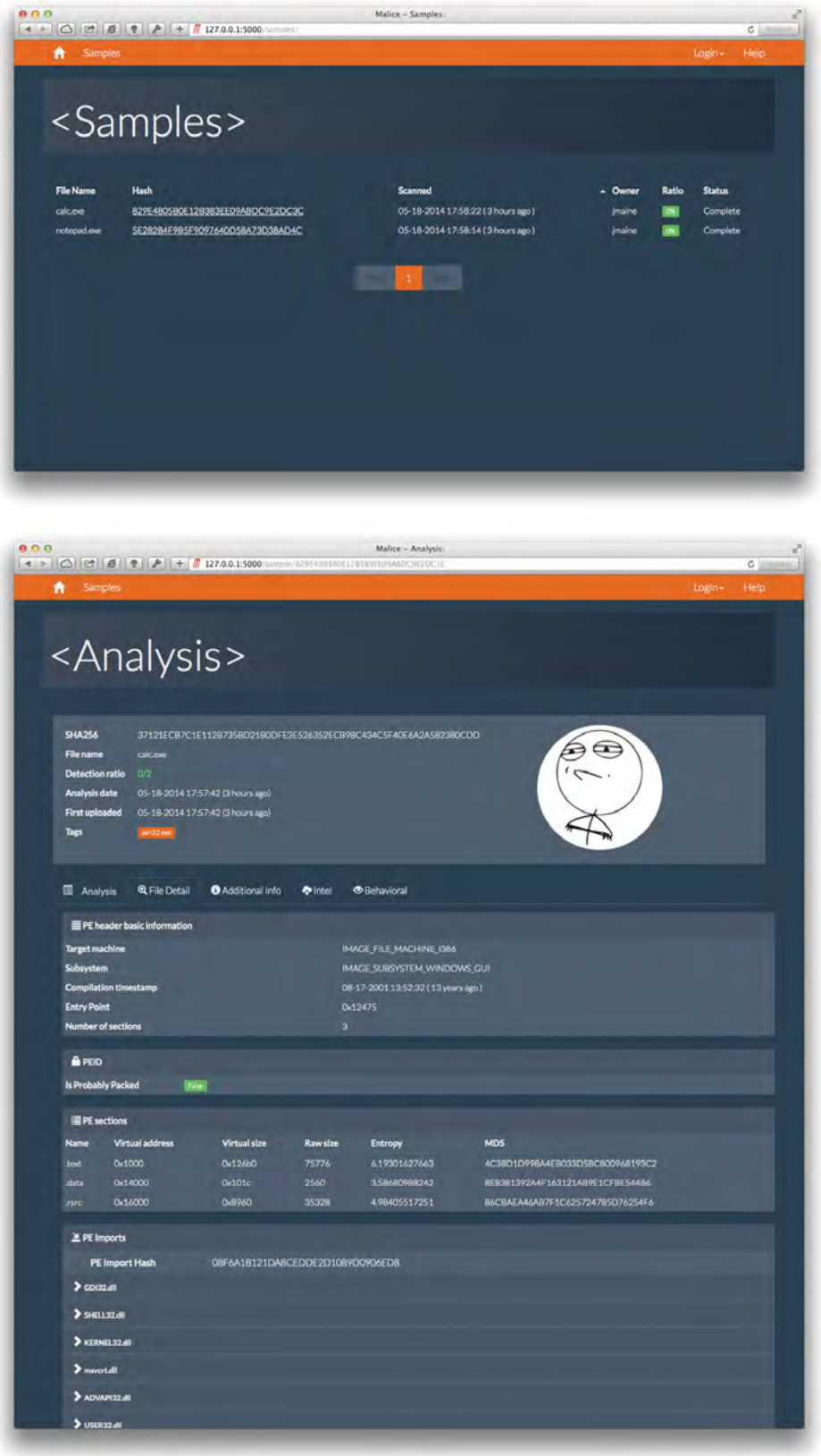
Está escrito en Go (se requiere la versión 1.5 o superior) y requiere Docker ya que el sistema irá levantando contenedores para el análisis según los plugins habilitados, todos controlados por un contendedor supervisor con ELK (Elasticsearch, Logstash y Kibana).

```
root@              :~/.malice# malice plugin list --all --detail
| Name          | Description                                | Enabled | Image                  | Category | Mime                        |
| ------------- | ------------------------------------------ | ------- | ---------------------- | -------- | ---------------------------- |
| nsrl          | NSRL Database Hash Search                  | false   | malice/nsrl            | intel    | hash                        |
| virustotal    | VirusTotal - files scan and hash lookup    | true    | malice/virustotal      | intel    | hash                        |
| shadow-server | ShadowServer - hash lookup                 | true    | malice/shadow-server   | intel    | hash                        |
| team-cymru    | TeamCymru - hash lookup                    | false   | malice/team-cymru      | intel    | hash                        |
| fileinfo      | ssdeep/TRiD/exiftool                       | true    | malice/fileinfo        | metadata | *                           |
| yara          | YARA Scan                                  | true    | malice/yara            | av       | *                           |
| avast         | Avast AntiVirus                            | false   | malice/avast           | av       | *                           |
| avg           | AVG AntiVirus                              | true    | malice/avg             | av       | *                           |
| bitdefender   | Bitdefender AntiVirus                      | true    | malice/bitdefender     | av       | *                           |
| clamav        | ClamAV                                     | true    | malice/clamav          | av       | *                           |
| comodo        | Comodo AntiVirus                           | true    | malice/comodo          | av       | *                           |
| fprot         | F-PROT AntiVirus                           | true    | malice/fprot           | av       | *                           |
| f-secure      | F-Secure AntiVirus                         | true    | malice/f-secure        | av       | *                           |
| sophos        | Sophos AntiVirus                           | true    | malice/sophos          | av       | *                           |
| pe            | PE - tool to triage portable executables   | false   | malice/pe              | exe      | application/x-dosexec       |
| floss         | FireEye Labs Obfuscated String Solver      | true    | malice/floss           | exe      | application/x-dosexec       |
| office        | Office - tool to triage OLE/RTF documents  | false   | malice/office          | document | *                           |
| pdf           | PDF - tool to triage PDF documents         | false   | malice/pdf             | document | application/pdf             |
| javascript    | Javascript - tool to triage JS scripts     | false   | malice/javascript      | document | application/javascript      |
| zip           | Zip - tool to unarchive archives           | false   | malice/zip             | archive  | archive                     |
root@              :~/.malice#
```

