Informe trimestral PandaLabs

Enero - Marzo 2013

01| Introducción

Comenzamos un apasionante 2013, un año que en el que parece que las noticias de seguridad nos van a tener pegados al asiento. En este informe analizamos en primer lugar las cifras que arrojan nuestros sistemas de análisis de malware desde la nube, donde veremos cómo los ciberdelincuentes han creado más de 6 millones y medio de nuevas muestras de malware.

Repasaremos diferentes ataques de los que hemos sido testigos durante estos 3 primeros meses de 2013, como hackeos de cuentas de Twitter de grandes empresas como Burger King o la BBC. Contaremos cómo se ha producido uno de los mayores ataques hasta la fecha, que ha ido a por las principales empresas tecnológicas del mundo: Twitter, Facebook, Apple y Microsoft.

También repasaremos algunas de las victorias logradas por las fuerzas de seguridad, como la detención de una banda dedicada a extorsionar a sus víctimas con el infame "virus de la policía".

En el ámbito de la ciberguerra / ciberespionaje daremos un repaso a cómo está la situación mundial, y qué papel está jugando el gobierno chino en los principales incidentes sucedidos durante estos tres meses, tales como el ataque a medios de comunicación (The New York Times, The Washington Post o The Wall Street Journal), a compañías como EADS (European Aeronautic Defence and Space Company) o la alemana ThyssenKrupp.

02| El trimestre de un vistazo

El pasado 11 de enero, la Comisión Europea inauguraba el European Cybercrimen Center (EC3) con el objetivo de ayudar a los estados miembros de la UE a luchar contra los ciberataques. Lo cierto es que los ciberdelincuentes siempre se han aprovechado de lo complicada que puede ser la coordinación policial entre diferentes países para llevar a cabo sus fechorías, por lo que este tipo de iniciativas siempre son bienvenidas.

Cibercrimen

En enero el FBI hizo pública una investigación que comenzó en 2010 y que ha conseguido detener a una banda de ciberdelincuentes que había logrado infectar más de un millón de ordenadores desde 2005. Esta operación es de destacar, entre otros motivos, por lo que significa respecto a la coordinación entre diferentes países: el FBI contó con la colaboración de las fuerzas de seguridad de Letonia, Moldavia, Rumanía, Holanda, Alemania, Finlandia, Suiza y Reino Unido.

Y dentro de la lucha contra la ciberdelincuencia podemos encontrar diferentes vertientes. Una de ellas, que no se suele nombrar de forma general, tiene que ver con la necesidad de concienciar a las empresas de que realmente dediquen los recursos necesarios para proteger los datos de sus clientes. En este ámbito, la división inglesa de Sony Computer Entertainment ha sido condenada a pagar 250.000 libras como consecuencia del robo de datos de clientes que sufrió en 2011. El motivo de esta condena está fundado en las escasas medidas de seguridad que la empresa tenía para proteger la información de sus clientes.

"EL VIRUS DE LA POLICÍA"

Uno de los grandes protagonistas desde hace algo más de un año es el conocido como "Virus de la Policía". En febrero este virus volvió a saltar a las portadas, pero esta vez por un motivo muy diferente, ya que la noticia era que nuestros amigos de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional, en colaboración con Europol y con Interpol, habían desmantelado la banda de ciberdelincuentes responsable del famoso "Virus de la Policía". Según el comunicado publicado por el Ministerio del Interior español, habían sido detenidas 10 personas pertenecientes a una de las células financieras del grupo, que manejaba un millón de euros al año, dinero obtenido de las víctimas del malware. Seis de ellos son ciudadanos rusos, dos ucranianos y dos georgianos, todos ellos residentes en España.

Además, fue detenido también el cabecilla de toda la operación. Se trata de un ciudadano ruso. Curiosamente, a pesar de ser residente ruso, fue detenido en Dubai (Emiratos Árabes) mientras se encontraba de vacaciones.

Nos llamó la atención que se hablara de la detención de "la banda de ciberdelincuentes" cuando por la información que tenemos en PandaLabs realmente existen diferentes bandas de ciberdelincuencia detrás de estos ataques. Hemos llegado a esta conclusión después de haber estudiado múltiples variantes a lo largo del tiempo y haber observado diferencias significativas entre ellas.

