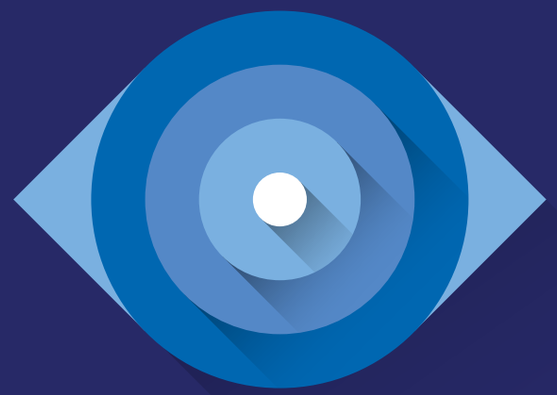
INFORME PANDALABS Q3 2016



panda

pandalabs

1. Introducción

2. El trimestre de un vistazo
   - Ransomware
   - Cibercrimen
   - Móviles
   - IoT
   - Ciberguerra

3. Conclusión

4. Sobre PandaLabs

1. INTRODUCCIÓN

1 Introducción

El cibercrimen no se detiene y el ingenio de los ciberdelincuentes despunta un trimestre más, utilizando innovadoras tecnologías y nuevas herramientas para su difusión. En el tercer trimestre de 2016 PandaLabs, el laboratorio de Panda Security ha capturado **más de 18 millones de nuevas muestras de malware, con una media de 200.000 al día**, manteniendo la tónica del segundo trimestre.

Los troyanos siguen liderando las estadísticas y son el tipo de malware más popular, teniendo al **ransomware como protagonista** destacado dentro de esta tipología.

Estos ataques continúan evolucionando y se está pasando de rescates de unos pocos cientos de euros a millones.

Los Terminales de Punto de Venta son objetivos cada vez más deseables para los ciberdelincuentes. Echamos la vista atrás y hablamos de la multitud de ataques que han tenido como objetivo los TPVs de restaurantes y negocios de todo tipo.

Este trimestre también destaca la gran **cantidad de ataques DDoS (Distributed Denial of Service) de gran magnitud** que se están produciendo y que además, en muchos de los casos, están ligados a redes de bots cuyos integrantes no son ordenadores, sino dispositivos inteligentes como cámaras IP.

Dentro del Internet de las Cosas (o el denominado IoT) profundizaremos en los últimos **ataques a vehículos conectados** perjudicando a marcas como Tesla, de la cual uno de sus modelos ha sido “víctima” de unos investigadores que han demostrado cómo podían controlar el coche de forma remota sin necesidad de tocarlo.

En el terreno móvil analizaremos algunos casos de ataques de Android y veremos la oleada de ataques de ransomware que están sufriendo los dispositivos basados en iOS.

2. EL TRIMESTRE DE UN VISTAZO

2

El trimestre de un vistazo

Ransomware

El negocio del ransomware aporta pingües beneficios, y según va madurando se va especializando más. En julio hemos visto cómo los creadores de los ransomware Petya y Mischa han decidido especializarse en la parte del desarrollo del malware y sus correspondientes plataformas de pago, dejando en manos de terceros la distribución del mismo, en lo que podría denominarse **Ransom as a Service (RaaS)**.

Básicamente ellos hacen su parte y son los distribuidores los que tienen que encargarse de la infección de las víctimas. Como en el mundo legal, el beneficio de los distribuidores es un porcentaje del dinero obtenido, y cuantas más ventas consigan mayor será el porcentaje que obtengan. Comienzan por un 25%, pero pueden llegar a quedarse un 85% si consiguen **rescates por valor de más de 125 bitcoins** (unos 75.000 dólares) a la semana.

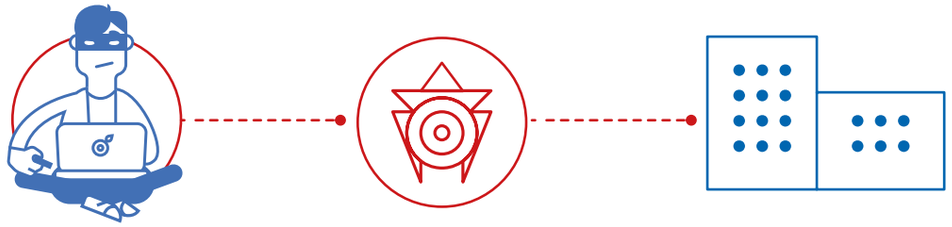
Desde PandaLabs realizamos un seguimiento muy cercano al ransomware y a su evolución, por lo que quincenalmente publicamos una serie de artículos titulados “Historias de Ransomware” donde, a través del Media Center de Panda Security, compartimos las últimas novedades y curiosidades sobre estos ataques.

