INFORME PANDALABS Q2 2016

panda

pandalabs

1. INTRODUCCIÓN

1 Introducción

El ciberespacio forma cada vez más parte de nuestra vida. La transformación digital afecta tanto al ámbito empresarial como al personal, incrementando el número de dispositivos conectados a la red.

Conceptos como “hogar digital” y “BYOD” (Bring Your Own Device) ya forman parte de nuestro universo hiperconectado, con sus consiguientes agujeros de seguridad. Nuevas amenazas, pero también nuevos retos y oportunidades para el mundo de la ciberseguridad.

Así lo confirman las 18 millones de nuevas muestras de malware detectadas por PandaLabs en el segundo trimestre del año.

Los troyanos siguen a la cabeza del ranking, destacando el incremento de los ataques del tipo ransomware, englobados dentro de la misma categoría. La media de nuevas amenazas detectadas a diario es de 200.000, cifra ligeramente inferior a la del anterior trimestre, cuando hablábamos de unas 227.000. **Junto al ransomware, el robo de información y de credenciales acapara la mayoría de la actualidad este trimestre**.

Las empresas podrían ver en el auge del **Internet de las Cosas una amenaza a corto plazo**, ya que se han convirtido en una fuente de ataques que puede afectar directamente a nuestras vidas facilitando, por ejemplo, que nos roben el coche tras haber desactivado la alarma por internet.

En el terreno de los móviles vemos cómo cada vez aparecen más vulnerabilidades y repasaremos la problemática derivada de que las actualizaciones dependan de los fabricantes de hardware.

2. EL TRIMESTRE DE UN VISTAZO

2

El trimestre de un vistazo

Ransomware

Sabemos que el ransomware es un gran negocio para los ciberdelincuentes pero cuantificarlo, si es que se puede llegar a hacer de forma fiable, es algo muy complejo.

En Estados Unidos, el Departamento de Justicia ha hecho público que durante 2015 ha recibido un total de 2.500 denuncias de ataques de ransomware a través del IC3 (Internet Crime Complaint Center) **cuyas víctimas han reconocido haber pagado un total de 24 millones de dólares**.

Extrapolando esta cifra a niveles mundiales, podemos deducir que se trata de un negocio que podría estar moviendo **miles de millones de dólares cada año**.

En los últimos meses, se han conocido multitud de casos de empresas del sector sanitario atacados por ransomware. Comenzamos el trimestre hablando de *MedStar Health*, que estuvo obligado a tener sus sistemas desconectados durante varios días debido a un ataque de ransomware dirigido que utilizaba una vulnerabilidad en sus sistemas.

Sin embargo, muchos de estos ataques se llevan a cabo a través de páginas web que han sido comprometidas. De hecho, en el mes de abril la web de *Maisto International*, la famosa fábrica de juguetes a control remoto, fue comprometida y sus visitantes estuvieron expuestos a un ataque de ransomware a través del conocido exploit kit Angler, cuyo objetivo es identificar intentos de descarga de un conjunto de herramientas para ejecutar un código malicioso que pone en peligro al ordenador a través de diversas vulnerabilidades de las aplicaciones instaladas.

Aunque no todos los ataques a través de páginas web son consecuencia del hackeo de las mismas. Los ciberdelincuentes también utilizan otra popular táctica, conocida como malvertising (del inglés malicious advertising, anuncios maliciosos) donde utilizan espacio publicitario en webs de mucho tráfico para infectar a sus visitantes.

En cuestión de unos días la conocida página perezhilton.com fue víctima de dos ataques de malvertising que utilizaban de nuevo el exploit kit Angler para infectar a los más de 500.000 visitantes diarios del popular blog.

Los ataques dirigidos utilizando una vulnerabilidad del sistema, el hackeo de páginas web y el malvertising son amenazas comunes.

Uno de los casos más curiosos de ransomware que vimos este trimestre, lo protagonizó una empresa de Eslovenia.

El responsable de seguridad de la empresa recibió un mensaje de correo desde Rusia, donde le comunicaban que le habían comprometido la red y habían dejado listo para ejecutar un ransomware en todos los ordenadores. **Si no pagaba unos 9000€ (en bitcoins) en el plazo de 3 días, ejecutarían el ransomware**. Para demostrar que efectivamente tenían acceso a su red le enviaron un fichero con el listado de todos los dispositivos conectados a la red interna de la empresa.

Hay víctimas que optan por pagar el rescate, aunque esto no garantiza la recuperación de la información. En mayo, el *Kansas Heart Hospital* fue atacado por ransomware y sus responsables aceptaron pagar el rescate para poder recuperar sus datos. Sin embargo, se llevaron una desagradable sorpresa cuando comprobaron que, con la clave recibida, sólo podían recuperar una pequeña parte de sus archivos. Los atacantes exigieron un segundo rescate para recuperar el resto de su información. En esa ocasión, el hospital no aceptó el chantaje.

Un equipo profesional de la NASCAR (National Association for Stock Car Auto Racing), el CSLFR, vio como 3 de sus ordenadores fueron atacados por ransomware, cifrando información que el equipo valoraba en más de 3 millones de dólares. En este caso pagaron un rescate de 500 dólares y pudieron recuperar todos los datos.

¿Es recomendable pagar estos rescates?

