INFORME TRIMESTRAL PANDALABS

ABRIL-JUNIO 2013

PANDA SECURITY

01| Introducción

En este informe vamos a analizar las cifras de malware que arrojan nuestros sistemas de análisis de malware desde la nube, donde veremos cómo los ciberdelincuentes no dejan de aumentar su actividad y crean cada vez más ejemplares de malware tratando de colapsar los laboratorios de las compañías antivirus.

Repasaremos diferentes ataques de los que hemos sido testigos durante estos tres meses de 2013, como los hackeos de cuentas de Twitter protagonizados por la "Syrian Electronic Army". Analizaremos uno de los últimos ataques de malware a la plataforma Android, y analizaremos también las cifras que muestran un preocupante aumento exponencial de malware para el popular sistema operativo de Google.

En el ámbito de la ciberguerra / ciberespionaje hablaremos de algunos de los casos más llamativos del trimestre, y veremos qué hay de cierto en una de las noticias que más ha dado que hablar, donde la NSA podría estar espiando indiscriminadamente a usuarios de las principales plataformas online del mundo, desde Facebook hasta Skype.

02| El trimestre de un vistazo

En muchas ocasiones los ciberdelincuentes tratan de aprovecharse de diferentes eventos, fechas señaladas, o noticias de gran impacto para tratar de propagar malware y conseguir nuevas víctimas.

CIBERCRIMEN

Comenzamos este trimestre con buenas noticias, cuando se supo que la policía rusa y ucraniana había detenido al líder de la banda de ciberdelincuentes responsable de la red de bots Caberp, junto con otras 20 personas que formaban parte del equipo de desarrollo del malware. Esta fue una acción conjunta de las fuerzas de seguridad rusas y ucranianas. El líder de la banda tiene 28 años y se trata de un ciudadano ruso que reside en Ucrania.

Pudimos ver que durante el 2º trimestre de 2013 utilizaron el atentado sucedido durante el **Maratón de Boston** para enviar spam con dicha temática. Los mismos ciberdelincuentes aprovecharon también el accidente ocurrido en una planta de fertilizantes en Tejas para lanzar el mismo tipo de ataque.

El atentado sucedido durante el **Maratón de Boston** fue utilizado por ciberdelincuentes para propagar malware a través de mensajes de spam hablando del suceso

Otro tipo de ataque utilizando fechas señaladas fue el que tuvo lugar el 1 de Mayo, Día Internacional de los Trabajadores. La página web del ministerio de trabajo estadounidense (US Department of Labor) fue comprometida ese mismo día y comenzó a propagar malware.

Cuando hablamos de ciberdelincuentes infectando los ordenadores de usuarios para robar sus datos y enriquecerse, lo primero que nos viene a la mente es el robo de las credenciales de banca online para hacerse pasar por nosotros y vaciar nuestras cuentas bancarias. Sin embargo hay otros tipos de robo, más imaginativos, que aunque parecidos tienen lugar en mundos virtuales. En este caso, **World of Warcraft**, el MMORPG más jugado del mundo, vio como ciberdelincuentes comenzaron a robar oro de las cuentas de diferentes jugadores, desaparecían millones de piezas de oro. Al investigar, se vio que alguien había utilizado ese oro para comprar diferentes ítems a través de la casa de subastas del juego. Finalmente se descubrió que los atacantes habían utilizado un error en la aplicación web y de móvil que permite acceder a la casa de subastas.

Un error en la aplicación para móviles **World of Warcraft** Armory fue utilizado por ciberdelincuentes para robar millones de piezas de oro

La federación de pequeñas empresas (FSB, Federation of Small Businesses) británica emitió un informe donde revelaba que el 41% de las pequeñas empresas habían sufrido ataques por parte de ciberdelincuentes a lo largo del año 2012, con un coste de 785 millones de libras.

El gobierno norteamericano protagonizó durante el 2º trimestre de 2013 uno de los grandes golpes al aparato financiero de las bandas de ciberdelincuentes de todo el mundo cuando cerró **Liberty Reserve**, conocido como el "banco preferido de los ciberdelincuentes". Esta empresa permitía hacer transacciones monetarias de forma anónima, y tras una investigación de varios años arrestaron a sus propietarios. No está claro qué es lo que sucederá con todo el dinero de clientes legítimos, que no realizaban ningún tipo de actividad ilegal.