Analizamos cómo (ab)usan los atacantes PowerShell, que viene por defecto con Windows 10, para lanzar ataques de ransomware sin siquiera necesitar descargarse binarios desde internet. Estos ataques además se ejecutan desde macros de documentos de Word enviados por correo electrónico, lo que se traduce en una auténtica pesadilla para las empresas de seguridad que principalmente ofrecen defensa perimetral, ya que a no ser que tengan presencia en el ordenador que está siendo atacado no pueden hacer nada.

Los ciberdelincuentes buscan continuamente nuevas medidas para evadir la detección de productos de seguridad, y en el caso de la familia Locky lo hemos visto claramente, al implementar un modo “offline” que le permite cifrar los ficheros cuando alguna protección impide que se comunique con el servidor del que obtiene la clave utilizada para cifrar.

A las tradicionales técnicas de infección a través de exploits y de spam, surgen otras muy efectivas dirigidas a empresas.

Lo vimos en septiembre, cuando unos atacantes lograron introducir el ransomware Crysis en el servidor de una empresa francesa.



Tras investigar lo sucedido, el servidor tenía el servicio Remote Desktop Protocol conectado a Internet y los atacantes habían estado intentando entrar con un ataque de fuerza bruta durante casi 4 meses. Tras más de 100.000 intentos consiguieron averiguar las credenciales.

Cibercrimen

Es muy complejo cuantificar la ciberdelincuencia. Los profesionales de la ciberseguridad que combaten día a día estas amenazas saben que es algo masivo y que no deja de crecer.

¿Realmente es tan grande el peligro?

Hay quien puede pensar que las grandes empresas de seguridad, como Panda, están especialmente interesadas en hacer creer que este es un gran problema para beneficiar su propio negocio. No obstante, los datos hablan por sí solos reflejando una realidad que, en ocasiones, supera a la ficción. Poco a poco van apareciendo estadísticas oficiales que nos ayudan a hacernos una idea real de cuál es la situación.

La National Crime Agency del Reino Unido afirma que más del 50% de los delitos cometidos en el país son cibercrimen.

El 2 de agosto se produjo uno de los mayores robos de bitcoin de la historia. Bitfinex, empresa de comercio y cambio de cripto-monedas fue comprometida y robaron el equivalente a 60 millones de dólares en bitcoins. Este dinero pertenecía a clientes que tenían depositados sus bitcoins en este “banco”. Aún no se tienen pruebas de quién ha llevado a cabo el atraco y la empresa no ha ofrecido información de cómo se ha producido ya que aún están las fuerzas del orden llevando a cabo la investigación del caso.

En septiembre el afamado periodista especializado en seguridad Brian Krebs destapó vDOS, una “empresa” que

ofrecía servicios de ataques DDoS. Poco después sus responsables, quienes en 2 años habían lanzado 150.000 ataques y obtenido un beneficio de 618.000$, fueron detenidos. Al poco tiempo, la página de Krebs comenzó a recibir un ataque DDoS masivo que finalmente llevó a dejar su página offline durante una semana. Finalmente Google, a través de su Project Shield, protegió su página y volvió a estar operativa.

Brian publicó un interesantísimo artículo, The Democratization of Censorship, detallando el suceso y las consecuencias que este tipo de ataques pueden tener.

Los servidores Battle.net de Blizzard han sido atacados por el grupo denominado PoodleCorp, afectando a los diferentes juegos online que tiene la compañía (World of Warcraft, Overwatch, Diablo 3, etc.). De hecho durante este trimestre han tenido lugar una gran cantidad de ataques de este estilo, como se detalla más adelante en la subsección IoT, ya que gran parte de los mismos están siendo lanzados desde redes de bots compuestas de dispositivos inteligentes, como cámaras IP, routers, etc.

Durante estos tres últimos meses se han producido muchos robos de datos que han afectado a millones de usuarios de todo el mundo. En julio los foros de Ubuntu- sistema operativo basado en GNU/Linux y que se distribuye como software libre- fueron hackeados siendo el botín de los ciberdelincuentes la dirección de correo, nombre de usuario y dirección IP de 2 millones de personas. Otros foros que estaban en el punto de mira de los Black Hat eran los vinculados al popular juego para dispositivos móviles **Clash of Kings**, viéndose del mismo modo comprometidos. En esta ocasión, **los atacantes se hicieron con los datos personales de 1.600.000 usuarios.**

El robo de información sensible, como credenciales y direcciones de correo electrónico de 1,9 millones de usuarios, fue el desenlace del hackeo a los foros del juego de Valve “Dota 2”. El mismo atacante robó 9 millones de códigos de juegos de Steam tras comprometer el sitio DLH.net.

Los ciberdelincuentes han encontrado un importante filón en estos sites de juegos.

