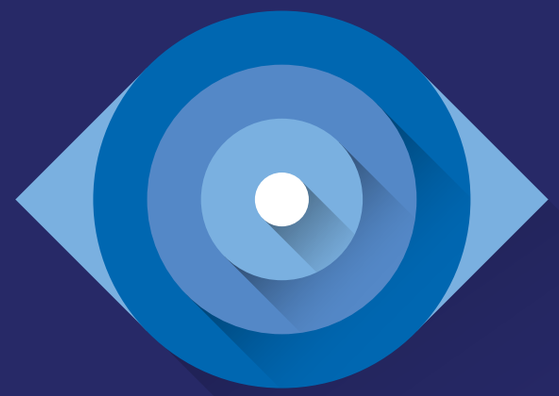
INFORME PANDALABS Q3 2015



panda

pandalabs

1. INTRODUCCIÓN

1 Introducción

Los últimos meses de 2015 no están dando tregua y la aparición de 21 millones de nuevos ejemplares de malware durante el tercer trimestre, es una buena muestra de ello. Durante estos meses hemos visto múltiples casos de empresas comprometidas, siendo los más llamativos el de Ashley Madison y el de Hacking Team.

La creciente tensión en el mundo de la ciberguerra y del ciberespionaje se pone de manifiesto con las acusaciones cruzadas entre las grandes potencias, principalmente Estados Unidos, Rusia y China.

Por otro lado, tenemos que destacar los múltiples problemas de seguridad que hemos visto este trimestre en dispositivos móviles, tanto en Android como en iOS.

Además, Internet de las Cosas va apareciendo como un nuevo vector de ataque.

Durante los meses de julio, agosto y septiembre destacan las vulnerabilidades que han sido encontradas en diferentes vehículos, uno de los cuales permitía tomar completamente el control del mismo de forma remota.

2. EL TRIMESTRE EN CIFRAS

2

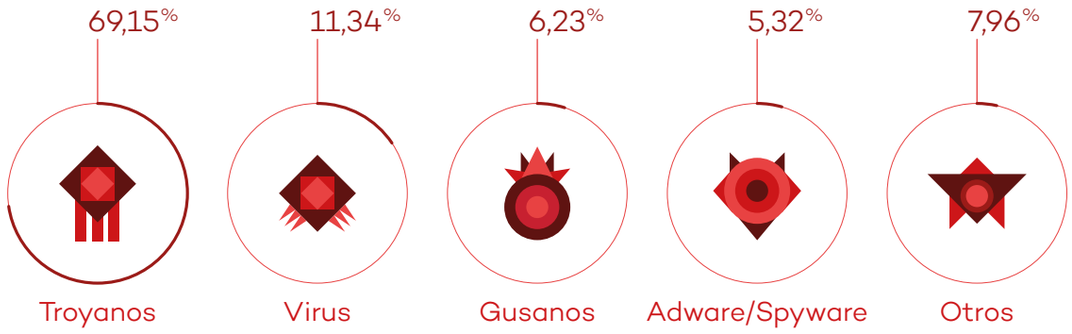
El trimestre en cifras

Durante la época estival suele bajar levemente el número de nuevos ejemplares de malware creados, pero no ha sido así este año. Se han vuelto a registrar 21 nuevos millones de amenazas, con una media de 230.000 al día.

Los troyanos son el tipo de malware más común, sumando un 69,15% de todas las muestras aparecidas durante este periodo. En segundo lugar –a gran distancia- se sitúan los clásicos virus, que alcanzan un 11,34%.

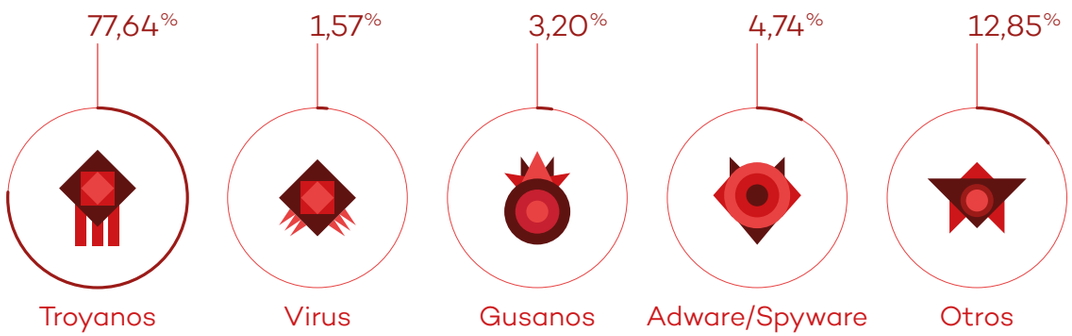
Estos son los datos de malware creado en este trimestre:

