Informe anual PandaLabs

Resumen 2012

01| Introducción

2012 ha acabado y llega el momento de dar un repaso a todo lo sucedido en el mundo de la seguridad durante estos 12 meses. La tendencia de crecimiento en la creación de malware sigue imparable, este año en PandaLabs hemos capturado 27 millones de nuevas muestras de malware, una media récord de 74.000 diarias. Asimismo, los ataques de ciberdelincuentes a empresas han sido grandes protagonistas del último año, contando entre sus víctimas a grandes multinacionales de todo el mundo y de diferentes sectores, desde el mundo de los videojuegos (Blizzard) hasta la automoción (Nissan).

Analizamos también las novedades en el mundo de los teléfonos móviles, donde vemos que el sistema operativo con más cuota de mercado (Android) es la plataforma elegida por los ciberdelincuentes para robar información y dinero a los usuarios a través de ataques de malware.

Hablaremos de las redes sociales, donde Facebook sigue reinando tanto en número de usuarios como en número de ataques, teniendo como principal gancho temáticas de ingeniería social.

Veremos qué ha sucedido en el mundo Mac, donde se ha producido la mayor infección registrada en la historia, y qué consecuencias ha tenido.

La ciberguerra / ciberespionaje ha sido un campo muy activo este año pasado, teniendo a Flame como uno de los casos más destacados. Analizaremos también otros ataques que han tenido especial protagonismo en Oriente Medio.

En este informe encontraréis los casos más destacados ocurridos a lo largo del año pasado, así como una mirada al futuro donde trataremos de vaticinar qué nos espera en este año 2013.

02| 2012 de un vistazo

En enero, Google tuvo que retirar varias aplicaciones del Android Market (renombrado semanas después a Play Store) debido a que eran maliciosas. Los ciberdelincuentes básicamente habían subido juegos populares (como Angry Birds o Cut The Rope) para confundir a los usuarios, quienes al instalarlos también instalaban un troyano que se dedicaba a enviar SMS a números Premium. De hecho, hemos sabido que Google, cansada de los problemas con aplicaciones maliciosas en su Play Store, ha comenzado analizar las aplicaciones antes de publicarlas, buscando comportamientos anómalos. Según ellos mismos han conseguido disminuir la descarga de aplicaciones maliciosas en un 40%.

Móviles

Aún así seguiremos viendo infecciones a través de la Play Store, aunque no siempre vienen por esta vía. Bmaster, un troyano con capacidad de RAT (Remote Access Tool, Herramienta de Acceso Remoto) se hacía pasar por una aplicación legítima, pero fuera de la Play Store.

Otros troyanos que hemos visto tienen el único objetivo de robar información de los terminales. La mayoría de ellos tratan de obtener la misma información: registro de llamadas y mensajes de texto y la agenda completa con todos los contactos. Un peligro que es más grande que en su principal competidor (iPhone con su iOS) ya que Android permite instalar aplicaciones que no sean descargadas de la tienda oficial de Android, e incluso instalando sólo aplicaciones de la tienda oficial hemos visto bastantes casos en los que ciberdelincuentes habían conseguido subir troyanos disfrazados de otras aplicaciones, algo que también puede suceder en la App Store de Apple pero de forma menos frecuente que en la Play Store de Android.

Opera Mini es la versión del navegador Opera para usuarios de dispositivos móviles. En los últimos meses ha ganado cierta popularidad como navegador alternativo al que encontramos por defecto en Android, y los ciberdelincuentes no han dejado pasar la ocasión de aprovecharse de su popularidad para engañar a los usuarios. En esta

ocasión ofrecían el navegador desde una tienda de aplicaciones alternativa a Play Store. Al instalar la aplicación se instalaba el navegador Opera real, pero al mismo tiempo se instalaba un troyano que enviaba mensajes a números Premium internacionales.

Así como en muchas ocasiones hemos visto en dispositivos móviles que los troyanos se hacen pasar por otras aplicaciones populares, en este caso lo llamativo es que el troyano incluye la aplicación por la que se hace pasar para así lograr un engaño completo y evitar que el usuario se dé cuenta de que ha instalado un troyano en su dispositivo.

Otro ataque bastante original lo hemos visto en China, donde un troyano se dedicaba a comprar aplicaciones desde el teléfono móvil infectado. Es un troyano diseñado específicamente para clientes de China Mobile, uno de los mayores operadores del mundo con más de 600 millones de abonados. Una vez infectado, el terminal accede a la tienda de aplicaciones oficial de China Mobile y compra diferentes aplicaciones sin que el usuario sea consciente de lo ocurrido hasta que es demasiado tarde. Este troyano ha sido distribuido desde tiendas de aplicaciones no oficiales.

Clientes de China Mobile, el mayor operador de telefonía móvil del mundo, fueron víctimas de un ataque mediante aplicaciones fraudulentas.

FIG.01. *CHINA MOBILE.*

A estas alturas muchos usuarios pensarán que resulta más seguro adquirir e instalar aplicaciones de las tiendas oficiales. Hasta cierto punto esto es cierto, pero hemos visto casos en el pasado donde se han "colado" aplicaciones maliciosas en dichas tiendas. Sin ir más lejos, este mismo trimestre hemos vuelto a ser testigos de otro caso en Play Store, la tienda de Android, donde un troyano se hacía pasar por 2 populares juegos, Super Mario Bros y GTA 3 Moscow City. Pasaron semanas hasta que se descubrieron las aplicaciones fraudulentas y fueron retiradas de la tienda.

FIG.02. *ANDROID YA CUENTA CON MÁS DE 500 MILLONES DE DISPOSITIVOS ACTIVADOS.*

¿Por qué Android es la plataforma móvil más atacada? Esto se debe a diferentes motivos: por un lado, Android permite que el usuario instale las aplicaciones que quiera, sin obligarle a pasar por la tienda oficial ni que tengan que venir firmadas las aplicaciones, como ocurre en iOS. Pero los ciberdelincuentes no se fijarían en esta plataforma si no tuviera un amplio número de usuarios. Google anunció en Junio que se había llegado a la cifra de 400 millones de dispositivos Android activados, y a principios de Septiembre ya había alcanzado los 500 millones, con un ritmo de activaciones de 1,3 millones al día.

Ransomware: "El virus de la policía"

Uno de los principales protagonistas de 2012 ha sido una "epidemia" de malware que ha infectado cientos de miles de equipos en todo el mundo utilizando el miedo y el chantaje como una forma de extorsión para que los usuarios paguen de su bolsillo directamente a los ciberdelincuentes.

Normalmente estamos acostumbrados a ver la mayoría de estos ataques utilizando como idioma el inglés, pero en este caso los ataques están localizados. Hemos visto cómo han usado el alemán, español, holandés o italiano (entre otros) en función del país de la víctima. Todos los ataques tienen como objetivo algún país europeo, por lo que parece que todos ellos están relacionados y podría ser la misma banda de ciberdelincuentes la que está detrás de los mismos.

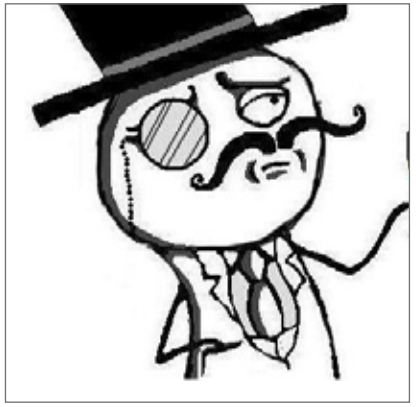


FIG.3. *ICONO UTILIZADO POR UN EJEMPLAR DEL "VIRUS DE LA POLICÍA.*

Analicemos uno de estos ataques: el fichero utiliza como icono el siguiente Internet meme, popular ya que el grupo LulzSec lo utiliza en sus comunicaciones:

Una vez que te has infectado, esto es lo que verás en tu escritorio:

FIG.04. *MENSAJE DEL TROYANO HACIÉNDOSE PASAR POR LA POLICÍA PARA OBTENER DINERO DE LA VÍCTIMA.*

El mensaje es claro, dice que ha sido detectado acceso a contenido ilegal desde ese ordenador (desde pornografía infantil a envío de spam con temática terrorista), y que el equipo será bloqueado para evitarlo. Eso sí, podemos solucionarlo pagando una multa de 100€.

