PREDICCIONES DE CIBERSEGURIDAD 2017

panda

pandalabs

1. ANÁLISIS

1 Análisis

La revolución tecnológica es ya un hecho consolidado. En el último trimestre del año podemos afirmar que las tecnologías digitales están transformando el mundo de los negocios, del trabajo y de la administración pública haciendo vital la creación de un clima de confianza digital que refuerce la protección de los usuarios. Por ello, la ciberseguridad se convierte en un elemento indispensable.

El año arrancó con más de 20 millones de nuevas muestras de malware detectadas y neutralizadas por PandaLabs, con una media de 227.000 al día. Se trata de una cifra ligeramente superior a la encontrada en el mismo trimestre del 2015, donde la media de nuevas muestras se situó en 225.000 al día. A lo largo de 2016 hemos visto como **la cantidad de nuevo malware creado ha sido ligeramente inferior a la del año anterior –unas 200.000 nuevas muestras de malware al día de media-, aunque los ataques son ahora más efectivos.**

Los ciberdelincuentes están adquiriendo cada vez más confianza en sus habilidades y a pesar de que cerremos el año con cifras más optimistas que cuando lo iniciamos, no hay que bajar la guardia. Los Black Hat focalizan sus esfuerzos en aquellos ataques que les pueden reportar más beneficios, utilizando tácticas y profesionalizando los ataques que les permitan ganar dinero fácil de una forma efectiva.

Básicamente se han centrado en la productividad, proliferando los ataques a empresas que manejan una cantidad ingente de datos e información sensibe (hospitales, farmaceúticas, hoteles, etc.) donde una vez que logran acceso infectan con ransomware el mayor número de ordenadores posible, permitiéndoles exigir rescates millonarios o poner a la venta esos datos en el mercado negro.

Si hay algo que no ha cambiado a lo largo del año es la tipología de malware más popular: los troyanos, con el ransomware a la cabeza, siguen liderando las estadísticas desde hace años.

2. RANKING: TOP ATAQUES 2016

2 Ranking: top ataques 2016

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. Sí hemos visto la evolución de estos ataques, como la función de chat para poder comunicarte directamente con los ladrones para "formalizar" el pago. Las técnicas también han avanzado y en algunos casos se han vuelto especialmente agresivas, como es el caso de **Petya,** que en lugar de cifrar documentos va directamente a por el Master Boot Record (MBR) del ordenador dejándolo inservible a no ser que se pague el rescate.

También ha aumentado el abuso de la herramienta del sistema **PowerShell** (tal y como pronosticábamos en el Informe Anual de PandaLabs de 2015), instalada por defecto en Windows 10 y que está siendo utilizado cada vez más en este tipo de ataques para tratar de evitar la detección por parte de las soluciones de seguridad instaladas en los ordenadores de las víctimas.

En el segundo trimestre, uno de los casos más curiosos de ransomware 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.

Ha sido en el tercer trimestre del año cuando hemos sido testigos de un mayor nivel de especialización en el negocio del ransomware. El mejor ejemplo es el protagonizado por los creadores de los ransomware Petya y Mischa, especializándose 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.

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.

Business Email Compromise Phishing

Este tipo de ataques se está popularizando mucho.

Los atacantes se hacen pasar por el presidente o el director financiero de una compañía y solicitan una transferencia a un empleado de la empresa.

Antes de hacerlo se informan de cómo funciona la empresa por dentro y se hacen con información de las víctimas a través de redes sociales para que el engaño sea creíble.