Tras una investigación de varios años, **Liberty Reserve** fue cerrada por el gobierno norteamericano y sus propietarios fueron arrestados

La empresa **LivingSocial** fue víctima de un ciberataque que podría afectar a más de 50 millones de clientes. Entre la información comprometida se encontraban nombres, direcciones de correo, fechas de nacimiento y contraseñas cifradas.

Una de las vías más comunes mediante las cuales los atacantes consiguen comprometer un ordenador es el uso de agujeros de seguridad. Algunas de las más importantes empresas de desarrollo de software, como **Google**, utilizan programas mediante los que premian a investigadores que consiguen descubrir nuevos problemas de seguridad, ofreciendo recompensas en función de la gravedad del problema descubierto. En este ámbito, **Microsoft** lanzó en junio un nuevo programa de recompensas que puede premiar hasta con 100.000 dólares a quien descubra nuevas formas de saltarse los mecanismos de protección que han implementado en la última versión de su sistema operativo, Windows 8.1. También ofrece otros 50.000 dólares más si la idea de saltarse los mecanismos de protección viene con sugerencias defensivas para contrarrestar dicho ataque.

En España, el Gobierno está promoviendo una reforma legal que permita a las fuerzas de seguridad la utilización de troyanos para, mediante control judicial, espiar a sujetos envueltos en determinadas investigaciones. La Ley aún no ha sido mandada al Parlamento para su aprobación, por lo que puede sufrir cambios. En cuanto fue anunciado el estudio realizado por una comisión de expertos, el caso levantó mucha polémica por las posibles violaciones de la intimidad que se podrían cometer. En el mundo apenas existe legislación sobre este tema, siendo Alemania uno de los pocos casos, donde en determinados lugares se acepta el uso de troyanos para investigaciones relacionadas con terrorismo.

REDES SOCIALES

Durante el 2º trimestre de 2013 tuvimos la oportunidad de comprobar las repercusiones que puede tener una cuenta comprometida de Twitter. El grupo "Syrian Liberation Army" que ya protagonizó a principios de año varios ataques similares, hackeó la cuenta de Twitter de Associated Press. Una vez consiguió el control de la cuenta, publicó una falsa noticia "Breaking: Two Explosions in the White House and Barack Obama is injured" donde decía que se habían registrado 2 explosiones en la Casa Blanca y que Barack Obama había sido herido. Acto seguido multitud de seguidores de la cuenta comenzaron a hacerse eco de la falsa noticia, lo que provocó que el Dow Jones cayera 155 puntos.

Por lo que pudo saberse, los atacantes mandaron un mail malicioso a numerosos empleados de AP haciéndose pasar por una noticia proveniente de un importante diario norteamericano, y para ampliar información incluía un enlace. Si el usuario pinchaba sobre dicho enlace, era llevado a una página similar a la de Twitter que solicitaba el nombre de usuario y password. Así fue como el grupo "Syrian Liberation Army" consiguió secuestrar la cuenta de Twitter de AP.

El mismo grupo ha seguido atacando, siendo una de sus víctimas la cadena norteamericana CBS, que vio comprometidas 3 de sus cuentas de Twitter, entre ellas la del popular programa "**60 Minutes**". Otra de las víctimas de este grupo fue la cuenta de Twitter del sitio de noticias de humor The Onion.

La cuenta de Twitter del popular programa de la CBS "**60 Minutes**" fue hackeada por el grupo "Syrian Liberation Army"

Siempre decimos que debemos ser precavidos con qué información compartimos a través de las redes sociales. En algunos casos, aunque tomemos todas las precauciones posibles un error puede dar al traste con nuestros esfuerzos. Facebook anunció que un error expuso él nº de teléfono y dirección de correo electrónico de 6 millones de sus usuarios.