A estos ataques hay que sumarle el acontecido contra GTAGaming.com, al que le robaron datos de 200.000 usuarios, o el de www.minecraftworldmap.com donde el atacante publicó la información de 71.000 de sus usuarios.

Otro ataque controvertido es el acaecido en el **sitio web pornográfico Brazzers,** el cual sufrió una brecha de seguridad en la que le robaron datos de **800.000 usuarios**. Por otro lado, otro ataque sonado por su proporción y alcance, ha sido el sufrido por el servicio ruso de mensajería instantánea QIP.ru en el que le robaron datos de más de 33 millones de usuarios.

Tampoco Dropbox escapa en los últimos meses de las garras del cibercrimen. El conocido servicio de compartición de ficheros sufrió un ataque en 2012 y se ha destapado ahora. El resultado final: la sustracción de un total de datos

pertenecientes a 68 millones de usuarios. Pero si de un robo debemos hablar, es el de **Yahoo**. Aunque tuvo lugar en 2014, hasta ahora no se ha conocido. Un total de **500 millones de cuentas han sido comprometidas, convirtiéndose en el mayor robo de la historia**.

Los TPVs: más en el punto de mira que nunca.

PandaLabs descubrió un ataque en el que **200 establecimientos de EEUU,** principalmente restaurantes, habían sido comprometidos y los datos de las tarjetas de crédito y débito de sus clientes habían sido robadas utilizando un malware conocido como **PunkeyPOS**.

La popular cadena de comida rápida Wendy's sufrió un ataque similar, con Terminales de Punto de Venta (TPVs) infectados con otra variante de PunkeyPOS que afectó a más de 1.000 de sus establecimientos.

Otro ataque similar fue también descubierto por nuestro laboratorio. De nuevo las víctimas eran restaurantes de EEUU, un total **300 establecimientos** cuyos TPVs habían sido infectados con el malware **PosCardStealer**.

Otra de las infraestructuras críticas que repasamos en cada informe son las cadenas hoteleras.

En este trimestre, la empresa HEI Hotels ha sufrido un ataque en diferentes hoteles de su propiedad, donde los atacantes han utilizado malware para robar datos de tarjetas de crédito en sus TPVs.

Entre los hoteles afectados hay establecimientos de Sheraton, Westin, Hyatt y Marriott.

Pero la ambición de los cibercriminales va más allá de los Terminales de Punto de Venta. No sólo son atacados estos dispositivos ya que en julio fuimos testigos de cómo decenas de cajeros en Taiwán pertenecientes al **First Bank fueron saqueados.** De forma coordinada los atacantes estaban esperando al lado de cada cajero, de los cuales **sacaron en total el equivalente a 2 millones de dólares**.

Por lo que se sabe hasta el momento, los asaltantes habían conseguido instalar malware en dichos cajeros (seguramente tras comprometer la propia red interna del banco) y dando una orden remota consiguieron extraer el dinero sin tener que tocar los cajeros, tal y como han demostrados los vídeos de las cámaras de seguridad.

Las entidades financieras son un jugoso premio en el que los bandidos pueden conseguir cientos de millones.

En agosto SWIFT emitió un comunicado en el que dijo que más ataques como el del Banco Central de Bangladesh están

teniendo lugar, sin especificar ni cuantías ni el número de bancos atacados. Sí mencionan que se trata de entidades cuyas medidas de seguridad no eran las más adecuadas.

Programas de recompensas para aquellos que descubran vulnerabilidades

El gigante tecnológico **Apple** ha sido una de las últimas empresas en comenzar un programa de recompensas en el que ofrece hasta **200.000 dólares** a aquellos investigadores que descubran vulnerabilidades en sus productos. Es cierto que resultaba bastante sorprendente que hasta ahora no tuvieran un programa de este tipo en marcha cuando todas las grandes compañía del sector lo tienen desde hace años.

De hecho hay muchos tipos de organizaciones que tienen programas de recompensas. Normalmente suelen ofrecer premios en metálico, aunque hay algunas que lo prefieren hacer en especie. Es el caso de **United Airlines**, por ejemplo, que en agosto se supo que premió al investigador de seguridad con **un millón de millas** de su programa de fidelidad al haber descubierto 20 agujeros de seguridad en su software.

En julio se hizo público que 5 miembros de una banda especializada en lavado de dinero proveniente de ciberdelitos habían sido detenidos en Londres, aunque todos ellos eran de nacionalidad rusa. Sus líderes eran Aslan Abazov, de 30 años, y Aslan Gergov, de 29. El primero ha sido condenado a 7 años y medio de prisión, y el segundo a 7 años y 3 meses.

Edward Majerczyk se ha declarado culpable del robo de fotografías pertenecientes a celebridades, tras llegar a un acuerdo y acceder a una condena de 9 meses de prisión (inicialmente la fiscalía solicitó 5 años). El acusado accedió a las cuentas de iCloud de sus víctimas tras lanzar un ataque de phishing en el que consiguió sus credenciales.

