INFORME PANDALABS Q2 2015

Abril- Junio 2015

panda

pandalabs

1. INTRODUCCIÓN

1 Introducción

El mundo de la seguridad no nos da descanso, el número de ejemplares de malware sigue aumentando sin cesar, con 21 millones de nuevos ejemplares creados durante estos tres meses.

Los casos de ransomware siguen multiplicándose, y todos los días diferentes grupos de atacantes lanzan nuevas campañas con miles de usuarios y empresas como objetivo.

Las empresas están sufriendo ataques constantes, y en este informe os contaremos algunos de los mayores ataques sucedidos durante este periodo, con robos masivos de información afectando a millones de personas.

En el mundo del ciberespionaje y de la ciberguerra siguen sucediendo ataques de todo tipo.

Hemos visto como la Casa Blanca fue atacada, el parlamento alemán. Hemos visto ataques perpetrados por el Estado Islámico o por defensores del régimen Sirio.

2. EL TRIMESTRE EN CIFRAS

2 El trimestre en cifras

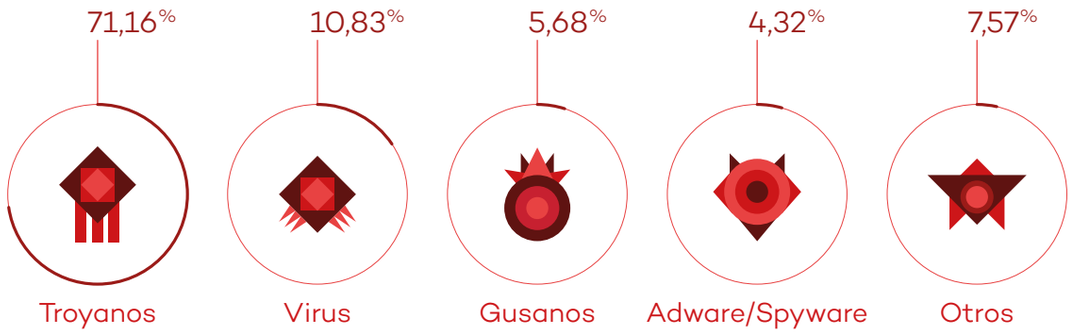
Continúa el crecimiento en la creación de ejemplares de malware, alcanzando este segundo trimestre de 2015 con una media de 230.000 nuevos ejemplares de malware al día, con más de 21 nuevos millones de amenazas generadas durante estos tres meses.

El gran número de ejemplares de malware son principalmente variantes o mutaciones de ejemplares de malware de familias ya conocidas. Los ciberdelincuentes multiplican la variedad de muestras para tratar de evitar su detección por parte de los laboratorios antivirus.

Los troyanos son el tipo de malware más común, sumando un 71,16% de todas las muestras aparecidas durante este periodo. En segundo lugar –a gran distancia- se sitúan los clásicos virus, que alcanzan un 10,83%.

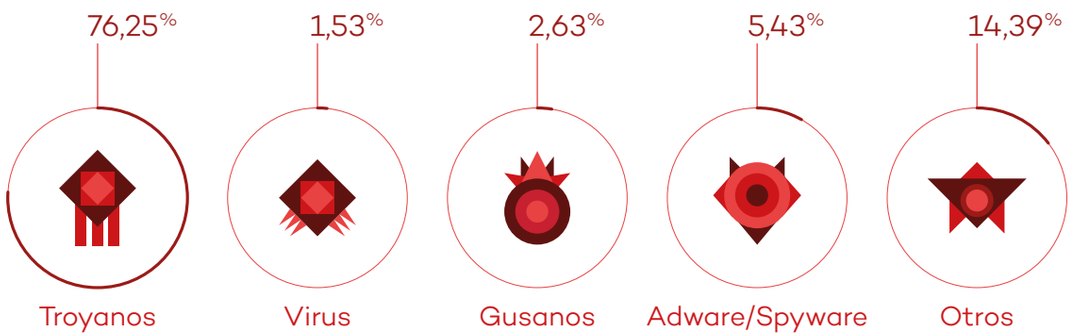
Estos son los datos de malware creado en este trimestre:

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



En la categoría otros se integran diferentes tipos de posibles amenazas, siendo la más prevalente los PUP (programas potencialmente no deseados). Si analizamos las infecciones que han tenido lugar en el mundo divididas por tipo de malware, observamos que, como es lógico, las cifras son cifras 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 SEGUNDO TRIMESTRE DE 2015



El ratio de infecciones a nivel mundial ha sido de un 33,21%.