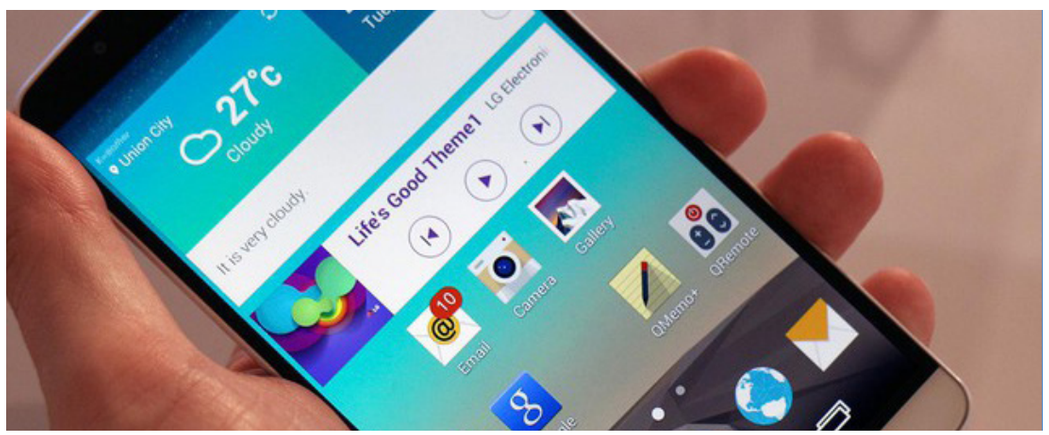
Uno de los casos más sonados este año ha sido el protagonizado por la empresa **Mattel,** el conocido fabricante de juguetes como Barbie o Hot Wheels.

Un alto ejecutivo recibió un mensaje del recientemente nombrado CEO solicitando una transferencia de tres millones de dólares a una cuenta en China. Una vez realizado el pago confirmó al CEO que lo había realizado, quien se sorprendió ya que él no había enviado dicha orden. Contactaron con las autoridades norteamericanas y con su banco, pero ya era tarde y el dinero se había transferido.

En este caso fueron afortunados, ya que era día festivo en China y hubo tiempo suficiente para alertar a las autoridades del país asiático.Congelaron la cuenta, por lo que Mattel consiguió recuperar su dinero.

Dispositivos Móviles

SNAP es el nombre de una de las vulnerabilidades más populares que hemos podido ver este año y que afecta a los teléfonos LG G3.



El problema viene por un error en la aplicación de notificaciones de LG llamada Smart Notice, permitiendo la ejecución de cualquier javascript. Los investigadores de BugSec que descubrieron la vulnerabilidad lo notificaron a LG, que publicó rápidamente una actualización que solucionaba el problema.

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.

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

El terreno automovilístico es uno de los más afectados. 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.** 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.

Los hogares conectados son también vulnerables a los ciberataques. El investigador Andrew Tierney mostró una prueba de concepto que él mismo **había elaborado para secuestrar un termostato.** Tras 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.

Ciberguerra

En el terreno de la ciberguerra, este 2016 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.

En el mes de 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.

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 se sustrajo todo tipo de información, que además se ha ido haciendo pública.**

Siguiendo con la temática electoral, el FBI lanzó una alerta tras detectar 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.

En agosto, un grupo autodenominado **“The Shadow Brokers” anunció que había 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.

Cibercrimen

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).

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.

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.

Ataques DDoS

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.

En el último trimestre de este año, una oleada de ciberataques masivos contra la empresa americana proveedora de Internet DynDNS, puso en jaque el servicio de páginas web de algunas

de las principales corporaciones globales. El brutal ataque afectó a grandes organizaciones y medios de comunicación internacionales, como Netflix, Twitter, Amazon o The New York Times. El servicio se vio interrumpido durante casi 11 horas, afectando a más de mil millones de clientes en todo el mundo.

TPVs y 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.

Este 2016, 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.**

Entidades financieras

Este año el Banco Central de Bangladesh sufrió un ataque en el que se consiguieron hacer transferencias por valor de 1.000 millones de dólares.

Afortunadamente, se 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.

Redes Sociales

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.