Lo peor para el usuario es que realmente bloquea el ordenador, por lo que no es sencillo de eliminar. Para hacerlo, debemos reiniciar el ordenador en modo seguro y analizar el ordenador con una solución antivirus que sea capaz de detectarlo.

¿Por qué aparece en español y suplanta a la policía española? Fácil: el malware se conecta a un servidor, donde en función de la dirección IP desde la que nos conectemos averiguará en qué país estamos, y nos mostrará el mensaje en el idioma adecuado y suplantando a la policía del país en cuestión. Casi todos los ataques suplantan a cuerpos de policía europeos, aunque también hemos visto ataques a otros países, como Canadá. Aquí podéis ver ejemplos de diferentes ataques similares ocurridos en el primer trimestre de 2012:

FIG.05. *MENSAJE DEL TROYANO EN ALEMÁN.*

FIG.06. *MENSAJE DEL TROYANO EN HOLANDÉS.*

FIG.07. *MENSAJE DEL TROYANO EN ITALIANO.*

FIG.08. *MENSAJE DEL TROYANO EN INGLÉS.*

FIG.09. *MENSAJE DEL TROYANO EN ESPAÑOL.*

Con el tiempo los ataques han ido evolucionando. Como hacerse pasar por la Policía no parecía ser suficiente, comenzaron a utilizar técnicas de ransomware, cifrando archivos del ordenador y exigiendo una cantidad económica a cambio de devolver el acceso a esos archivos. Básicamente han tomado esta funcionalidad del troyano PGPCoder, diseñado para cifrar archivos que sólo libera una vez la víctima paga el rescate a los ciberdelincuentes que lo crearon.

Las primeras versiones de este nuevo virus de la policía sólo cifraban archivos .doc, y el cifrado no era muy complejo realmente, por lo que era posible desbloquearlos sin necesidad de tener la clave. Sin embargo, los cibercriminales se dieron cuenta de que habían cometido un error y lanzaron una nueva versión. En esta ocasión se utilizaban técnicas más avanzadas de cifrado, de tal forma que la clave fuera imprescindible. Y no sólo eso, ya que la clave era diferente para cada equipo infectado, por lo que a menos que alguien fuera capaz de acceder al servidor donde se almacenan las claves, no habría forma de recuperar esos archivos. Además, el cifrado ya no era sólo de archivos .doc, algunas variantes incluían una lista de extensiones de archivos a cifrar, otras

variantes contaban con una lista de exclusión para evitar "secuestrar" cualquier archivo crítico del sistema, cifrando todos los demás archivos.

¿Cuánto más lejos pueden llegar? Al final, lo que estos ciberdelincuentes pretenden es asustar a los usuarios lo máximo posible, de tal forma que éstos paguen el rescate (la "multa"). Otra nueva evolución activaba la cámara web del equipo infectado. ¿Para qué?: Han modificado la típica página de advertencia que venían utilizando hasta ahora:

FIG.10. *IMAGEN UTILIZADA HASTA AHORA POR EL VIRUS DE LA POLICÍA.*

La han sustituido por una nueva que incluye un cuadro que muestra la imagen tomada por la cámara web:

FIG.11. *NUEVA IMAGEN UTILIZADA AHORA POR EL VIRUS DE LA POLICÍA, INCLUYENDO UN CUADRO DE VIDEO QUE MUESTRA LO CAPTADO POR LA CÁMARA WEB DE NUESTRO ORDENADOR.*

Como podéis ver, hay un marco donde se muestran las imágenes que está capturando la webcam en tiempo real, y una leyenda que dice "Grabación de video". Sin embargo, realmente no está grabando las imágenes ni enviándolas a ningún sitio, simplemente muestra la imagen tomada por la cámara web. Por supuesto, esto el usuario no lo sabe y la mayoría de ellos entrarán en fase de pánico y pagarán lo antes posible para evitar seguir "siendo espiado por los cuerpos de seguridad", como se les hace creer. La nueva variante no tiene función de cifrado de archivos, los cibercriminales deben haber pensado que incluir las imágenes de la webcam era suficientemente aterrador.

Redes sociales

Facebook sigue siendo la red social por excelencia, y por lo tanto también la preferida por los ciberdelincuentes. Nada más comenzar el año se descubrió un gusano que tenía almacenadas un total de 45.000 cuentas de Facebook robadas a usuarios. Se sospecha que las usaba para publicar en el muro de sus víctimas y que así sus contactos se infectaran con el gusano.

¿Y qué hace Facebook ante esto para proteger a sus usuarios? La buena noticia es que no se queda cruzada de brazos, sino que está comprometida en la lucha contra los ciberdelincuentes.

FIG.12. *FACEBOOK HA HECHO PÚBLICAS LAS IDENTIDADES DEL GRUPO DE DELINCUENTES DETRÁS DEL GUSANO KOOBFACE.*

En Enero hizo pública información sobre los ciberdelincuentes que se encuentran detrás de Koobface, un gusano que lleva años abusando de la red social. Las identidades de estas personas son: Stanislav Avdeyko (leDed), Alexander Koltysehv (Floppy), Anton Korotchenko (KrotReal), Roman P. Koturbach (PoMuc) y Svyatoslav E. Polichuck (PsViat y PsycoMan). Lamentablemente, todos ellos siguen en libertad, viviendo cómodamente con millones de dólares robados a usuarios de todo el mundo en la ciudad de San Petersburgo, en Rusia.

A pesar de la cantidad de engaños que se expanden como la pólvora en Facebook, la curiosidad de los usuarios parece que hace que no aprendamos de nuestros errores. En este año, entre otros engaños, hemos visto como un supuesto video casero de Katy Perry y Russell Brand no para de aparecer en los muros de cientos de usuarios. Lo que vemos si uno de nuestros amigos ha caído en la trampa es lo siguiente:

FIG.13. *MENSAJE.*

FIG.14. *MENSAJE.*

Todos los likes, comentarios, etc. son falsos, ya que se trata de una imagen. Si pinchamos en "Install Plugin" efectivamente si somos usuarios de Firefox o de Chrome se nos instalará un nuevo plugin que lo que hará será empezar a publicar en nuestro muro dicho video. En caso de ser usuarios de Internet Explorer, al no tener un plugin que les pueda hacer este trabajo han optado por diversificar y mostrarnos el siguiente engaño:

FIG.15. *MENSAJE.*

Como se puede observar conserva el aspecto de Facebook, para que no nos demos cuenta de que realmente no estamos en la red social. Si pinchamos en cualquiera de los links nos llevará a una página donde nos solicitarán nuestro número de teléfono móvil para así poder pasar a cobrar por sus "servicios".

