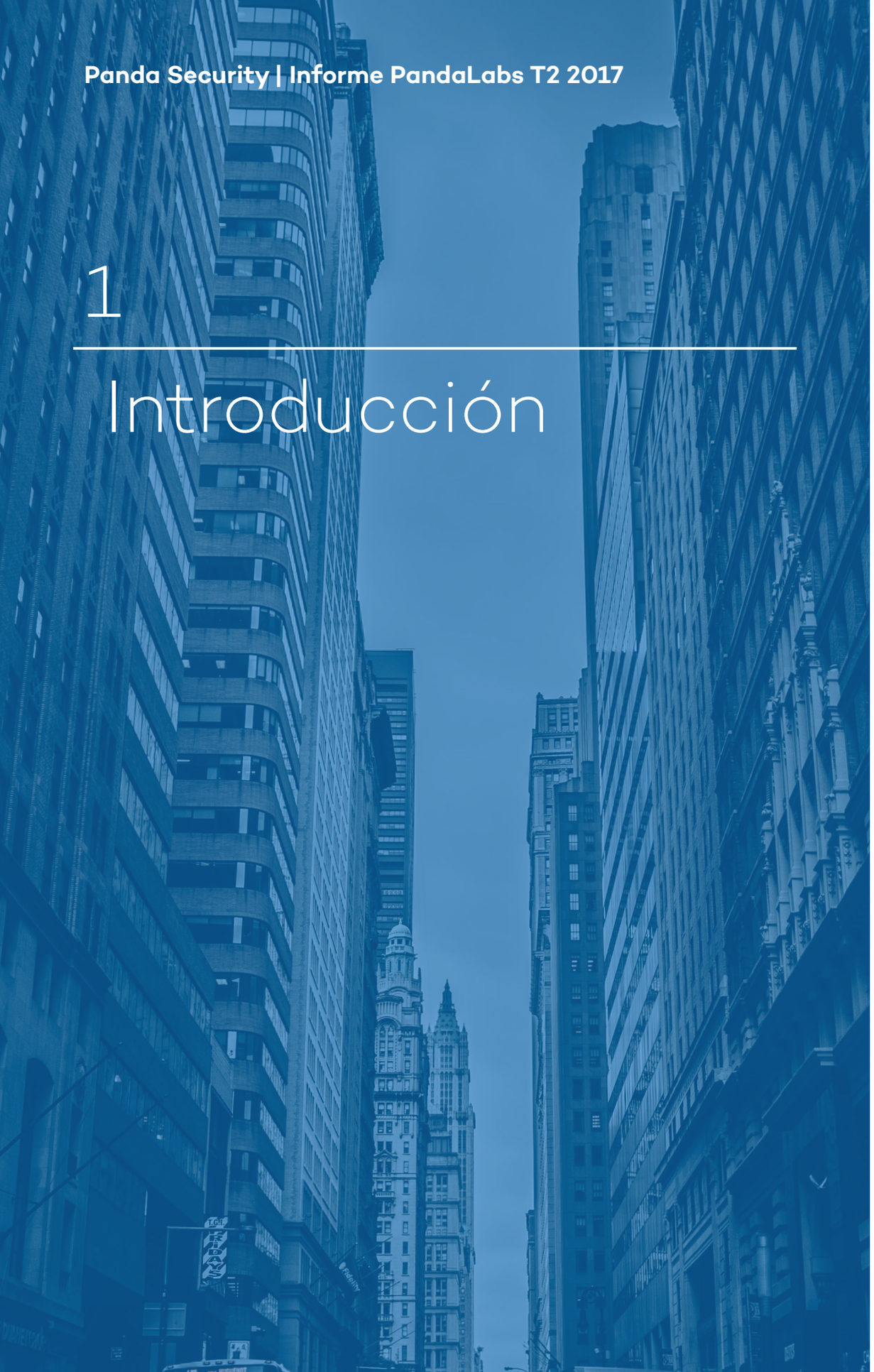
INFORME TRIMESTRAL PANDALABS T2 2017

panda

pandalabs

1. INTRODUCCIÓN



1 Introducción

Este segundo trimestre de 2017 ha sido uno de los más trepidantes en lo que a la seguridad informática se refiere de los últimos años. Sin duda, **el ataque de WannaCry en mayo y el de GoldenEye/Petya en junio han afectado a países de todo el globo**, generando grandes pérdidas en multitud de empresas. Diferentes estudios sitúan estas cifras entre los 1.000 y 4.000 millones de dólares.

Además, estos ataques están íntimamente ligados con los manejos que diferentes países llevan a cabo en el campo de la ciberguerra. Ambos utilizaban una vulnerabilidad que previamente había sido utilizada por la NSA y que el grupo de hackers **Shadow Brokers** publicó en abril. A esto, hay que añadir que algunas evidencias apuntan a Corea del Norte como origen del ataque de WannaCry, mientras que otra hipótesis es que el ataque de GoldenEye/Petya estaba dirigido a sabotear empresas e instituciones ucranianas, poniendo en el punto de mira a Rusia como probable promotor del ataque.