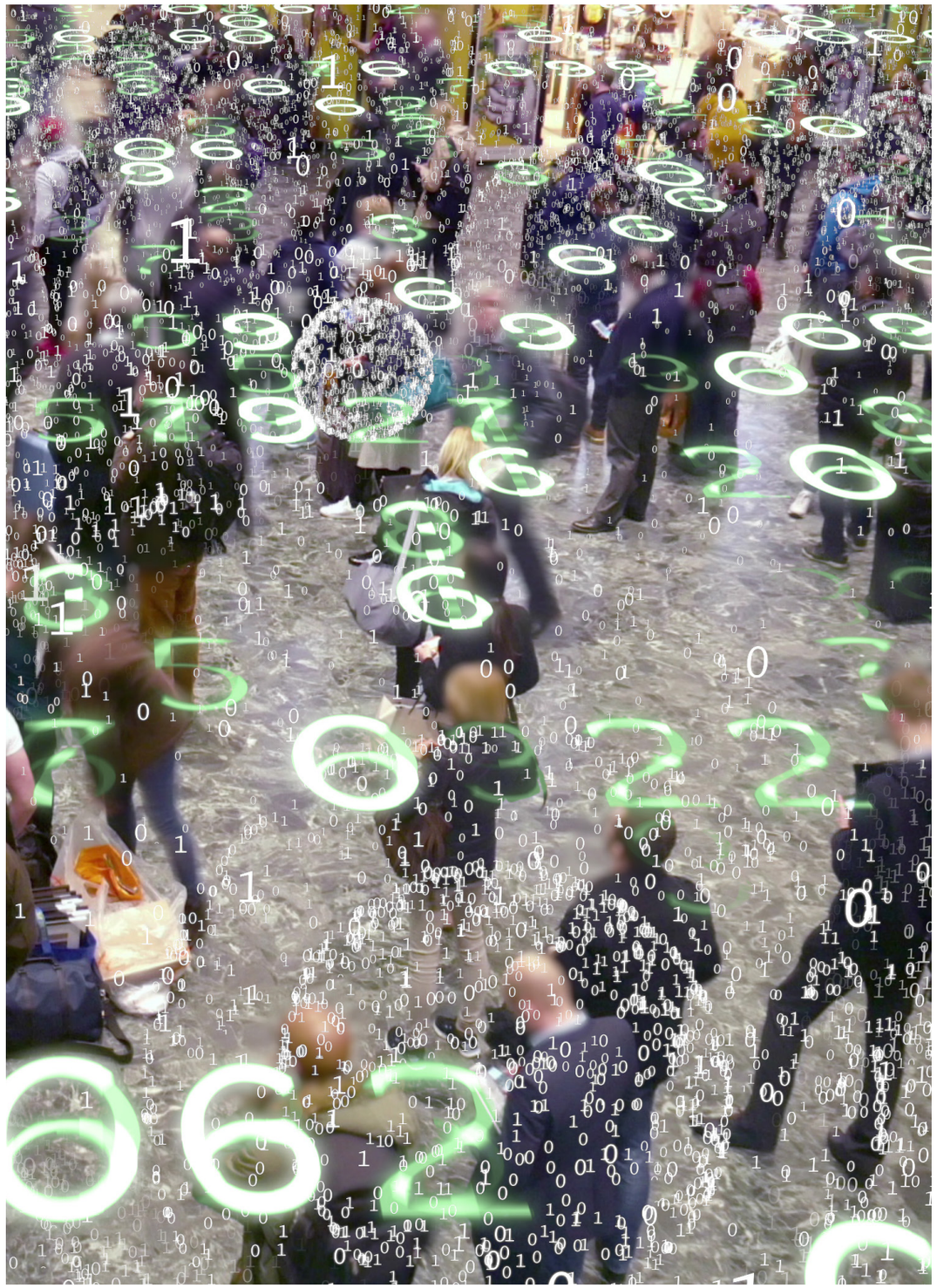
En Twitter, 32 millones de usuarios y contraseñas fueron puestos a la venta por unos 6.000 $.

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.