Uno de los objetivos de los ciberdelincuentes en las redes sociales es conseguir acceso a nuestra cuenta, de tal forma que puedan escribir en nuestro nombre, o acceder a nuestra información personal y a la que compartan nuestros amigos. En Twitter, tener acceso a nuestra cuenta les puede permitir mandar mensajes directos (DM) a nuestros amigos. Un caso que puede ilustrar estos ataques es el siguiente: recibimos un DM de uno de nuestros contactos indicando que han publicado fotos nuestras comprometedoras. Al pinchar en el enlace, nos lleva a la siguiente página:

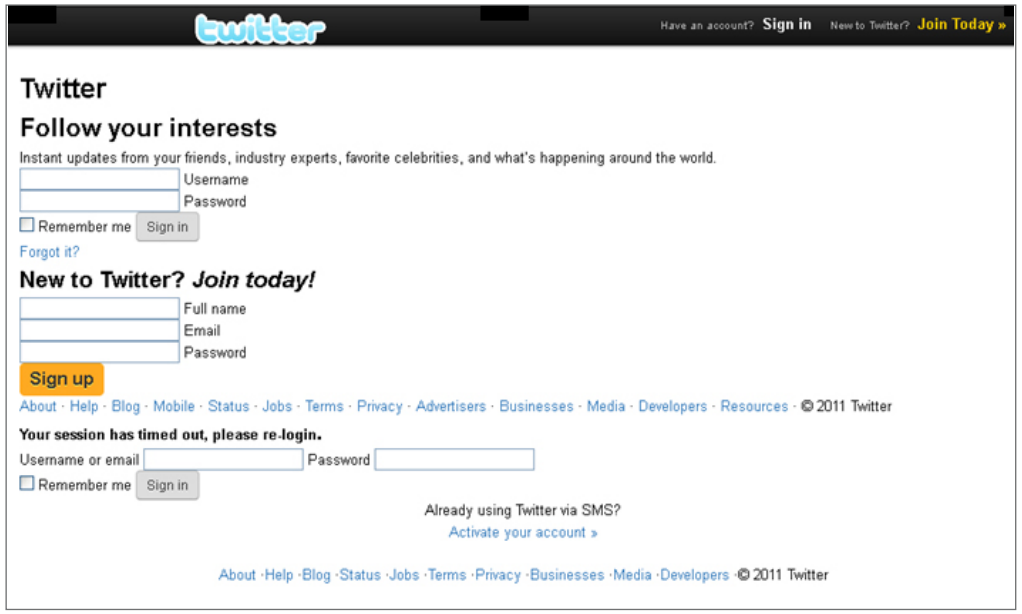


FIG.16. *PÁGINA DE PHISHING UTILIZADA PARA ROBAR CREDENCIALES DE USUARIOS DE TWITTER.*

En la página a la que somos dirigidos se nos dice que nuestra sesión en Twitter ha caducado, y nos solicita introducir de nuevo nuestro usuario y contraseña. Para hacerlo aún más creíble, todos los links que vemos en la página son los de Twitter, a excepción de los botones "Sign in" y "Sing up", que enviarán nuestra información a los ciberdelincuentes. Una vez han conseguido robarla, comenzarán a enviar DMs a todos nuestros contactos con el mismo enlace que habíamos recibido. De esta forma consiguen una gran cantidad de credenciales que pueden utilizar para propagar malware, enviar spam o sacar beneficio económico directo vendiéndolas a otros ciberdelincuentes.

LinkedIn, la conocida red social profesional, ha sufrido una intrusión en la que le han sustraído al menos 6 millones y medio de contraseñas, que fueron hechas públicas. La buena noticia es que no tenían almacenadas las contraseñas en texto plano, sino que estaban cifradas. La parte mala es que no había ningún tipo de protección extra, por lo que si no lo habéis hecho aún cambiad ya vuestra contraseña de LinkedIn. Y si compartíais la misma contraseña con algún otro servicio, haced lo mismo, y tratad de usar contraseñas diferentes.

Mac

Cuando hablamos de malware para Mac solemos mostrar alguno de los casos más llamativos. Afortunadamente, se trata normalmente de ataques que no llegan a ser muy masivos, ya que el número de nuevas amenazas para Mac, aunque creciente, no se acerca a lo que vemos en PC. Lamentablemente muchos usuarios piensan que es imposible infectarse en Mac, aunque poco a poco la gente se va dando cuenta de lo que realmente sucede, incluso en Apple. En la información de la misma página de Apple, donde te explican por qué es mejor que un PC, podíamos leer información donde explica que no pueden infectarse con virus de PC (algo falso, ya que por ejemplo los virus de macro funcionan en ambas plataformas):

FIG.17. *INFORMACIÓN MOSTRADA EN LA PÁGINA DE APPLE DONDE EXPLICAN QUE NO SE PUEDE INFECTAR GRACIAS A LAS DEFENSAS QUE TIENE SU SISTEMA OPERATIVO.*

Parece que desde Apple ya reconocen que esto no es así, ya que han eliminado dicha información de su página, poniendo en su lugar otro mensaje:

FIG.18. *NUEVO MENSAJE DE LA PÁGINA DE APPLE DONDE YA NO DICE QUE NO PUEDEN SER VÍCTIMAS DE UN VIRUS.*

Es más que probable que este cambio haya venido dado por los sucedido con un troyano, conocido como Flashback, que ha protagonizado la mayor infección conocida hasta la fecha de ordenadores Mac. Más de 600.000 Mac estaban a las órdenes de este troyano, formando una botnet nunca antes vista en esta plataforma. Una de las características más curiosas de este troyano es que antes de infectar el ordenador comprobaba si tenía instalado alguna protección antivirus. En caso afirmativo el ordenador no se infectaba, en caso negativo infectaba el Mac y comenzaba a funcionar.

Este caso ha venido a demostrar que aún hay una gran cantidad de usuarios de Mac que se creen inmunes a las infecciones, algo que los ciberdelincuentes están aprovechando.

Cibercrimen

En el caso de fraudes relacionados con entidades financieras, estamos acostumbrados a ver avanzados ataques cuyo objetivo es robar la identidad de los usuarios para así hacerse pasar por ellos y vaciar sus cuentas. Sin embargo, comenzamos 2012 con un caso bastante atípico. En Sudáfrica, el South African Postbank sufrió pérdidas de 6,7 millones de dólares en un ataque sucedido durante los 3 primeros días del año. El grupo de ciberdelincuentes detrás del ataque lo llevaba planeando desde hacía meses, y además había conseguido el control del ordenador de un empleado de la entidad.

El caso Megaupload

En enero, la conocida página Megaupload fue cerrada por el FBI, acusada de "copyright infringement" (violación de copyright). Podéis leer la nota de prensa del FBI aquí (en inglés) donde se explican los detalles del caso, y podéis ver cómo cada persona de las acusadas se podría enfrentar hasta a 50 años de cárcel.

La reacción de Anonymous no se hizo esperar, comenzando un ataque DDoS contra varias páginas web, entre las que se encontraban la del Department of Justice (Ministerio de Justicia estadounidense), la de la RIAA (Recording Industry Association of America) y la de Universal Music.

Volviendo a la nota de prensa del FBI, podemos leer lo siguiente:
"This case is part of efforts being undertaken by the Department of Justice Task Force on Intellectual Property (IP Task Force) to stop the theft of intellectual property."

(En la lengua de Cervantes: "Este caso es parte de los esfuerzos realizados por el Grupo de Trabajo sobre Propiedad Intelectual del Ministerio de Justicia para detener el robo de propiedad intelectual")

Como sabemos, en el mundo real miles de millones de dólares son robados cada año por cibercriminales (dinero real, robado de tarjetas de crédito y cuentas bancarias). Pero parece que por parte de las autoridades se da más importancia al robo de propiedad intelectual. Como todo, estamos tratando de prioridades, y parece que en este caso no están ajustadas del todo a la protección del individuo.

FIG.19. *IMAGEN QUE SE PODÍA VER AL ACCEDER A LA PÁGINA DE MEGAUPLOAD TRAS SER INTERVENIDA POR EL FBI.*

En la lucha contra el cibercrimen real, tenemos buenas noticias. Interpol ha anunciado que abrirá en 2014 un "Global Cybercrime Center" en Singapur, para mejorar la coordinación de los diferentes cuerpos de seguridad del mundo.

Tanto el grupo Anonymous como LulzSec han estado presentes a lo largo de 2012.

En Enero, con la polémica de la ley SOPA norteamericana y el ACTA, desde una de sus cuentas de Twitter el grupo dejó claras sus intenciones: "If you hated #SOPA, you'll burst into flames about #ACTA ~~http://is.gd/Bo68r4~~ Negotiated in secret. iPod searches at border crossings.". Dicho esto, comenzaron ataques contra webs oficiales de diferentes países del mundo.