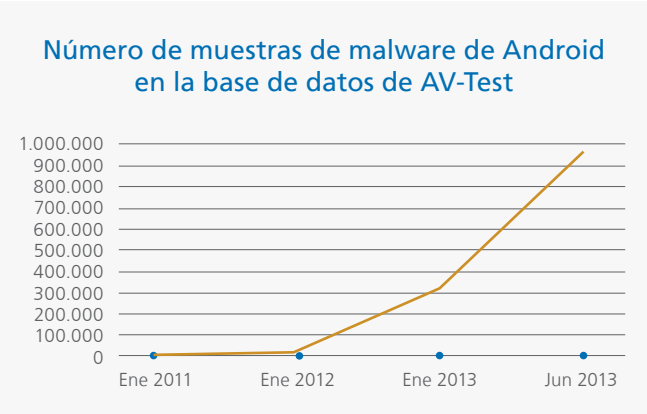
MÓVILES

En abril se descubrió un nuevo tipo de ataque a usuarios del sistema operativo **Android**. En este caso se había distribuido malware a través de aplicaciones no maliciosas. Muchas aplicaciones gratuitas incluyen algún tipo de publicidad como forma de financiación, en lugar de cobrar por la aplicación.

En este caso, parece que los ciberdelincuentes publicaron aplicaciones que no eran maliciosas en sí mismas, pero ellos mismos controlaban la publicidad que mostraban. En cuanto consiguieron suficientes usuarios de estas aplicaciones, comenzaban a mostrar anuncios con falsas notificaciones de actualización de aplicaciones, que si eran instaladas en el dispositivo lo comprometían con un troyano que enviaba SMS a números de tarificación especial. Las aplicaciones publicadas eran 32, y el total de descargas de usuarios que consiguieron a través de Google Play llegaba a los 9 millones.

Si bien la cantidad de malware para Android sigue siendo baja en comparación con el de Windows, el crecimiento que está teniendo es digno de mención.

Según **datos publicados por AV-Test**, en Junio de 2013 ya existían más de 900.000 ejemplares de malware distintos para esta plataforma. A continuación podemos ver reflejados los datos de muestras de malware para Android, según el prestigioso laboratorio independiente AV-Test.



CIBERGUERRA

El número de novedades que surgen en este campo del ciberespionaje y ciberguerra no deja de crecer de forma exponencial, por lo que aquí cubriremos algunos de los casos más llamativos. Si tratáramos de narrar todos los casos sobre los que tenemos conocimiento requeriría un informe entero sólo para esta sección.

Hemos sabido cómo hackers de origen chino consiguieron acceder a planos de más de dos docenas de sistemas de armas norteamericanos. El Washington Post consiguió acceso a un informe interno del Defense Science Board (DSB) del Pentágono donde se detallaba cómo habían obtenido acceso de **misiles Patriot** o de diferentes **cazas en desarrollo, como el F-35**.

> Hackers chinos han robado **planos del caza F-35**, entre otros sistemas armamentísticos

En cualquier caso, no es algo nuevo que ataques cuyo origen es claramente chino tengan como objetivo Estados Unidos. De hecho el mismo Pentágono en su informe anual en el Congreso acusó a China de estar detrás de numerosos ataques cuyo objetivo es hacerse con secretos norteamericanos. Según un informe de la Oficina de Seguridad Nacional de Taiwán, la "ciberarmada" china no deja de crecer y cuenta ya con unos 100.00 efectivos.

Todos estos ataques causan gran preocupación en los diferentes gobiernos, que tratan de tomar medidas. Uno de los últimos en anunciar la creación de un cibercomando fue Indonesia; su ministro de defensa anunció que el principal objetivo de la nueva unidad será protegerse de ciberataques dirigidos a portales y páginas web gubernamentales.

Normalmente, cuando hablamos de ciberespionaje nos imaginamos a 2 potencias enfrentadas tratando de acceder a secretos de su rival. Este caso existe, como hemos visto y narrado en este y en otros informes. Sin embargo, estaríamos muy equivocados si pensamos que sólo se ciñe a esto. Históricamente los servicios de inteligencia de un país no sólo tratan de obtener información de naciones "enemigas", sino también de naciones amigas. Es más, en algunos casos incluso tratan de obtener la máxima información posible de todo el mundo, ya que en el momento actual de globalización donde las personas y la información fluyen como nunca lo habían hecho en la historia de la humanidad, el querer mantener cierto control sobre lo que sucede implica que tengas que acceder a todo tipo de información incluso de tus propios ciudadanos, por mucho que sea tanto inmoral como ilegal.