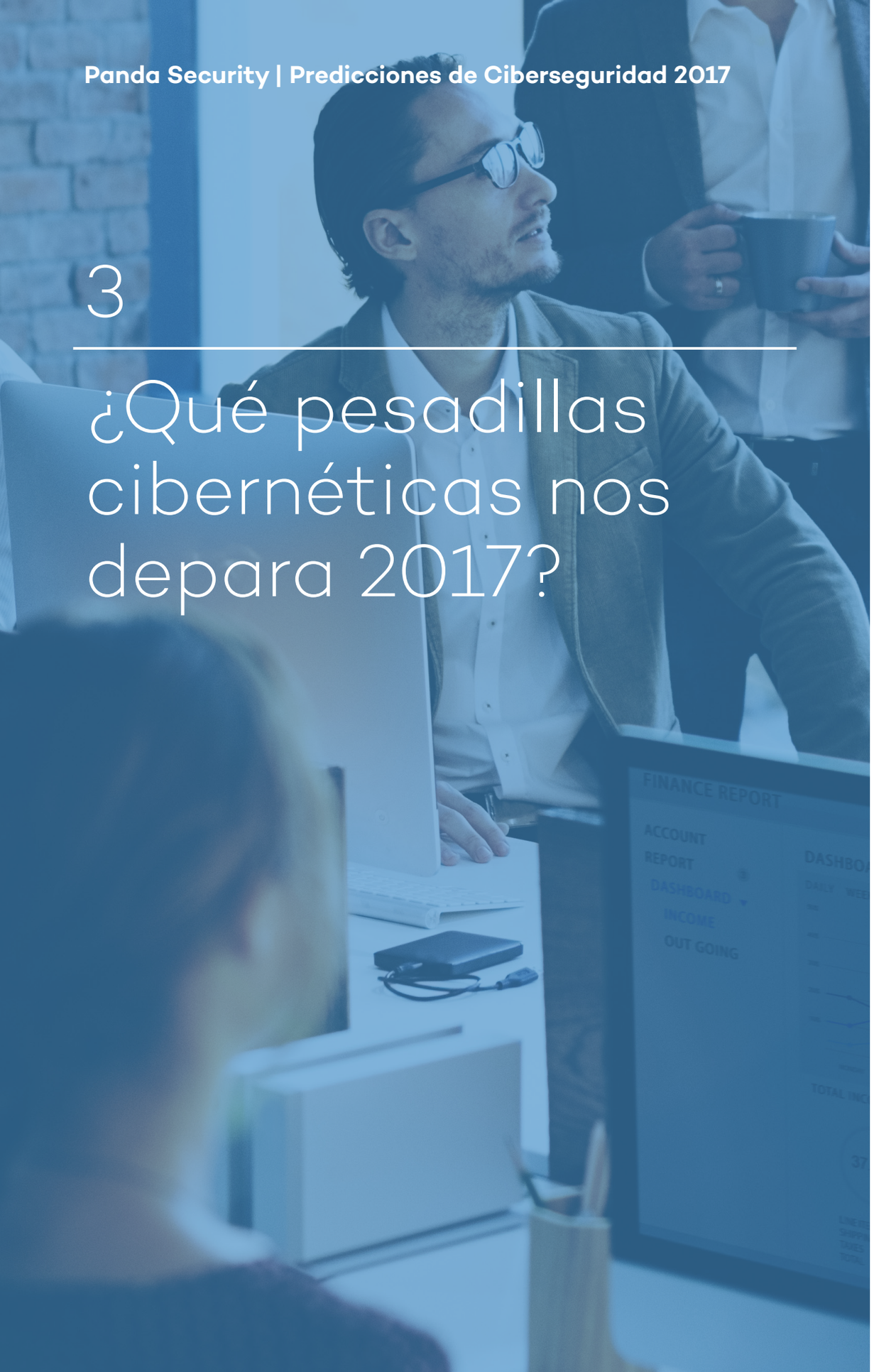
Resulta que, aunque ya prácticamente nadie la utiliza, **MySpace** ha sido atacada. La intrusión se produjo en 2013, aunque hasta mayo de este año no se ha sabido. Han sido sustraídos nombres de usuario, contraseñas y direcciones de correo electrónico, pudiendo alcanzar la cifra de **360 millones de 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.