Cada vez que una víctima paga aumenta la cuenta de resultados de los ciberdelincuentes, por lo que éstos atacarán a más usuarios y nuevos grupos se unirán por lo lucrativos que resultan estos ataques; así que a largo plazo es algo que nos perjudica a todos.

El pago de los rescates no garantiza la total recuperación de la información robada y fomenta la actividad criminal.

No obstante, no deja de ser un tema polémico. Un buen ejemplo son las declaraciones hechas el año pasado por el FBI, donde reconocían que en muchos casos aconsejaban el pago del rescate. Afortunadamente en abril han hecho público un comunicado donde James Trainor, adjunto al director de la Ciber-División del FBI, dejó clara la postura de la agencia:

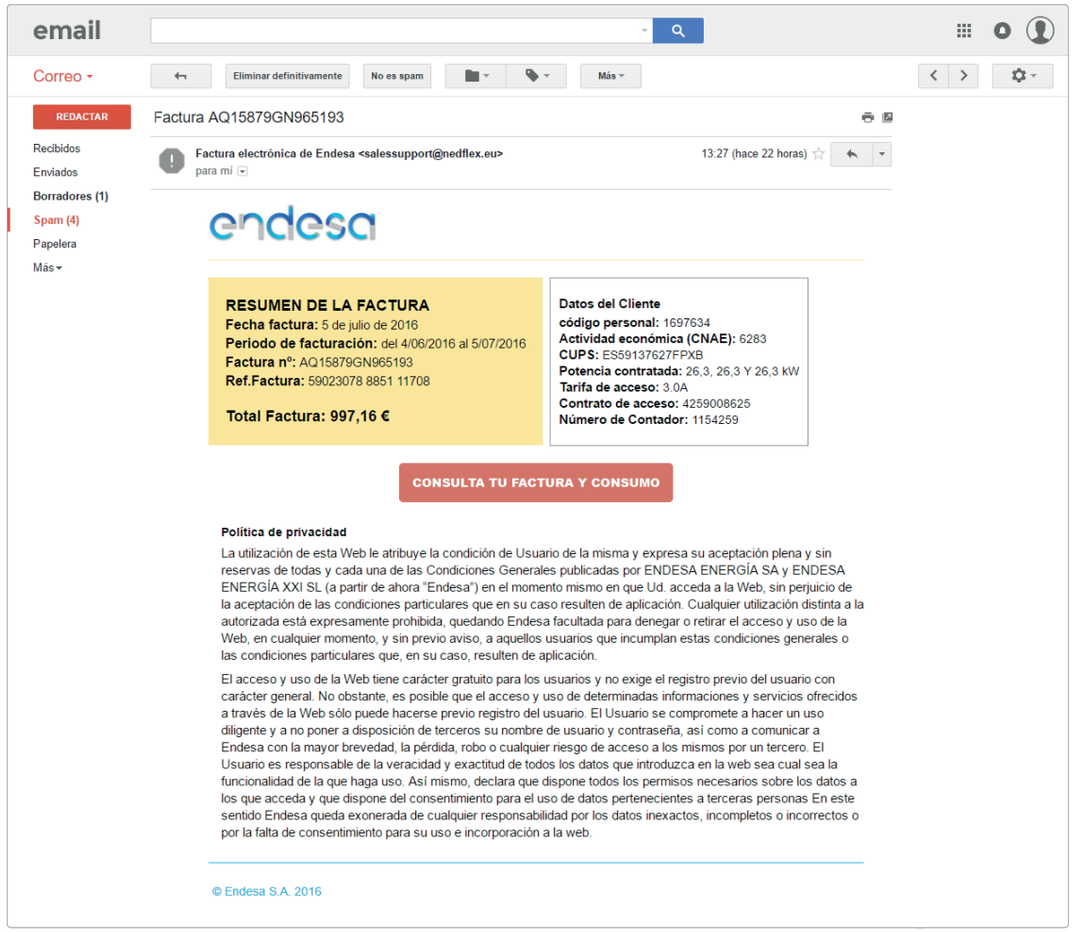
> *"Pagar un rescate no garantiza que una organización recupere sus datos -hemos visto casos donde las organizaciones nunca recibieron una clave de descifrado después de haber pagado. Pagar un rescate no sólo anima a los delincuentes cibernéticos a atacar a más organizaciones, también ofrece un incentivo para que otros criminales se involucren en este tipo de actividad ilegal. Por último, mediante el pago de un rescate, una organización puede fundar ocasionalmente otras actividades ilícitas asociadas con criminales mediante su financiación".*

La evolución del emailing malicioso.

Los ataques no sólo vienen a través de malvertising o páginas web comprometidas. Una gran parte de ellos siguen llegando a través de correo electrónico en forma de facturas falsas o notificaciones de todo tipo.

Uno de estos ataques se produjo en, al menos, dos países europeos, Polonia y España, donde los cibercriminales se hicieron pasar por sendas compañías eléctricas locales.

El mensaje no contenía ningún adjunto, solo mostraba los datos de facturación en texto y un enlace en el que podías consultar el detalle de esa factura. El gancho era un importe excesivamente alto que motivase la indignación del receptor para que, en pleno estado de ofuscación, no se plantease otra cosa que consultar la supuesta factura.



