INFORME PANDALABS Q1 2015

Enero - Marzo 2015

panda

pandalabs

panda

pandalabs

1. INTRODUCCIÓN

1 Introducción

Comienza un año que promete ser apasionante en el mundo de la seguridad que nos ocupa. Si creéis que el mundo de Internet sólo os afecta en las pequeñas cosas, es hora de cambiar el chip. Como ejemplo os podemos citar la histórica decisión del gobierno estadounidense de imponer sanciones a Corea del Norte en respuesta al ciberataque del que Sony fue víctima el año pasado.

El mundo de la ciberdelincuencia no para, y tiene a las empresas en su punto de mira.

Gran parte de los ataques de ransomware que se han producido estos meses están dirigidos a empresas. En este informe os contaremos algún caso llamativo donde incluso instituciones públicas han cedido al chantaje y han optado por pagar un rescate para recuperar su información.

Siguen además produciéndose ataques a grandes cuentas con robos masivos de información. Hemos sabido que el famoso ataque de Target, por el que fueron comprometidas más de 40 millones de tarjetas de crédito de sus clientes, costará a la empresa la friolera cifra de 191 millones de dólares. La compañía Anthem, víctima también de otro ataque durante este trimestre, tendrá que afrontar gastos por unos 100 millones de dólares como consecuencia del mismo.

En medio de todo este maremágnum, la creación de ejemplares de malware sigue batiendo récords.

Durante los tres primeros meses de 2015 han aparecido más de 20 millones de nuevas muestras, alcanzando una media diaria de 225.000.

2. EL TRIMESTRE EN CIFRAS

2 El trimestre en cifras

El primer trimestre de 2015 comienza con un notable aumento en la creación de malware.

Si acabamos el año 2014 con una media de 205.000 nuevos ejemplares de malware al día, durante estos últimos tres meses la cifra ha aumentado hasta 225.000, con lo que la cantidad total de nuevas amenazas generadas durante este periodo supera los 20 millones.

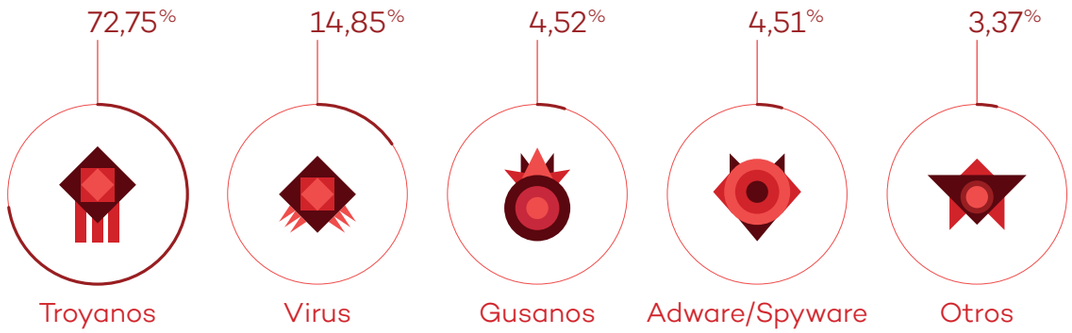
Como es habitual, la mayoría de estos ejemplares son variantes conocidas de malware modificadas por sus creadores parar tratar de evitar su detección por parte de los laboratorios antivirus.

Los troyanos son el tipo de malware más común, sumando un 72,75% de todas las muestras aparecidas durante este periodo.

En segundo lugar -a gran distancia- se sitúan los clásicos virus, que alcanzan un 14,85%.