En el blog de PandaLabs hemos informado en diferentes ocasiones sobre el Virus de la Policía, comentando cómo iba evolucionando y cambiando de técnicas. Estas evoluciones son normales y no implican en absoluto que existan distintos grupos detrás de los ataques, ya que es algo natural que los ciberdelincuentes vayan probando nuevas técnicas para lograr el mayor número de víctimas posibles dispuestas a pagar.

Sin embargo, existen otras evidencias que no hemos comentado anteriormente. Por ejemplo, cómo ciertas técnicas que supuestamente habían quedado superadas vuelven a surgir (entre ellas, el cifrado de ficheros del ordenador atacado); o cómo para hacer lo mismo (mostrar la pantalla con el falso aviso de la policía), diferentes variantes utilizan funciones completamente diferentes, dejando claro que se trata de proyectos diferentes, etc.

En cualquier caso, es una circunstancia relativamente normal, y extrapolable a distintos ámbitos. Si analizamos la situación desde un punto de vista meramente comercial, es frecuente que cuando alguien tiene una idea con la que comienza a hacer mucho ruido y dinero, rápidamente, otras personas conscientes de ese éxito traten de subirse al carro y hacer lo mismo. En el caso que nos ocupa, parece que diferentes grupos de ciberdelincuentes están dedicándose al mismo negocio.

Desde PandaLabs hemos decidido tirar un poco más del hilo y sacar algunas cifras para ver si son coherentes con las pruebas anteriormente descritas. Como ya hemos comentado en anteriores ocasiones, la mayoría de las infecciones se llevan a cabo mediante los conocidos "exploit kits", herramientas que utilizan las bandas de ciberdelincuentes para infectar los ordenadores de los usuarios con la simple visita a una página web comprometida, sin que el usuario tenga que realizar ninguna acción adicional. Para infectar se utilizan diferentes agujeros de seguridad, la mayoría de ellos basados en Java o en Adobe (Flash, Reader), ya que se trata de aplicaciones con muchos agujeros en este sentido, y que además muchos usuarios no actualizan. Esto es, que infectar a usuarios es casi un juego de niños.

Por este motivo, en 2012 desplegamos una tecnología en Panda Cloud Antivirus que permite bloquear infecciones en cuanto se detecta alguna vulnerabilidad de este tipo (incluso aunque nos sea desconocida), y además envía a la nube información del fichero con el que se trataba de infectar el sistema.

De entre esta colección de datos, hemos seleccionado un par de familias distintas del Virus de la Policía, y hemos contabilizado las infecciones bloqueadas desde diciembre de 2012 hasta mediados de febrero de 2013. Es decir, estamos hablando de usuarios de Panda Cloud Antivirus que mientras navegaban por Internet fueron atacados con un exploit para el que no estaban actualizados (como comentaba anteriormente, la mayoría son de Java o de Adobe), y cuyo objetivo era infectarles con una de estas dos familias del Virus de la Policía.

El cabecilla ruso fue detenido en Dubai (Emiratos Árabes) en diciembre. Si realmente se trata de la persona que estaba detrás del Virus de la Policía, como hemos podido leer en algunos medios, este número de infecciones debería haber descendido hasta cero o, al menos, mostrar un claro descenso. Sin embargo, este es el resultado:

