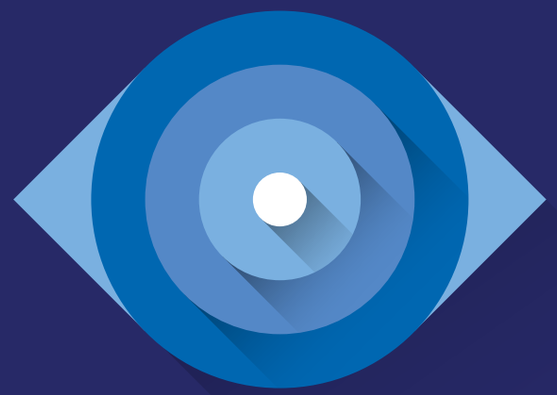
INFORME PANDALABS Q1 2016



panda

pandalabs

1. INTRODUCCIÓN

1 Introducción

Comienza el año 2016 cargado de novedades en el mundo de la seguridad. La creación de malware sigue batiendo récords con más de 20 millones de nuevas muestras identificadas por PandaLabs durante los tres primeros meses del año y una media de 227.000 al día.

Cada vez son más la empresas que están cayendo en las redes del ransomware, por lo que detallaremos todas las novedades ocurridas alrededor de este tipo de ataques que han ampliado sus objetivos (Linux, Mac y hasta páginas web). Veremos cómo se está pasando de rescates de unos pocos cientos de euros a millones y haremos un análisis de los ataques sufridos estos meses por hospitales.

Las infraestructuras críticas son un punto muy sensible y el foco de los cibercriminales desde hace tiempo. Uno de los mayores ataques se ha producido recientemente ha sido en Ucrania, donde en invierno los atacantes lograron –de forma remota- cortar el suministro eléctrico de más de 200.000 clientes durante horas.

Otro terreno vulnerable es del de los smartphones, donde los ataques siguen creciendo sin parar, al igual que en el también creciente sector del Internet de las Cosas, donde veremos cómo nos pueden atacar a través de algo aparentemente tan inocente como el timbre de la puerta.

2. EL TRIMESTRE EN CIFRAS

2

El trimestre en cifras

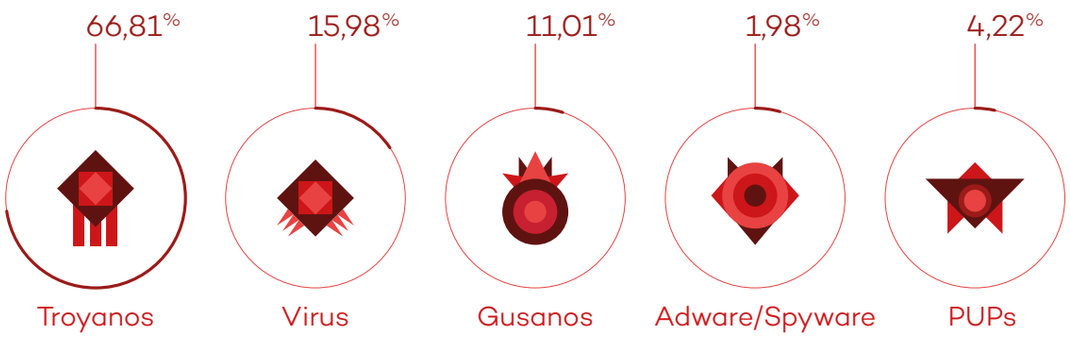
Comenzamos el año con más de 20 millones de nuevas muestras de malware detectadas y neutralizadas por PandaLabs, el laboratorio de Panda Security, con una media de 227.000 al día. Se trata de una cifra ligeramente superior a la encontrada en el mismo trimestre del 2015, donde la media de nuevas muestras se situó en 225.000 al día.

Dentro de todas las muestras de malware siguen destacando los troyanos, que llevan liderando estas estadísticas desde hace años.

Cabe destacar que los ataques de malware tipo ransomware –que se encuentran englobados en esta misma categoría- han aumentado notablemente.