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 47,53% delas infecciones. Le siguen Perú (43,11%) y Turquía (41,97%).

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

PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

China	47,53%
Turquía	43,11%
Perú	41,97%
Rusia	41,15%
Argentina	40,93%
Bolivia	40,13%
Taiwán	39,57%
Guatemala	39,21%
El Salvador	39,02%
Ecuador	38,89%

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 (38,48%), Brasil (38,21%), Eslovenia (38,05%), Colombia (37,86%), España (36,37%), Costa Rica (35,19%), Chile (34,05%) e Italia (33,97%).

Veamos a continuación los países menos infectados del mundo:

PAÍSES CON MENOR ÍNDICE DE INFECCIÓN EN ESTE TRIMESTRE

Países Bajos	27,83%
Portugal	27,39%
Bélgica	26,96%
Francia	26,52%
Alemania	25,87%
Reino Unido	25,17%
Suiza	24,41%
Japón	23,57%
Noruega	22,22%
Suecia	21,57%

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

Suecia (21,57%), Noruega (22,22%) y Japón (23,57%) 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 (28,95%), Panamá (29,57%), Canadá (29,95%), Austria (30,53%), Venezuela (31,15%), Uruguay (31,35%), Australia (31,54%), Estados Unidos (32,03%), Chequia (32,46%), México (32,76%) y Hungría (33,01%).

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 segundo trimestre del año.

El ransomware tipo CryptoLocker sigue campando a sus anchas causando estragos, especialmente a las empresas que están en el punto de mira de los ciberdelincuentes ya que muchas de ellas optan por pagar el rescate para recuperar su información.

Hablaremos también de WhatsApp, la popular aplicación de mensajería instantánea que los ciberdelincuentes están utilizando cada vez más como gacho para engañar a sus víctimas, el creciente número de empresas que están siendo comprometidas y las últimas noticias sobre ciberespionaje.

Cibercrimen

Una de las “nuevas” técnicas (rescatadas del baúl de los recuerdos, ya que los primeros ataques de este tipo se registraron hace casi 20 años) por parte de los ciberdelincuentes para engañar e infectar a usuarios con ramsomware es el uso de macros en documentos de Office (principalmente de Word).

La mayoría de usuarios tienen la falsa sensación de seguridad de que un documento de texto no va a contener ningún tipo de amenaza.

Sabiendo esto y siendo conscientes de que los filtros perimetrales no actúan contra este tipo de ficheros, se han

incrementado de forma sustancial los ataques utilizando esta mecánica.

El punto débil de este ataque es que el usuario debe habilitar las macros, sin embargo los ciberdelincuentes son perfectamente conscientes de esto y han conseguido elaborar técnicas de ingeniería social realmente ingeniosas.

Una que descubrimos desde PandaLabs se trataba de un documento de Word que contenía una imagen difuminada.

En la parte superior del documento en mayúsculas y negrita aparecía un mensaje indicando que por motivos de seguridad la imagen estaba difuminada, y que si se quería acceder a la información se debían habilitar las macros, con una flecha apuntando al botón que se debía pulsar en Word para acceder a la activación de las mismas. Una vez activada la macro, te muestra la imagen sin difuminar mientras que al mismo tiempo te infecta con una variante de CryptoLocker.

Otro ransomware se ha hecho bastante popular, principalmente en Australia, aunque posteriormente se ha visto en otros países, debido a que usaba imágenes de la conocida serie de televisión Breaking Bad.

Ryanair, la conocida aerolínea de bajo coste, fue víctima de un ataque en el que le sustrajeron cinco millones de dólares. Si bien no se han desvelado los detalles de cómo consiguieron los atacantes realizar el robo, se sabe que se produjo a través de una transferencia a un banco chino. La compañía denunció el caso e informó que habían conseguido congelar el dinero robado y que esperaban recuperarlo pronto.