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



3. ¿QUÉ PESADILLAS CIBERNÉTICAS NOS DEPARA 2017?



3

¿Qué pesadillas cibernéticas nos depara 2017?

Ransomware

Ha sido el gran protagonista de 2016, y presumiblemente lo seguirá siendo a lo largo de 2017. En cierta forma **este tipo de ataques está canibalizando a otros más tradicionales basados en el robo de información.**
El ransomware ha hecho que sea más sencillo y directo obtener ganancias, eliminando intermediarios y riesgos innecesarios.Hay víctimas que optan por pagar el rescate, aunque esto no garantiza la recuperación de la información.

Empresas

Las empresas sufrirán más ataques y cada vez más avanzados.

Las compañías son ya el objetivo predilecto de los ciberdelincuentes, tienen información más valiosa que los usuarios particulares.

Los ciberdelincuentes están continuamente buscando puntos débiles para entrar en las redes corporativas. Una vez allí utilizan movimientos laterales para acceder a los recursos necesarios y obtener la información que buscan. También pueden lanzar ataques de ransomware masivos (infectando con ransomware todos los ordenadores disponibles), para pedir cantidades astronómicas de dinero para recuperar la información de las empresas afectadas.

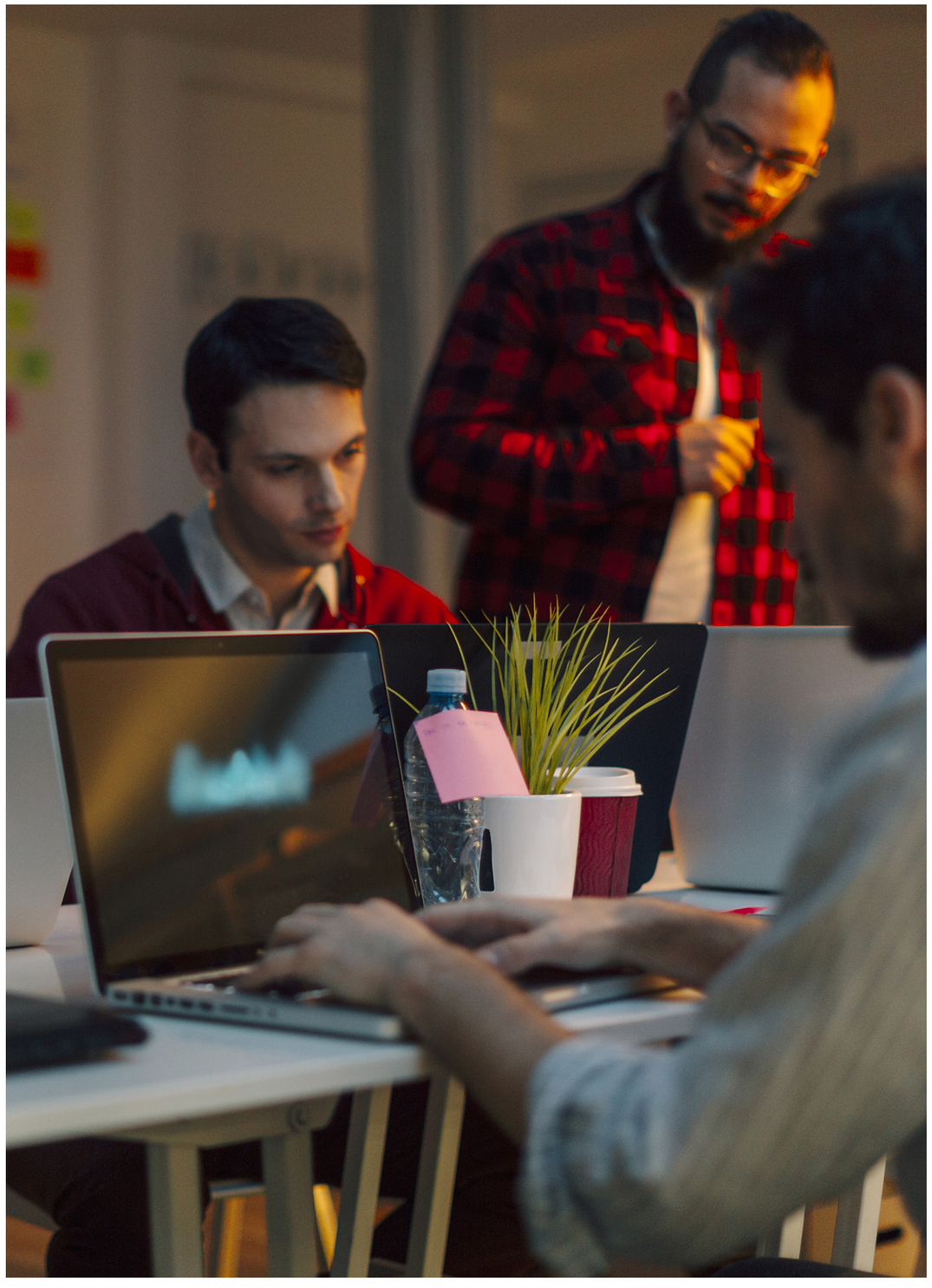
Internet Of Things