Listado de plugins de Malice

La herramienta está diseñada para que su uso sea intuitivo y rápido, permitiendo a la comunidad de analistas de seguridad compartir y desarrollar plugins para mejorar la solución.

Malice también ha sido comúnmente empleado entre los desarrolladores de malware, ya que permite analizar payloads maliciosos sin la necesidad de remitir ningún tipo de información a los diferentes fabricantes de antivirus, exponiendo de esa forma su existencia.



Ejemplo de consola de análisis

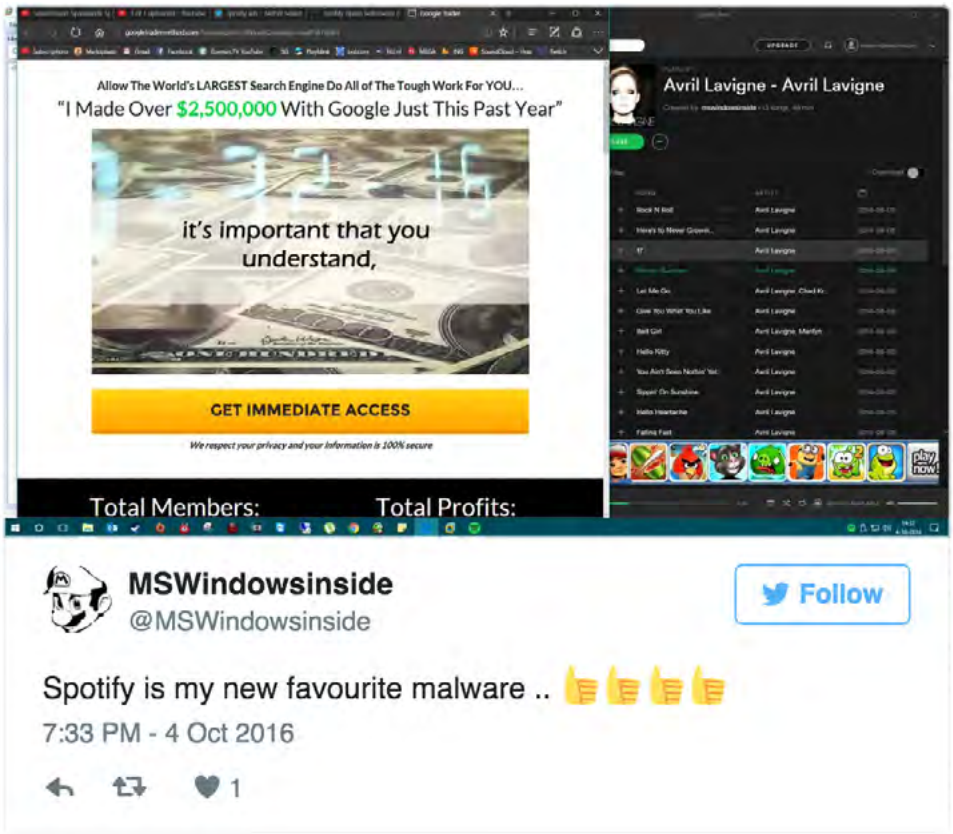
6 Análisis de los Ciberataques del mes de octubre de 2016

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

CIBERCRIMEN

El popular servicio de streaming de música *Spotify ha estado sirviendo publicidad con malware* en los equipos de algunos usuarios, según reportaron múltiples clientes en los foros de la comunidad de Spotify y en sus redes sociales. Los usuarios han informado de que los anuncios y banners publicitarios que se muestran con Spotify Free, el producto gratuito de la empresa sueca, han lanzado automáticamente sitios web maliciosos en sus escritorios sin su permiso.

Los primeros incidentes fueron reportados el martes 4 de octubre por el usuario Tonyonly en el foro de la comunidad de Spotify. Transcurridos unos momentos, múltiples usuarios alegaron ha-ber experimentado problemas similares en Windows 10, MacOS y Ubuntu, en los que sus na-vegadores web estaban lanzando y produciendo los anuncios sospechosos.