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



En la categoría “Otros” se integran diferentes tipos de posibles amenazas, la más prevalente son los PUP (programas potencialmente no deseados). Si analizamos las infecciones que han tenido lugar en el mundo divididas por tipo de malware, observamos que las cifras son cifras similares a las de nuevos ejemplares de malware creado, excepto en la categoría “Otros”, cuyo porcentaje es superior en esta estadística:

INFECCIONES POR TIPO DE MALWARE
EN EL TERCER TRIMESTRE DE 2015



El ratio de infecciones a nivel mundial ha sido de un 32,12%.

Este dato refleja el número de ordenadores protegidos por Panda Security 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 45,35% delas infecciones. Le siguen Perú (42,89%) y Turquía (40,99%).

A continuación, mostramos el top 10 de países con mayor ratio de infección:

PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

China	45,35%
Turquía	42,89%
Perú	40,99%
Rusia	38,32%
Taiwán	37,82%
Bolivia	37,13%
Guatemala	36,75%
El Salvador	35,32%
Ecuador	35,02%
Argentina	34,78%

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 (34,54%), Brasil (34,32%), Eslovenia (33,98%), Colombia (33,11%), España (32,50%), Costa Rica (32,33%), Chile (32,19%) e Italia (32,15%).

Veamos a continuación los países menos infectados del mundo:

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

Portugal	26,38%
Países Bajos	26,22%
Bélgica	25,96%
Francia	25,02%
Alemania	24,87%
Reino Unido	24,17%
Suiza	22,75%
Japón	23,57%
Suecia	21,33%
Noruega	20,12%

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

Noruega (20,12%), Suecia (21,33%) y Japón (22,75%) 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 (26,50%), Finlandia (26,78%), Panamá (27,01%), Canadá (27,42%), Austria (28,53%), Venezuela (29,25%), Uruguay (29,54%), Australia (29,92%), Estados Unidos (30,13%), Chequia (30,46%), México (31,76%) y Hungría (32,02%).

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

3. EL TRIMESTRE DE UN VISTAZO

3

El trimestre de un vistazo

Cibercrimen

Uno de los ataques más mediáticos de este periodo ha sido sin duda el de la empresa de contactos Ashley Madison. Los atacantes, autodenominados “Impact Team”, mostraron un mensaje en su página web exigiendo que cerraran el negocio o que publicarían toda la información robada. Poco después, al no ceder la empresa al chantaje, publicaron un torrent con 10 Gb de información comprimida.

Entre la información publicada se encontraban los datos de sus 37 millones de clientes, transacciones realizadas, direcciones de correo, preferencias sexuales, etc. Además, también contenía todo tipo de documentación interna de la empresa.

Durante este trimestre no han dejado de aparecer nuevas vulnerabilidades utilizadas por ciberdelincuentes como medio para acceder a sus víctimas. Además de las (tristemente)

típicas aparecidas en Flash o en Java, el sistema operativo de Apple Mac OS X ha sufrido un par de ellas de mucha gravedad:

la primera de ellas, descubierta por el investigador Stefan Esser, permitía tener acceso root y ya se ha visto utilizada por Adware como método de ataque en ordenadores Mac.

La segunda vulnerabilidad fue descubierta por investigadores de la compañía MyK. Se trataba de una vulnerabilidad en el sistema de administración de contraseñas que podría permitir a un atacante obtener todas las credenciales almacenadas.

Uno de los métodos de ataque que más se están popularizando es el que trata de comprometer routers de hogares y empresas, de tal forma que quedan bajo el control del atacante. Se ha descubierto que routers de las empresas ASUS, DIGICOM, Observa Telecom, PLDT y ZTE incluyen credenciales predefinidas en su código. Esto permitiría a atacantes a hacerse con el control de los mismos desde el exterior. Hay que recordar que los ataques que lanzaron un DDoS contra Xbox Live y PSN en navidades de 2014 utilizaron un ejército de routers infectados que tenían bajo su control.