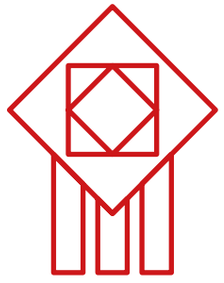
Otros se decantan por los personajes públicos. Es el caso de Marcel Lehel Lazar, rumano de 44 años, el cual fue sentenciado a 52 meses de prisión por hackear a personalidades de relevancia. Entre sus 100 víctimas se encuentran Hillary Clinton, George Bush (padre e hijo), Colin Powell, Nicole Kidman, Robert Redford...

Móviles

Android está en el punto de mira de todos los ciberdelincuentes interesados en los móviles, ya que es el sistema operativo con mayor cuota de mercado y permite además instalar programas desde fuera de la tienda oficial. Es por ello que Google está reforzando la seguridad y en Nougat, la versión 7 de Android, está activando diferentes medidas defensivas provenientes de las últimas versiones del kernel de Linux.

Aun así, en muchas ocasiones ni siquiera añadir estas protecciones al sistema operativo es suficiente. La compañía de seguridad **Checkpoint ha descubierto 4 problemas de seguridad que pueden poner en riesgo a los 900 millones de dispositivos Android que utilizan procesadores Qualcomm**, fabricantes de los conocidos SnapDragon que llevan la mayoría de teléfonos móviles y tablets Android.

Gugi, un troyano de Android, ha conseguido traspasar las barreras de seguridad que tiene Android 6 para robar credenciales bancarias de otras aplicaciones instaladas.



Para ello, cuando se están utilizando las aplicaciones legítimas, Gugi superpone una pantalla pidiendo los datos que serán enviados directamente a los delincuentes sin el conocimiento de sus víctimas.

Últimamente **están proliferando los ataques de ransomware en iPhones y iPads**. Pero al contrario que sus homólogos de Windows, en esta ocasión el ciberdelincuente no utiliza malware y usa su ingenio un paso por delante.

Para llevar a cabo el ataque la estrategia utilizada es utilizar el AppleID de la víctima y su contraseña (probablemente obtenida o bien mediante phishing o por reutilizar contraseñas en diferentes sitios web) y desde la aplicación "Buscar mi iPhone" activa el modo Perdido añadiendo un mensaje que pide un rescate en bitcoins a cambio de dar la contraseña necesaria para desbloquearlo.

En agosto Apple publicó de forma urgente la **versión 9.3.5 de iOS**, su sistema operativo para dispositivos móviles. Esta versión **soluciona tres vulnerabilidades 0-day empleadas por un software espía conocido como Pegasus**, desarrollado por la organización israelí NSO Group, una empresa con productos similares a los ofrecidos por Hacking Team.

Internet of Things

Durante la conferencia DefCon celebrada en agosto en Las Vegas, el investigador **Andrew Tierney** mostró una prueba de concepto que él mismo había elaborado para secuestrar un termostato. T**ras tomar el control del termostato (introduciendo una tarjeta SD en el mismo), subía la temperatura hasta los 99 grados Fahrenheit y solicitaba un PIN para poder desactivarlo**. El termostato se conectaba a un canal IRC, dando la dirección MAC como identificador de cada dispositivo comprometido, solicitando un bitcoin para poder obtener el PIN –que cambiaba cada 30 segundos. Si bien sólo se trataba de una prueba de concepto y necesitaba el acceso físico al dispositivo, **nos sirve para hacernos una idea de los ataques a los que nos vamos a tener que enfrentar en los próximos años** ante la cantidad de aparatos domésticos que van a estar conectados en red en nuestros hogares.

De todos modos no hace falta esperar, ya a día de hoy tenemos millones de dispositivos pertenecientes al Internet de las Cosas que están comprometidos. La red de bots LizardStressed, creada por el grupo Lizzard Squad (que lanzó en su día un demoledor ataque DDoS contra los servicios de juego online de Playstation y Xbox) está principalmente compuesta por este tipo de dispositivos.

Según Arbor Networks la mayoría de ellos son cámaras IP, y la forma de comprometerlos es simplemente probando combinaciones de usuarios y contraseñas. Como la mayoría de usuarios no cambian las credenciales que vienen de fábrica, conseguir acceso a ellos es en muchos casos algo trivial, y ya han conseguido lanzar ataques de hasta 400 Gbps. Otro de los dispositivos favoritos para llevar este tipo

de ataques son los routers, que desde hace tiempo se vienen utilizando para lanzar este mismo tipo de ataques.