Al pinchar en dicho enlace el usuario era dirigido a una página web que parecía la real de la compañía a la que suplantaban y en la que podía descargarse la factura. Si el cliente la descargaba y ejecutaba, se veía infectado por un ransomware.

¿Qué le dirías al ciberdelincuente que te pone en su punto de mira?

Hemos sido testigos de la evolución de este tipo de malware. Generalmente dan todas las instrucciones detalladas para poder realizar el pago, pero alguna ha ido más allá incorporando **un chat para poder hablar en tiempo real con los extorsionadores** y así poder negociar con ellos los términos de pago, como es el caso de una nueva variante de la familia Jigsaw.

Ahora es posible chatear con los ciberdelincuentes para poder negociar el pago del secuestro de datos.

Uno de los ataques más originales -y peligrosos- de ransomware durante los últimos meses tuvo lugar en Rusia. Su originalidad reside en la forma de propagación. El malware se envía a través de correo electrónico pero no con un ejecutable al uso, de hecho, está programado en un lenguaje propio de un fabricante de software ruso que sólo funciona si tienes instalado dicho software en el ordenador (más de 1 millón de compañías de Rusia y de repúblicas de la antigua Unión Soviética, lo tienen).

Se hace pasar por una actualización y, si se ejecuta, se conecta a la base de datos de ese software en busca de direcciones de email a las que re-enviarse automáticamente. Al mismo tiempo, infecta el ordenador con un ransomware, cifrando ficheros y solicitando el rescate habitual.

Cibercrimen

Estos meses han sido muy intensos en este campo y vamos a repasar algunos de los sucesos más significativos. Como veremos afectan a todo tipo de entidades, desde organizaciones de caridad hasta entidades financieras, pasando por páginas de contenido pornográfico, datos de votantes... hasta la policía se ve afectada por estos casos, nadie está libre de riesgo.

Robo de información.

Team Skeet, una web de distribución de vídeos pornográficos perteneciente a la red de *Paper Street Media*, sufrió un ataque en el que le fueron robados los datos de 237.000 usuarios. Dentro de la información robada no sólo estaban las habituales credenciales y direcciones de correo electrónico, sino que también se encontraban las direcciones físicas de los usuarios. **Los datos están siendo vendidos por Internet a razón de 400$ por credencial**. El precio es sin duda desmesurado (supondría que el total de credenciales valdrían casi 95 millones de dólares), por lo que seguramente los delincuentes optarán por bajar dicha cantidad.

El ransomware y el robo de información a usuarios y empresas son tácticas utilizadas en el cibercrimen.

En Londres, la organización caritativa *National Childbirth Trust* sufrió una brecha de seguridad en la que le robaron datos de 15.085 usuarios, incluyendo sus nombres de usuarios, contraseñas (encriptadas) y direcciones de correo electrónico.

Acer, el fabricante taiwanés, sufrió un ataque a su tienda online en el que robaron datos de 34.500 usuarios. **Lo más grave es que han estado comprometidos durante un año (de mayo de 2015 a abril de 2016) sin haberse dado cuenta hasta ahora**.

En junio un delincuente apodado "*TheDarkOverlord*", puso a la venta en el mercado negro datos de pacientes de 3 entidades Estadounidenses. Había robado datos de más de 650.000 pacientes y pedía por ellos unos 700.000$. Poco después, puso a la venta datos de 9.300.000 clientes de una aseguradora médica por 750 bitcoins (alrededor de medio millón de dólares).

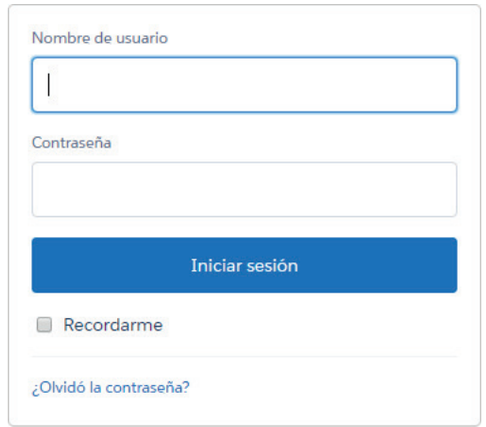
En España, **el grupo Anonymous hizo público un listado con los datos de 5.000 miembros de la Policía Nacional**. La información no fue conseguida de los servidores de la policía, los obtuvieron atacando a la web mupol.es, de la Mutualidad de Previsión Social de la Policía.

Pero si hay un nombre que debe sonarnos en la lucha contra el cibercrimen es el de *Chris Vickery*. Este investigador de seguridad encontró **una base de datos de registro de votantes de México con 93,4 millones de registros**, dentro de un servidor en la nube de Amazon, donde alguien la había dejado. La información incluía dirección postal, identificación oficial, etc. Vickery lo reportó a las autoridades mexicanas y la base de datos fue eliminada. Aún no se sabe cómo llegó allí. Seguramente alguien la robó y utilizó el servidor de Amazon para almacenar temporalmente la información.

Chris Vickery descubrió también otro robo de información, en la página de contactos *beatifulpeople.com* con datos de 1.100.000 usuarios. A pesar de reportarlo a los responsables del sitio web algún delincuente ya se había hecho con la base de datos y la estaba vendiendo en el mercado negro.

Pero, además de ciberdelincuentes, también hemos visto el caso de herramientas comunes que se vuelven en nuestra contra.