Adobe Flash, conocido por sus casi infinitos agujeros de seguridad, podría morir en breve.

iOS no permitía su ejecución desde los inicios del sistema operativo y en Android tampoco se ejecuta. Ahora Google ha dado un paso más y bloquea todo el contenido Flash que haya en una web si se navega desde su navegador Chrome. Y el gigante de las ventas online Amazon también ha anunciado que prohíbe en su plataforma cualquier anuncio desarrollado en este problemático formato.

El FBI ha detenido a 5 individuos que estuvieron envueltos en el hackeo sufrido por JPMorgan en 2014.

En este ataque consiguieron hacerse con las credenciales de un empleado, y luego fueron utilizadas para acceder a 90 servidores de la compañía y robar información perteneciente a 76 millones de individuos y 7 millones de empresas, todos ellos clientes de la entidad.

Microsoft, en su estrategia de mejora de la seguridad de sus productos y soluciones, ha decidido doblar la máxima recompensa que da a investigadores capaces de descubrir nuevos errores críticos en sus soluciones, pasando de 50.000 a 100.000 dólares.

Si bien este tipo de recompensas es habitual en empresas tecnológicas, aún no lo es tanto en otros sectores, aunque cada vez son más las empresas que recurren a este tipo de técnicas para que los investigadores que descubran algún problema se lo comuniquen a ellas antes de vender la información a otro postor. Es el caso de United Airlines, la aerolínea con base en Chicago, que tiene la peculiaridad de dar recompensas en millas. Ha reconocido que ha llegado a dar hasta un millón de millas a investigadores que les han informado de errores para que pudieran ser solucionados.

El FBI también ofrece recompensas, aunque en este caso están dedicadas a quienes colaboren con información que ayude a detener a los ciberdelincuentes más buscados. La recompensa más alta es de 3 millones de dólares para cualquiera que pueda ayudar a capturar a Evgeniy Mikhailovich Bogachev, la mente criminal que está tras la red de bots Gameover ZeuS.

Redes sociales

Facebook anunció que estaba estudiando incorporar un botón de “No me gusta”, y, como era de esperar, los ciberdelincuentes se pusieron manos a la obra para ser los primeros en darnos esta opción.

En pocas horas comenzaron a aparecer todo tipo de engaños prometiendo añadir el famoso botón, buscando en todos los casos víctimas a las que poder robar información.

Móviles

En julio, la empresa Zimperium dio a conocer una gravísima vulnerabilidad en Android que afecta a 950 millones de dispositivos con este sistema operativo.

La gravedad no sólo reside en la cantidad de móviles, tablets y demás aparatos afectados, sino en lo sencillo que resulta comprometer de forma remota cualquiera de ellos.

Simplemente enviando un MMS malicioso puedes hacerte con el control de cualquier teléfono, por lo que sólo haría falta poseer el número de teléfono de la víctima. Ni siquiera es necesario abrir dicho MMS, ya que Android procesa las imágenes de forma automática, así que sólo con recibirlo ya puede infectar nuestro terminal.

Aunque se ha corregido el problema, la gran cantidad de diferentes fabricantes y versiones del sistema operativo que existen en el mercado hacía temer que la solución no fuera aplicada a un gran número de terminales.

Sin embargo Google ha convencido a la mayoría de grandes fabricantes (Samsung, Sony, LG, Motorola, etc.) para que pongan esta actualización a disposición de sus clientes. Además tanto Google como Samsung anunciaron que ofrecerán actualizaciones mensuales a sus clientes para soluciones las diferentes vulnerabilidades que vayan apareciendo en Android.

De hecho, poco después, dos investigadores del equipo XForce de IBM publicaron otro problema de seguridad que permitía a un atacante sustituir una aplicación legítima instalada por una maliciosa, de tal forma que esta última podría tener acceso a todos los permisos de la que estaba sustituyendo. Google ya ha publicado la actualización que soluciona este nuevo problema de seguridad.