En Febrero hicieron pública la grabación de una conferencia entre el FBI y Scotland Yard. Surgieron muchas especulaciones sobre cómo habrían podido hacerse con la grabación, hasta que Anonymous filtró un email que habían conseguido, enviado por un agente del FBI con el nº de

teléfono y los códigos de acceso de la conferencia, por lo que parece que han conseguido acceso a la cuenta de correo de alguno de los destinatarios, todos ellos miembros de las fuerzas del orden en diferentes países.

All,

A conference call is planned for next Tuesday (January 17, 2012) to discuss the on-going investigations related to Anonymous, Lulzsec, Antisec, and other associated splinter groups. The conference call was moved to Tuesday due to a US holiday on Monday.

Date: Tuesday, January 17, 2012
Time: 4:00 PM GMT=20
BridgeTN: 202-393-2430
Access Code: 6513211#

Please contact me if you have any questions.

Regards,

Tim
Federal Bureau of Investigation

FIG.20. *MENSAJE DEL FBI INTERCEPTADO POR ANONYMOUS.*

En Febrero Anonymous publicó el código fuente de PcAnywhere y Norton, que había sido robado en 2006. El robo fue llevado a cabo por un grupo de ciberdelincuentes que trató de chantajear a Symantec. Al ver que la compañía americana no estaba dispuesta a pagar, decidieron dar el botín a Anonymous para que lo hicieran público.

A primeros de Marzo, en una operación policial que llevaba en marcha desde el año anterior, varios miembros de LulzSec fueron arrestados. Inmediatamente se supo que Sabu, el líder de LulzSec, llevaba desde Agosto de 2011 trabajando con el FBI para conseguir datos del resto de miembros del grupo para poder identificarlos y arrestarlos.

Luis Corrons, desde el blog de PandaLabs, publicó un breve artículo al respecto haciéndose eco de la noticia y horas más tarde la reacción de Anonymous fue hackear el servidor externo donde se encuentra alojado el blog, llevando a cabo un defacement del mismo. Anonymous, en sus numerosos mensajes de Twitter, lleva a gala defender la libertad de expresión; por lo tanto, lo lógico sería pensar en un ataque contra alguna web del FBI u otros cuerpos policiales involucrados en la operación (ya han realizado acciones similares en el pasado). Sin embargo parece que la libertad de expresión sólo la defienden cuando les es favorable. En Twitter, un periodista británico les preguntó por esta cuestión, que quedó sin respuesta.

FIG.21.*ARTÍCULO EN EL BLOG DE PANDALABS HACIÉNDOSE ECO DEL ARRESTO DE MIEMBROS DE LULZSEC.*

FIG.22. *PREGUNTA DE UN PERIODISTA INGLÉS A ANONYMOUS, QUE QUEDA SIN RESPUESTA.*

Un día más tarde decidieron ir a por El Vaticano, cuya página web quedó inaccesible. 5 días más tarde volvieron a la carga, accediendo además a una base de datos de Radio Vaticana, emisora oficial de la Santa Sede, y publicando diferentes nombres de usuario y contraseñas .

Pero Anonymous y Lulzsec no son los únicos que realizan este tipo de ataques. En Febrero, la tienda de Microsoft en India fue hackeada por un grupo de ciberdelincuentes chinos. Además de realizar un defacement (sustitución de la página principal de la tienda), fueron robados los datos personales de sus clientes.

FIG.23. *LA TIENDA DE PRODUCTOS MICROSOFT EN INDIA FUE HACKEADA.*

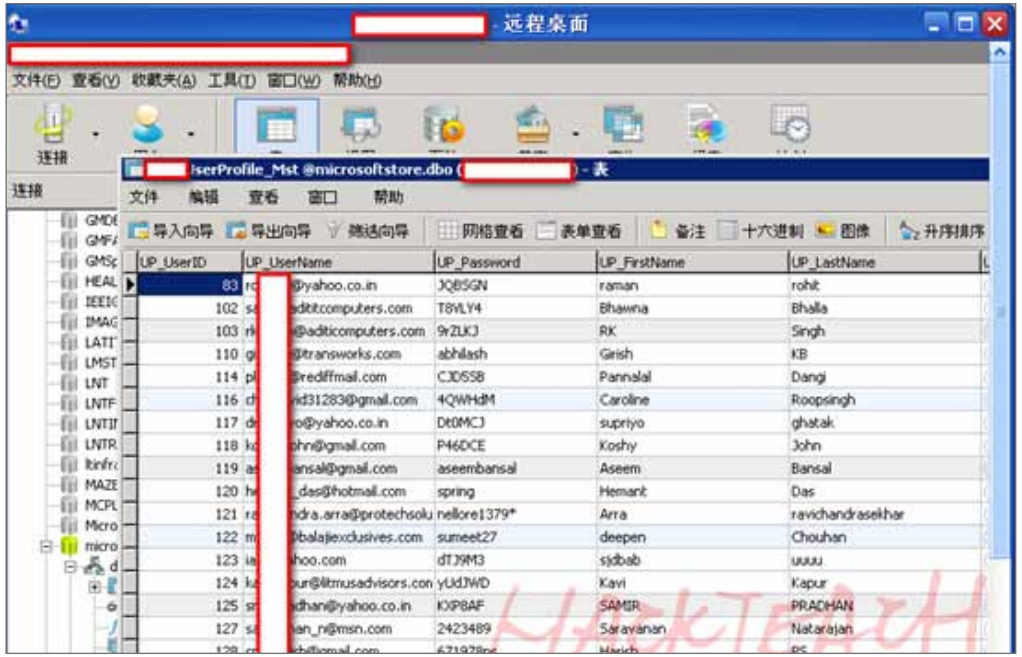


FIG.24. *CAPTURA DE PANTALLA MOSTRADA POR LOS DELINCUENTES PARA DEMOSTRAR EL ROBO DE DATOS PERSONALES DE LOS CLIENTES DE LA TIENDA DE MICROSOFT.*

El mismo mes de febrero, una famosa web de videos pornográficos, YouPorn, fue hackeada y se robaron datos de miles de sus usuarios. Estos datos fueron hechos públicos en Pastebin, lo que puso en peligro a miles de usuarios debido a la reutilización de contraseñas en múltiples servicios, práctica muy desaconsejable pero tristemente común hoy en día.

En marzo se publicó que Sony Music había tenido un problema de seguridad en el mes de mayo de 2011 y todo el catálogo de Michael Jackson había sido robado, incluyendo material inédito. Esto sucedió después de que Sony fuera hackeada el año pasado, cuando la información personal de 100 millones de clientes había sido sustraída en 2 incidentes diferentes que afectaron a la PlayStation Network y a Sony Online Entertainment.

FIG.25. *SONY MUSIC SUFRIÓ EL ROBO DE TODO EL CATÁLOGO DE MICHAEL JACKSON.*

Parece que los cibercriminales relacionados con este hackeo de Sony Music pensaron que podría ser fácil acceder a la información confidencial de la compañía, y tristemente estaban en lo cierto, aunque al menos en este caso fueron arrestados y serán juzgados a lo largo de 2013.

FIG.26. *USUARIOS AFECTADOS POR UN COMPLEMENTO MALICIOSO DEL NAVEGADOR CHROME HAN VISTO CÓMO LAS PÁGINAS DE WIKIPEDIA SE LLENABAN DE PUBLICIDAD.*

Wikipedia ha sido "víctima" de un ataque, o para ser precisos las víctimas han sido los usuarios de Wikipedia. La organización detrás de este proyecto lanzó un mensaje donde explicaba que un complemento malicioso para el navegador Google Chrome hacía que apareciera publicidad al visitar Wikipedia. En el mensaje recordaban que su sitio se financia con donaciones y que no muestran publicidad.

En muchas ocasiones hemos comentado cómo los ciberdelincuentes se han profesionalizado y siempre intentan mejorar. Un caso muy llamativo que ha sucedido este año ha tenido como protagonista a una versión del troyano bancario **SpyEye**. En esta ocasión, incorporaba un módulo que utilizaba la webcam del PC. ¿Cuál era el objetivo? Estudiar la reacción de los usuarios cuando el troyano les mostraba páginas modificadas cuando accedían a la banca online.