A continuación mostramos los datos de la proporción de malware creado en 2015 por tipo:

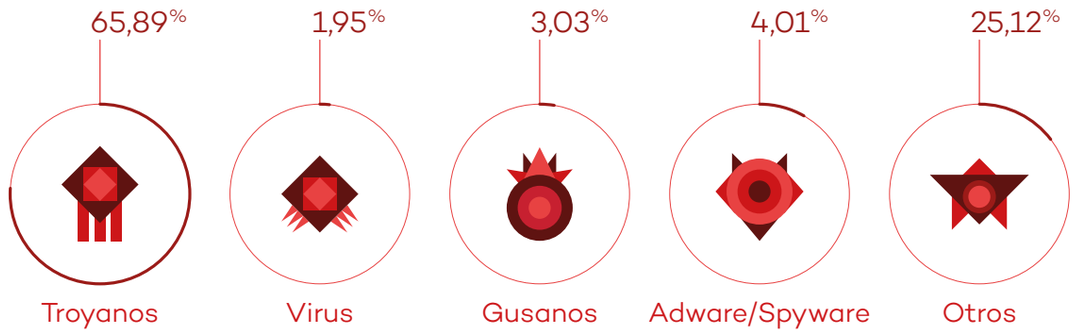
NUEVO MALWARE CREADO
EN EL PRIMER TRIMESTRE DE 2016, POR TIPO



Los troyanos están en primera posición con el 66,81% de las muestras creadas a lo largo del trimestre, aumentando respecto al año anterior. A continuación se sitúan los virus (15,98%), gusanos (11,01%), PUPs (4,22%) y Adware/Spyware con un 1,98%.

Al analizar las infecciones causadas por el malware en el mundo, gracias a los datos aportados por la Inteligencia Colectiva, vemos que las infecciones también están protagonizadas por los troyanos, con un 65,89% de los casos. Veamos cómo se reparten las infecciones en todas las categorías:

INFECCIONES POR TIPO DE MALWARE
EN EL PRIMER TRIMESTRE DE 2016



Es normal tener a los troyanos en primera posición, sobre todo teniendo en cuenta el auge en las infecciones de ransomware, uno de los ataques más populares perpetrados por los ciberdelincuentes ya que les permite obtener dinero de forma sencilla y segura para ellos. Los PUPs se posicionan en segundo lugar con un cuarto de las infecciones, muy por delante del Adware/Spyware (4,01%), gusanos (3,03%) y virus (1,95%). Las técnicas agresivas de distribución junto a programas de software legítimos utilizadas por los PUPs hacen que consigan un alto ratio de instalación en los ordenadores de los usuarios.

Si miramos al porcentaje global de ordenadores infectados, este es del 33,32%, cifra algo superior a la del año anterior, incremento debido tanto a los ataques de ransomware como

a los PUPs. Hay que destacar que se trata del porcentaje de ordenadores que han tenido algún tipo de encuentro con malware, lo que no significa necesariamente que se hayan infectado. A nivel geográfico los países más infectados del mundo están liderados por China, con un 51,35% de infecciones, seguida de Tuquía (48.02%) y Taiwán con un 41,24%.

A continuación, podemos ver los 10 países con mayor índice de infección:

PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

China	51,35%
Turquía	48,02%
Taiwán	41,24%
Ecuador	39,59%
Guatemala	38,01%
Rusia	37,98%
México	36,32%
Perú	36,02%
Polonia	35,55%
Brasil	34,00%

Asia y Latinoamérica son las regiones con mayores infecciones. El resto de países, con un porcentaje mayor a la media mundial, son Uruguay, (33,98%), Chile (33,88%), Colombia (33,54%) y España (33, 05%).

Si analizamos los datos de los países mejor posicionados, aquellos cuyo índice de infección es más bajo, podemos observar que prácticamente todos ellos son europeos.

Los países escandinavos, como es habitual, copan las primeras posiciones: Suecia se sitúa a la cabeza de la clasificación, con un 19,80% de infecciones, seguida de cerca por Noruega con un 20,23%; y Finlandia, con un 20,45% de infecciones.

A continuación podemos ver los 10 países con menor índice de infección:

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

Países Bajos	26,15%
Dinamarca	25,43%
Japón	24,99%
Alemania	23,64%
Reino Unido	23,61%
Bélgica	22,87%
Suiza	21,43%
Finlandia	20,45%
Noruega	20,33%
Suecia	19.80%

El resto de países con un porcentaje menor a la media mundial son Australia (26,79%), Francia (27,20%), Portugal (27,47%), Austria (28,69%), Canadá (30,30%), Estados Unidos (30,84%), Hungría (31,32%), Italia (32,48%), Venezuela (32,89%) y Costa Rica (33,01%).