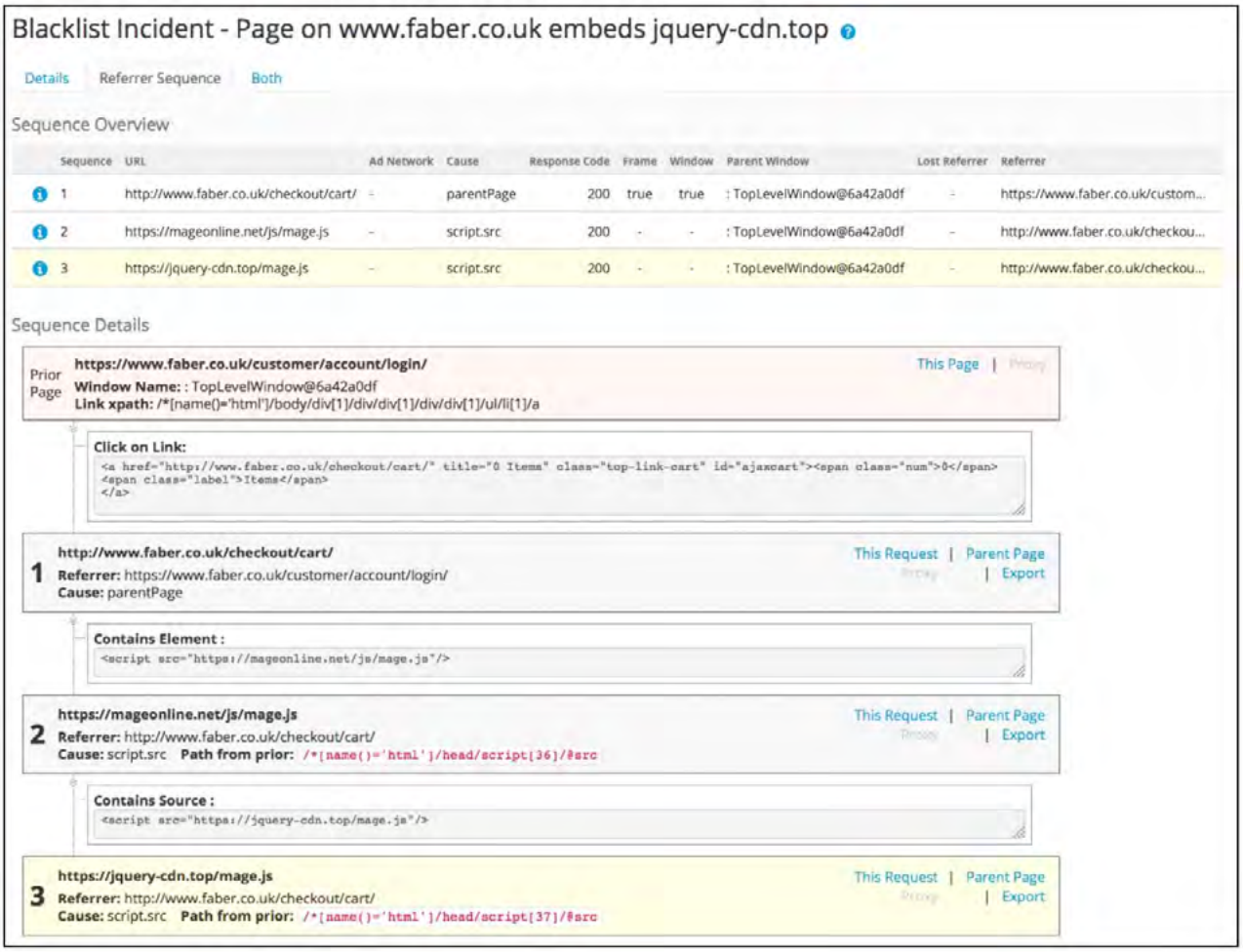


Ejemplo del adware malicioso distribuido por Spotify

El 6 de octubre, las compañías de seguridad *RiskIQ y ClearSky hicieron público un informe* en el que revelaron que diversos sitios web de comercio electrónico populares han sido infectados con keyloggers basados en web que han sido empleados para robar datos de tarjetas de crédito al ser introducidos en formularios de pago online. Se han identificado más de 100 si-tios comprometidos, pero el número podría ser muy superior.

Algunos de las web afectadas pertenecen a Everlast Worldwide, el sitio de comercio electrónico australiano del gigante de prendas de vestir Guess y FidelityStore de Fidelity Investments.

La campaña parece estar vinculada a un solo grupo de cibercriminales no identificado, detectándose el origen de su actividad en marzo. Muchos de los sitios vulnerados siguen robando datos de tarjetas de crédito.