La compañía **Nissan** fue víctima de un ataque, en el que le robaron información perteneciente a sus propios empleados. Robaron los identificadores de usuario y las contraseñas cifradas, por lo que no se descarta que se trate de un caso de espionaje industrial.

Khosrow Zarefarid, ciudadano iraní, encontró una vulnerabilidad en el sistema bancario de su país y mandó una carta a los responsables de todos los bancos de su país afectados. Al no recibir respuesta, hackeó 3 millones de cuentas bancarias pertenecientes a al menos 22 entidades financieras distintas y creó un blog donde publicó toda la información, que incluía el nº de tarjeta de crédito junto a su correspondiente PIN. Google cerró el blog de Zarefarid (alojado en la plataforma Blogger) y todos los bancos afectados urgieron a sus clientes a que cambiaran el código PIN de sus tarjetas.

El Departamento de Salud de UTAH sufrió una intrusión desde un país de Europa del Este, donde le robaron información de al menos 900.000 ciudadanos, incluyendo entre la información su número de la Seguridad Social.

La empresa Dropbox sufrió una intrusión en la que fueron robados datos de clientes. De hecho, algunos de ellos dieron la voz de alarma cuando comenzaron a recibir spam en cuentas de correo que tenían como única función recibir comunicaciones de Dropbox.

FIG27. *DROPBOX.*

En Corea del Sur, KT Corp. fue víctima del robo de datos personales 8,7 millones de sus clientes de telefonía móvil. La policía anunciaba poco después el arresto de 2 programadores por su relación con el robo.

La agencia de noticias **Reuters** ha sufrido dos hackeos en su plataforma de blogging. En el primero fueron publicadas informaciones falsas sobre el conflicto en Siria, lo que obligó a dejar offline durante unas horas la plataforma. Apenas 2 semanas después un incidente similar tuvo lugar y se publicó una falsa noticia anunciando la muerte del príncipe Saud al-Faisal, ministro de Asuntos Exteriores de Arabia Saudí.

FIG.28. *REUTERS.*

Blizzard, la famosa compañía de videojuegos detrás de obras como Warcraft, Starcraft o Diablo, informó en Agosto que había sufrido una intrusión en su red interna y aconsejaba a todos sus usuarios que cambiaran su contraseña de acceso a su servicio online Battle.net. Confirmó que habían sido robadas tanto direcciones de correo como las contraseñas (que se encontraban cifradas).

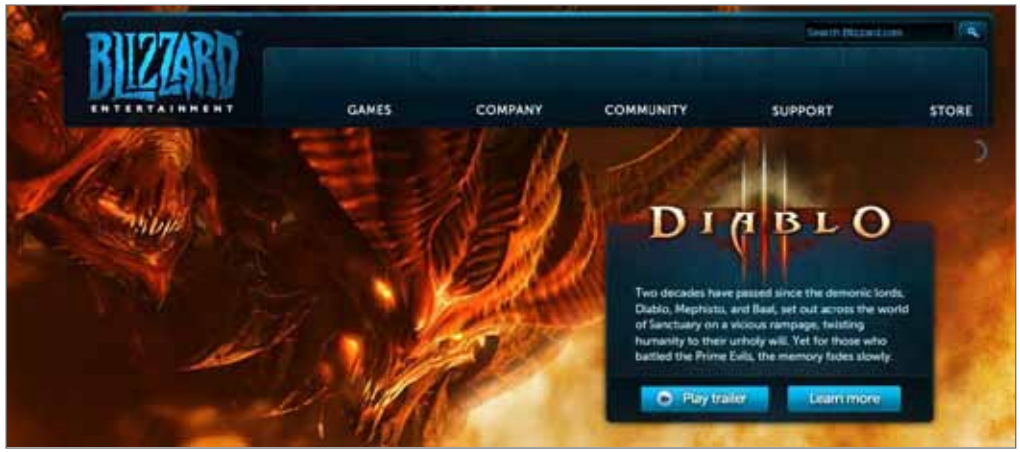


FIG.29. *BLIZZARD.*

En septiembre se supo que Adobe fue atacada, pero en este caso no para tratar de robar información de clientes sino para acceder a uno de sus servidores internos y firmar con un certificado digital de la empresa dos ejemplares de malware. El ataque sucedió en julio de este mismo año.

La compañía de seguros norteamericana Nationwide sufrió un ataque en su red que tuvo como resultado el robo de datos de más de 1 millón de clientes y empleados. La información incluía el nombre completo, dirección, número de la seguridad social y múltiples datos personales.

Además de empresas, organismos públicos de toda índole son víctimas de ataques y robo de datos. En noviembre, la Agencia Internacional de Energía Atómica dependiente de la ONU fue atacada por un grupo denominado "Parastoo", que publicó parte de la información robada en Pastebin. Este mismo mes, la Agencia de Exploración Aeroespacial de Japón descubrió que el ordenador donde almacenaban información de su programa de investigación de combustible sólido para cohetes estaba infectado con un troyano diseñado para robar información.

Aparte de todos estos ataques, también se han producido buenas noticias en la lucha contra la ciberdelincuencia:

En Reino Unido, Edward Pearson ha sido condenado a 26 meses de prisión por robar información personal de más de 8 millones de personas. Sin salir del país, Lewys Martin, conocido como el "hacker de Call of Duty" (por distribuir un troyano haciéndolo pasar por un parche del conocido

juego) ha sido condenado a 18 meses de prisión por robar datos de usuarios y posteriormente venderlos en el mercado negro.

Ryan Cleary, joven británico de 19 años que fue arrestado el año pasado por participar en diferentes ataques como miembro de LulzSec, ha ingresado en prisión de nuevo por violar su libertad condicional. Tenía prohibido acceder a Internet y las pasadas navidades accedió para comunicarse con Hector Xavier Monsegur (alias "Sabu") el cabecilla de LulzSec que llevaba meses colaborando con el FBI.

El tejano Higinio O. Ochoa III fue detenido por el FBI, acusado de hackear páginas web de diferentes fuerzas del orden y publicar listados de direcciones y teléfonos de docenas de agentes de policía. En este caso su arresto fue facilitado por el descuido del detenido, ya que en la cuenta de Twitter que utilizaba publicó una foto de los pechos de una mujer junto con un cartel que mencionaba su alias ("w0rmer"). La fotografía fue tomada con un iPhone, y la publicó sin quitar ninguno de los metadatos que por defecto son incluidos en la fotografía, como las coordenadas GPS que apuntaban a la casa de la mujer fotografiada. Esto facilitó identificar a dicha mujer, que se trataba de la novia australiana de Ochoa.

FIG.30. *FOTO PUBLICADA POR HIGINIO O. OCHOA III QUE FACILITÓ SU DETENCIÓN.*

John Anthony Borell III, otro miembro de Anonymous, ha sido arrestado por el FBI en Ohio. En esta ocasión el detenido estaba manejando su cuenta de Twitter a través de la conexión a Internet de un vecino, por lo que el FBI no tuvo muchas dificultades en dar con el delincuente.

Junaid Hussain, de Birmingham, Reino Unido y líder de TeaMp0isoN, se declaró culpable de hackear la cuenta de gmail del ex-primer ministro británico Tony Blair. Semanas más tarde se le condenó a 6 meses de prisión.

FIG.31. *TEAMPOISON.*

Joshua Schichtel, de Phoenix, Estados Unidos, ha sido condenado a 30 meses de prisión por utilizar una red de bots de 72.000 ordenadores. En concreto se dedicaba a instalar diferente malware en estos ordenadores a cambio de dinero. En uno de los casos recibió 1.500$ por instalar un troyano en cada uno de los ordenadores de la red de bots.