Es el caso de la popular herramienta de acceso remoto *TeamViewer*, a través de la cual accedieron a un gran número de ordenadores y robaron a sus usuarios. Debido a la ingente cantidad de casos, en un principio se pensó que alguien había podido entrar en TeamViewer y robar una base de datos con credenciales para llevar a cabo los accesos no autorizados. Pero resultó que los "culpables" eran los propios usuarios por utilizar las mismas credenciales en diferentes servicios.



Esta es una táctica muy utilizada por los delincuentes. **Una vez logran robar una credencial, intentan utilizar la misma combinación de usuario y contraseña en diferentes webs**, porque saben que mucha gente usa las mismas credenciales en la mayoría de sitios. En este caso, cuando los atacantes conseguían acceder al ordenador de la víctima, entraban a sus cuentas de PayPal y se llevaban todo el dinero que encontraban.

TPVs y tarjetas de crédito: en el punto de mira.

Otro de los robos más extendidos y populares hoy en día, son los que afectan a los TPVs (Terminales de Punto de Venta). Estos aparatos no dejan de ser ordenadores susceptibles de ser infectados con malware diseñado para robar la información de las tarjetas de crédito utilizadas en estos terminales.

Como vimos en el ataque al *Hard Rock Hotel & Casino* de Las Vegas, donde sus terminales han estado infectados desde octubre de 2015 hasta marzo de 2016 robando los datos de todas las tarjetas de crédito utilizadas en ese establecimiento.

Estos casos se repiten en todo el mundo. Recientemente una cadena española de hoteles de lujo sufrió un ataque perfecta y exclusivamente diseñado para ellos. Para comunicarse con el exterior y pasar desapercibidos, los atacantes habían registrado el dominio con el nombre de la víctima en un país africano. En este caso el ataque fue detenido a tiempo y no consiguieron llegar a los terminales de punto de venta, frustrando el robo.

Los TPVs de hoteles, restaurantes y comercios son objetivos cada vez más deseables por los hackers.

Pero no sólo los TPVs de establecimientos hoteleros están en el punto de mira, los restaurantes son otro de los grandes focos de robo de datos de tarjetas de crédito. La popular cadena de comida rápida *Wendy's* ha visto como más de 1.000 de sus establecimientos tenían sus Terminales de Punto de Venta infectados con malware que robaba la información de las tarjetas con las que pagaban sus clientes.

En PandaLabs descubrimos un ataque realizado con el malware conocido como PunkeyPOS con el que habían infectado a más de 200 restaurantes en Estados Unidos.

Foto: Imagen génerica de los restaurantes Wendy's, no implica que este local en concreto fuese afectado.

Entidades financieras, el botín más perseguido.

¿Qué robo puede ser más suculento que cualquiera de los que hemos relatado hasta ahora? Lo único que puede resultar más lucrativo es robar directamente a los bancos. Algo muy complejo pero que hemos descubierto que está sucediendo.

Se ha descubierto que el *Banco Central de Bangladesh* sufrió un ataque en el que consiguieron hacer transferencias por valor de 1.000 millones de dólares. Afortunadamente, cuando se dieron cuenta pudieron bloquear gran parte de esas transferencias, aunque los ladrones ya habían conseguido llevarse 81 millones de dólares.

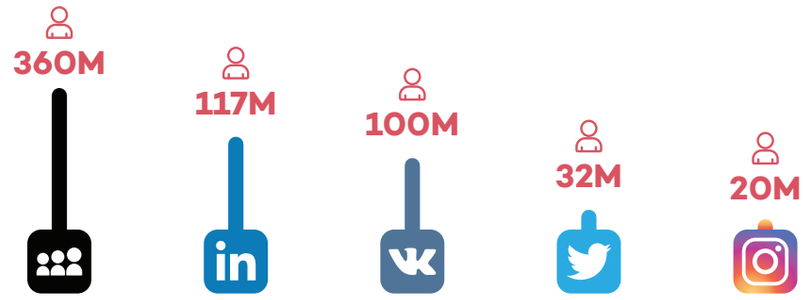
Poco después conocimos 2 casos similares: uno contra un banco de Vietnam y otro contra un banco en Ecuador.

A pesar de que perseguir los ciberdelitos es una tarea muy compleja, acaba dando sus frutos. En abril se supo que *Dmitry Fedotov*, alias "Paunch" y autor del exploit kit Blackhole ha sido condenado en Rusia a 7 años de prisión.

Aleksandr Panin, ruso de 27 años, ha sido también condenado a 9 años y medio de prisión en Estados Unidos. Aleksandr estaba detrás de SpyEye, un conocido troyano bancario.

Redes Sociales

Si algo debemos destacar en lo sucedido durante este trimestre en redes sociales es la cantidad de credenciales robadas que, de una u otra forma, han acabado en malas manos. Hagamos un repaso por las más populares:



Linkedin.

La seguridad de **117 millones de usuarios** de LinkedIn se ha visto vulnerada al publicarse un listado con sus direcciones de correo y los hashes de sus respectivas contraseñas. La brecha de seguridad se produjo en 2012, aunque hasta ahora no se había publicado el listado completo.

La mejor forma de protegerse ante estos ataques es activar el doble factor de autenticación. Así, aunque nuestras credenciales caigan en malas manos, no podrán acceder a nuestra cuenta.