Si bien no se puede decir que se esté librando una ciberguerra de manera formal, sí que hay escaramuzas y ataques como WannaCry o GoldenEye que de una forma u otra nos afectan a todos los ciudadanos del planeta. Aparte de estos ataques evidentes, **están teniendo lugar otros de forma silenciosa pero que son si cabe aún más graves, como los claros intentos de manipulación de las elecciones** en países como Francia o Estados Unidos, tratando de favorecer a candidatos cercanos al gobierno ruso (Trump en el caso de Estados Unidos y Le Pen en Francia).

Mientras tanto el resto del mundo, además de lidiar con las **intrigas y ser víctimas colaterales de esta ciberguerra oculta**, debemos hacer frente a multitud de ciberdelincuentes cuyo objetivo es enriquecerse a costa de sus víctimas.

2. CIFRAS DEL TRIMESTRE

2

Cifras del Trimestre

Tanto en nuestros informes como en los del resto de fabricantes de soluciones de seguridad siempre encontramos el mismo tipo de cifras sobre malware: cuánto malware nuevo ha aparecido en un periodo de tiempo, tipos de malware, etc. Aunque ese tipo de cifras está muy bien y puede conseguir grandes titulares, desde PandaLabs decidimos en 2017 ir un paso por delante y mostrar datos que tengan un significado y aporten un valor real.

Para calcular las cifras mostradas a continuación decidimos no contar ninguna detección de todo aquel malware que ya detectamos por firmas (cientos de millones) ya que se trata de malware conocido y del que en mayor o menor medida todo usuario con un antivirus básico está protegido. Tampoco incluimos las detecciones heurísticas, que son capaces de detectar malware que no se conoce previamente.

El razonamiento para tomar esta decisión es que los atacantes profesionales como mínimo se aseguran de hacer al menos unas pruebas básicas con los motores antivirus para cerciorarse de que sus nuevas muestras de malware no son detectadas, y estos motores incluyen detecciones tanto de firmas como heurísticas. Es decir, podemos dar por descontadas estas cifras, ya que los usuarios estaban en todo momento protegidos y no corrían riesgo real de infección.

Vamos a tener en cuenta los datos de nuevo malware no detectado ni por firmas ni por heurísticos, tanto los ataques protagonizados por malware como por los ataques sin fichero (fileless) **y aquellos realizados a través del abuso de herramientas legítimas del sistema**, algo cada vez más habitual en entornos corporativos, como vimos en el caso de GoldenEye/Petya el pasado mes de junio.

Pero, ¿cómo vamos a medir algo que no somos capaces de detectar?

La cuestión es que sí somos capaces de detectar y parar estos ataques, a pesar de que nunca antes hayan sido vistos ni detectados por firmas o por heurísticas. Para ello utilizamos una serie de tecnologías propias, englobadas en lo que llamamos "Inteligencia Contextual", que nos permite revelar patrones de comportamiento malicioso y generar acciones de ciberdefensa avanzada contra amenazas conocidas y desconocidas.

Esta capa de Inteligencia Contextual es la que nos permite tener unos ratios de detección excelentes en todos los test llevados a cabo con una metodología que imita los ataques tal y como suceden en el mundo real. En los tests llevados a cabo por AV-Comparatives durante los 6 primeros meses de 2017, Panda Security obtiene en el Real World Test unos ratios excelentes, obteniendo el máximo galardón con Panda Free Antivirus, la solución más básica del portfolio de productos de ciberseguridad.

A continuación pasamos a analizar **los datos de ataques que hemos obtenido**: de todas las máquinas protegidas por alguna solución de Panda Security, el **3,44%** de ellas ha sufrido ataques de amenazas desconocidas, lo que supone **un incremento de casi el 40% respecto al trimestre anterior**. Si miramos por tipo de cliente, los usuarios domésticos y pequeñas empresas tienen un **3,81%** de ataques mientras que en el caso de medianas y grandes empresas la cifra es del **2,28%.**

Los usuarios domésticos cuentan con muchas menos medidas de protección, por lo que se encuentran más expuestos a los ataques. Por eso, aunque los entornos corporativos son más rentables, muchos de los ataques que en un entorno doméstico pueden funcionar son detenidos en las primeras instancias en redes corporativas.

Dentro de nuestros clientes corporativos tenemos aquellos que utilizan soluciones tradicionales, y los que optan por nuestra solución EDR (Adaptive Defense), que va mucho más allá de un antivirus y ofrece funcionalidades extra, niveles de protección mucho más amplios, clasificación y monitorización en tiempo real de todos los procesos que se ejecutan en servidores y estaciones de todo el parque, análisis forenses, etc. Tiene sentido que el nº de ataques que consiguen saltarse todas las capas de protección en Adaptive Defense de EDR sean mucho menores que aquellos que se tienen que enfrentar sólo con tecnologías tradicionales.

El **2,67%** de las máquinas protegidas por soluciones tradicionales reciben intentos de ataque de amenazas desconocidas, mientras que en aquellas protegidas por Adaptive Defense el porcentaje de esos intentos baja hasta el **1,21%**. En cualquiera de los casos, las soluciones de Panda Security han conseguido neutralizar esos ataques a tiempo, sin que hayan podido tener efecto en los equipos.