3. EL TRIMESTRE DE UN VISTAZO

3

El trimestre de un vistazo

Comenzamos el repaso a lo sucedido durante estos meses inaugurando una nueva subsección dedicada en exclusiva al ransomware. Si bien es verdad que desde que estos ataques aparecieron los hemos tratado en nuestros informes, la prevalencia de los mismos continúa aumentando –especialmente en el entorno empresarial-, por lo que hemos decidido tratarlos de forma conjunta.

Ransomware

Una demostración de lo lucrativos que resultan estos ataques lo podemos ver en cómo se están diversificando las plataformas atacadas: además de los habituales (y mayoritarios) ataques a Windows hemos visto cómo salen nuevas variantes mejoradas del Linux/Encoder, que van a por servidores que utilizan el sistema operativo del pingüino. Mac tampoco se libra y hemos visto un ransomware basado en el Encoder, denominado KeRanger, que consiguió infectar a usuarios de Apple.

No obstante, los ataques ya no sólo van dirigidos a cifrar ficheros de los ordenadores, sino que han comenzado a atacar sitios web, cifrando su contenido.

En concreto hemos visto casos donde los atacantes hackeaban sitios web basados en Wordpress para, a continuación, cifrar los ficheros y modificar el index.php o el index.html con el contenido del mensaje que anuncia que tienes que pagar el rescate para recuperarlos.

Además han incluido una 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.

Los ataques a empresas están siendo cada vez más sofisticados. Ya no se conforman con atacar alguno de los ordenadores de una empresa. En los últimos tiempos hemos sido testigos de ataques donde, tras comprometer un servidor de la empresa, utilizaban movimientos laterales para infectar con ransomware tantos ordenadores de la red de la empresa como fuera posible, de tal forma que pueden pedir rescates muchos mayores.

La distribución del ransomware también aumenta y durante estos meses hemos visto casos donde se han utilizado páginas web de primera línea (The New York Times, BBC, MSN, AOL, etc.) para infectar a sus visitantes.

Las páginas web mencionadas no son hackeadas, sino que lanzan los ataques a través de los anuncios mostrados en las mismas, controlados por los ciberdelincuentes y que llaman a un servidor con algún tipo de exploit kit (Angler, etc.) que infectará a aquellos usuarios que no tengan todas sus aplicaciones convenientemente actualizadas.

Según una encuesta realizada por la Cloud Security Alliance, algunas empresas estarían dispuestas a pagar hasta un millón de dólares para poder recuperar sus datos. Aunque pueda parecer una cifra exagerada hay que tener en cuenta que algunos ataques no sólo cifran la información de la empresa, sino que pueden llegar a llevársela, lo que explica que algunas empresas estén dispuestas a pagar aunque dispongan de copias de seguridad para evitar que se haga pública la información robada.

En el mes de enero, The Economic Times publicó que en India tres bancos y una compañía farmaceútica habían sido objeto de un ataque de ransomware.

El ataque comenzó comprometiendo ordenadores de responsables de informática de las diferentes empresas para luego ir infectando el resto de ordenadores de cada compañía llegando a pedir un rescate de 1 Bitcoin por cada ordenador infectado, por lo que el total del rescate sería de varios millones de dólares.

Si hay un sector empresarial que está sufriendo este tipo de ataques es el hospitalario. En los últimos meses hemos visto cómo los casos se multiplicaban de manera alarmante. A continuación repasamos algunos de los casos más llamativos:

El Hollywood Presbyterian Medical Center de Los Ángeles declaró una “emergencia interna” y dejó a sus empleados sin acceso a los historiales médicos de sus pacientes, al correo electrónico y otros sistemas. Como consecuencia de esto algunos pacientes no pudieron recibir tratamiento y otros tuvieron que ser trasladados a diferentes hospitales.

El rescate solicitado por los ciberdelincuentes ha sido de 3,7 millones de dólares. Finalmente, el CEO del hospital llegó a un acuerdo y pagó unos 17.000$ para poder recuperar los ficheros secuestrados.

MedStar Health ha reconocido también que tuvo que desconectar algunos de sus sistemas en hospitales de Baltimore debido a un ataque similar.