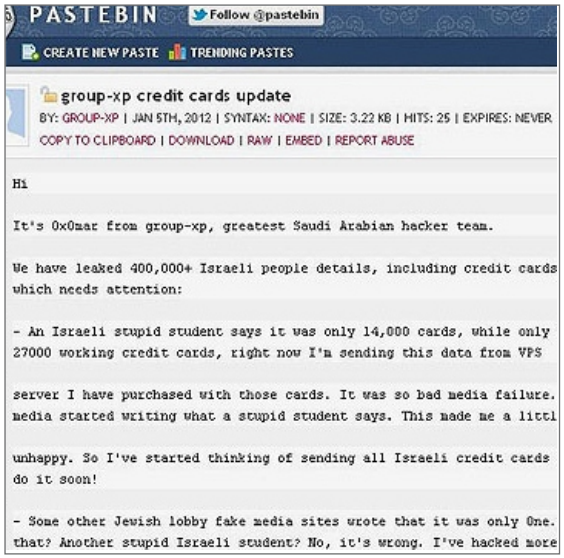
Christopher Chaney, que hackeó las cuentas de diferentes celebridades de Hollywood, como Scarlett Johansson o Mila Kunis, ha sido sentenciado a 10 años de prisión tras ser declarado culpable por hacerse con el control de 50 cuentas de correo electrónico.

En Francia, un hombre de 20 años ha sido arrestado por robar medio millón de Euros por un troyano de su creación que distribuía haciéndose pasar por diferentes aplicaciones legítimas de Android.

Todos estos hechos nos muestran cómo está cambiando el paisaje en la lucha contra la ciberdelincuencia. En Japón, por ejemplo, la Agencia Policial Nacional (equivalente al FBI en EEUU) ha ofrecido la máxima recompensa (36.000 US$) para quien pueda darles información para capturar a un ciberdelincuente. Hasta ahora este tipo de recompensas siempre se habían ofrecido para capturar sospechosos de asesinatos o incendios, pero nunca para capturar a un ciberdelincuente.

Ciberguerra

2012 ha sido un año muy activo en este campo. El 2 de Enero tuvo lugar el robo de datos de miles de tarjetas de crédito de ciudadanos israelíes. Este robo fue reivindicado por un tal 0x0mar, identificándose a sí mismo como saudí. Investigaciones posteriores revelaron la verdadera identidad de esta persona: Omar Habib, joven de 19 años de los Emiratos Árabes Unidos que vive en México. Posteriormente 0x0mar desmintió esta información.



32. MENSAJE DE 0X0MAR DONDE DECLARA HABER HECHO PÚBLICA INFORMACIÓN ROBADA DE 400.000 ISRAELÍS.

Y esta fue la primera acción que trajo tras de sí una serie de ataques y contraataques de todo tipo: robos de información de atacantes israelíes a ciudadanos saudís y viceversa, se produjo un ataque que bloqueó los sitios web de la Bolsa de Tel Aviv y la aerolínea israelí El Al, a los que han seguido otros en una espiral de ciber-violencia. Un grupo israelí afirmó haber intervenido páginas web en Arabia Saudí (Tadawul) y los Emiratos Árabes Unidos (ADX), incluyendo las de las Bolsas de Arabia Saudí y Abu Dhabi, en venganza por ataques previos de sitios web israelíes, donde habrían dejado un mensaje en la web diciendo: "Operamos en el nombre de las Fuerzas de Defensa de Israel. Si no dejáis de atacarnos, paralizaremos vuestra economía".

Por si los ánimos no estaban suficientemente crispados, Tariq al-Suwaidan, influyente predicador televisivo kuwaití, llamó a unir fuerzas en una cyberyihad contra Israel. Por si fuera poco, desde su cuenta de twitter escribió: "Creo que es necesario que las fuerzas de los hackers se unan para el proyecto de una guerra santa electrónica contra el enemigo sionista. Esa será una yihad importante y activa para el que, con la bendición de Dios, habrá una importante recompensa".

Sin alejarnos de oriente medio, otro incidente tuvo lugar en el vecino país de Siria, donde un atacante saudí consiguió hacerse con correos electrónicos del mismísimo presidente de Siria, Bashar Asad.

Y ahora pasamos de oriente medio al lejano oriente, donde desde Japón nos llegó la sorprendente noticia de que el ministerio de Defensa del país nipón había encargado a Fujitsu el desarrollo de una "ciberarma", un virus que supuestamente sería capaz de identificar, localizar y desactivar ciberataques. La información al respecto de este tema es confusa, pero en cualquier caso se trata de una mala idea, ya que aunque realizado con las mejores intenciones pueden suceder efectos adversos no contemplados que vuelvan el arma contra su creador o contra el resto del mundo. En cualquier caso nuestros usuarios pueden estar tranquilos, desde Panda detectaremos todos los virus que se creen, los hagan delincuentes públicos o privados.

Volvamos la vista ahora a los dos protagonistas habituales de esta sección, China y Estados Unidos. En Enero se publicó que hackers chinos habían utilizado un troyano para romper el código de smart cards utilizadas por el Departamento de Defensa estadounidense, tarjetas necesarias para acceder tanto a lugares físicos como dentro de la red que requieren un acceso restringido. Si realmente consiguieran romper la seguridad de las smart cards podrían acceder de forma relativamente sencilla a información confidencial.

Sin dejar China, supimos también que desde ese país se había estado espiando a la empresa Nortel, tras comprometer las credenciales de 7 ejecutivos de la compañía, incluido su CEO. Al menos desde el año 2000 habrían estado accediendo a información interna de la empresa.

En la mayoría de casos de ciberguerra o ciberespionaje sólo podemos deducir / especular con que hay un país detrás de un determinado ataque. No es usual que un país diga abiertamente que ellos han sido los atacantes. Sin embargo, las cosas están cambiando y cada vez se habla más abiertamente de estos temas; sin ir más lejos, Hillary Clinton, Secretaria de Estado estadounidense hizo unas declaraciones en mayo donde reconoció que EEUU había hackeado páginas web pertenecientes a un grupo de Al Qaeda que operaba en Yemen.

En concreto dichas páginas contenían anuncios vanagloriándose del asesinato de americanos, y en el hackeo los modificaron mostrando información sobre civiles musulmanes asesinados en ataques terroristas perpetrados por Al Qaeda.

En Corea del Sur, un alto oficial ha denunciado que Corea del Norte está tratando de robar secretos militares y sabotear sus sistemas de defensa de la información utilizando expertos entrenados específicamente para penetrar en su red de información militar.

Flame

Si tenemos que elegir un protagonista del año, sin duda el elegido sería Flame. Es un troyano que ha infectado ordenadores en países de oriente medio y su objetivo es el robo de información.

Se trata claramente de un caso de ciberespionaje, y además está relacionado con el famoso Stuxnet (troyano diseñado para sabotear el programa nuclear iraní, organizado por los gobiernos de Estados Unidos e Israel). Normalmente los ataques dirigidos se llevan a cabo con troyanos, sin embargo en esta ocasión Flame es un gusano. Los gusanos se autoreplican, por lo que en un momento dado el creador / propietario del gusano no puede controlar a quién está infectando o dónde, y cuando tienes unos objetivos específicos quieres permanecer por debajo de la señal del radar para evitar ser descubierto. ¿Cómo ha solucionado Flame este inconveniente? Aunque es un gusano, sus mecanismos de infección están desactivados. Parece que quien está detrás de este ataque puede activar esta característica cuando lo necesite, una estrategia inteligente cuando quieres pasar desapercibido.

Una de las características más llamativas de Flame es que puede robar información de múltiples formas al mismo tiempo, y tiene una serie de módulos que le dan la capacidad de robar todo tipo de información de su objetivo, incluso puede llegar a encender el micrófono para grabar cualquier conversación que esté manteniéndose cerca del ordenador.

Como hemos apuntado, se ha tratado de un ataque dirigido a víctimas concretas en países de Oriente Medio. Esto ha posibilitado que Flame pudiera estar trabajando durante años hasta que las compañías de seguridad han conseguido detectarlo. No ha faltado quien se ha apuntado a la típica teoría de la conspiración donde se apunta a que determinados gobiernos hayan forzado a las compañías antivirus para que no detectaran Flame. Por supuesto esto es totalmente falso, y de hecho en cuanto se ha conocido, ha sido detectado por todas ellas.