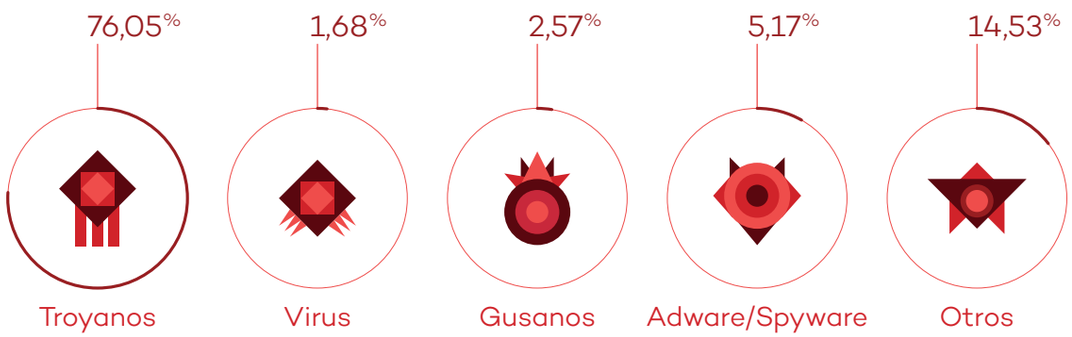
Estos son los datos de malware creado en este trimestre:

NUEVO MALWARE CREADO
EN EL PRIMER TRIMESTRE DE 2015, POR TIPO



Si analizamos las infecciones que han tenido lugar en el mundo divididas por tipo de malware, observamos que, como es lógico, las cifras son similares a las de nuevos ejemplares de malware creado. Sólo encontramos una excepción en la categoría “Otros”, cuyo porcentaje es superior en esta estadística:

INFECCIONES POR TIPO DE MALWARE
EN EL PRIMER TRIMESTRE DE 2015



El ratio de infecciones a nivel mundial ha sido de un 36,51%.

Este dato refleja el número de ordenadores protegidos por Panda que han tenido un encuentro con malware, lo que no implica que hayan sido infectados. En cuanto a los datos registrados en los diferentes países, China, una vez más, se sitúa en cabeza, con un 48,01% de las infecciones. Le siguen Turquía (43.33%) y Perú (42,18%).

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

PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

China	48,01%
Turquía	43,33%
Perú	42,18%
Bolivia	41,45%
Rusia	41,38%
Argentina	41,03%
Ecuador	40,57%
Taiwán	40,21%
El Salvador	39,89%
Guatemala	39,58%

Como podemos observar, el top de países con mayor ratio de infección está copado por países asiáticos y latinoamericanos. Otros países con un nivel de casos que superan la media mundial son: Polonia (39,48%), Brasil (39,21%), Eslovenia (39,05%), Colombia (38,86%), España (38,37%), Costa Rica (38,19%), Chile (38,05%) e Italia (37,97%).

Veamos a continuación los países menos infectados del mundo:

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

Portugal	27,83%
Bélgica	27,39%
Países Bajos	26,96%
Alemania	26,52%
Francia	25,87%
Reino Unido	25,11%
Suiza	24,61%
Japón	23,97%
Suecia	22,42%
Noruega	22,07%

Europa es la zona del mundo donde el índice de infección es más bajo, con 9 países en este ranking.

Noruega (22,07%), Suecia (22,42%) y Japón (23,97%) son los países menos infectados a nivel mundial.

Otros países que no han conseguido posicionarse en este Top 10, pero que sí han logrado situarse por debajo de la media mundial de infecciones, son: Dinamarca (28,18%), Finlandia (28,59%), Panamá (29,77%), Canadá (30,03%), Austria (30,55%), Uruguay (32,15%), Venezuela (33,35%), Australia (33,54%), Estados Unidos (34,03%), Chequia (35,46%), México (35,31%) y Hungría (35,99%).

Y así es como queda el mapa de calor según las infecciones sufridas en todo el mundo:

Como podemos ver, los puntos calientes del mapa se concentran en Asia y América del Sur. Mientras que las zonas más seguras son Europa y Japón.

3. EL TRIMESTRE DE UN VISTAZO

3

El trimestre de un vistazo

A continuación repasamos algunas de las noticias más relevantes sucedidas en el mundo de la seguridad durante este primer trimestre del año.