¿Cómo se reparten a nivel geográfico? Hemos calculado el **porcentaje de máquinas atacadas en cada país**, a mayor porcentaje, mayor probabilidad de sufrir un ataque de nuevas amenazas si utilizamos ordenadores en esos países.

Top 10 Países Más Atacados

El Salvador	10,85%
Brasil	10,04%
Bangladesh	9,77%
Honduras	9,44%
Rusia	8,96%
Venezuela	8,87%
Colombia	8,29%
Pakistan	8,17%
Mexico	7,99%
Ecuador	7,67%

Top 10 Países Menos Atacados

Austria	1,14%
Bélgica	1,06%
Alemania	0,97%
Japón	0,90%
Países Bajos	0,87%
Dinamarca	0,71%
Finlandia	0,64%
Eslovenia	0,64%
Noruega	0,47%
Suecia	0,42%

Listado Completo de Países

El Salvador	10,85%
Brasil	10,04%
Bangladesh	9,77%
Honduras	9,44%
Rusia	8,96%
Venezuela	8,87%
Colombia	8,29%
Pakistan	8,17%
Mexico	7,99%
Ecuador	7,67%
Bolivia	7,58%
Indonesia	7,57%
Taiwan	7,46%
Tailandia	7,30%
Iran	6,58%
Singapur	6,30%

Perú	5,62%
Macedonia	5,59%
Turquía	5,18%
Paraguay	5,11%
Guatemala	5,03%
Bosnia yHerzegovina	4,69%
Panamá	4,62%
Letonia	4,40%
Argentina	4,35%
Lituania	4,18%
Serbia	4,10%
Bulgaria	4,03%
República Checa	4,00%
Uruguay	3,69%
Croacia	3,65%
Hong Kong	3,61%
Polonia	3,61%
Chile	3,39%
Malasia	3,39%
Italia	3,28%
Rumania	3,21%
Eslovaquia	2,86%
Costa Rica	2,25%
Sudáfrica	2,16%

Estados Unidos	1,99%
Canadá	1,80%
Hungría	1,71%
Grecia	1,55%
España	1,50%
Francia	1,49%
Chipre	1,48%
Suiza	1,44%
Portugal	1,41%
Reino Unido	1,35%
Puerto Rico	1,25%
Austria	1,14%
Bélgica	1,06%
Alemania	0,97%
Japón	0,90%
Países Bajos	0,87%
Dinamarca	0,71%
Finlandia	0,64%
Eslovenia	0,64%
Noruega	0,47%
Suecia	0,42%

3. EL TRIMESTRE DE UN VISTAZO

3

El trimestre de un vistazo

WannaCry **ha sido uno de los mayores ataques de la historia**. Si bien por número de víctimas y velocidad de propagación hemos visto ataques en el pasado mucho más potentes (como el Blaster o el SQLSlammer, por poner sólo un par de ejemplos), lo cierto es que el daño que causaban era colateral a su propagación. Sin embargo, WannaCry es un ransomware con funcionalidad de gusano de red, por lo que cada ordenador infectado acababa con sus documentos secuestrados. Teniendo en cuenta que hablamos de unos **230.000 ordenadores infectados**, y sabiendo que las **pérdidas se calculan entre los 1.000 y los 4.000 millones de dólares**, el coste medio del ataque por ordenador se situaría entre los 4.300 en el supuesto más optimista- o de más de 17.000 en el caso más pesimista-, por lo que sin duda alguna podemos hablar del ataque que más daño ha causado en la historia.

En el siguiente enlace podéis acceder al webinar impartido por Luis Corrons, Director Técnico de PandaLabs, donde realiza un análisis detallado de lo sucedido y de las medidas que se deben tomar para estar protegido ante ataques de este tipo: https://youtu.be/CPlB65lt1Ko.

GoldenEye/Petya ha sido el segundo ataque que más repercusión ha tenido este trimestre, como una réplica al terremoto que supuso WannaCry. A pesar de que sus víctimas estaban en principio limitadas a una zona geográfica concreta (Ucrania), **acabó afectando a empresas en más de 60 países**.

El ataque, cuidadosamente planeado, se llevó a cabo a través de una aplicación de contabilidad muy popular entre empresas en Ucrania, MeDoc. Los atacantes comprometieron el servidor de actualizaciones de dicho software, de tal forma que todos los ordenadores con MeDoc instalado pudieron ser infectados al momento de forma automática.

Este ataque ha sido tan sofisticado como dañino. Además de cifrar los ficheros, en caso de que el usuario que tiene la sesión iniciada en el ordenador tenga permisos de administrador, el malware va a por el MBR (Master Boot Record) del disco duro. En principio aparentaba ser un ransomware al estilo de WannaCry, pero tras analizarlo a fondo vimos que realmente sus autores no tenían intención de dejar que la información secuestrada fuera recuperada.

Parece claro que se trató de un ataque dirigido a sabotear los ordenadores de empresas e instituciones ucranianas. Pero como cualquier arma de destrucción masiva, es inevitable que se produzcan "daños colaterales". GoldenEye/Petya, una vez dentro de una red corporativa se propagaba por la misma utilizando diversas –y muy efectivas- técnicas, lo que provocó que empresas extranjeras con oficinas en Ucrania se vieran afectadas afectando sus operaciones.