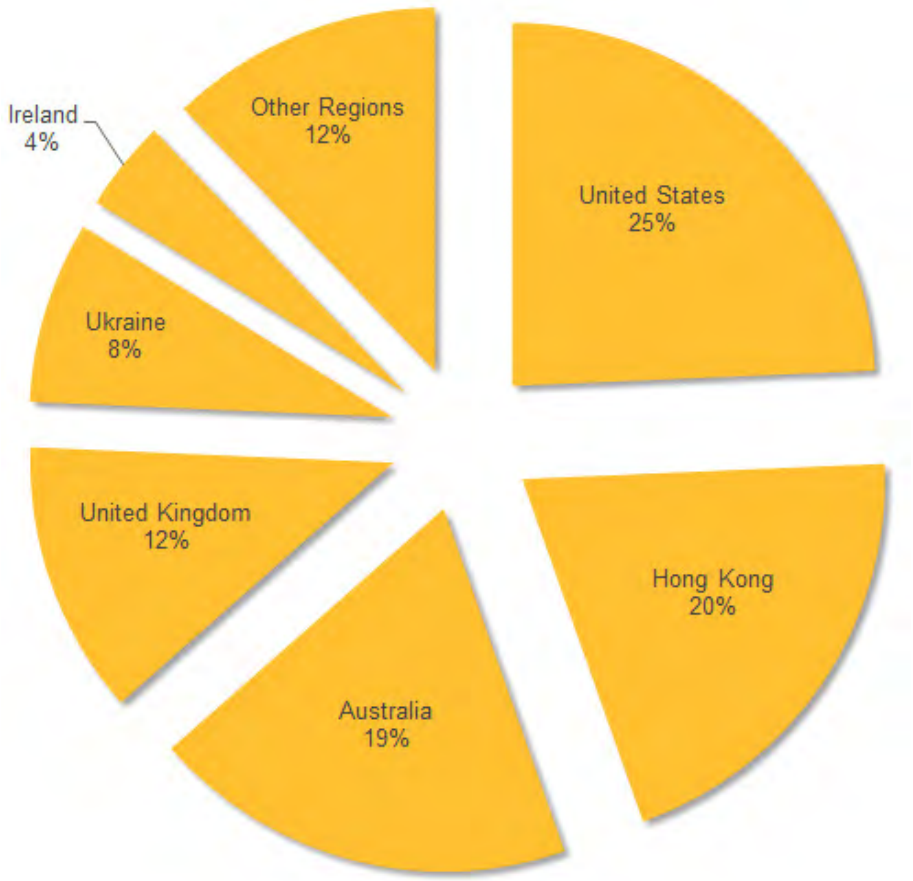


Muestra del keylogger embebido en webs de comercio electrónico

Symantec reveló a mediados de mes que un segundo grupo de hackers estaba intentando robar diversas entidades financieras atacando a los usuarios de SWIFT, desplegando los mismos métodos y vectores de ataque que ya se usaron en el ciberataque al Banco Central de Bangladesh. Las herramientas utilizadas están vinculadas al grupo Odinaff, que desde el comienzo del año, se han estado centrando en las instituciones financieras de todo el mundo.

En su blog, Symantec detalla el esquema del ataque empleado contra SWIFT, una red de pagos que las entidades financieras usan para transferir fondos. Los atacantes están utilizando herramientas maliciosas para supervisar los mensajes SWIFT enviados a los equipos infectados con números de cuentas bancarias u otras palabras clave relacionadas con transacciones específicas. Cuando se intercepta un mensaje que contiene una cadena de texto relacionada, los atacantes utilizan un componente "supresor" para expulsarlo del sistema de archivos local para evitar que el destinatario lo lea o lo recupere.

Con el fin de realizar este tipo de seguimiento, los atacantes están haciendo uso de un troyano llamado Odinaff que se conecta a un equipo remoto y puede descargar archivos cifrados con RC4 y ejecutarlos. Junto con eso, están utilizando una gama de herramientas ligeras de hacking y software legítimo.



Infecciones de Odinaff por región

CIBERESPIONAJE

En un comunicado especial lanzado el 1 de octubre, *el gobierno surcoreano reconocía que el cibercomando de su nación había sufrido varios incidentes informáticos* tras ser objetivo de diversos y reiterados ataques en los últimos días.

El representante Kim Jin-pyo, legislador del principal partido de oposición Minjoo de Corea del sur, en un comunicado público afirmó que "se ha identificado un código malicioso en uno de los principales routers del cibercomando, habiendo aprovechado una vulnerabilidad del servidor. Como medida cautelar, el router ha sido separado de la red."

Dicho router está encargado de la seguridad de los equipos que el ejército tiene para fines de conexión a Internet. Se sabe que alrededor de 20.000 ordenadores militares han sido conectados al servidor de routing.

El gobierno afirma que las posibilidades de una fuga de información confidencial "son muy bajas" dado que la intranet del cibercomando no está conectada a dicho elemento de red. Paralelamente, se están realizando pesquisas sobre la potencial autoría del ataque, señalando a una posible implicación de Corea del Norte.

A mediados de mes, se hizo público el ciberataque sufrido por unos investigadores del Centro de Investigación de Isótopos de Hidrógeno de la Universidad de Toyama en Japón. Los datos de la investigación y la información personal podrían haber sido sustraídos de un ordenador personal perteneciente a un investigador de tritio, un isótopo radiactivo de hidrógeno. La mayor parte de los datos de la investigación potencialmente afectados ya se habían publicado o estaban programados para ser publicados, por lo que ninguna información confi-dencial fue comprometida, según confirmó la universidad en un comunicado oficial.