A finales de septiembre, la empresa de hosting francesa **OVH comenzó a recibir ataques DDoS masivos, el mayor de ellos llegó a 799 Gbps, el mayor registrado hasta la fecha**. En combinación han llegado a recibir ataques con un tráfico que supera 1 Tbps. Por los datos que OVH ha facilitado el ataque se ha lanzado desde 152.000 dispositivos, la mayoría de ellos perteneciente a IoT (cámaras IP, grabadores de video, etc.).

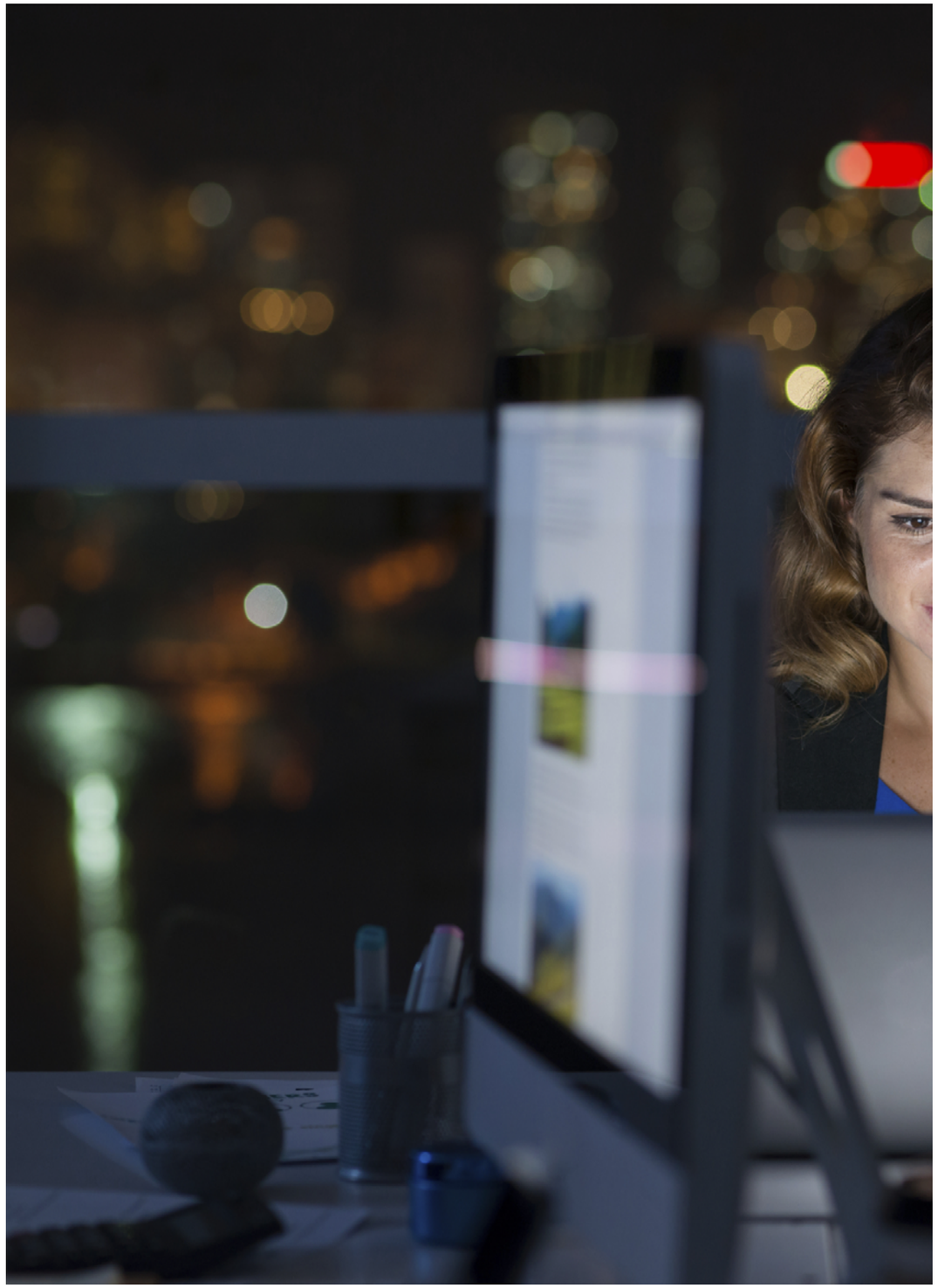
En el terreno automovilístico, investigadores de la universidad de **Birmingham** mostraron cómo habían conseguido **comprometer el sistema de apertura de puertas de todos los vehículos vendidos por el Grupo Volkswagen** en los últimos 20 años. A través de ingeniería inversa consiguieron hacerse con la clave criptográfica que utilizan todos los coches del grupo. Una vez obtenida, lo "único" que necesitan hacer es acercarse a menos de 300 metros de cualquier de los vehículos afectados y mediante un dispositivo de radia esperar a que se accione el mando a distancia, momento en el que pueden interceptar otra clave, única para cada coche. Una vez obtenida dicha información ya pueden clonar el control remoto que permite la apertura y cierre.