La compañía norteamericana CareFirst BlueCross BlueShield, aseguradora médica, fue víctima de un ciberataque en el que le robaron información de 1,1 millones de clientes.

Cada vez las empresas están más en el punto de mira de delincuentes para robar información de forma masiva, y este simplemente es un ejemplo de los cientos de casos que suceden en todo el mundo.

AdultFriendFinder, una compañía de contactos online, sufrió un ataque en el le robaron los datos de sus usuarios, y los atacantes la ofrecieron online al primero que pagara 70 bitcoins, unos 17.000 dólares al cambio en ese momento. Al poco tiempo la base de datos al completo fue publicada en Internet.

LastPass, compañía líder en gestores de contraseñas, fue otra de las víctimas de un ataque en el que le robaron información. Afortunadamente parece que los atacantes no lograron información de las contraseñas, aunque consiguieron los hashes de las contraseñas maestras de sus usuarios.

El complejo cálculo de estos hashes (salteados, con múltiples pasadas) hace muy complicado que los atacantes pudieran llegar a descubrir la contraseña real, a pesar de lo cual es recomendable cambiarla si utilizamos una contraseña débil.

El Hard Rock Hotel & Casino de Las Vegas comunicó que han estado comprometidos durante ocho meses durante los cuales los atacantes pudieron robar información de sus clientes, como sus nombres, números de tarjeta de crédito y débito y los códigos CVV de las mismas. Afectó a los clientes que pagaron en restaurantes, bares y tiendas del complejo, aunque no a los sistemas de pago del hotel y del casino.

Este ataque recuerda a otros que hemos visto en el pasado (Target, Home Depot, UPS, Neiman Marcus) donde los terminales de punto de venta fueron infectados para robar la información de las tarjetas utilizadas por los clientes.

Hubo rumores de que Uber había sido víctima de un ataque tras detectarse que usuarios de este servicio habían visto como desconocidos hacían uso de sus cuentas. Sin embargo parece que todo fue debido a ataques de phishing donde los usuarios facilitaron sus credenciales a los atacantes tras ser engañados.

A finales de junio 1.400 pasajeros de la aerolínea polaca LOT quedaron en tierra en el aeropuerto Chopin de Varsovia tras un ataque perpetrado contra el sistema informático de tierra de la compañía utilizado para confeccionar los planes de vuelo.

Redes sociales

Todas las conexiones del usuario con los servidores de Facebook, incluidos los mensajes que envías y recibes, se transmiten ya mediante el protocolo seguro HTTPS. Por si esto fuera poco, la red social también estableció su servicio en la red Tor para que los usuarios más exigentes en materia de privacidad pudieran estar tranquilos. Sin embargo, además de las conexiones que establecen los usuarios a través del propio servicio, hay otras comunicaciones que se realizan vía Facebook de forma indirecta, a través de correo electrónico. Son las notificaciones que te llegan, por ejemplo, cuando un amigo te ha enviado un mensaje directo (salvo que lo hayas desactivado).

Como la seguridad de estos mensajes no estaba tan garantizada, Facebook ha anunciado que, a partir de ahora, todos sus usuarios podrán recibirlos – si así lo deciden – protegidos por el popular software de cifrado Pretty Good Privacy (PGP).

PGP oculta los emails de cara a los posibles intrusos a partir de un sistema de claves basado en una pública (que debe tener el emisor del mensaje) y otra privada (que solo tienes el receptor).

El proceso de configuración es sencillo: Acceder a nuestro perfil, entrar en el apartado ‘Información‘ e ir a ‘Información básica y de contacto’, donde podremos introducir aquí nuestra

clave pública PGP (si no sabes qué es o cómo conseguirla, lo mejor es que leas un tutorial), que se mostrará en el perfil, a disposición de cualquiera que desee mandarnos un correo electrónico cifrado.