Días después del ataque, el gobierno ucraniano acusó abiertamente a Rusia de estar detrás del ataque. Desde PandaLabs desgranan las claves este ataque y de sus autores en la presentación que podéis ver aquí.

Ransomware

Además de WannaCry y GoldenEye/Petya, **los ataques de ransomware llevados a cabo por ciberdelincuentes siguen en auge**. La empresa de alojamiento de páginas web Nayana, de Corea del Sur, fue atacada y el ransomware cifró información de 153 servidores Linux.

Los atacantes exigieron un rescate de 1,62 millones de dólares. La empresa negoció con los delincuentes y rebajó la cifra a 1 millón de dólares, a pagar en 3 veces.

Ciberguerra

Hay sospechas de que detrás de estos 2 grandes ataques podría haber gobiernos (Corea del Norte en el caso del WannaCry y Rusia en el de GoldenEye/Petya), pero estos son únicamente un par de casos dentro de la ciberguerra más o menos encubierta que está teniendo lugar en el ciberespacio.

Los protagonistas principales se repiten de forma constante: Estados Unidos, Rusia, Corea del Norte... sorprendentemente –ya que suele ser un habitual en estos temas- China no parece haber protagonizado ningún escándalo estos meses. Una explicación de esto podría ser el ciberacuerdo cerrado entre China y EEUU para poner fin a las hostilidades cibernéticas, aunque bien podría ser que se estén llevando a cabo ataques que no hayan sido aún identificados.

En **Estados Unidos** están claramente preocupados por los ataques en los que instituciones norteamericanas son el objetivo. Samuel Liles, director en funciones de la ciberdivisión del DHS (Department of Homeland Security) declaró ante el Comité de Inteligencia del Senado que ataques de **hackers que contaban con el apoyo del gobierno ruso arremetieron contra sistemas relacionados con las elecciones de al menos 21 estados**.

El Comité de Inteligencia del Congreso llevó a cabo una audiencia para tratar el impacto del hackeo por parte de Rusia de las elecciones presidenciales de 2016. Allí el antiguo Secretario del DHS bajo la administración Obama, Jeh Johnson, reiteró que el presidente ruso Vladimir Putin había ordenado el **ataque con la intención de influir en el resultado de las elecciones presindenciales de EEUU**. También dijo que no habían conseguido manipular votos en estos ataques.

En junio, el gobierno norteamericano lanzó una alerta en la que culpaba al gobierno de Corea del Norte por una serie de ciberataques ocurridos desde 2009, y advirtiendo que es probable que cometan aún más. La advertencia, que vino del DHS y del FBI, se refería a un grupo de atacantes, "Hidden Cobra", que han atacado a medios de comunicación, sectores como el aeroespacial y el financiero, así como infraestructuras críticas tanto en EEUU como en otros países.

Si bien el nombre de "Hidden Cobra" no es muy conocido, a este grupo se le conoce como "Lazarus Group", que ha sido asociado a ataques como el que sufrió Sony Pictures Entertainment en 2014.

Hay sospechas de que Corea del Norte puede ser también quien está detrás de los robos perpetrados en el Banco Central de Bangladesh así como en otras entidades financieras. Y no sólo esto, sino que hay evidencias que relacionan el reciente ataque de WannaCry con el mismo grupo, "Lazarus Group".

Durante el GARTNER SECURITY & RISK MANAGEMENT SUMMIT que se celebró en Washington en junio, el exdirector de la CIA, John Brennan, dijo que la supuesta alianza entre el gobierno ruso y cibedelincuentes para llevar a cabo el robo de cuentas de Yahoo se trata sólo de la punta del iceberg, y que futuros ciberataques llevados a cabo por gobiernos seguirán este tipo de fórmula y se incrementarán.

En la misma charla afirmó que los Servicios de inteligencia rusos no se encuentran realmente limitados por las leyes, mientras que las agencias estadounidenses sí lo están. Hay quien podría encontrar estas declaraciones cínicas, ya que se ha sabido gracias a documentos publicados por WikiLeaks que la CIA ha estado hackeando routers wifi domésticos, de empresas y públicos durante años para llevar acabo vigilancias clandestinas.

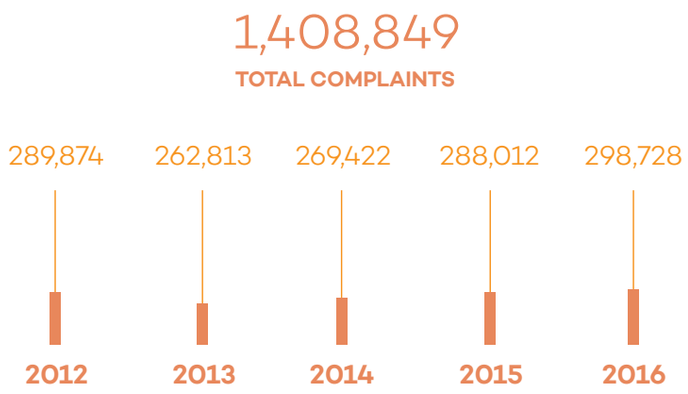
En el informe anterior comentamos como en Francia habían descartado el uso del voto electrónico por parte de sus ciudadanos residentes en el extranjero ante el riesgo "extremadamente elevado" de que se produjeran ciberataques. Finalmente hubo al menos un ciberataque, y apenas a dos días de celebrarse las elecciones se publicó multitud de información privada del entonces candidato a la presidencia de la república Emmanuel Macron, quien rápidamente envió un comunicado de prensa indicando que habían sido hackeados. Investigaciones posteriores ligaron el hackeo con el grupo "Fancy Bear", del que se sospecha que está detrás el gobierno ruso.