Los investigadores **Charlie Miller y Chris Valasek**, que el año pasado **demostraron como hackear de forma remota un Jeep Cherokee**, han ido más allá este año demostrando como podían accionar a su antojo el acelerador, el freno, y hasta el volante estando el coche en marcha.

Al contrario que en el anterior caso, para llegar a este tipo de control necesitan tener un ordenador conectado directamente al coche. En cualquier caso este es un importante toque de atención, ya que podríamos estar asistiendo a formas en que se puede atentar contra la vida de una persona a través de la manipulación del vehículo en el que está montado.

En septiembre, investigadores chinos de Keen Security Labs demostraron cómo comprometer un coche Tesla de forma remota, tanto en modo de aparcamiento como en modo de

conducción. En el vídeo mostrado se podía observar cómo sin tocar el coche lo podían abrir y cerrar, abrir el maletero en marcha e incluso accionar el freno estando a kilómetros de distancia. Los investigadores habían mandado con antelación la información al fabricante, quien publicó una nueva versión de su firmware que corregía los problemas de seguridad detectados.



Ciberguerra

En plena campaña electoral a la presidencia de Estados Unidos, uno de los casos más relevantes que han tenido lugar estos meses es el descubrimiento de un **ataque al DNC (Democratic National Committee) en el que les sustrajeron todo tipo de información, que además se ha ido haciendo pública.** Si bien atribuir con certeza quién está detrás de un ataque es muy complejo y en muchas ocasiones imposible, parece que en este caso está claro que los atacantes eran de origen ruso, y han saltado acusaciones diciendo que el gobierno de dicho país estaba detrás, queriendo perjudicar la campaña de la candidata demócrata. Aparentemente había 2 grupos diferentes de atacantes (ambos rusos) y al menos uno de ellos **filtró 20.000 correos electrónicos a WikiLeaks**.

Siguiendo con la temática electoral, el **FBI ha lanzado una alerta ya que han detectado ataques a 2 webs electorales**, y al menos en uno de ellos los atacantes –que identifican como extranjeros- habrían podido llevarse información del registro de votantes.

Los gobiernos tienen más claro que nunca que deben tomar medidas para protegerse, de hecho Obama hizo unas declaraciones recientemente donde reconocía que quedaba mucho trabajo por hacer tras recordar que en el pasado han penetrado en la red de la Casa Blanca. En septiembre nombró al **primer CISO (Chief Information Security Officer) de la historia del país**.

Este pasado mes de agosto, un grupo autodenominado **"The Shadow Brokers" anunció que habían hackeado a la NSA y publicó algunas de las "ciber-armas"** con las que se había hecho, prometiendo vender el resto a aquel que les ofreciera más dinero. No se sabe quién puede estar detrás, aunque se ha especulado que Rusia es uno de los candidatos más probables. En cualquier caso, parece ser que sí se trata de herramientas utilizadas por la NSA para lanzar sus ataques.