Twitter.

32 millones de usuarios y contraseñas de Twitter fueron puestos a la venta por 10 bitcoins, unos 6.000 $. La red social negó que las cuentas se hubieran obtenido de sus servidores. De hecho, las contraseñas estaban en texto plano y la mayoría pertenecían a usuarios rusos, lo que indica que podrían haber sido obtenidas mediante phishing o troyanos.

VKontakte.

El “Facebook ruso” ha visto cómo se ponían a la venta datos de **100 millones de sus usuarios** con nombres, direcciones de correo, direcciones postales, números de teléfono y contraseñas. Al igual que en el caso de LinkedIn, los datos se han puesto a la venta ahora pero el ataque se produjo hace varios años.

Instagram.

El consultor de seguridad Arne Swinnen encontró un fallo de seguridad en Instagram que permitiría comprometer **20 millones de cuentas** de la red social. Tras reportarlo a la compañía, Facebook (propietaria de Instagram) premió al investigador a través de su programa de recompensas con 5.000 $. Esta no es la mayor recompensa que Facebook ha dado en este periodo, un niño finlandés de 10 años recibió 10.000 $. Jani había encontrado un fallo de seguridad que le permitía borrar comentarios de cualquier usuario de Instagram.

MySpace.

Resulta que, aunque ya prácticamente nadie la utiliza, ha sido atacada. La intrusión se produjo en 2013, aunque hasta mayo de este año no se ha sabido. Han sido sustraídos nombres de usuario, contraseñas y direcciones de correo electrónico, pudiendo alcanzar la cifra de **360 millones de cuentas** afectadas. Aunque un usuario lleve años sin utilizar MySpace, si se acostumbra a reutilizar contraseñas, es momento de cambiar este hábito y de activar el doble factor de autenticación.

Sino que se lo digan a Mark Zuckerberg, fundador de Facebook, que vio cómo sus cuentas en Twitter, Pinterest e Instagram fueron hackeadas por unos bromistas autodenominados *OurMine*. Al parecer la contraseña utilizada en LinkedIn, era la misma para todas sus otras cuentas.

Activar el doble factor de autentificación, no reutilizar las contraseñas en diferentes sitios y establecer claves complejas, son consejos de ciberseguridad a seguir.

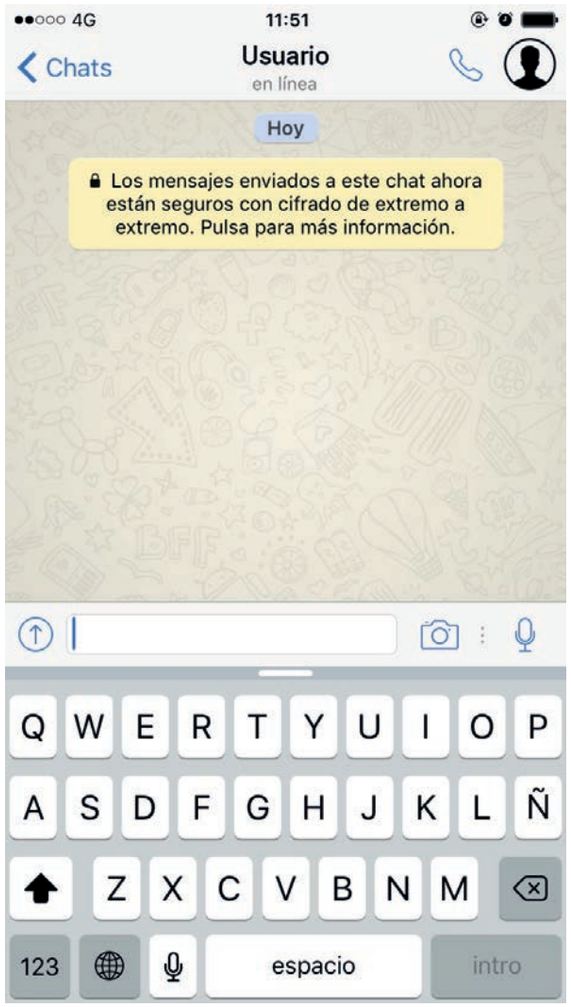
Además es importante que las contraseñas sean relativamente complejas. Un estudio de la compañía *Kore Logic,* realizado sobre los 117 millones de contraseñas, demuestra que la mayoría de usuarios opta por contraseñas extremadamente simples. La siguiente muestra las más utilizadas:

Nº USUARIOS	CONTRASEÑA
1.135.936	123456
207.488	linkedin
188.380	password
149.916	123456789
95.854	12345678
85.515	111111
75.780	1234567
51.969	654321
51.870	qwerty
51.535	sunshine

Hay que aplaudir la iniciativa de *Microsoft*, al respecto. Ha prohibido el uso de contraseñas demasiado utilizadas y que se encuentran en listados de este tipo. Esperemos sea seguida por otros proveedores de servicios.

WhatsApp protagoniza otro ejemplo de buena práctica en seguridad. La aplicación de mensajería más popular del planeta y su actual propietario, Facebook, han decidido aumentar la privacidad cifrando por defecto todos los mensajes que se envían a través de la aplicación.

De hecho, está previsto que Facebook Messenger incorpore también esta funcionalidad en los próximos meses.