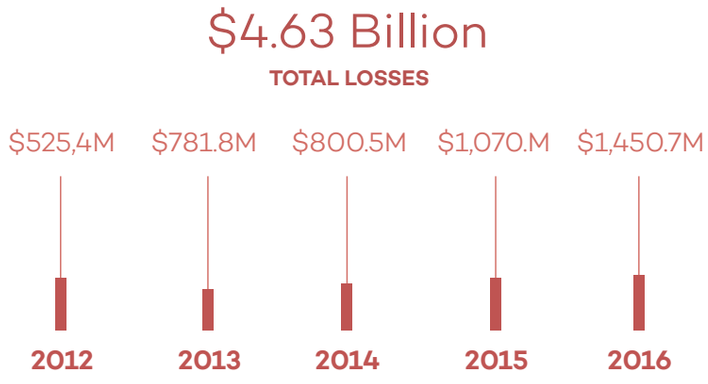
Miembros del parlamento británico han sido objetivo de intentos de ataques para hackear sus cuentas, según publicó el Financial Times, en lo que se cree que es un ataque patrocinado por una potencia extranjera.

Toda esta vorágine está afectando a empresas tecnológicas. El FSB ruso está demandando a compañías como CISCO, SAP o IBM el código fuente de sus soluciones de seguridad para buscar posibles puertas traseras (backdoors). Días después el gobierno norteamericano ha prohibido a todas las agencias federales del país que utilicen soluciones de Kaspersky debido a su cercanía al gobierno ruso y al FSB.

Cibercrimen

Según el informe "2016 Internet Crime Report" publicado por el Internet Crime Complaint Center (IC3) del FBI, **las pérdidas debidas al cibercrimen aumentaron un 24%, superando los 1.300 millones de dólares**. Hay que tener en cuenta que esto contabiliza sólo la cantidad reportada por víctimas (estadounidenses) al IC3, que estima que se trata de un 15% de las mismas, por lo que la cifra total (sólo para Estados Unidos) aumentaría hasta las 9.000 millones de dólares de pérdidas solamente para 2016.





Los **exploits más codiciados para lanzar ataques son aquellos conocidos como "0-day"**, desconocidos por el fabricante del software afectado y que permite a los atacantes comprometer a los usuarios aunque tengan todo su software actualizado.

En abril se descubrió una de estas vulnerabilidades que afectaba a las diferentes versiones de Microsoft Word, y se sabe que al menos desde enero de este año había estado siendo utilizada por atacantes. El mismo mes de abril Microsoft publicó la actualización correspondiente para proteger a sus usuarios de Office.

Historiales médicos de al menos 7.000 personas han sido comprometidos por una brecha de seguridad en el Bronx Lebanon Hospital Center en Nueva York.

Otro tipo de incidentes de seguridad donde no hay atacantes directamente implicados son aquellos en los que, debido a un error o negligencia, datos que deberían estar protegidos se exponen a que cualquiera pueda acceder a ellos. Esto le ha sucedido a la Automobile Association (AA), que durante varios días en abril dejó en abierto más de 13Gb de datos, entre los que había más de 100.000 direcciones de correo e información de tarjetas de crédito.

Un caso similar, aunque a un nivel aún mayor, ha ocurrido en EEUU. **Unas empresas de marketing contratadas por el partido republicano dejaron accesible a todo el mundo datos de 198 millones de votantes registrados**, lo que supone casi la totalidad de votantes (en total son algo más de 200 millones). Los datos estuvieron accesibles durante al menos un par de días y contenían todo tipo de información de los votantes: nombres, fechas de nacimiento, direcciones, etc.

El **tráfico de datos de clientes de Apple en China** ha terminado con la detención de 22 personas en el país asiático. Todo parece indicar que se trata de un trabajo desde dentro, ya que algunos de los detenidos trabajaban para empresas subcontratadas por Apple y que tenían acceso a la información con la que los detenidos estaban traficando.

InterContinental Hotels Group (IHG) fue noticia al saberse que había sido víctima de robo de información de sus clientes. Si bien la empresa dijo en febrero que el ataque únicamente había afectado a una docena de sus hoteles, se ha sabido ahora que tenían TPVs (Terminales de Punto de Venta) infectados en más de 1.000 de sus establecimientos. En un comunicado, la empresa confirma que las tarjetas correspondían a pernoctaciones realizadas entre el 29 de septiembre y el 29 de diciembre de 2016. Asimismo, también ha explicado que "aunque no hay evidencia de acceso no autorizado a los datos de las tarjetas de pago después del 29 de diciembre de 2016, la confirmación de que el malware fue erradicado no ocurrió hasta febrero y marzo de 2017". Entre las diferentes marcas de hoteles que posee el grupo se encuentran Holiday Inn, Holiday Inn Express, InterContinental, Kimpton Hotels, y Crowne Plaza.