Debajo del cuadro veremos una casilla que tendremos que marcar si queremos que todos los correos que nos envíe Facebook, a partir de ahora, también incorporen esta capa de seguridad. Como siempre que se emplea el cifrado, es muy importante que recordemos la clave que establecimos para proteger nuestro correo electrónico con PGP. Si algún día la olvidáramos, no podríamos leer las notificaciones de Facebook, y podríamos llegar a perder nuestra cuenta en la red social.

WhatsApp es un gancho habitual para atraer usuarios y tratar de infectarles. Hemos detectado un bulo con el que pretenden enganchar a los usuarios de la aplicación de mensajería instantánea.

En concreto, se llama WhatsApp Trendy Blue. Una nueva "versión" que promete nuevas opciones de personalización de WhatsApp cuando, en realidad, lo único que hace es suscribir al usuario a un servicio de tarificación especial, no precisamente barata.

Este programa exige que la invitación de, al menos, 10 de nuestros contactos a los que les llegará nuestro mensaje para que se inscriban en esta web fraudulenta.

Móviles

Fujitsu, en colaboración con la operadora japonesa NTT Docomo, ha lanzado su terminal Arrows NX F-04G basado en Android, y se ha convertido en el primer móvil Android que incluye como capa de seguridad el escaneo del iris, un método biométrico mucho más seguro y fiable que el popularizado lector de huellas dactilares que utilizan terminales populares de la competencia, como el Apple iPhone 6 o el Samsung Galaxy S6.

En junio detectamos una campaña de phishing dirigida a desarrolladores de Android que publican sus creaciones en Google Play, la tienda de apps oficial del popular sistema operativo. El campo "De" del mensaje dice "Play Developer Support", con el asunto "Update your Account Informations". Al pinchar en el enlace proporcionado, eres redirigido a una página web que parece de Google, donde te solicitan las credenciales.

Los ataques de phishing están diseñados para robar las credenciales y la identidad del usuario, por eso son extremadamente populares los ataques dirigidos a clientes de entidades financieras y de todo tipo de plataformas de pago.

Este caso, sin embargo, es diferente ya que no están buscando vaciar la cuenta bancaria del usuario, quieren esas credenciales porque pueden usarlas para propagar malware a través de Google Play.

Lo más preocupante es lo fácil que resultaría para los delincuentes el automatizar todo este proceso. Lo único que necesitan es:

- Construir una "araña" (crawler, hay unos cuantos proyectos de código abierto que les pueden ayudar en esta tarea) para descargarse información de todas las apps publicadas en Google Play.
- Analizar toda esa información para obtener las direcciones de correo de los diferentes desarrolladores.
- Enviar una campaña personalizada de phishing, incluso la página web podría ser personalizada para el desarrollador específico, hacienda que el engaño sea mucho más creíble y obtener un mejor "ratio de conversión".
- Como el atacante tiene la información de todas las apps publicadas por cada desarrollador, podría desarrollar un sistema de alarma que le alertara cada vez que un desarrollador con una app popular (millones de descargas) hubiera caído en la trampa.

Desde este punto, uno de los más fáciles (y poco sofisticados) ataques sería publicar apps maliciosas desde esa cuenta. Imaginad que alguien consigue robar las credenciales de los desarrolladores de Candy Crush y publicaran Candy Crush 2 desde la misma cuenta... Si los atacantes fueran más hábiles y encontraran una forma de modificar la aplicación sin utilizar la llave privada (que no puede ser obtenida con las credenciales robadas), podrían publicar y actualizar cualquier app. En el ejemplo anterior, imaginad que los atacantes crean una actualización de Candy Crush que incluye un troyano: cientos de millones de usuarios se lo descargarían e instalarían sin sospechar nunca que están siendo comprometidos.

Google ha creado crea un nuevo programa bajo el nombre de Android Security Rewards que recompensará las contribuciones de los investigadores de seguridad que descubran nuevas vulnerabilidades en Android.

La cuantía de la de recompensa se basa en la gravedad de las vulnerabilidades, la cantidad base son 2.000 dólares para vulnerabilidades críticas, 1.000 para las de gravedad alta, y 500 para las moderadas. Sin embargo, en función de la gravedad del problema, la calidad del informe, etc. pueden subir hasta los 38.000 dólares.