El Methodist Hospital en Henderson, Kentucky, ha sido otra de las víctimas. En este caso también pagaron un rescate de 17.000$, aunque se comenta que el pago ha podido ser sensiblemente superior a esta cifra.

Prime Healthcare Management, Inc. Ha caído también en las redes de los cibercriminales con dos hospitales atacados (Chino Valley Medical Center y Desert Valley Hospital) y muchos otros afectados por el mismo ataque. En esta ocasión, la compañía no ha pagado ningún rescate.

No sólo hospitales norteamericanos son el objetivo, sino que en Europa hemos visto casos similares. Un ejemplo es el publicado en el Deutsche Welle, según el cual varios hospitales han sufrido ataques de ransomware, como el Lukas Hospital

en Neuss y el Klinikum Arnsberg en North Rhine-Westphalia. En ninguno de los dos casos, sin embargo, se ha pagado el rescate.

Cibercrimen

Facebook Neiman Marcus informó que las cuentas de algunos de sus clientes habían sido comprometidas por atacantes. El número de cuentas afectadas fue de 5.200. Al parecer la empresa no sufrió un robo de credenciales, sino que los atacantes utilizaron credenciales robadas a otras empresas e intentaban ver cuáles podían ser válidas en su servicio online.

Conocemos así la importancia de habilitar el segundo factor de autenticación que muchos servicios online ofrecen, ya que aunque en un momento dado nuestras credenciales se vean comprometidas, si no superan este segundo factor no podrán acceder a nuestra cuenta.

La cadena de hoteles Rosen Hotels & Resorts ha sido víctima de un ataque que ha estado activo desde septiembre de 2014 hasta febrero de 2016. La compañía ha alertado a sus usuarios que, en el caso de haber utilizado una tarjeta de crédito o débito en sus establecimientos durante esas fechas, sus datos podrían haber sido robados por los atacantes.

Un grupo hacktivista chileno ha robado datos de 304,189 chilenos de la base de datos de CONADI (Corporación Nacional de Desarrollo Indígena) organismo público dependiente del gobierno chileno. Los atacantes publicaron la base de datos junto con un mensaje donde denunciaban la pobre seguridad de los sistemas y exigían la dimisión de la presidenta chilena.

La norteamericana Verizon ha sido también víctima de un ataque en el que le han robado datos de un millón y medio de clientes. Según Brian Krebs, que ha destapado el caso, los ciberdelincuentes venden el total de la información robada por 100.000 dólares, dando también la opción de comprar “trozos” de la misma por 10.000 dólares.

Una nueva vulnerabilidad que afecta a OS X podría dar acceso total a un atacante. La vulnerabilidad permite saltarse la protección “System Integrity Protection” (SIP), introducida por primera vez en “El Capitan”.

Cuando hablamos de ataques de phishing solemos pensar en los típicos correos electrónicos que se hacen pasar por

nuestro banco para tratar de engañarnos y conseguir nuestras credenciales.

Sin embargo, hay intromisiones más sofisticadas y ambiciosas, como el que se ha conocido que sufrió 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. Tuvieron suerte, 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.

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.

21st Century Oncology Holdings, clínica especializada en tratamientos contra el cáncer con sede en Florida, avisó en marzo a 2,2 millones de pacientes y trabajadores que sus datos personales podían haber sido comprometidos.

El ataque tuvo lugar en octubre de 2015, pero el FBI pidió no hacer pública la información hasta que no avanzaran más en la investigación. Los atacantes accedieron y robaron datos personales (nombre, números de la seguridad social, diagnósticos, tratamientos, datos del seguro médico, tarjetas de crédito, etc.).

Algunos recordaréis al famoso "virus de la policía", precursor del ransomware actual, que haciéndose pasar por fuerzas de seguridad del país donde se encontraba el ordenador solicitaban una multa de unos 100€. Una de estas bandas fue desmantelada por la policía en España y este trimestre hemos conocido la condena que van a tener. La banda la conformaban 12 personas: el responsable de la organización, Alexander Krasnokutsy, ha sido condenado a seis años y su lugarteniente Dmytro Kovalchuk cumplirá tres años de condena. Por su parte, los hermanos Sergey e Ivan Barkov han pactado dos años y el resto de integrantes de la organización tendrán penas de hasta 6 meses de cárcel.