Internet de las Cosas (IoT del inglés, Internet of Things) es la próxima pesadilla de seguridad. Todo tipo de dispositivos conectados a la red que además pueden ser utilizados como vía de entrada a la red corporativa de las empresas. La mayoría de estos dispositivos no han sido diseñados teniendo en cuenta la seguridad como punto fuerte. No suelen contar con actualizaciones de seguridad automáticas, utilizan contraseñas débiles, reutilizan las mismas credenciales en miles de dispositivos, etc. Todo esto los hace muy vulnerables a ataques desde el exterior.

DDoS

Los últimos meses de 2016 han tenido lugar los ataques de DDoS más potentes de la historia. Comenzó en septiembre con el ataque sufrido por Brian Krebs tras denunciar la existencia de una empresa israelí que ofrecía este tipo de servicios. Le siguió el de la francesa OVH (llegando a 1Tbps de tráfico) y el de la americana Dyn que dejó sin servicio a varios de los mayores gigantes tecnológicos.

Estos ataques además han sido realizados por redes de bots que contaban con el efecto de miles de dispositivos IoT (cámaras IP, routers, etc.) afectados. **Es seguro que en 2017 veremos un incremento de este tipo de ataques, que suelen utilizarse para chantajear a empresas o para dañar su negocio (impedir acceso a web, tienda online, etc.).**



Móviles

El objetivo es claro aquí también, los dispositivos Android se llevan la peor parte. Es lógico, Android tiene la mayor cota de mercado, es el sistema operativo de la mayoría de dispositivos. Apple mantiene un porcentaje discreto con iOS y el resto de alternativas son residuales. Centrarse en un único sistema operativo, facilita a los ciberdelincuentes fijar el objetivo para maximizar la dispersión y rentabilidad de los ataques.