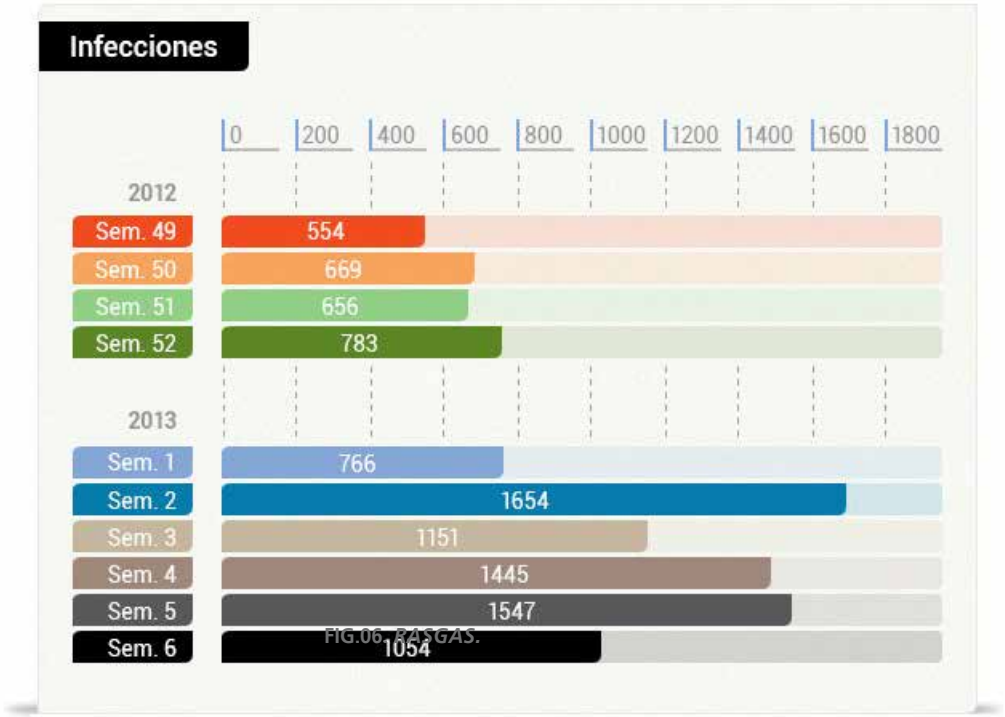

FIG.01. *EVOLUCIÓN DE INFECCIONES DE DOS VARIANTES DEL VIRUS DE LA POLICÍA DESDE EL ARRESTO DE SU CABECILLA.*

Como podemos observar, el número de intentos de infección no sólo no disminuyó, sino que, además, se multiplicó por dos. Esta es una prueba empírica evidente, que demuestra que aún tenemos Virus de la Policía para rato, y que no debemos bajar la guardia.

Twitter, Facebook, Apple y Microsoft víctimas del mismo ataque

El pasado 1 de febrero, Twitter publicaba un artículo en su blog (en inglés, "Keeping our users secure") explicando cómo la propia red social ha sido víctima de un ataque, que ha acarreado el acceso ilícito a información de hasta 250.000 de sus usuarios.

Un par de semanas más tarde, Facebook publicaba también un artículo en su blog, titulado "Protecting People On Facebook" (en inglés). Aparentemente, y según fuentes de la red social, no fueron comprometidos datos de clientes en este ataque.

La siguiente víctima fue Apple. Tan sólo unos pocos días después del anuncio de Facebook, representantes de Apple dijeron a Reuters que también habían sido objetivo del mismo ataque.

Y finalmente, aunque no menos importante, Microsoft reconoció que también había sido víctima de esta misma agresión.

No es una mala lista de empresas ¿verdad? En principio, y hasta el momento, ninguna otra gran compañía ha declarado haber sufrido el referido ataque. En cualquier caso, podemos obtener puntos positivos de esta situación:

- Las empresas no tienen miedo de reconocer ser objetivo de este tipo de agresiones.
- Son muchas las empresas que cuentan con buenos equipos de seguridad que han sido capaces de identificar los ataques mientras estaban en curso.

Eso sí, todas esta agresiones utilizaron un agujero de seguridad en Java desconocido hasta el momento y para el que no existía parche, lo que se conoce como una vulnerabilidad zero day ó 0-day

Las personas involucradas en seguridad informática saben que no existe un lugar 100% seguro. Es posible tomar un gran número de medidas preventivas que funcionarán bien la mayoría de las veces. Pero siempre existirá algún punto débil, una nueva vulnerabilidad, algún error humano… que podría dar finalmente con el éxito de alguno de los miles de ataques que compañías tan grandes como las mencionadas reciben constantemente.

Y, en este punto, ser capaces de identificar un ataque que está ocurriendo en el mismo momento resulta crítico. Y Twitter, Facebook, Apple y Microsoft fueron capaces de ello. Todas estas compañías están recogiendo información sobre el ataque. Todas ellas están trabajando con la policía para averiguar quién está detrás del mismo.