Si Flash es el complemento del navegador con más agujeros y más atacado por parte de ciberdelincuentes para infectar a nuevas víctimas, Java le sigue de cerca en segunda posición, y respecto a esto tenemos una buena noticia:

Oracle, la compañía detrás de Java ha anunciado que va a discontinuar el producto.

La última versión del plugin será publicada en septiembre de este año, y ya no publicarán más. Uno de los motivos que llevan a la compañía a tomar esta decisión es que los fabricantes de los principales navegadores o bien han dejado de soportar la tecnología de plugins por los problemas que genera (principalmente de seguridad) o bien ya tienen un calendario para dejar de soportarla.

En una operación sin precedentes, el FBI ha identificado a 1.500 personas que traficaban con pornografía infantil.

El año pasado incautaron los servidores de Playpen, una página situada en la Internet Oculta (Dark Web) publicada en agosto de 2014 y que permitía a usuarios registrarse y subir y descargar imágenes de esta temática. Este sitio ha llegado a tener 225.000 usuarios registrados. Lo que hizo el FBI fue durante dos semanas seguir con el sitio web pero desde sus propios servidores y utilizando herramientas que les permitían identificar, entre otras cosas, la dirección IP de quien la visitaba.

Si bien averiguar la dirección IP de un visitante de una página web normal es algo trivial, en el caso de la Internet Oculta es algo mucho más complejo, de hecho la herramienta utilizada hackeaba a los visitantes de Playpen a través de vulnerabilidades que existen en algunos navegadores específicos para la Internet Oculta. Una vez accedido al ordenador que visitaba la página, la herramienta capturaba información del mismo (dirección IP, dirección MAC, versión del sistema operativo, nombre de usuario, etc.).

Hablando de hackeos por parte de fuerzas de seguridad, en Alemania el Ministerio de Interior ha autorizado el uso de troyanos para acceder tanto a ordenadores como a smartphones de sospechosos. El troyano ha sido desarrollado

por la propia policía y les dará acceso tanto a comunicaciones que se producen como a ficheros.

Móviles

Es habitual que hablemos de vulnerabilidades en móviles y este trimestre no sólo no es una excepción, sino que hemos podido ver vulnerabilidades que afectan a estos dispositivos desde diferentes ángulos: software instalado por un fabricante, el procesador del dispositivo, el sistema operativo...

SNAP es el nombre de una vulnerabilidad 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.

Metaphor es el nombre de una vulnerabilidad dada por la compañía NorthBit a una vulnerabilidad que permite hackear terminales Android tan sólo en 10 segundos tras visitar una página web que contiene un fichero multimedia malicioso.

Muchos aficionados a la tecnología reconocerán el nombre Snapdragon, seguramente el procesador más conocido de Qualcomm que es utilizado en más de mil millones de dispositivos, principalmente en móviles. Nuestros colegas de Trend Micro encontraron dos vulnerabilidades en estos procesadores que permiten a un atacante obtener acceso root al dispositivo. Google ha sacado una actualización que soluciona el problema.

Internet of Things

El Tal y como hemos contado en informes anteriores, la seguridad del Internet de las Cosas deja mucho que desear. Algunos fabricantes comienzan a concienciarse del problema, de hecho el gigante General Motors acaba de lanzar un nuevo programa de recompensas para hackers que sean capaces de encontrar vulnerabilidades en sus vehículos. Esto, que es normal en compañías tecnológicas (Microsoft, Google, Facebook, etc. tienen este tipo de programas desde hace años) es una novedad en compañías tradicionales como las automovilísticas, por lo que la iniciativa de General Motors es una gran noticia.

El fabricante de coches japonés Nissan ha deshabilitado una aplicación que permite a los propietarios de coches eléctricos Nissan LEAF controlar la calefacción y el aire acondicionado de sus vehículos.

Todo ha venido por un investigador australiano que ha descubierto que podía controlar desde la misma aplicación estas funciones en cualquier Nissan LEAF simplemente con su VIN (vehicle identification number, número de identificación del vehículo).