La **empresa OneLogin,** un servicio que ofrece a los usuarios un inicio de sesión único para todo tipo de plataformas en la nube de manera que permite un uso más cómodo y seguro, fue irónicamente hackeada. La compañía anunció a través de su blog que había sido atacada y que intrusos habían conseguido entrar en su centro de datos en Estados Unidos, accediendo a tablas de sus bases de datos y dejando expuestos a piratas informáticos información de usuario, aplicaciones y claves.

Móviles

Desde el 1 de junio Google ha aumentado las recompensas para quien encuentre los fallos de seguridad más graves que se pueden dar (no ha sido descubierto ninguno en los últimos años). La primera recompensa aumenta de 50.000 a 200.000 dólares, y la segunda de 30.000 a 150.000.

Una vulnerabilidad (CVE-2017-6975) en el firmware de los chips Broadcom Wi-Fi HardMAC SoC cuando se renegocia una conexión a la red WiFi obligó a Apple a lanzar una actualización de iOS (10.3.1).

Esta vulnerabilidad, sin embargo, no sólo afecta a iPhones y iPads, sino también a dispositivos móviles de otros fabricantes como Samsung o los mismos Nexus de Google, que recibieron en abril su actualización de seguridad para solventar este problema de seguridad.

IoT

Que vivimos en un mundo cada vez más conectado es algo a lo que nos estamos habituando. Una de las consecuencias que esto tiene es que ataques como el de WannaCry pueden llegar mucho más lejos de lo que pensamos.

Las **Smart Cities,** que es como conocemos al tejido informático que conecta millones de dispositivos en una ciudad para que

todo sea más eficiente, son buena prueba de esta implantación tecnológica en nuestra vida diaria. **Las ciudades de todo el mundo son cada vez más "inteligentes" y se calcula que en 2020 habrá más de 50.000 millones de este tipo de dispositivos conectados a Internet,** con los riesgos implícitos como como la modificación de semáforos o cortar el suministro de agua de una ciudad.

El pasado mes de junio, WannaCry afectó en Australia 55 cámaras de tráfico ubicadas en semáforos y controles de velocidad después de que un trabajador de una subcontrata conectara un ordenador infectado a la red donde éstas se encontraban. La policía tuvo que retirar 8.000 multas de tráfico después del incidente.

El pasado 7 de abril en Dallas, Texas, 156 sirenas de emergencia se pusieron a sonar al unísono desde las 23:40 de la noche. Funcionarios lograron pararlas 40 minutos después, tras echar abajo todo el sistema de emergencias. Aún se desconoce quién fue el responsable del hackeo que provocó este incidente.

Se ha sabido una **nueva vulnerabilidad afectando a coches,** en este caso de la marca Mazda. Sin embargo, al contrario que en otros casos que hemos visto en el pasado, para poder comprometer el sistema del coche se necesita introducir un USB mientras el motor está en marcha en un modo de funcionamiento determinado.

4. CONCLUSIÓN

4

Conclusión

Shadowbrokers tiene previsto seguir publicando información robada a la NSA, y la carrera ciberarmamentística está en plena ebullición, así que todos –y muy especialmente las empresas- deben extremar las medidas de seguridad.

Si miramos por tipo de cliente, los usuarios domésticos y pequeñas empresas son los que tienen más probabilidad de infección, siendo geográficamente los países más proclives a padecer infecciones por nuevas amenazas El Salvador, Brasil, Bangladesh, Honduras, Rusia y Venezuela.

WannaCry y Petya nos demuestran que hay gobiernos a los que no les tiembla la mano a la hora de llevar a cabo ciberataques y que todos los internautas podemos convertirnos en víctimas colaterales de sus acciones. Debería estudiarse la posibilidad de elaborar un tratado internacional al que pudieran adherir los países –al estilo de la Convención de Ginebra- para limitar lo que los estados pueden hacer en caso de ciberataques.