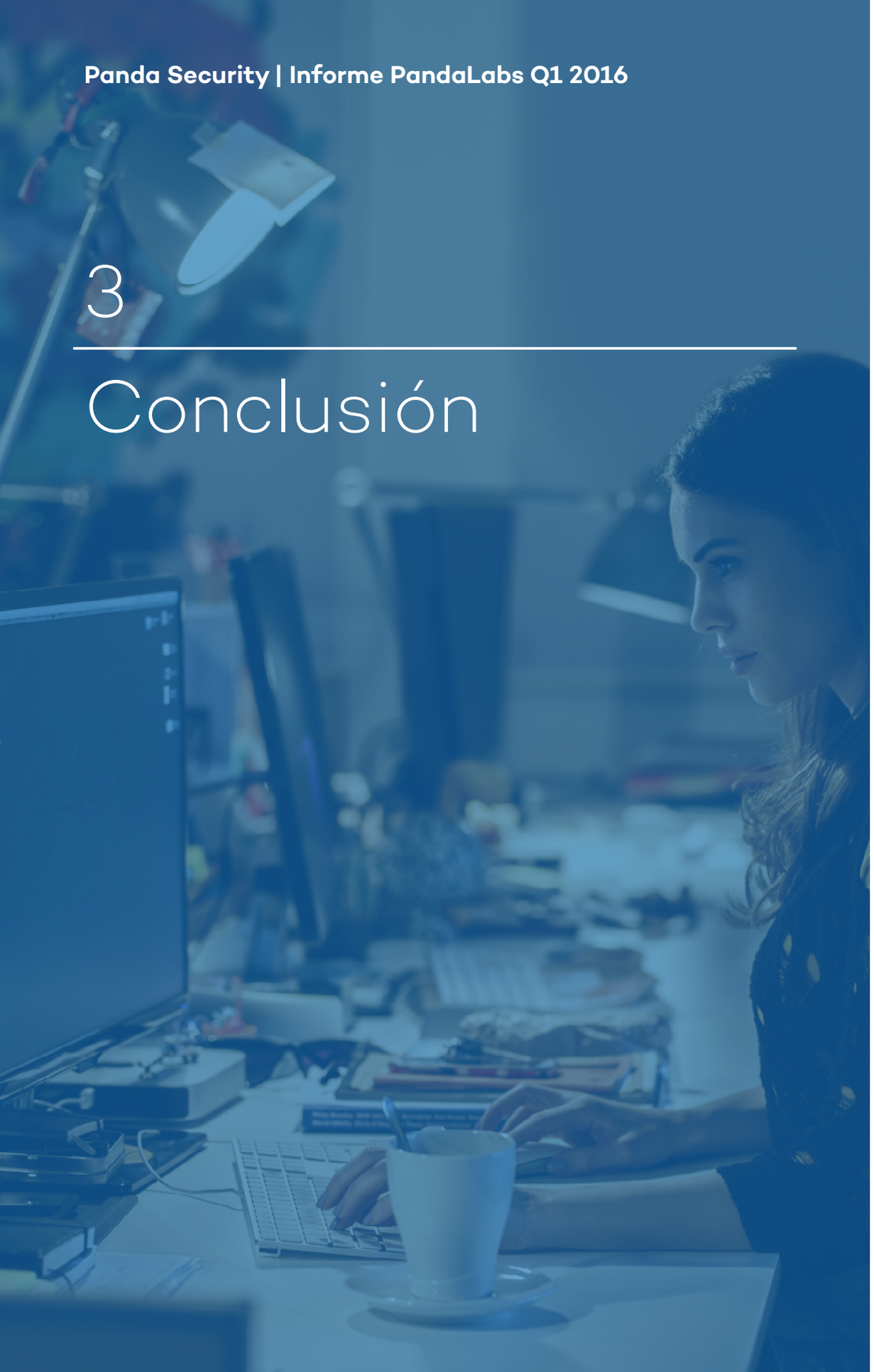
En muchas ocasiones hablamos de ataques perpetrados o patrocinados por gobiernos de diferentes países, pero la verdad es que, al igual que con el cibercrimen, es prácticamente imposible cuantificarlos.

Sin embargo, **Google** nos sorprendió cuando uno de sus altos ejecutivos, Diane Greene dijo que cuando detectaban un ataque de este tipo lo notificaban a sus clientes y que actualmente llevaban a cabo **4.000 notificaciones al mes.**

En **Corea del Sur**, la fiscalía cree que norcoreanos han sido los responsables del **hackeo de docenas de cuentas de correo** electrónico pertenecientes a funcionarios del gobierno.

El ataque a infraestructuras críticas ha vuelto a primera plana tras saberse que **Irán había tenido que eliminar malware de 2 plantas petroquímicas**. Se da la circunstancia de que anteriormente habían sucedido varios incendios en el país en estas plantas, por lo que se está investigando si el malware podría estar relacionado.