Poco a poco van introduciéndose nuevos aparatos inteligentes en nuestra casa. La empresa Ring tiene un timbre de puerta que cuenta con cámara, sensor de movimiento, y conexión WiFi. La compañía Pen Test Partners estuvo estudiando una de las unidades y descubrieron que simplemente accediendo al botón de setup del dispositivo podían llegar a obtener las credenciales de la red WiFi a donde estaba conectado. El fabricante respondió rápidamente con una nueva versión del firmware del dispositivo que solucionaba el problema.

Ciberguerra

Investigadores rusos del Industrial Controls Systems Supervisory Control and Data Acquisition (ICS/SCADA) han publicado un listado de equipamiento industrial que vienen con las mismas contraseñas por defecto para forzar a los fabricantes a implementar mejores controles de seguridad. El listado ha sido bautizado como “SCADAPass”,y contiene las credenciales por defecto de más de 100 productos de fabricantes como Allen-Bradley, Schneider Electric, y Siemens.

Y es que este tipo de productos son los que, en muchos casos, se utilizan en instalaciones críticas que pueden ser objetivo de ataques. De hecho, a finales de 2015 hubo un incidente en Ucrania que finalmente se ha demostrado como un ciberataque a la infraestructura eléctrica del país.

En concreto 225.000 clientes de una zona de Ucrania se quedaron sin electricidad (con lo que esto supone en pleno invierno) debido a este ciberataque. El ataque ha sido relacionado con un grupo de ciberdelincuentes rusos conocidos como “Sandworm”.

El Departamento de Defensa estadounidense ha presentado un programa piloto de recompensas llamado “Hack the Pentagon”, donde se ofrecerán recompensas a los hackers que logren

Todo el mundo puede ser víctima de un robo de información y esto incluye también a grupos terroristas como el ISIS.
Un desertor se llevó consigo un a memoria USB con datos de 22.000 miembros de ISIS que antes de unirse al grupo deben rellenar un formulario con toda esta información.

Tres grupos de atacantes latinoamericanos consiguieron comprometer los servidores de correo del ejército boliviano, descargándose los correos electrónicos que posteriormente publicaron en parte. Consiguieron acceder a la información fácilmente a través de un antiguo agujero de seguridad en el servicio Zimbra de VMWare que los responsables de seguridad del ejército no habían parcheado.

En marzo, la agencia de inteligencia de Corea del Sur denunció un ataque en el que habían comprometido 40 teléfonos móviles de agentes de seguridad del país, acusando a Corea del norte del ataque. Días después el gobierno norcoreano negó que ellos fueran los responsables.

4. CONCLUSIÓN

4 Conclusión

Como habéis podido ver, el año ha empezado fuerte. Seguiremos de cerca la evolución del ransomware, ya que todo apunta a que seguirá con nosotros durante mucho tiempo. Además, debemos estar muy atentos al avance de Internet de las Cosas y los múltiples problemas de seguridad que rodea a todos estos dispositivos.

Esperamos que este informe os haya sido de utilidad y seguiremos informando desde nuestro blog en http://www.pandasecurity.com/spain/mediacenter/ y en próximos informes.

5. SOBRE PANDALABS

5 Sobre PandaLabs

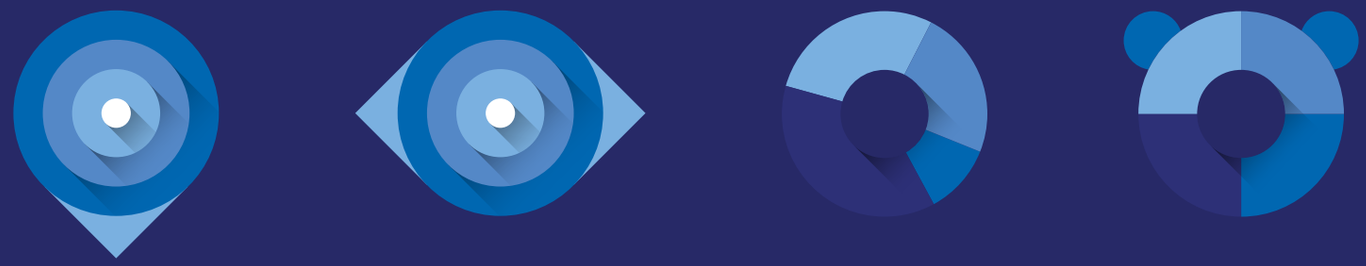
PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- 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