Puede que los responsables de una pequeña o mediana empresa piensen que no tienen que preocuparse tanto por su seguridad como estos gigantes, ya que no son objetivos aparentemente tan "sexys". Y es parcialmente cierto. Probablemente recibirán un número muy pequeño de ataques dirigidos (o incluso ninguno), sin embargo serán bombardeados con agresiones de ciberdelincuentes que infectan a millones de ordenadores. Y a los ciberdelincuentes les encantan los objetivos fáciles. En suma, todos aquellos que cuenten con ordenadores sin protección, con software desactualizado y sin una estrategia seria de seguridad son objetivos certeros.

JAVA

La mayoría de infecciones hoy en día se producen a través de los conocidos "exploit kits", que infectan los ordenadores de los usuarios sin su conocimiento a través de alguna vulnerabilidad. Más del 90% de estos casos son vulnerabilidades de Java a través del navegador. Los ataques que recibieron Microsoft, Apple, Facebook y Twitter este mismo trimestre utilizaron Java. La mayoría de infecciones del "Virus de la Policía" consiguen llegar a los ordenadores de sus víctimas gracias a que éstas cuentan con versiones desactualizadas de Java.

¿Cuál es el mejor método de evitar estas infecciones? Muy sencillo: basta con eliminar Java del navegador. Si por algún motivo necesitas Java en el navegador para utilizar alguna aplicación, utilízala en un navegador secundario que sólo emplees para dicha tarea.

CIBERATAQUES

La cantidad y variedad de ataques que han tenido lugar durante este trimestre son, cuanto menos, llamativos. Además de los ya descritos en el informe, todo tipo de entidades y empresas han sufrido agresiones destacables. **Evernote** fue víctima de una intrusión que hizo a la empresa lanzar un comunicado pidiendo a más de 50 millones de usuarios que cambiaran su contraseña. La página web de la **Reserva Federal** estadounidense fue atacada, según un comunicado que publicó la propia entidad, aunque no aclaraba si se produjo algún tipo de robo de información. Sin embargo coincidió con la publicación, por parte de Anonymous, de datos personales de 4.000 ejecutivos de la banca estadounidense, lo que hace pensar que el ataque sufrido por la FED fue llevado a cabo por este grupo. La NASA fue también víctima de una intrusión. A través de la popular web Pastebin se publicó información interna que incluía direcciones de correo, nombres reales, contraseñas…

Redes sociales

Durante este trimestre diferentes cuentas de Twitter, tanto de empresas como de personajes conocidos, han sido hackeadas. Uno de los casos más llamativos fue el de Burger King, donde los atacantes al parecer lograron adivinar la contraseña de la cuenta y hacerse con ella. Acto seguido cambiaron la imagen de fondo por la de McDonalds y comunicaron que acababan de ser adquiridos por su principal competidor.

La cuenta de Twitter del fabricante automovilístico Jeep sufrió una agresión muy similar. En este caso se anunció que habían sido adquiridos por Cadillac. Otro tipo de hackeos en cuentas de Twitter que hemos observado en este trimestre tienen un tinte más político. Un grupo de ciberdelincuentes autodenominado "Syrian Electronic Army" consiguió hackear diferentes cuentas pertenecientes a diferentes organizaciones.

FIG.02. *IMAGEN DE LA CUENTA DE TWITTER DE BURGER KING TRAS HABER SIDO HACKEADA.*

Por lo que se ha podido saber, primero lanzaron ataques de phishing para poder obtener las credenciales de acceso a Twitter y posteriormente secuestrar las cuentas. Entre sus víctimas figuran Human Rights Watch, el servicio de noticias francés France 24 o el servicio meteorológico de la BBC.