Los ciberdelincuentes no dejan de lanzar ataques con un mismo motivo: conseguir dinero.

Un objetivo que pretenden conseguir bien mediante el robo de información (lo que explica el creciente número de intrusiones en empresas para hacerse con todos los datos que puedan, tanto de clientes como internos), bien mediante la extorsión directa (lo que explica por qué los ataques de ransomware están en auge).

Cibercrimen

Si hay que destacar algún tipo de ataque durante este inicio de 2015, sin duda alguna debemos hablar del ransomware, también conocido como Cryptolocker.

Este tipo de ataques afectan a todo el mundo, pero hemos visto cómo los delincuentes se centran en las empresas, ya que poseen información valiosa por la que están dispuestos a pagar un módico rescate. Se sabe que las compañías víctimas, siempre que no cuenten con algún tipo de copia de seguridad, en muchas ocasiones acaban pagando el rescate para poder recuperar la información.

En febrero supimos que una comisaría de policía de Illinois pagó hasta 500 dólares para recuperar la información de uno de sus ordenadores que había sido víctima de uno de estos ataques.

Los ciberdelincuentes utilizan diferentes técnicas para infectar y robar información de los usuarios. Una de las vías de entrada más comunes es la utilización de exploits, programas que explotan vulnerabilidades de programas instalados en las máquinas de sus víctimas.

En enero se supo que a su arsenal acababan de incorporar un nuevo exploit que afectaba a Flash Player. En este caso se trataba de una vulnerabilidad zero-day (día cero), lo que significa que era completamente desconocida y no existía actualización para corregirla en el momento de su descubrimiento.

Flash es uno de los componentes más atacados y que más vulnerabilidades tiene.

Casi al nivel de Java, otro de los grandes agujeros de seguridad presente en nuestros ordenadores.

Cuando hablamos de phishing muchas veces lo relacionamos con mensajes que tratan de hacerse pasar por nuestro banco. Si bien los ataques de phishing comenzaron así, y aún hoy en día siguen siendo muy numerosos, las empresas cuyos clientes son objetivo de estos ataques no se limitan a entidades financieras.

En enero, ciberdelincuentes lanzaron un ataque de phishing haciéndose pasar por Apple.

El remitente era “Apple Support”, y como asunto utilizaba un truco recurrente: asustar al usuario con un supuesto problema de seguridad: “Tu ID de Apple ha sido suspendido”.

El mensaje indicaba que alguien había tratado de acceder a tu cuenta desde un dispositivo no autorizado, y que iban a proceder a bloquearla. Para demostrar que efectivamente eras el usuario legítimo de la cuenta te proporcionaban un enlace que lleva a una página con el look & feel de Apple y en la que pedían gran cantidad de información: nombre completo, dirección, teléfonos, datos de tarjeta de crédito, etc.

En febrero la compañía norteamericana Anthem reconoció que fue víctima de un ataque en el que le robaron datos de 80 millones de clientes. Los ciberdelincuentes pudieron acceder a una base de datos gracias al uso de una contraseña robada con acceso al sistema. Se calcula que el coste del ataque para Anthem podría llegar a los 100 millones de dólares.

En marzo, la compañía norteamericana Slack envió un mensaje a todos sus usuarios indicando que habían detectado accesos no autorizados a una de sus bases de datos que contiene información del perfil de sus clientes. Aunque no fue robada información crítica (de hecho la compañía decía específicamente en su mensaje que no hacía falta cambiar la contraseña del servicio), se habilitó un sistema de doble factor de autenticación (2FA), recomendándose a todos sus usuarios que lo habilitaran para aumentar su protección.

Redes sociales

En enero, al mismo tiempo que Obama daba a conocer una serie de iniciativas legislativas para ayudar en la lucha contra la ciberdelincuencia, un grupo de atacantes relacionados con ISIS se hicieron con el control de las principales cuentas de redes sociales del pentágono.

Uno de los ataques más extendidos que suceden hoy en día en Facebook es el que trata de regalarnos tarjetas de alguna empresa popular.