Estamos ya acostumbrados a ver ataques de ransomware en PC y, cada vez más, a los intentos que se hacen en Android, de hecho uno aparecido durante estos meses llamó la atención por su originalidad a la vez que simpleza.

Lo que hace la aplicación maliciosa es cambiar el código PIN del terminal y solicitar un rescate de 500 dólares.

En cualquier caso, este tipo de estrategia tiene sus limitaciones. Por ejemplo, los usuarios de nuestro antivirus para Android pueden cambiar el código PIN de su móvil desde su panel de control web desde otro lugar, anulando el ataque de los ciberdelincuentes sin tener que pagar un solo dólar.

El sistema operativo móvil de Apple también ha sufrido numerosos ataques durante estos meses.

La compañía Appthority ha descubierto una vulnerabilidad bautizada como Quicksand que afecta a las instalaciones y despliegues corporativos que hacen uso de sistemas MDM (Mobile Device Management) y que podría permitir el acceso a información confidencial de la compañía. Apple lo ha solucionado a partir de la versión de iOS 8.4.1.

Otra vulnerabilidad solucionada con esa actualización se llama Ims0mnia, que permite a una aplicación maliciosa evitar las restricciones de ejecución en segundo plano de Apple. Por ejemplo, se podría activar en segundo plano el micrófono y la cámara del usuario para espiarle.

Apple tuvo que retirar numerosas aplicaciones de su App Store debido a un ataque conocido como XcodeGhost. Los atacantes publicaron una versión modificada del software de desarrollo de aplicaciones para iOS, de tal forma que aquellos desarrolladores que lo utilizaron para desarrollar sus apps incluían funcionalidad maliciosa sin su conocimiento.

Otro ataque sufrido por usuarios de Apple consiguió credenciales de iCloud de 225.000 usuarios. El ataque afecta a usuarios que previamente habían hecho un jailbreak de su dispositivo, lo que elimina controles de seguridad instalados en iOS y es utilizado por usuarios para instalar aplicaciones sin tener que hacer uso de la App Store.

Internet of Things

En julio, HP Fortify publicó los resultados de un estudio realizado sobre smartwatches, donde encontraron que el 100% de los dispositivos analizados eran vulnerables a ataques.

Si bien cualquier dispositivo puede ser vulnerable a ataques en un momento dado, en este estudio daban pistas de los principales problemas encontrados. Por ejemplo, ninguno de los smartwatches disponía de doble autenticación a la hora de vincularlo a un móvil, y permitían meter contraseñas equivocadas de forma repetida.

Los investigadores de seguridad Charlie Miller y Chris Valasek hicieron una demostración en julio que dejó a todo el mundo boquiabierto.

Convencieron a Andy Greenberg, periodista de Wired, para que condujera un Jeep Cherokee mientras los 2 investigadores le hackeaban el coche desde la casa de uno de estos.

El ataque comenzó mostrando la toma de control de algunos elementos del coche no críticos: encendieron el aire acondicionado al máximo, activar el limpiaparabrisas, cambiar la emisora de radio y subir el volumen, poner una foto suya en la pantalla del coche... hasta desactivar el aceleradoro los frenos y llegando a tener un control total del coche.

Llevaban varios meses trabajando en estos ataques, y de hecho se los habían comunicado al fabricante en 2014, lo que le había dado la oportunidad de publicar una actualización que solucionara el problema. Los investigadores hablaron más en detalle del problema en la charla que dieron en agosto en la BlackHat, una de las conferencias de seguridad más importantes del año que tiene lugar en Las Vegas.

También en julio Land Rover avisó que debía actualizar 65.000 vehículos por un fallo en el software de determinados modelos que llevaban a la venta desde 2013 y que permitía que se pudieran desbloquear las puertas.

Los investigadores Kevin Mahaffey y Marc Rogers mostraron en Defcon, conferencia de seguridad que tiene lugar a continuación de la BlackHat, cómo hackear un Tesla Model S. Si bien necesitaban acceso físico al coche para poder llevar a cabo este ataque, descubrieron 6 nuevas vulnerabilidades que les permitían incluso parar el motor cuando se circulaba a baja velocidad. El fabricante ya ha publicado la actualización que parchea las 6 vulnerabilidades.

Ciberguerra

Hacking Team es una empresa conocida por ser proveedora de herramientas de ciberespionaje y ciberataque para multitud de gobiernos de todo el mundo.