Móviles

La práctica totalidad de noticias sobre seguridad y ataques de malware en plataformas móviles las protagoniza Android, sistema operativo que tiene la mayor cuota de mercado en este segmento. Además de los ataques habituales, este trimestre hemos descubierto alguna nueva técnica curiosa digna de mención. Un malware para Android, que se encontraba escondido dentro de Google Play, no sólo infectaba el móvil ¡sino que, además, está preparado para infectar el ordenador desde smartphones o tabletas. La técnica utilizada es muy sencilla: una vez que se ejecuta en el teléfono, se conecta a Internet para descargarse ficheros que guarda en la raíz de la tarjeta de almacenamiento del dispositivo, de tal forma que cuando se conecte al ordenador a través del cable USB se ejecute automáticamente uno de los ficheros, que se trata de un troyano de Windows.

Ciberguerra

China suele ser uno de los protagonistas de esta sección, pero en este trimestre el gigante asiático se ha ganado el protagonismo absoluto. El pasado 30 de enero, el diario norteamericano **The New York Times** publicaba en portada una noticia en la que explicaba cómo habían sido víctimas de un ataque que se había saldado con el acceso a su ordenadores y el consiguiente espionaje durante cuatro largos meses. Casualmente, el ataque se produjo justo después de un artículo de investigación publicado en el diario donde se contaba como Wen Jiabao -primer ministro chino- y su familia habían amasado una fortuna de miles de millones de dólares.

Un día más tarde, el diario económico **The Wall Street Journal** anunciaba que también habían sido víctimas de una agresión similar por parte de lo que parecían ser hackers chinos. El gobierno chino, ofendido por lo que se consideran como "ataques injustificados", protestó y Hong Lei -Ministro de Asuntos Exteriores de China- hizo unas declaraciones donde decía que insinuar que los ataques procedían de China era algo irresponsable y poco profesional, pues todo estaba basado en meras especulaciones (*"It is unprofessional and groundless to accuse the Chinese military of launching cyber attacks without any conclusive evidence"*).

Curiosamente, en estos dos incidentes los atacantes pudieron acceder a todo tipo de información de los medios (datos de clientes, etc.), sin embargo se centraron únicamente en la información sobre periodistas y empleados, tratando de encontrar cualquier referencia a investigaciones periodísticas sobre China, y principalmente buscando las fuentes utilizadas para elaborar los artículos de investigación sobre el país asiático en cuestión.

El día siguiente a la revelación de The Wall Street Journal, otro gigante de los medios norteamericanos, **The Washington Post**, hizo público que ellos habían sufrido un ataque similar en 2011 con origen de nuevo en China.

FIG.03. *PORTADA DE NEW YORK TIMES ANUNCIANDO EL ATAQUE RECIBIDO DESDE CHINA.*

Semanas más tarde, la compañía norteamericana Mandiant publicó un demoledor informe de 76 páginas (APT1: Exposing One of China's Cyber Espionage Units, (http://intelreport.mandiant.com) donde detallaba cómo la Unidad 61398 del ejército chino estaba especializada en ataques de ciberespionaje. El informe revela más de 3.000 evidencias que demuestran cómo esta unidad llevaba en marcha al menos desde el año 2006, robando información en al menos 141 organizaciones de todo el mundo.

Es posible que no nos percatemos de la importancia que tiene este informe de Mandiant y de las repercusiones que puede llegar a acarrear a medio y largo plazo. Demostrar quién está detrás de cualquier ataque es algo muy complejo, incluso en casos de ciberdelincuencia normales. Cuando hablamos de ciberespionaje es aún más complicado por el simple hecho de que quien está detrás es gente altamente cualificada y con medios más que suficientes para ir cubriendo su rastro. Desde hace años todas las miradas se volvían a China cada vez que se daba un caso de este tipo, pero sin pruebas reales de que realmente el gobierno chino estuviera detrás de los mismos. Pues bien, por primera vez se ha demostrado que el ejército chino está activamente realizando labores de espionaje a nivel mundial, infiltrándose en empresas de todos los sectores y robando información.

La semana siguiente a la publicación del informe de Mandiant continuaron apareciendo noticias de casos de ciberespionaje que apuntaban a China: EADS (European Aeronautic, Defence and Space Company), fabricante del avión de combate Eurofighter y dueña de Airbus, fue atacada por hackers de origen chino, según informaba el diario alemán Der Spiegel (http://www.spiegel.de/international/world/digital-spying-burdens-german-relations-with-beijing-a-885444.html). En la misma noticia se hablaba de otro ataque similar del que había sido víctima el gigante alemán ThyssenKrupp.