En enero fuimos testigos de uno de estos engaños en el que en cuestión de horas cayeron miles de personas de todo el mundo. En este caso crearon un evento en Facebook prometiendo repartir 430 tarjetas regalo de ZARA de 500€ cada una. Para participar en el supuesto sorteo debías unirte al evento, escribir en tu muro “Gracias Zara”, e invitar a 50 de tus contactos. En muy poco tiempo más de 5.000 personas se habían unido, enviándose más de 124.000 invitaciones.

Móviles

Comenzamos este año con una amenaza que en buena medida nos recuerda a los antiguos gusanos de correo electrónico o de mensajería instantánea, apoyándose esta vez en los SMS.

El ataque comienza cuando recibes un SMS preguntándote si esa es tu foto, y un enlace a la supuesta fotografía.

Dicho enlace realmente descarga un fichero .APK, aplicación para móviles Android. Si el usuario la instala, la aplicación maliciosa enviará un SMS idéntico al recibido a toda tu lista de contactos.

Ciberguerra

Por primera vez en la historia, Estados Unidos impuso sanciones a un país en respuesta a un ciberataque. El país en cuestión era Corea del Norte, debido a su implicación en el ataque contra Sony a finales de 2014, que se cree motivado por el estreno de la película The Interview, una comedia donde la CIA pedía a unos periodistas asesinar al líder norcoreano.

Siguen publicándose nuevos datos de los documentos filtrados por Edward Snowden a la prensa. En enero, el diario alemán Der Spiegel daba a conocer que China se había hecho con Terabytes de datos sobre el caza F-35, incluyendo información sobre el sistema de radar, esquemas de los motores, etc.

4. CONCLUSIÓN

4 Conclusión

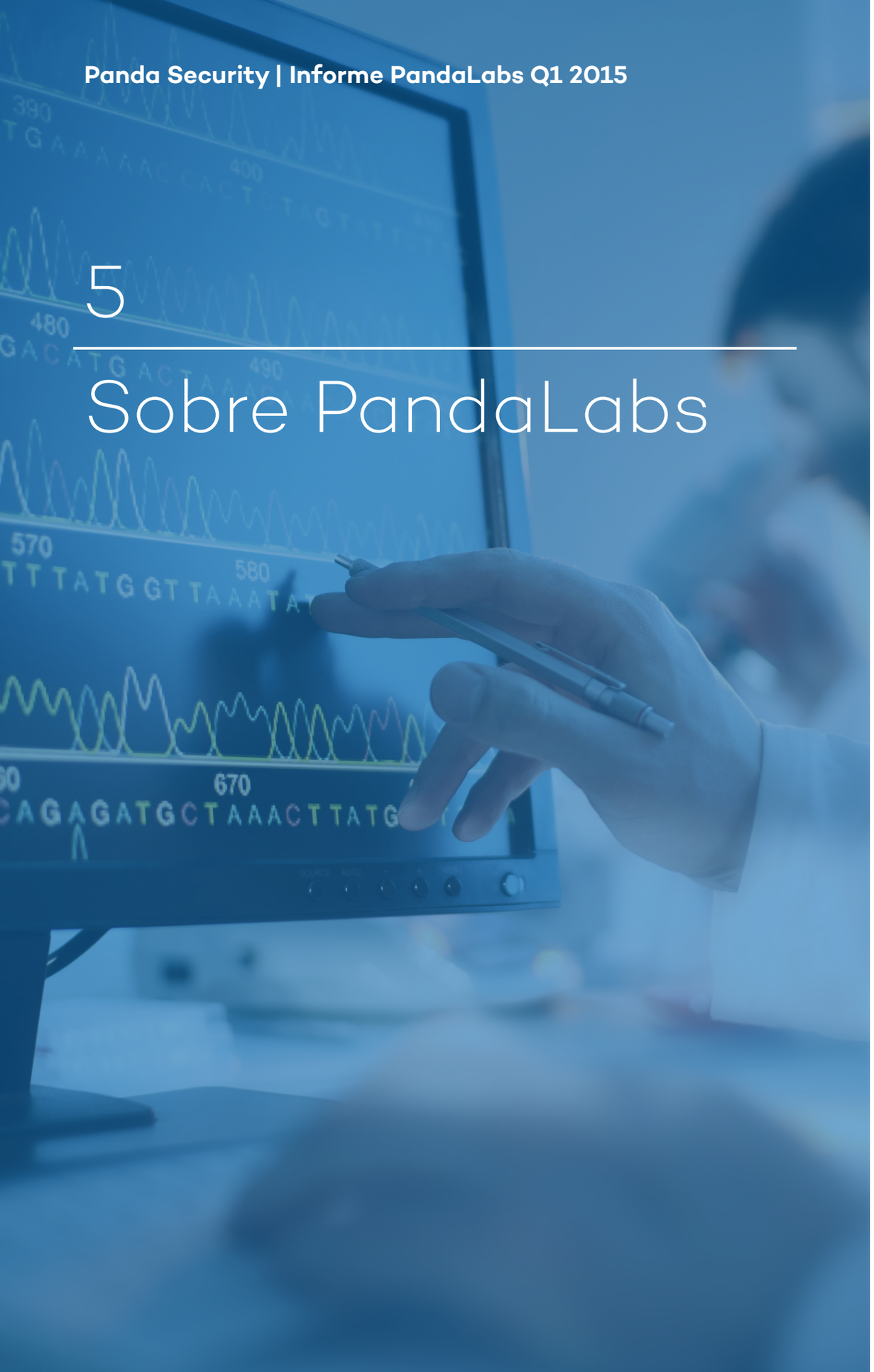
El año 2015 ha comenzado con fuerza en el mundo de la seguridad, tal y como preveíamos. El número de nuevos ejemplares de malware creados llega ya a los 225.000 al día, cifra estratosférica aunque no tiene visos de dejar de aumentar.