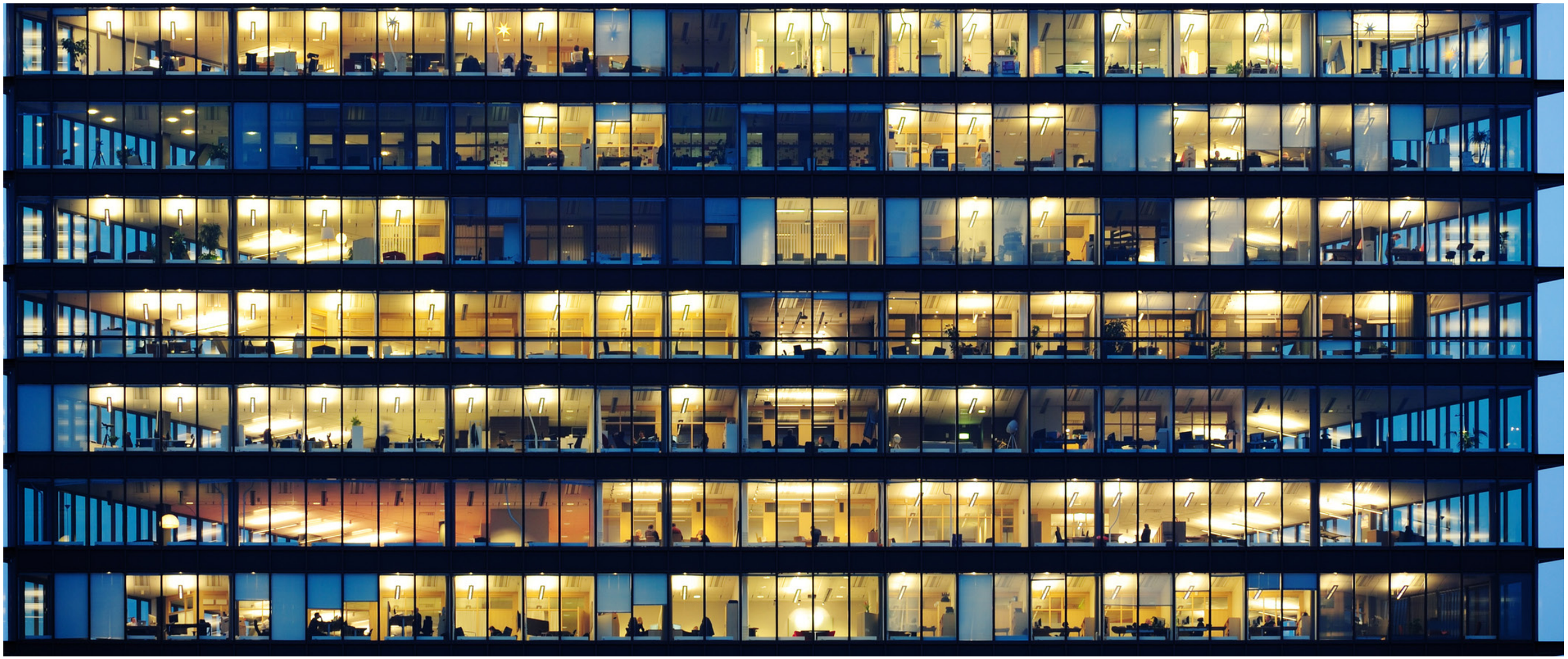
Los ataques de ransomware siguen en auge, y la única explicación es que hay víctimas que pagan. Si no se produjeran pagos, los ataques desaparecerían. Está en las manos de todos nosotros poner fin a estos ataques, por un lado protegiéndonos para evitar convertirnos en víctimas y por otro tener siempre copias de seguridad de nuestra información para no pagar jamás un rescate.

Los exploits más codiciados para lanzar ataques son aquellos conocidos como “0-day”, desconocidos por el fabricante del software afectado. También ataques de insiders o a TPVS son en la actualidad las principales tretas en cibercrimen.

El tener más conexiones a Internet, desde móviles a todo tipo de dispositivos IoT, hace que las consecuencias de ser atacados vayan mucho más allá de lo que hasta hace no mucho estábamos acostumbrados.

Esta es una tendencia que no va a dejar de crecer, ya que en breve tendremos decenas de miles de millones de dispositivos conectados a Internet, y esto sólo va a ir a más.

Por un lado aumentará la superficie de ataque, y por otro provocará que los ataques puedan tener consecuencias mucho más graves y costosas.



05. RECOMENDACIONES

5 Recomendaciones

Las soluciones de seguridad tradicionales, aunque eficaces en la protección contra el malware, no son capaces de hacer frente a ataques donde se utilizan herramientas no maliciosas y otras técnicas avanzadas como las descritas en este informe.

Es imprescindible utilizar software de seguridad adecuado al nivel de amenaza al que nos estamos enfrentando. Soluciones tipo EDR (Endpoint Detection & Response) como **Adaptive Defense** son las únicas que nos proporcionan las herramientas necesarias para protegernos de los sofisticados ataques que se están produciendo.