Además de los datos de la investigación, los atacantes podrían haber robado información personal de unas 1.500 personas, incluyendo otros investigadores.

Según la universidad, dos miembros del personal del centro recibieron mensajes de correo electrónico que contenían un virus en noviembre de 2015 resultando infectado un portátil de un miembro del personal docente. El portátil mantuvo un canal de comunicación encubierto con el servidor del atacante externo durante cerca de seis meses.

La sensibilidad de los datos afectados es relevante por su relación con el desarrollo de un programa nuclear. El centro lleva a cabo investigaciones sobre el hidrógeno, el deuterio y el tritio, incluido su uso en ámbitos energéticos. El tritio es considerado un posible combustible para reactores de fusión nuclear, y es también uno de los contaminantes del agua que se acumulan en la planta nuclear número 1 de Fukushima.

Centro de Investigación de Isótopos de Hidrógeno de la Universidad de Toyama

Finalmente, entre el 10 y el 12 de octubre, una gran cantidad de activistas y periodistas independientes rusos han recibido advertencias notificándoles que unos ciberatacantes "respaldados por el gobierno" podrían estar tratando de acceder ilegalmente a sus buzones de correo electrónico.

Según publicó en redes sociales el activista *Oleg Kozlovsky* al menos 16 personas fueron objetivo de estos ataques. En una lista publi-cada en Facebook, otros cuentas afectadas estaban relacionadas con el activista político Nikolay Kavkazsky, el activista de derechos civiles Roman Dobrokhotov y la periodista Vera Kichanova.

Según *Global Voices Advocacy*, que fueron los primeros en alertar sobre el incidente, se cree que al menos tres ONGs fueron blanco de los atacantes potencialmente con patrocinio estatal.

La autoría sigue siendo desconocida. Sin embargo, diversos activistas afectados sospechan la implicación de la inteligencia rusa o

hackers con apoyo estatal rusos. Algunos de los activistas afectados, colaboradores habituales en la emisora de noticias independiente Bellingcat, también se vieron afectados en otro ataque sobre dicha emisora online que se efectuó en septiembre. Según la investigación realizada por la firma de seguridad ThreatConnect, se encontraron evidencias de que sus colaboradores habían sido blanco del famoso grupo Fancy Bears.

Oleg Kozlovsky
11 de octubre a las 18:35 ·

Итак, на данный момент известно о 24 целях взлома почтовых ящиков (в основном Gmail) в течение последних суток:
список обновляется
- Andrey F. Babitsky
- Roman Dobrokhotov
- Alexei Zakharov
- Nikolay Kavkazsky
- Максим Кац
- Vera Kichanova
- Ilya Klishin
- Darya Kostromina
- Alexander Kynev
- Arsenii Levinson
- Yaroslav Nikitenko
- Elena A. Panfilova
- Alexandr Peredruk
- Maxim Polyakov
- Roman Popkov
- Anastasia Popova
- Anastasia Sergeeva
- Dmitry Tkachev
- Aric Toler
- Max Trudolubov
- Вера Челищева
- Olesya Shmagun
- Katerina Shcherbakova
- и я

Alexey Shlyapuzhnikov сообщает еще о 16 атаках (часть, наверное, пересекается) + 3 доменах НКО (где потенциально десятки ящиков). Из них только один взлом был удачный.

В большинстве случаев почтовые сервисы сообщали, что атаки осуществляются, по-видимому, силами спецслужб.

UPDATE: Поскольку большинство людей в этом списке узнали о попытке взлома из предупреждения Гугла, вполне возможно, что это только верхушка айсберга: те атаки, которые Google распознал и смог предотвратить. Остальные, скорее всего, так ничего и не подозревают.

Listado de cuentas de email de activistas rusos afectadas por el ciberataque

HACKTIVISMO

El pasado 8 de octubre, un sitio web llamado *'Bohrileaks'* publicó los registros de asistencia a la Ashara de los musulmanes Bohri de todo el mundo -incluyendo nombres, números de teléfonos móvil- en lo que se afirma es un esfuerzo por exponer lo mal protegidos que están los datos personales de la comunidad musulmana.