Móviles

Google parece que ha mejorado el parcheo de agujeros de seguridad en su sistema operativo con actualizaciones mensuales que corrigen todas las nuevas vulnerabilidades que van encontrando.

De hecho, en mayo corrigieron 25 vulnerabilidades (algunas muy graves que permiten ejecución remota de código), aunque ninguna de ellas ha sido vista utilizada por atacantes. Esta es una de las actualizaciones más grandes hasta la fecha que ha llevado a cabo el gigante tecnológico.

A pesar de los avances introducidos, el ecosistema Android se tambalea en cuestiones de seguridad.

Sin embargo, como ya hemos comentado alguna vez, uno de los mayores problemas de Android es la lentitud de las actualizaciones que, en gran parte, dependen del fabricante del hardware de cada dispositivo. Si bien aquellos productos controlados directamente por Google (teléfonos y tablets Nexus) reciben estas actualizaciones de forma inmediata, muchos usuarios tendrán que esperar meses para recibir estas actualizaciones y, en algunos casos, no las recibirán nunca.

Esto hace que cada vez haya más dispositivos vulnerables a problemas de seguridad conocidos, lo que tarde o temprano **llevará a una situación en la que el ecosistema Android sea realmente peligroso** y los ataques aumenten de forma exponencial.

Internet of Things

Últimamente en esta sección siempre aparece alguna noticia sobre vehículos hackeados y en esta ocasión la víctima ha sido el Mitsubisi Outlander. Este coche híbrido tiene su propia red WiFi, de tal forma que con la app del fabricante puedes conectarte y modificar la temperatura, cambiar el programa de carga de batería del motor eléctrico, etc.

El investigador de seguridad Ken Munro fue capaz de averiguar la clave de la red WiFi mediante un ataque de fuerza bruta; una vez dentro de la red podía sabotear el coche, por ejemplo descargando completamente la batería del motor eléctrico. Pero lo más grave es que de esta forma puede desactivar la alarma de forma remota, algo de lo que muchos delincuentes pueden aprovecharse.

La consultora Gartner ha publicado un interesante informe sobre la seguridad en IoT. En él vaticina que en el **25% de los ataques que sufrirán las empresas en 2020 estarán implicados dispositivos IoT**. Se espera que en 2016 haya 6.400 millones de estos dispositivos conectados (un 30% más que en 2015) y para 2018 calculan que llegará a los 11.400 millones.

El gasto en seguridad IoT irá aumentando paulatinamente, aunque viendo las predicciones de ataques es probable que no sea suficiente:

Gasto Mundial Previsto en Seguridad IoT
(Millions of Dollars)

2014	2015	2016	2017	2018
231.86	281.54	348.32	433.95	547.20

Fuente: Gartner (Abril 2016)

Ciberguerra

El año pasado contamos cómo la empresa *Hacking Team,* conocida por vender malware a gobiernos y fuerzas de seguridad de todo el mundo, había sido hackeada. Ahora vuelve a ser noticia por haber perdido su licencia de exportación, según publicó el periódico "Il Fatto Quotidiano". Prácticamente se les inabilita a vendar sus programas fuera de la Unión Europea, al menos sin tener que pasar por farragosos procedimientos burocráticos en cada ocasión.

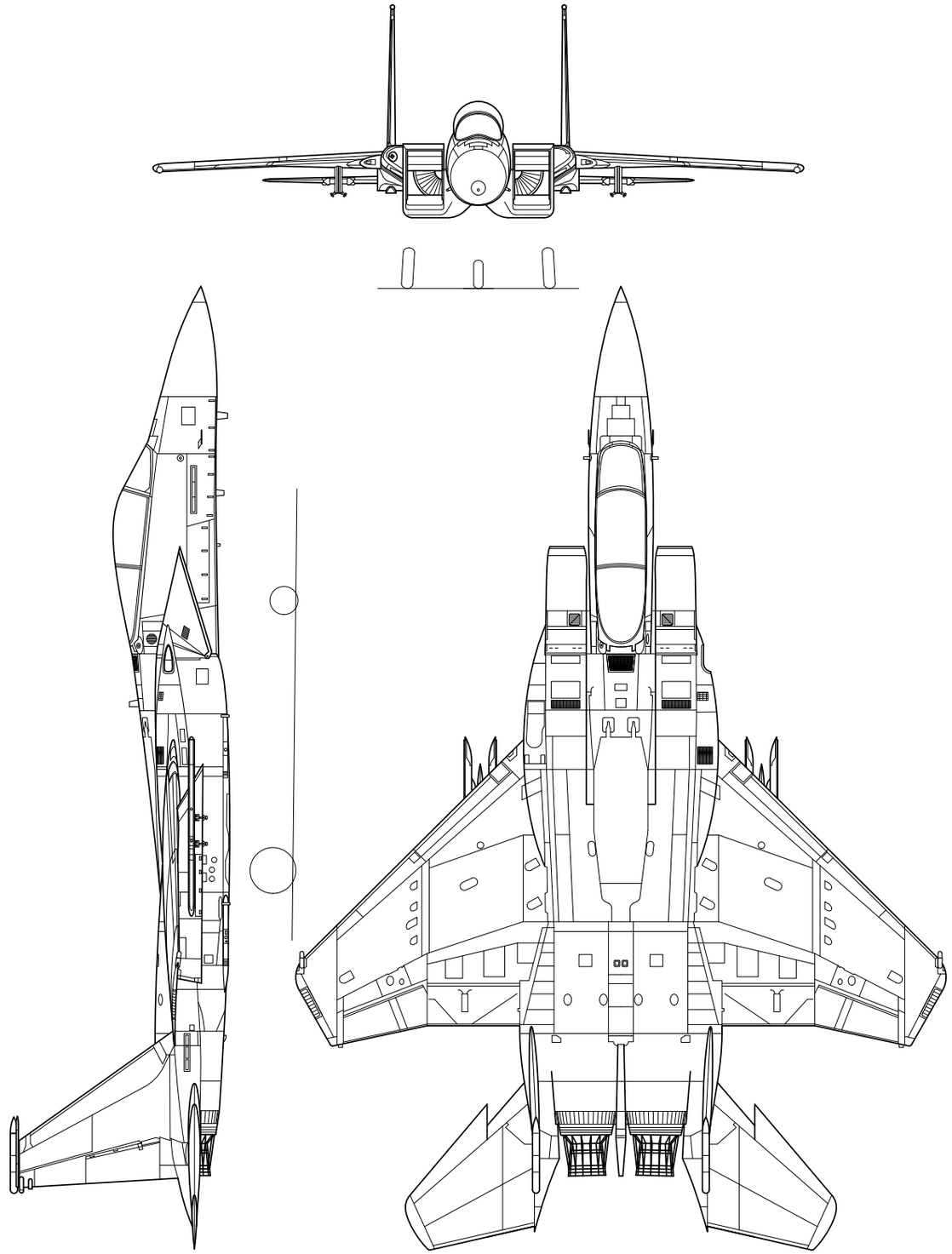
En la mayoría de ocasiones, cuando hablamos de ciberguerra, hablamos de ataques supuestamente patrocinados por diferentes gobiernos, aunque es raro encontrar pruebas que garanticen la autoría del ataque.