En junio salió a la luz una noticia que recorrió el mundo entero en cuestión de minutos: según revelaba el día 6 de junio el Washington Post en exclusiva, la **Agencia de Seguridad Nacional norteamericana, NSA** en sus siglas en inglés, había estado espiando "a todo el mundo" a través de un programa llamado PRISM y para ello había contado con la ayuda voluntaria de 9 gigantes del sector tecnológico: Microsoft, Apple, Google, Yahoo, Facebook, Youtube, Skype, AOL, y PalTalk.

Según se decía, la NSA podía obtener todos los datos que quisiera de todos los clientes de esas compañías. Rápidamente

medios y agencias de todo el mundo se hicieron eco de lo publicado por el diario norteamericano.

La **NSA** fue protagonista al hacerse público su programa PRISM mediante el que puede obtener datos de usuarios de las más populares plataformas online

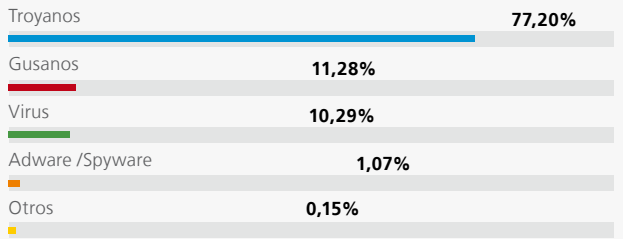
Dichas compañías negaron categóricamente esto. De hecho, el mismo Washington Post cambió la noticia publicada el día anterior, modificando el titular y eliminando partes como en la que se decía que las compañías estaban voluntariamente facilitando todo tipo de datos de sus clientes a la NSA. En unos días diferentes medios comenzaron a *preguntarse* y *cuestionar* la noticia inicial, que parece que se debió a una malinterpretación de una presentación interna de la NSA que habían recibido.

03| El trimestre en cifras

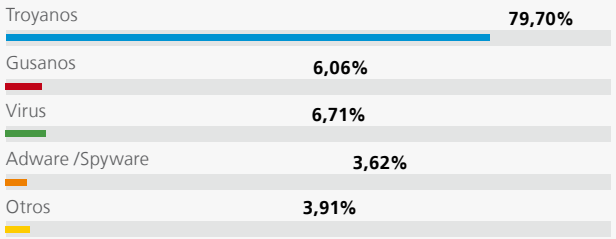
El número de nuevas muestras de malware sigue creciendo de forma imparable. En este segundo trimestre de 2013 se han creado un 12% más de muestras de malware que en el mismo trimestre del año pasado.

Si comparamos conjuntamente los datos del primer y segundo trimestre de 2013 con los del año 2012, este aumento llega al 17%. Respecto a la tipología de malware creado, los troyanos son los líderes en este campo con un 77,20% de las nuevas muestras de malware creadas, aún más alto que el último trimestre.

Nuevo malware creado en el segundo trimestre de 2013, por tipo



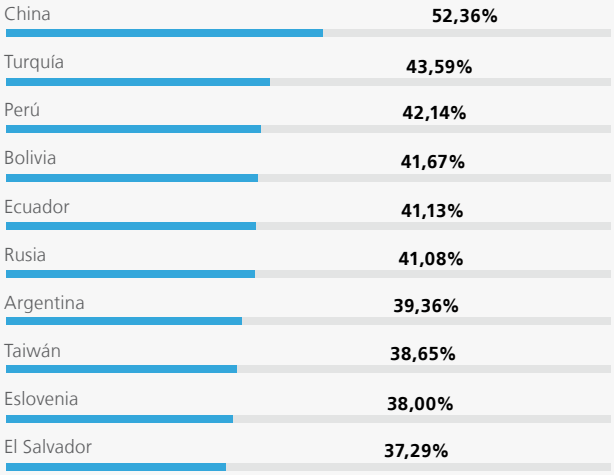
Infecciones por tipo de malware en el segundo trimestre de 2013



Las infecciones de troyanos se mantienen en cifras récord. Los ciberdelincuentes utilizan los troyanos como una de sus principales herramientas para infectar a los usuarios, cambiando las muestras de forma constante, y en muchos casos, de forma automatizada. Utilizan scripts y herramientas creadas con el objetivo de cambiar los binarios que ejecutan en las máquinas de sus víctimas, tratando de evadir la detección por firmas de los productos antivirus.