El dawat Dawoodi Bohra Fatemi mantiene un registro meticuloso de los miembros musulmanes de esta rama, creando la denominada tarjeta eJamat, emitida en el momento del nacimiento y cuyos registros se van manteniendo actualizados a lo largo de la vida de los miembros.

Aspecto de la web bohrileaks.is

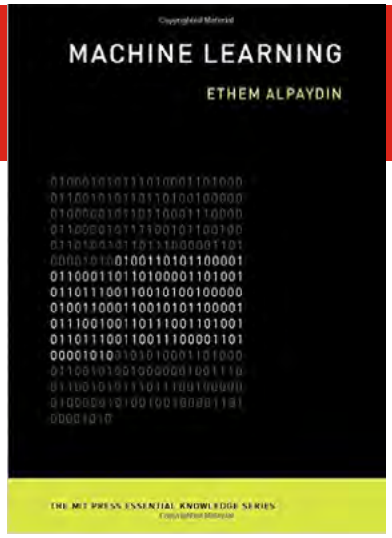
7 Recomendaciones

7.1 Libros y películas

Película:
CIBER GUERRILLA: HACKERS, PIRATAS Y GUERRAS SECRETAS

Sinopsis: Las principales potencias mundiales se preparan ya para la primera guerra en Internet: los hackers controlan los conflictos cibernéticos y saben cómo hacer fortuna a costa de los ciudadanos y los usuarios de las grandes empresas.

Correo basura, estafas, propagación de virus destructivos no son más que el comienzo de las nuevas posibilidades, ya que cada día la delincuencia en Internet es una feria donde se ponen de manifiesto la creatividad individual y colectiva de las maneras más sorprendentes. Este documental que Odisea les presenta viajará hasta Rusia, Estados Unidos, Estonia e Israel para investigar los puntos calientes donde compiten los piratas informáticos y los gobiernos.

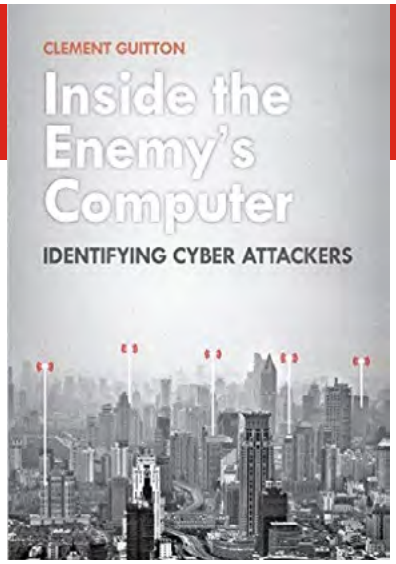


Libro:
MACHINE LEARNING

Autor: Ethem Alpaydin
Num. Paginas: 224
Editorial: MIT Press
Año: 2016
Precio: 16.00 Euros
Sinopsis: En este nuevo libro de la seria MIT Essential, el autor analiza los conceptos básicos del aprendizaje automático o aprendizaje de máquinas, una rama de la inteligencia artificial cuyo objetivo es desarrollar técnicas que permitan aprender a las computadoras.

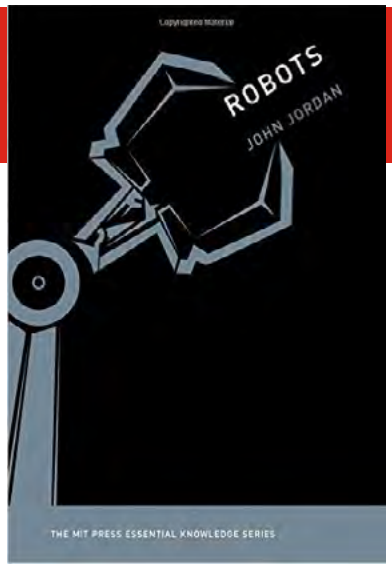
Libro:
EL CISNE NEGRO

Autor: Nassim Nicholas Taleb
Num. Paginas: 210
Editorial: Booklet
Año: 2002
Precio: 9.95 Euros
Sinopsis: El autor nos enseña a reconocer, dentro de la complejidad de la era digital, que no todo está predeterminado ni determinado; que siempre puede aparecer un cisne negro, una excepción.