En julio sufrieron un hackeo masivo en el que les robaron todo tipo de información. El ataque se dio a conocer a través de la propia cuenta de Twitter de Hacking Team, también comprometida por el atacante, en la que se cambió su nombre a “Hacked Team” y se daba un enlace para poder descargar por torrent la información sustraída:

Se hicieron públicos listados de clientes (agencias de policía y de inteligencia de multitud de países, desde Estados Unidos a Uzbekistán). Se hizo público un certificado corporativo de desarrollador utilizado por Hacking Team, contraseñas que utilizaban en sus sistemas más protegidos, listas de productos que vendían, código fuente de sus aplicaciones, datos financieros, etc. Incluso se publicó una web con un buscador que permitía hacer una búsqueda entre todos los correos electrónicos que tenían almacenados en Hacking Team.

Pocos días después se descubrió un zero day en Adobe Flash gracias a la información robada a Hacking Team.

James Comey, director del FBI, dijo en un foro de seguridad que habían detectado un creciente interés por parte de terroristas sobre estrategias para lanzar ataques ciberterroristas contra Estados Unidos. No especificó el tipo de ataques y dijo que parecía que estaban todavía en los inicios de planificación, tratando de ver cómo de efectivos podrían llegar a ser, pero que se trata de un problema que puede ir a más.

El 25 de julio, hackers rusos consiguieron comprometer el sistema de correo electrónico no clasificado del Pentágono, del que robaron información. Según fuentes oficiales se trató de un ataque muy sofisticado y que claramente había algún gobierno detrás del mismo.

En septiembre, investigadores de DGI publicaron un trabajo sobre la unidad del ejército chino 78020, donde mostraban que era quien estaba detrás del grupo conocido como Naikon, que está detrás de diferentes ataques de ciberespionaje con objetivos militares, diplomáticos y económicos en diferentes países de la zona. Entre sus víctimas a lo largo de cinco años se encuentran Camboya, Indonesia, Laos, Malasia, Myanmar, Nepal, Filipinas, Singapur, Tailandia, Vietnam, el Programa de Desarrollo de Naciones Unidas y la Asociación de Naciones del Sudeste Asiático.

4. CONCLUSIÓN

4 Conclusión

Ya casi estamos terminando 2015 y podemos comprobar que se han ido cumpliendo las previsiones que hicimos hace casi un año. Por primera vez hemos incluido en el informe un apartado donde se reflejan los problemas de seguridad de dispositivos IoT, con smartwatches y coches como protagonistas.

El robo de información de empresas no deja de suceder, y eso que sólo podemos reflejar aquellos casos que son más llamativos. Las empresas deben estar preparadas para poder protegerse y mitigar los ataques a los que están siendo sometidas.

Volveremos con nuestro próximo informe dentro de tres meses, mientras tanto podéis informaros de las principales novedades en http://www.pandasecurity.com/spain/mediacenter/

5. SOBRE PANDALABS

5 Sobre PandaLabs

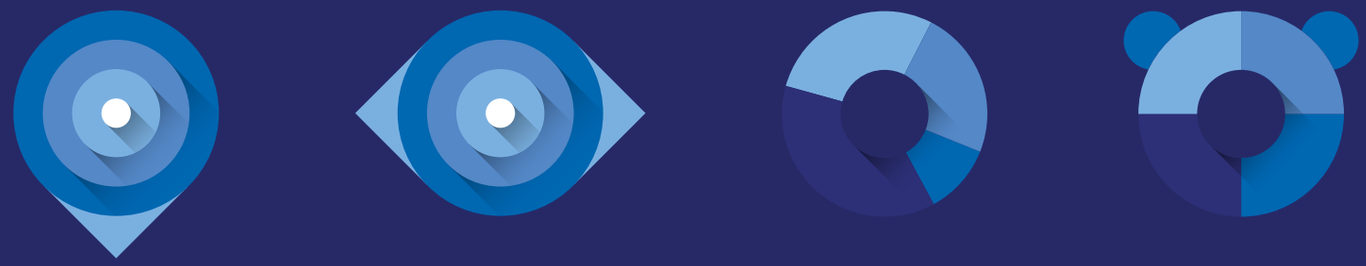
PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- 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