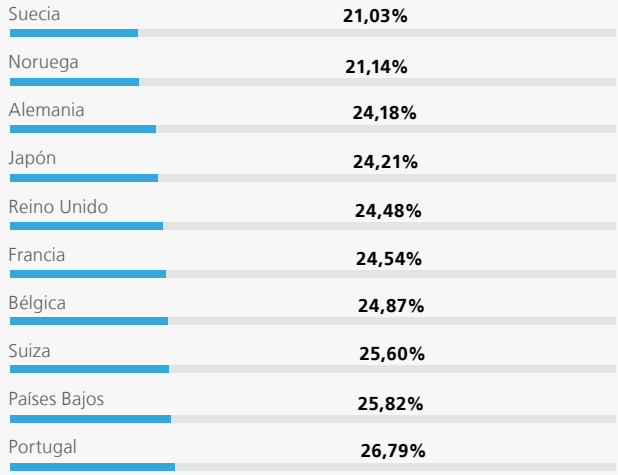
Pasemos a realizar un análisis geográfico de las infecciones: **en este 2° trimestre de 2013 el ratio de infecciones a nivel mundial ha sido del 32,77%**, aumentando respecto al primer trimestre de este año. En cuanto a los datos de los diferentes países, China repite en la primera posición, siendo el único país del mundo con un ratio de infección superior al 50%. Le siguen Turquía (43,59%) y Perú (42,14%).

Países con mayor índice de infección



Vemos que en este "Top 10" están representados países de lugares dispares, aunque hay un **claro protagonismo de países de Latinoamérica**. Además de estos, los siguientes países también tienen un índice de infección superior a la media mundial: Brasil (35,83%), Polonia (35,59%), Guatemala (35,51%), Colombia (33,86%), España (33,57%), Costa Rica (33.33%) y Chile (33,22%).

Países con menor índice de infección



Europa sigue siendo la zona del mundo donde el índice de infección es más bajo. Suecia (21.03%), Noruega (21,14%) y Alemania (25,18%) son los países del mundo con un menor índice de Infección. **El único país no europeo entre los 10 mejores es Japón,** en 4ª posición con un 24,21%. 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 (27,08%), Finlandia (27,16%), Panamá (27,52%), Canadá (27,54%), Austria (28,74%), Uruguay (28,89%), Venezuela (30,11%), Australia (30,45%), Estados Unidos (31,16%), República Checa (31,58%), México (32,35%), Hungría (32,74%) e Italia (32,76%).

04| Conclusión

Cerramos este 2º trimestre de 2013 viendo cómo la creación de malware llega a cifras récord, habido creciendo un 17% la primera mitad de 2013 respecto al mismo periodo de 2012.

Los ciberdelincuentes siguen tratando de engañar a los usuarios utilizando todo tipo de tácticas, aunque ello signifique utilizar cualquier tragedia, como el caso analizado del atentado en el maratón de Boston. Se han dado pasos importantes en la lucha contra estas bandas, como vemos con el cierre de Liberty Reserve por parte del gobierno de Estados Unidos tras una investigación abierta hace años.

En el ámbito de la ciberguerra / ciberespionaje China sigue protagonizando muchos de los titulares con nuevos casos de espionaje, aunque este trimestre Estados Unidos ha estado en el ojo del Huracán tras hacerse público el programa PRISM que la NSA utiliza para obtener información de usuarios de grandes plataformas como Facebook, Youtube o Skype.

05| 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 de informar al público en general.

Del mismo modo, **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. Su objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.

Se puede obtener información sobre las últimas amenazas descubiertas por en el blog de **PandaLabs** en:
http://pandalabs.pandasecurity.com/

06| Panda en la Red

facebook
https://www.facebook.com/PandaSecurity

twitter
https://twitter.com/PandaComunica

google+
https://plus.google.com/b/114692356211770437886/114692356211770437886/posts

youtube
http://www.youtube.com/pandasecurity1

linkedin
http://www.linkedin.com/company/panda-security