Los ataques a compañías tanto para chantajearlas con ransomware como para robarlas información continúan en auge, siendo necesario para las mismas aumentar las medidas de seguridad que toman. Tener el parque informático actualizado y con antivirus es necesario pero no suficiente, hay que adaptarse al tipo de ataques a los que nos enfrentamos con las herramientas adecuadas. Es necesario conocer el estado de seguridad de nuestra red y tener un control absoluto de todas las aplicaciones que se ejecutan en la misma.

Volveremos con nuestro próximo informe dentro de tres meses, mientras tanto podéis informaros de las principales novedades en:

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

5. SOBRE PANDALABS



5 Sobre PandaLabs

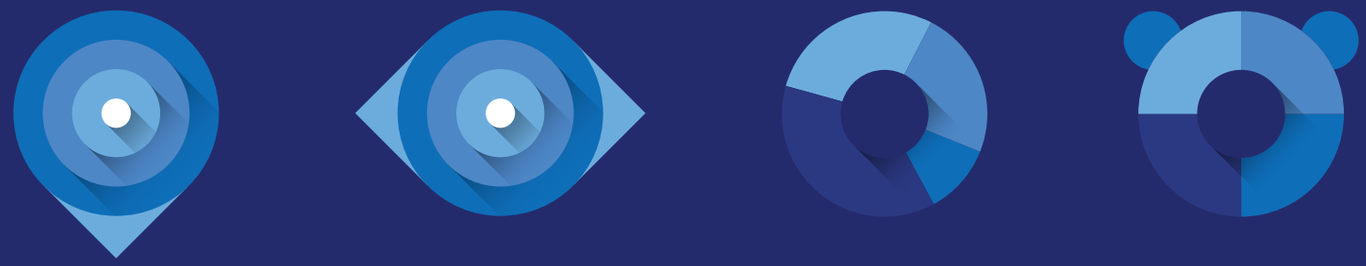
PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- 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