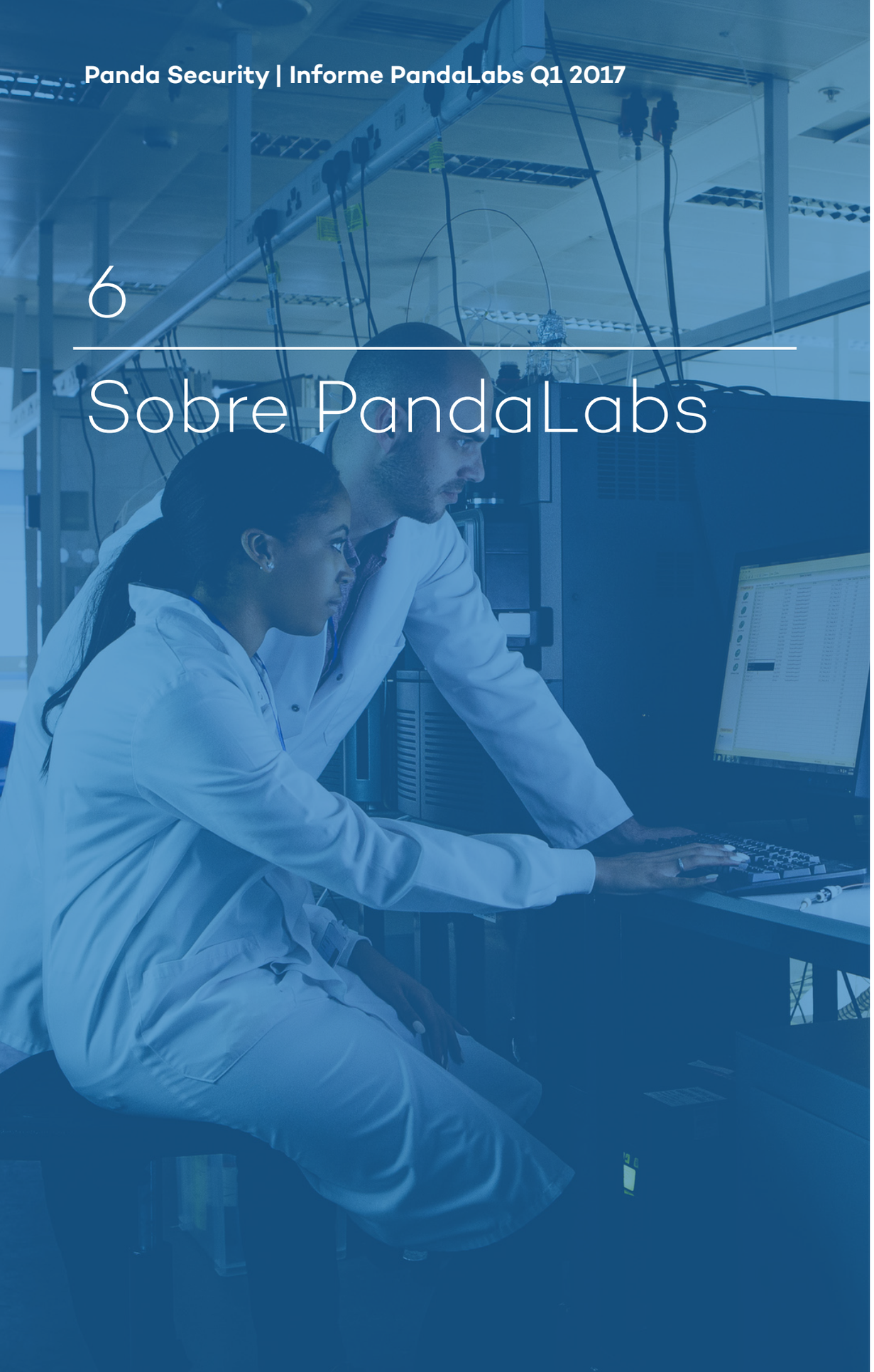
Lo más importante en caso de sufrir un ataque es contar con toda la información del mismo: qué ha pasado, cuándo, cómo, saber si ha habido robo de información, etc. La solución de seguridad que utilicemos debe ser capaz de proporcionarnos todos estos datos, tanto en tiempo real como a posteriori, de tal forma que podamos realizar análisis detallados de los incidentes.

Debemos a su vez tener listos planes de contingencia, pues tarde o temprano podemos ser víctimas de un ataque y reaccionar de forma adecuada puede minimizar los daños de forma espectacular.

Gobiernos y grandes empresas públicas y privadas ya están apostando por esta estrategia, convirtiendo a Adaptive Defense en la solución de seguridad mejor vendida de la historia de Panda Security. Multinacionales en todo tipo de sectores estratégicos (financieros, telecomunicaciones, militares, energía, etc.) confían en Panda Security para proteger sus sistemas con **Adaptive Defense.**

Desde PandaLabs os mantendremos informados de todas las novedades del mundo de la seguridad a través de nuestro Media Center.

6. SOBRE PANDALABS



6 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:

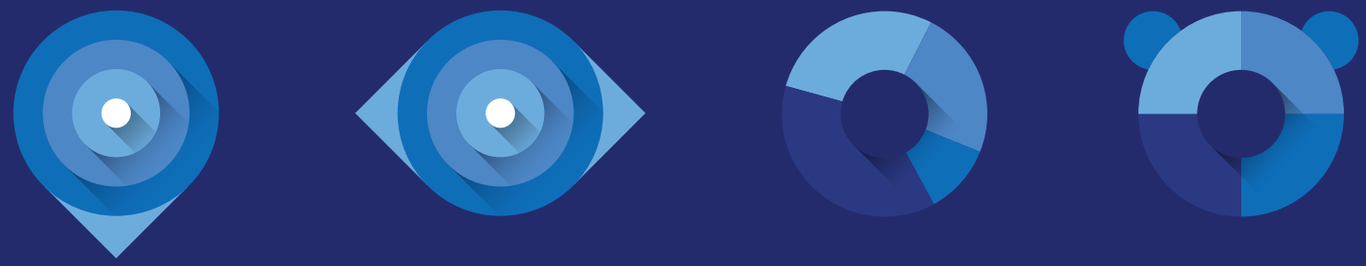
Desde **PandaLabs** se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.

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