Sin embargo, Estados Unidos ha pasado a la ofensiva y reconoce que está lanzando ciberataques contra objetivos del Daesh. Robert Work, adjunto al Secretario de Defensa de EEUU lo dejó claro en declaraciones a la CNN:

> *"Estamos lanzando bombas cibernéticas. Nunca hemos hecho eso antes. Al igual que tenemos una campaña aérea, quiero tener una campaña cibernética. Quiero utilizar todas las capacidades espaciales que tengo"*.

En junio, la policía de Corea del Sur hizo público un ataque proveniente de Corea del Norte. Al parecer el ataque comenzó hace más de un año, teniendo como primer objetivo 140.000 ordenadores pertenecientes a organizaciones y agencias gubernamentales, así como a contratistas de defensa. Pero hasta febrero de este año no se ha descubierto el ataque, de acuerdo con las declaraciones de la policía, **habrían robado más de 42.000 documentos, de los cuales un 95% estaban relacionados con defensa**, como por ejemplo los planos y especificaciones de las alas del caza norteamericano F15.

Por su parte, el Comité Nacional del Partido Demócrata en EEUU ha reconocido que ha sido comprometido al menos desde hace un año. Creen que los atacantes pertenecen a la inteligencia rusa y han tenido acceso a correos electrónicos, chats y documentos de investigación de todo tipo. **Todos los ordenadores del departamento de investigación habían sido accedidos y algunos archivos, robados**.



3. CONCLUSIÓN

3 Conclusión

No dejan de aumentar los ataques que roban dinero e información. En muchas ocasiones los usuarios sufren el robo indirecto de sus cuentas e identidades, cuando sus datos se encontraban almacenados en bases de datos custodiadas por empresas que han sido visto comprometidas.

El hecho de que la mayoría de usuarios reutiliza las contraseñas agrava la situación, facilitando aun más los robos. Podría ser solucionado por los propios usuarios de forma relativamente sencilla, por ejemplo, activando el doble factor de autenticación que la mayoría de sitios ofrecen. Otra medida sería que los servicios activasen por defecto estas medidas. Pero es menos probable que ocurra porque prima la usabilidad sobre la seguridad.