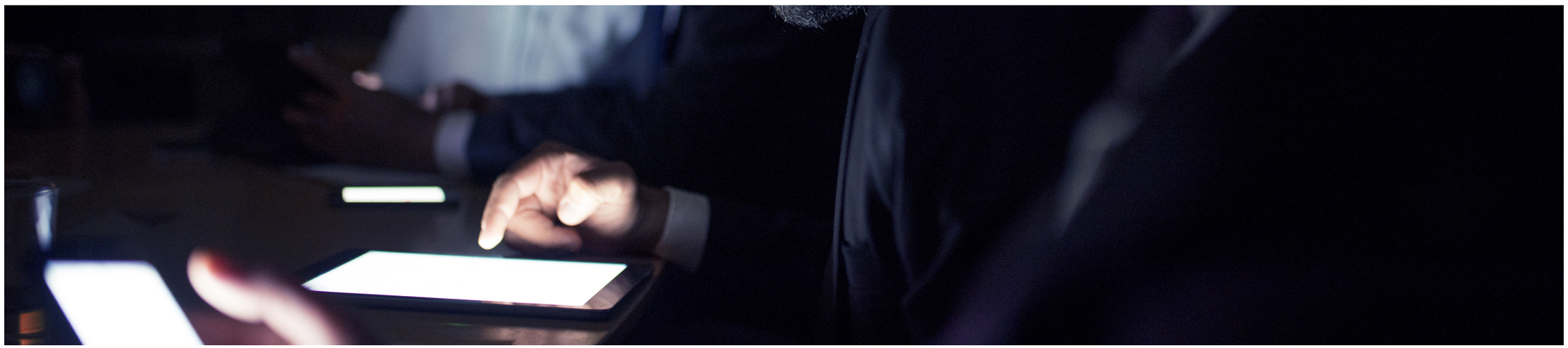
Para complicar la situación (o facilitársela al delincuente), las actualizaciones no sólo dependen del despliegue que pueda hacer Android, sino también de cada fabricante de hardware sobre cómo y cuándo decide aplicarlas (si es que lo hace). Con la cantidad de problemas de seguridad que aparecen cada mes, esta situación no hace más que poner a los usuarios en mayor riesgo.