3. CONCLUSIÓN



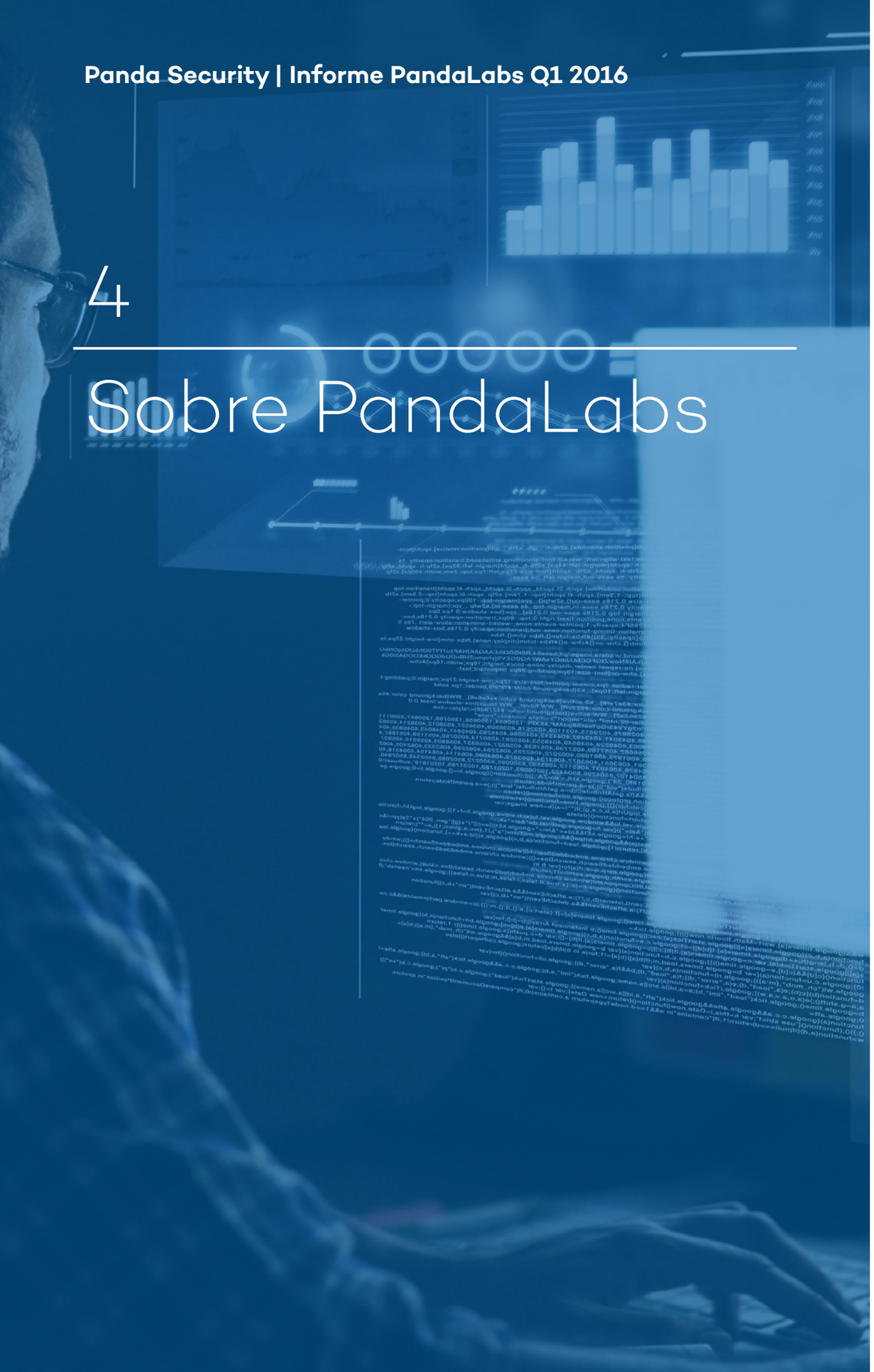
3 Conclusión

Nos acercamos a la recta final de 2016. **Tendremos que estar muy atentos a la evolución de los ataques DDoS**. La combinación de millones de **dispositivos "hackeables" pertenecientes al ámbito de IoT** y las conexiones cada vez más rápidas que tenemos en nuestros hogares pueden convertir a estos ataques en una de las grandes pesadillas de Internet, afectando especialmente a empresas que pueden ser objetivo de extorsionadores profesionales.

Los robos de datos se superan cada vez más, habiendo batido el récord este último trimestre con los datos de 500 millones de usuarios de Yahoo. **Es hoy en día más importante que nunca activar el doble factor de autenticación** en cualquier servicio en el que nos registremos, de tal forma que aunque alguien consiga nuestras credenciales no pueda comprometer nuestras cuentas.

Desde PandaLabs os mantendremos informados de todas las novedades del mundo de la seguridad a través de nuestro Media Center, y nos vemos dentro de 3 meses para analizar lo sucedido durante el cuarto trimestre de 2016.

4. SOBRE PANDALABS



4

Sobre PandaLabs

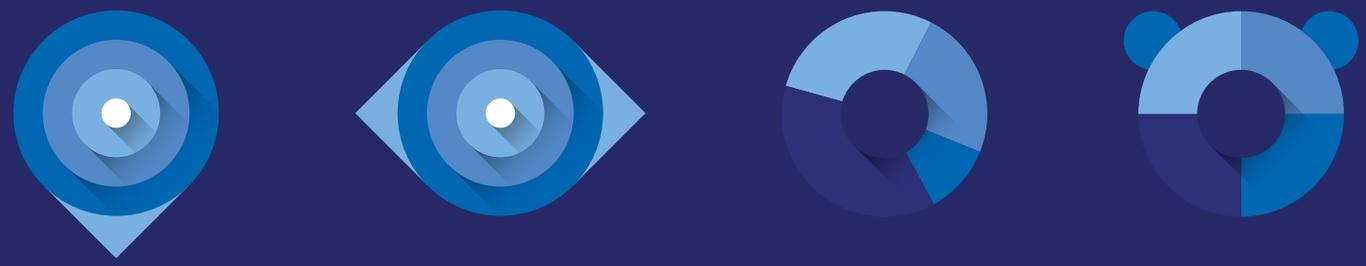
PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- 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.

pandalabs



panda

pandalabs