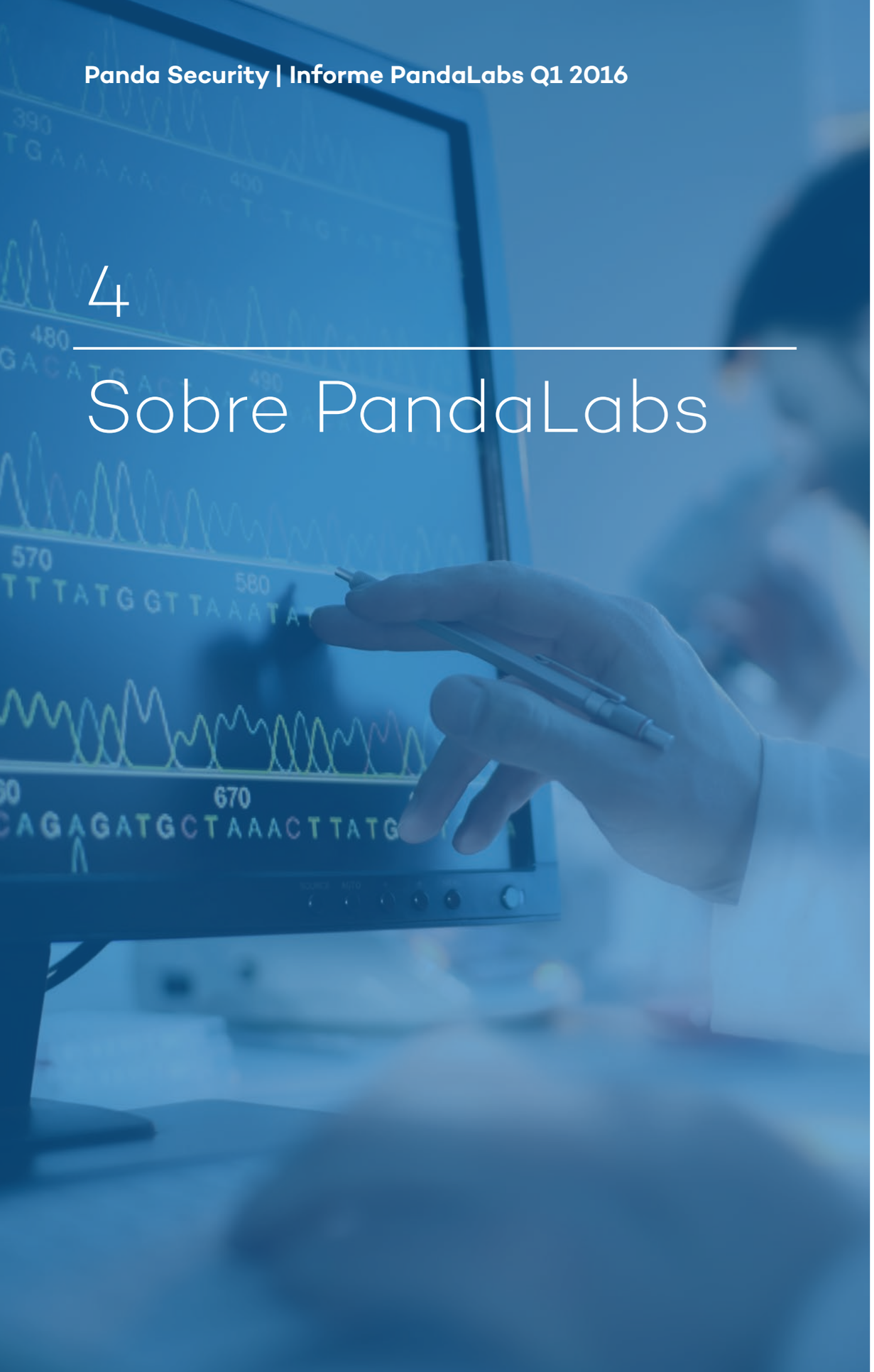
Los ataques de ransomware están creciendo en sofisticación y los delincuentes están consiguiendo ingentes beneficios. En los próximos meses comprobaremos cómo seguirán en auge.

Otro panorama preocupante es el del robo de tarjetas de crédito en TPVs. Muchos de los establecimientos afectados son pequeñas empresas (restaurantes, bares, comercios de todo tipo) que no cuentan con personal especializado en seguridad. Teniendo en cuenta lo fácil que es vender esta información robada en el “mercado negro” y lo fácil que resulta comprometer estos TPVs a través de internet de forma anónima, es lógico que estos terminales sean objetivo cada vez más deseables para los ciberdelincuentes.

Nos vemos dentro de 3 meses para analizar lo sucedido durante el 3er trimestre de 2016. Mientras tanto, desde PandaLabs os mantendremos informados de todas las novedades del mundo de la seguridad a través de nuestro blog:

http://www.pandasecurity.com/spain/mediacenter/

4. SOBRE PANDALABS



4

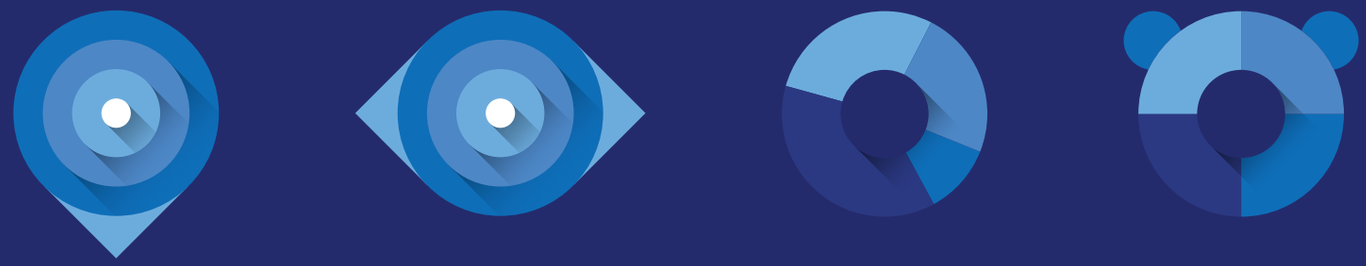
Sobre PandaLabs

PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- Desde PandaLabs se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.
- PandaLabs se encarga asimismo de llevar a cabo el análisis detallado de todos los tipos de malware, con la finalidad de mejorar la protección ofrecida a los clientes de Panda Security, así como para informar al público en general.

PandaLabs mantiene un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad.

El objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.



panda

pandalabs