Ciberguerra

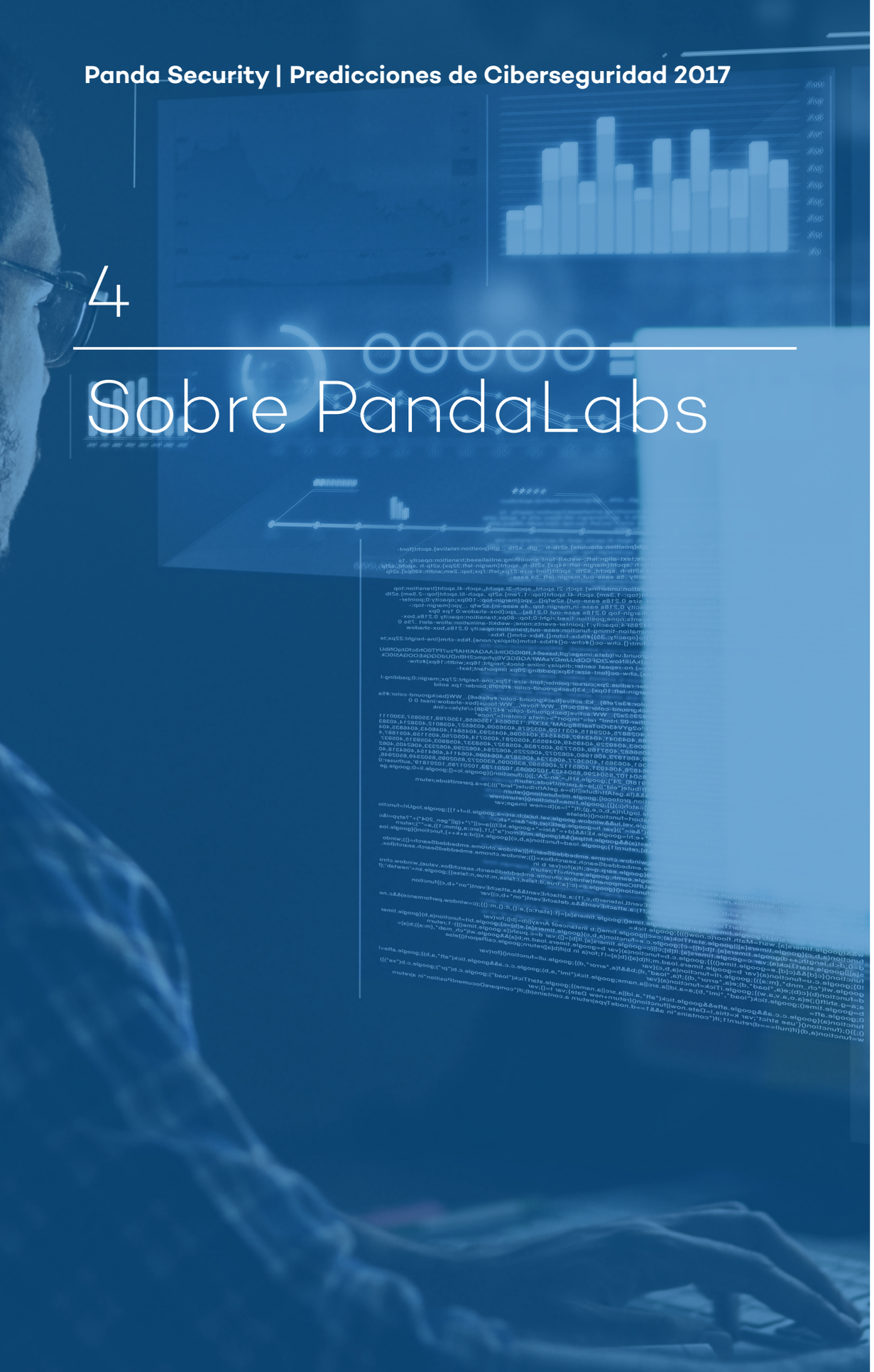
Vivimos uno de los momentos más delicados de los últimos años a nivel de relaciones internacionales. Amenazas de guerras comerciales, espionaje, arancelarias que pueden polarizar las posiciones de las grandes potencias. Esto sin duda puede tener grandes -y graves- efectos en el campo de la seguridad informática.

Los gobiernos querrán tener acceso a más información aún (en un momento en el que el cifrado se está popularizando), y las agencias de inteligencia estarán aún más interesadas en obtener información que pueda beneficiar a las industrias de su país.

Una situación mundial así podría entorpecer las iniciativas de compartición de información. Datos que grandes empresas ya están compartiendo para poder protegerse mejor de la ciberdelincuencia, estableciendo estándares y protocolos de actuación internacionales.



4. SOBRE PANDALABS



4

Sobre PandaLabs

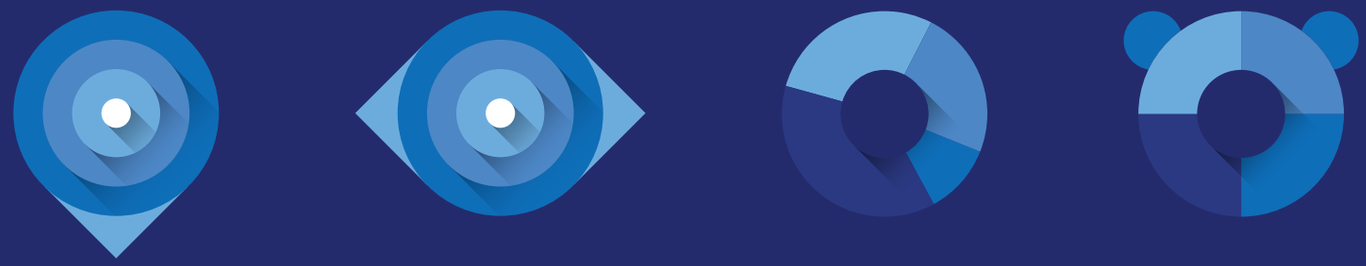
PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- 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