¿Por qué se ha tardado tanto en detectar Flame? Ningún antivirus puede garantizar un 100% de detección de amenazas desconocidas. Es bastante sencillo de entender, los ciberdelincuentes profesionales intentarán por todos los medios eludir la detección de su creación antes de empezar a utilizarla. Probarán todos y cada uno de los antivirus no sólo para probar que no es detectado por firmas, sino por ninguna de las diferentes capas de protección existentes (análisis heurísticos, bloqueo por comportamiento, etc.). Teniendo suficientes recursos puedes montar un proceso de Calidad que garantice que no haya ninguna detección, al menos en un primer momento. Será cuestión de tiempo que los antivirus detecten la amenaza, así que la tarea más importante a partir de ese momento es pasar desapercibidos. Por ejemplo, infectando sólo un pequeño número de ordenadores donde se encuentra la información que quieres robar, en lugar de llevar a cabo una infección masiva.

Este año también hemos sido testigos de varios casos de ciberespionaje dirigido a periodistas que tratan de informar en diferentes países. Por ejemplo, en Marruecos una serie de periodistas locales premiados por Google por su trabajo durante la "Primavera Árabe" fueron infectados con un troyano para Mac. En China, corresponsales extranjeros en Pekín fueron víctimas de dos oleadas de ataque de malware a través de mensajes de correo semanas antes del congreso del Partido Comunista Chino.

FIG.33. *SAUDI ARAMCO.*

Este trimestre también hemos visto un par de casos de infecciones en empresas energéticas de Oriente Medio que aún no sabemos si podrían estar relacionados entre sí o ni siquiera si se trata de algún tipo de ciberataque, aunque en base a nuestra experiencia parece que todo apunta a ello. Saudi Aramco (Saudi Arabian Oil Co) fue víctima de una infección que llevó a la empresa a cortar completamente la conexión al exterior de todos sus sistemas informáticos de forma preventiva

FIG.34. *RASGAS.*

Por otro lado RasGas, compañía qatarí de energía dedicada al gas natural licuado sufrió una infección. Ni en este caso ni en el de Saudi Aramco la producción de ambas compañías fue afectada.

03| El 2012 en cifras

A lo largo de 2012 han aparecido 27 millones nuevas muestras de malware, 74.000 al día. En total tenemos registradas 125 millones de muestras de malware en PandaLabs. El crecimiento sigue imparable, impulsado por ciberdelincuentes cuyo ánimo de lucro les impulsa a tratar de saltarse las protecciones antivirus. Los troyanos han sido los grandes protagonistas, 3 de cada 4 nuevas muestras de malware creadas son de este tipo. Aquí tenemos los datos en detalle:

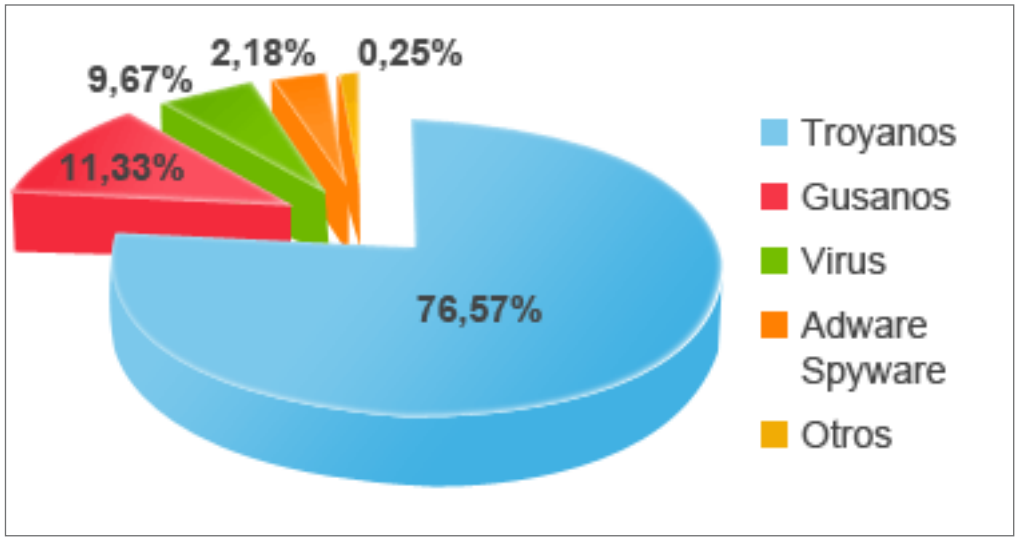


FIG.35. *NUEVO MALWARE CREADO EN 2012, POR TIPO.*

Comparando los datos con años anteriores podemos observar cómo la proporción de troyanos no deja de aumentar. En 2010 ya eran más de la mitad de todo el malware creado, el 56%, en 2011 subió de forma espectacular al 73,31% y en 2012 ya llegamos al 76,57%. Los gusanos pasan a ser el 2º tipo de malware, con un 11,33% frente al 8,13% de 2011, y los virus bajan a la 3ª posición con un 9,67%, cuando en 2011 eran el 14,24%.

Si analizamos las infecciones causadas por el malware en el mundo, gracias a los datos aportados por la Inteligencia Colectiva, vemos que las infecciones también están protagonizadas por los troyanos con un 76,56%, casi el mismo porcentaje de troyanos creados. Parece que los ciberdelincuentes han conseguido infectar con troyanos más ordenadores que en años anteriores. En 2011 el porcentaje de ordenadores infectados con troyanos era del 66,18 por lo que vemos cómo han logrado una subida de algo más de 10 puntos. Una de las causas por la que se explica este aumento de infecciones es por el cada vez más frecuente uso de kits de infección, como el Black Hole, que integran diferentes tipos de vulnerabilidades para infectar automáticamente ordenadores sin la intervención del usuario. Veamos cómo se reparten las infecciones en todas las categorías:

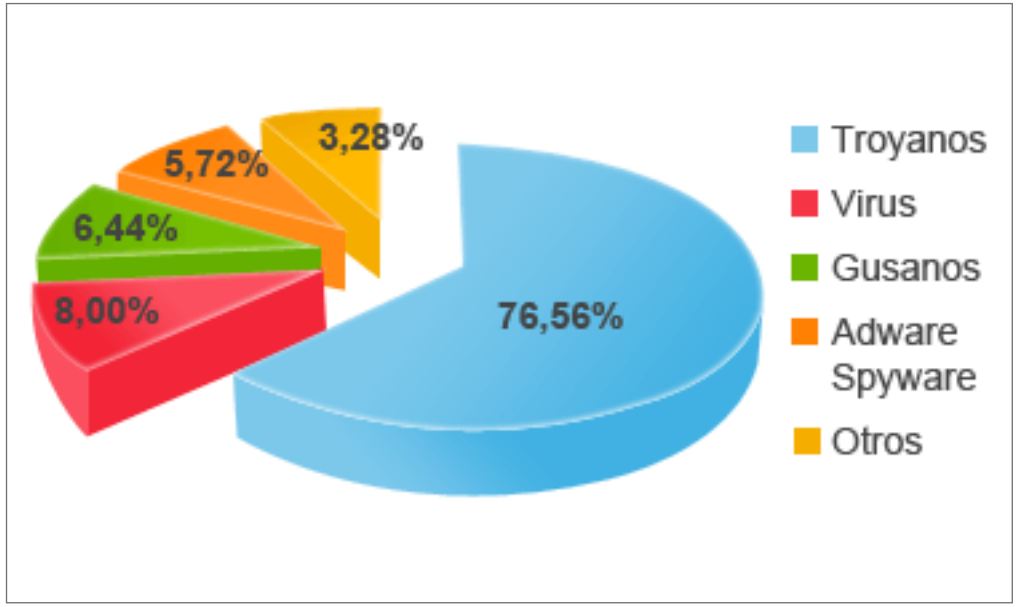


FIG.36. *INFECCIONES POR TIPO DE MALWARE EN 2012.*

No todo son victorias para los ciberdelincuentes, si vemos el porcentaje global de ordenadores infectados veremos que es del 31,98%, una bajada considerable si comparamos con los datos de 2011, que arrojaban un 38,49% de infecciones.