Ciberguerra

El viceconsejero de Seguridad Nacional de la Casa Blanca, Ben Rhodes, comunicó que la Casa Blanca había sido víctima de un ataque informático.

En una entrevista con CNN, Rhodes afirmó que los atacantes obtuvieron acceso no autorizado al sistema no clasificado de los ordenadores y robaron información de gran importancia, aunque el sistema clasificado no fue hackeado. Lo que no quiso confirmar Rhodes es si el ataque había sido realizado por hackers rusos ni cuándo había tenido lugar, pero sí dio a entender que no se había producido durante los últimos días. Sin querer entrar en más detalles, durante su intervención comentó que ya tomaron "una serie de medidas de seguridad para evaluar y mitigar los daños".

En junio supimos que la Office of Personnel Management (OPM), agencia del gobierno federal estadounidense de recursos humanos fue comprometida y robaron información personal de al menos 4 millones de trabajadores públicos.

El ataque tuvo lugar 2 meses antes, aproximadamente al mismo tiempo que la Casa Blanca fue comprometida. Sin embargo parece que ambos ataques no están conectados, ya que este último parece ligado claramente a atacantes chinos, aunque el gobierno no hizo ninguna declaración oficial al respecto.

Simpatizantes de ISIS atacaron a la cadena de televisión francesa TV5MONDE, consiguiendo sabotear la emisión. No sólo consiguieron esto, sino que tomaron el control tanto de su página web como de su página de Facebook.

El conocido grupo Syrian Electronic Army consiguió comprometer la página web de la armada de Estados Unidos, publicando contenido propagandístico a favor del régimen sirio de Assad.

El parlamento alemán fue víctima de un ataque donde consiguieron comprometer diferentes ordenadores y llegaron a robar información de los mismos. Se cree que el ataque vino de Rusia, aunque es difícil que se pueda llegar a demostrar quién estuvo realmente detrás del mismo.

Hemos conocido que la NSA utilizó una versión modificada de Stuxnet para sabotear el programa nuclear de Corea del Norte, aunque en esta ocasión no tuvieron éxito. Hay que recordar que con Stuxtet lograron destruir al menos 1.000 centrifugadoras de uranio de una planta en Natanz, Irán.

4. CONCLUSIÓN

4 Conclusión

Los ataques están a la orden del día, más que nunca las empresas deben estar preparadas para esta avalancha masiva de robo de información. Deben reforzar sus equipos y soluciones de seguridad, tener claro que sólo con un antivirus no es suficiente y que ha llegado el momento de adoptar defensas avanzadas que complementen la seguridad de sus redes y les permitan bloquear y detectar cualquier intrusión, obteniendo información forense de cualquier incidente que suceda en sus estaciones de trabajo y servidores.

Los costes económicos asociados a estos ataques no dejan de aumentar, por lo que en los próximos meses / años veremos un cambio de filosofía que las empresas más concienciadas están ya aplicando actualmente.

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

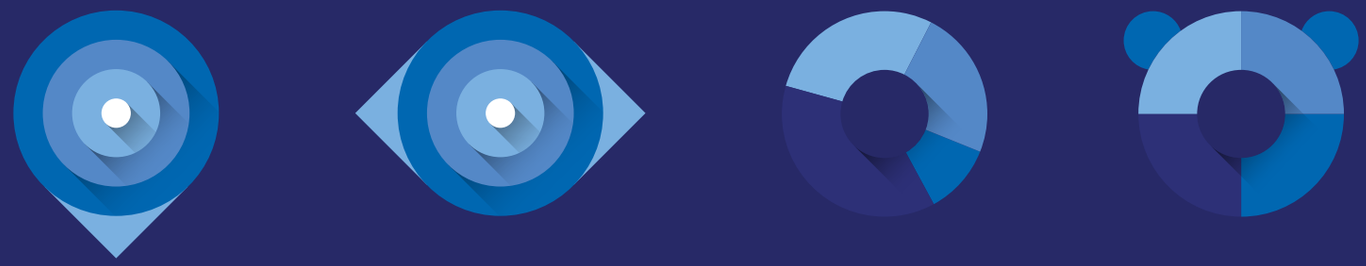
PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- 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