Libro:
INSIDE THE ENEMY'S COMPUTER

Autor: Clement Guitton
Num. Paginas: 224
Editorial: C Hurst & Co
Año: 2016
Precio: 30.00 Euros
Sinopsis: El autor realiza un pormenorizado análisis de la irresoluble problemática de la atribución cibernética desde dos perspectivas: la tecnológica y la política.



Libro:
ROBOTS

Autor: John Jordan
Num. Paginas: 272
Editorial: MIT Press
Año: 2016
Precio: 16.00 Euros
Sinopsis: No cabe duda de que los robots forman parte de nuestra vida cotidiana. Por ello, el autor del libro realiza un interesante análisis del por qué la robótica no debe ser una tecnología controlada únicamente por expertos en la materia ya que sus implicaciones trascienden más allá de la vertiente tecnológica.

7.2 Webs recomendadas

https://cchs.gwu.edu/
Sitio web del think tank "Center for Cyber and Homeland Security" adscrito a la Universidad George Washington.

http://www.defensenews.com/cyber
Sección de ciberseguridad y ciberdefensa del portal estadounidense de noticias del sector de la defensa Defense News.

http://www.usma.edu/acc/SitePages/Home.aspx
Sitio web del Instituto de Ciberdefensa del U.S Army.

http://www.simonroses.com/
Blog de Simon Roses, CEO de VULNEX, compañía española de ciberseguridad.

http://www.cyberdefensemagazine.com/
Sitio web de CyberDefense Magazine, editado por Pierluigi Paganini.

http://www.colcert.gov.co/
Sitio web del Grupo de Respuesta a Emergencias Cibernéticas del Gobierno de Colombia.

7.3 Cuentas de Twitter

@gwcchs

@CapacityCentre

@arg_cibersegura

@Aristot73

@Beatriz_Sercas

8 Eventos

FECHA	LUGAR	ORGANIZADOR	TÍTULO	URL
1 Nov	Doha, Qatar	QNB	Third Annual Information Security Conference for the Financial Sector	https://www.qcb.gov.qa/agenda/
1- 4 Nov	Londres	Black Hat	Black Hat Europe 2016	https://www.blackhat.com/eu-16/
2 - 3 Nov	Londres	ACI	Cyber Security - Oil, Gas, Power Conference	http://www.wplgroup.com/aci/event/cyber-security-oil-gas-power/
4- 5 Nov	Quebec	HackFest	Hackfest	http://www.hackfest.ca/
5- 9 Nov	Delhi, India	Indian Infosec Consortium	Ground Zero Summit 2016	http://www.g0s.org/g0s15/index.html
7 - 8 Nov	Berlin	Management Circle	Global Cyber Security Leaders 2016	http://www.global-leaders-summits.com/summit/global-cyber-security-leaders
7 - 10 Nov	Bruselas	IAAP	IAPP Europe Data Protection Congress 2016	https://iapp.org/conference/iapp-europe-data-protection-congress/
8 - 9 Nov	Viena	DeepSec	DeepSec 2016	https://deepsec.net/
11 Nov	Lisboa	Bsides	BSides Lisbon 2016	http://www.bsideslisbon.org/
14 - 17 Nov	Tel Aviv	Mº de Defensa de Israel	The 4th International HLS & CYBER Conference	https://www.israelhlscyber.com/
14 Nov	Madrid	CSA-ES	VI Encuentro del capítulo Español de Cloud Security Alliance	https://www.ismsforum.es/evento/641/vi-encuentro-de-cloud-security-alliance-espana/
15 - 16 Nov	Madrid	CSA	CSA Congress EMEA 2016	https://csacongress.org/event/emea-congress-2016/
15 - 16 Nov	Abu Dabhi	RSA	RSA Conference Abu Dhabi 2016	https://www.rsaconference.com/events/ad16
17 - 18 Nov	Hong Kong	Rooted	Rooted CON Hong-Kong	https://www.rootedcon.com/
17 Nov	Madrid	CNPIC	IV Jornada de Infraestructuras Críticas	http://www.seguritecnia.es/revistas/seg/fundacion_borreda/PIC_2016/PIC2016_programa.pdf

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