03| El trimestre en cifras

En los primeros tres meses de 2013 hemos recogido en el laboratorio más de seis millones y medio de muestras. Los troyanos siguen siendo los protagonistas, copando la creación de malware con casi tres de cada cuatro muestras. Las cifras son muy similares a las que vimos el pasado año 2012.

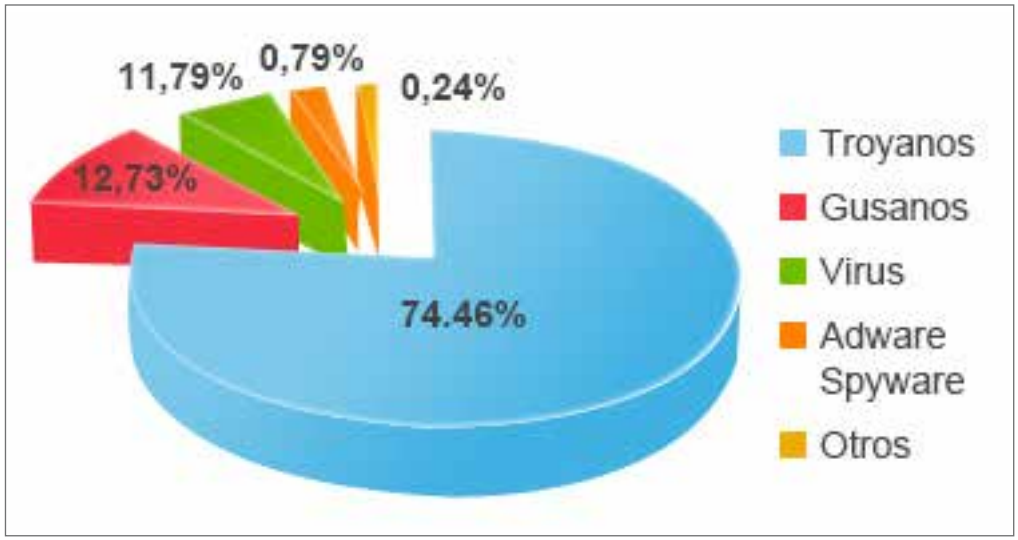

FIG.4. *NUEVO MALWARE CREADO EN EL PRIMER TRIMESTRE DE 2013, POR TIPO.*

Veamos cuántas infecciones ha causado cada tipo de malware en el mundo. Como hemos comentado en anteriores informes, una de las características de los troyanos es que no se replican, por lo que su capacidad teórica de infección es mucho menor en comparación a virus o gusanos, que pueden infectar por sí mismos gran cantidad de PCs. Veamos cómo se reparten las infecciones:

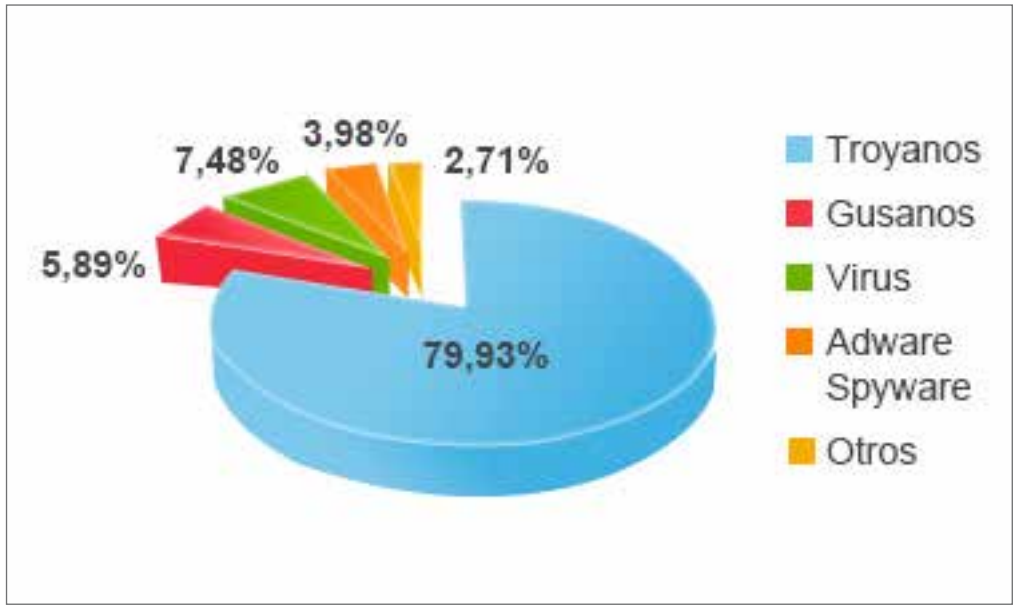

FIG.5. *INFECCIONES POR TIPO DE MALWARE EN EL PRIMER TRIMESTRE DE 2013.*

Las infecciones de troyanos han alcanzado una cifra récord llegando a protagonizar casi el 80% de todas las infecciones. ¿Cómo es esto posible si son ejemplares de malware que no se replican por sí mismos? La clave está en la última parte de la pregunta: "por sí mismos". Hoy en día la mayoría de las infecciones por troyanos se llevan a cabo a través de páginas web comprometidas, utilizando normalmente algún tipo de vulnerabilidad basada en Java o en Adobe. Esto implica que en cuestión de minutos (en caso de que se trate de una página web popular) puedan producirse miles de infecciones de un mismo troyano. O incluso de troyanos diferentes, ya que los atacantes tienen la capacidad de cambiar el troyano con el que infectan en función de multitud de parámetros, como el lugar de origen de la víctima, el sistema operativo que utiliza, etc.

Si realizamos el análisis geográfico de las infecciones, este primer trimestre de 2013 el ratio de infecciones ha sido del 31,13%. Como viene siendo habitual, China encabeza el ranking mundial en este apartado, siendo el único país del mundo que supera el 50% de infecciones. Le siguen en el ranking Ecuador, con un 41,01% y Turquía con un 40,38%.

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

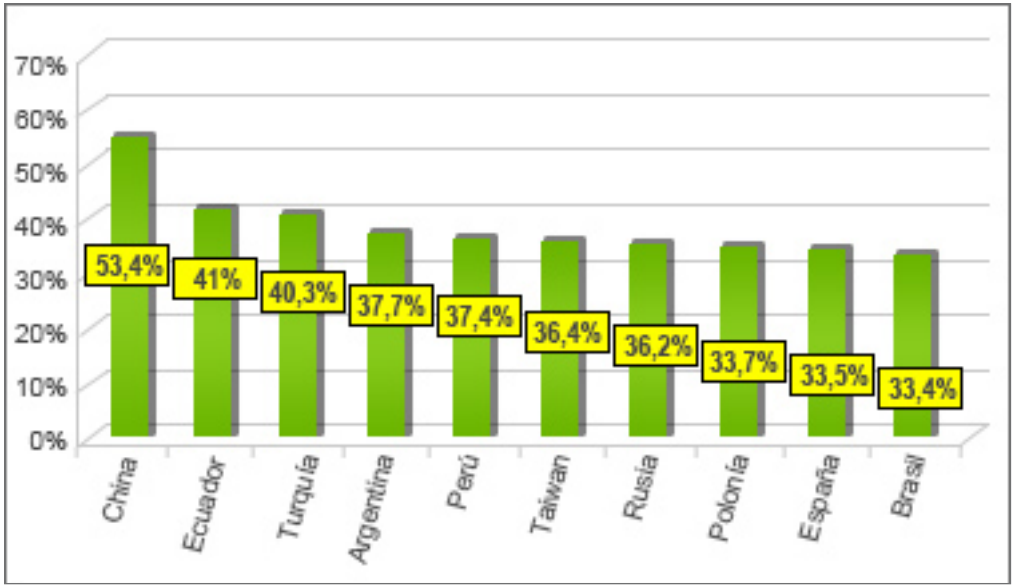

FIG.6. *PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN.*

Todos estos países tienen un índice de infección por encima de la media mundial, lógicamente. Hay otros cuatro países que también superan la media: Chile (33,37%), Colombia (32,01%), Italia (31,97%) y Venezuela (31,45%).

Veamos a continuación los países menos infectados del mundo:

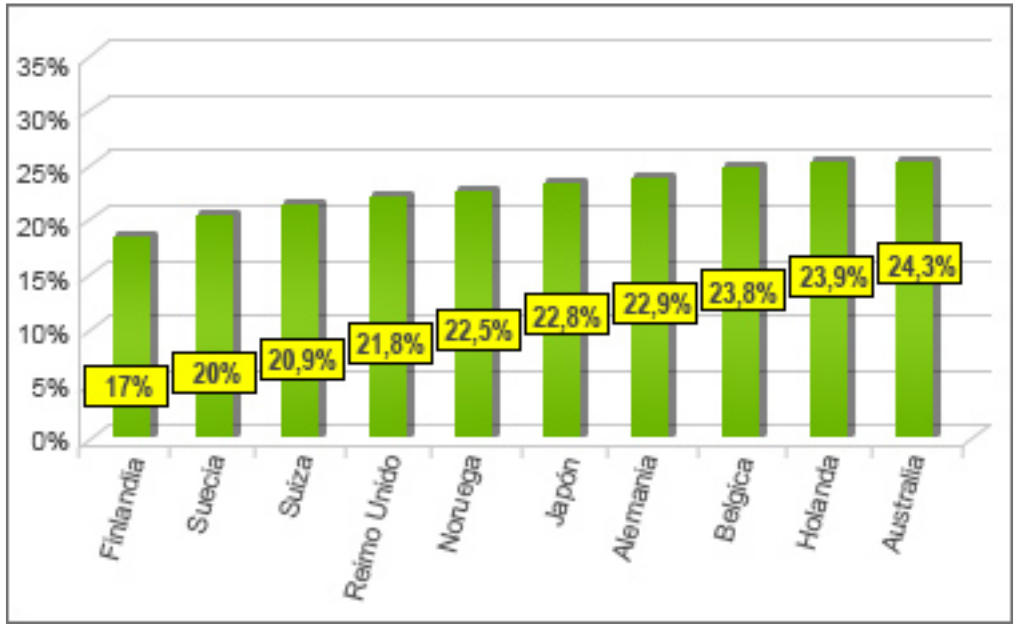

FIG.7. *PAÍSES CON MENOR ÍNDICE DE INFECCIÓN.*

Europa sigue siendo la zona del mundo donde el índice de infección es más bajo. Finlandia, que encabeza este ranking, cuenta tan sólo con un 17,0% de ordenadores infectados, seguido por Suecia (20,01%) y Suiza (20,99%). 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: Canadá (24,89%), Dinamarca (25,72%), Portugal (26,91%), Costa Rica (27,22%), Francia (27,43%), Estados Unidos (27,79%), México (29,91%) y Hungría (30,69%).

04| Conclusión

Como habéis podido leer, a lo largo de estos tres meses han tenido lugar incidentes cuyas consecuencias darán que hablar durante mucho tiempo, y aún nos queda por delante la mayor parte de 2013. La lucha contra la ciberdelincuencia discurre por buen camino, y aunque aún queda un largo trecho por recorrer, lo cierto es que estamos observando cómo la cooperación internacional de los diferentes cuerpos de seguridad va dando sus frutos, y ciberdelincuentes de todo el mundo van siendo arrestados.

En el ámbito de la ciberguerra / ciberespionaje el ambiente se está poniendo más que interesante. El malestar de muchos países hacia China, que es sospechosa de muchos de los ataques que tienen lugar tanto en grandes empresas como en instituciones públicas de todo el mundo, puede hacer que derive en consecuencias en el mundo real. Hay quien aboga por acuerdos internacionales, del estilo de las Convenciones de Ginebra, para tratar de "regular" los límites a los que se puede llegar. Estaremos atentos a lo que suceda durante los próximos meses ya que puede llegar a cambiar Internet tal y como la conocemos.

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/

Síguenos 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

PANDA SECURITY