Otro análisis que podemos realizar es el geográfico. ¿Qué países están más infectados? ¿Cuáles están mejor protegidos? El país más infectado del mundo en 2012 ha sido China, triste protagonista habitual de este ranking, con más de la mitad de sus ordenadores infectados: un 54,89%. En segunda posición le sigue de cerca Corea del Sur, con un 54,15% de infecciones, y más alejado ya en tercera posición tenemos a Taiwán con un 42,14%

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

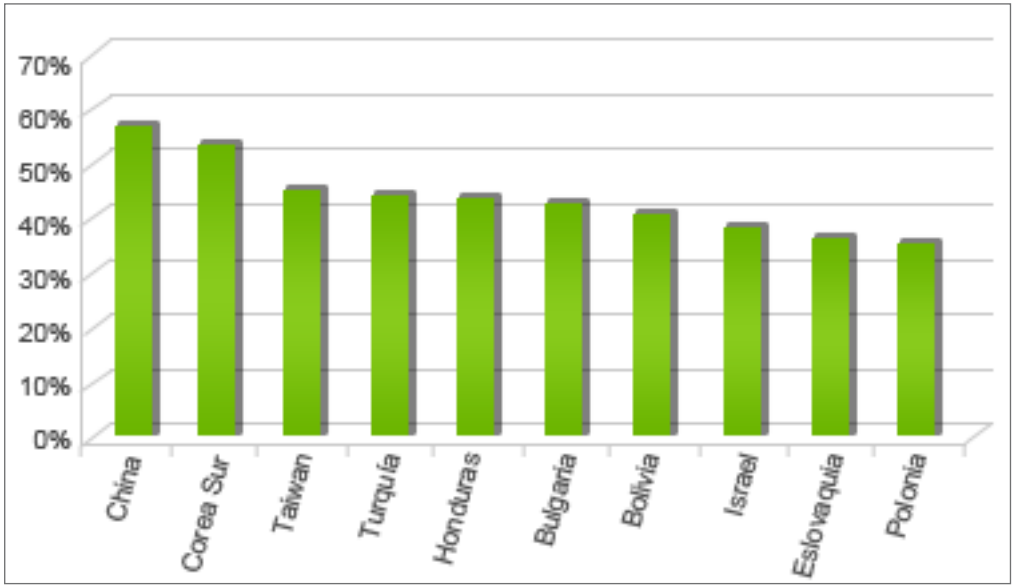


FIG.37. *PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN.*

Vemos que los países más infectados están muy repartidos geográficamente, con países de Asia, Europa, Centroamérica y Sudamérica. El resto de países con un porcentaje mayor a la media mundial son Lituania (35,46%), Tailandia (35,37%), Perú (35,05%), Argentina (34,79%), España (34,06%), Nicaragua (34,03%), Guatemala (33,89%), Ecuador (33,68%), El Salvador (32,86%), Brasil (32,09%) y Chile (31,98%).

Si analizamos los datos de los países mejor posicionados, aquellos cuyo índice de infección es más bajo, podemos observar que 9 de ellos son europeos, siendo Canadá el único país no perteneciente al viejo continente. Suecia se sitúa a la cabeza, con un 20,25% de infecciones, seguido de cerca por Suiza, con sólo un 20,35%. En tercer lugar está Noruega con un 21,03% de infecciones.

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

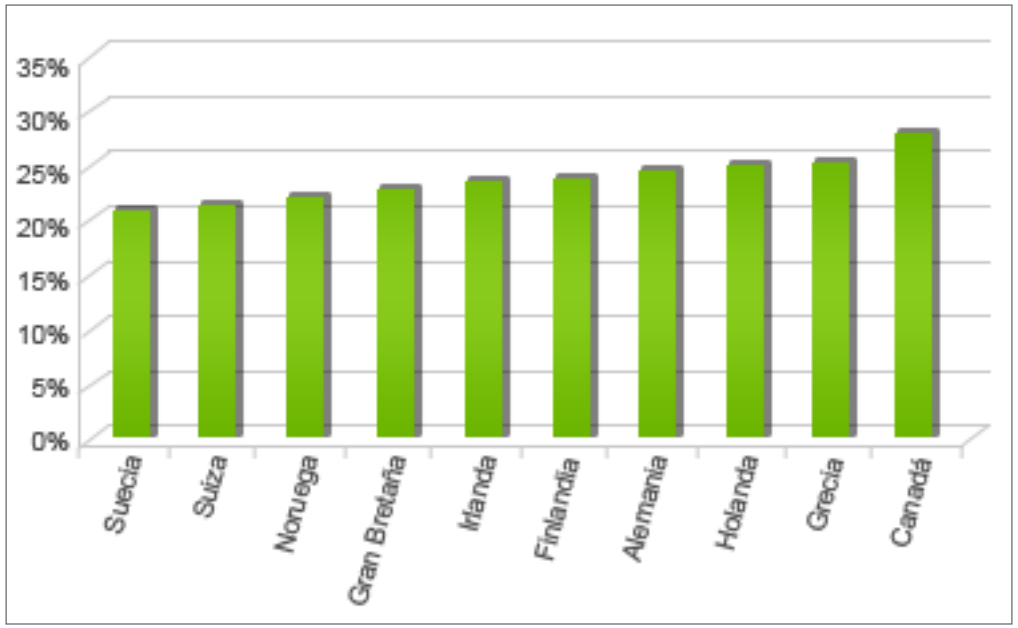


FIG.38. *PAÍSES CON MENOR ÍNDICE DE INFECCIÓN.*

El resto de países con un porcentaje menor a la media mundial son República Checa (31,84%), Rumanía (31,54%), Colombia (31,49%), Estonia (31,33%), Estados Unidos (30,52%), Eslovenia (30,37%), Italia (30,25%), Venezuela (29,81%), México (29,81%), Costa Rica (29,73%), Panamá (29,61%), Francia (29,19%), Paraguay (28,57%), Sudáfrica (27,94%), Dinamarca (27,65%), Hungría (27,37%), Uruguay (27,23%), Austria (27,03%), Bélgica (27,02%), Portugal (26,78%), Australia (26,60%), Letonia (26,06%), Japón (26,00%) y Nueva Zelanda (25,76%).

04| Tendencias de Seguridad 2013

Hemos visto cómo ha transcurrido todo 2012: ataques en redes sociales y ciberdelincuencia por doquier. ¿Qué podemos esperar para 2013?

Vulnerabilidades

Se trata, sin duda, del método de infección predilecto utilizado tanto por ciberdelincuentes como por agencias de inteligencia de países para lograr comprometer sistemas de forma transparente. En 2012 hemos visto como Java, que está instalado en cientos de millones de dispositivos, ha sido comprometido de forma recurrente y utilizado de forma activa para infectar a millones de usuarios. En 2º lugar se encuentra Adobe, ya que dada la popularidad de sus aplicaciones (Acrobat Reader, Flash, etc.) y sus múltiples agujeros de seguridad, es uno de los objetivos preferidos para infectar de forma masiva a usuarios, además de como herramienta para realizar ataques dirigidos.

Si bien podemos pensar que quienes corren un mayor riesgo son los usuarios domésticos, hay que recordar que la actualización de aplicaciones, algo primordial para protegerse ante este tipo de ataques, es un proceso muy complejo en empresas, donde hay que coordinar la actualización de todos los equipos. Además, al mismo tiempo hay que asegurarse de que todas las aplicaciones que se utilizan en la empresa deben funcionar correctamente. Esto hace que los procesos de actualización sean lentos, lo que abre una ventana de tiempo que es explotada tanto para robar información en general, como para realizar ataques dirigidos en busca de información confidencial.

Redes sociales

La segunda técnica más utilizada es la ingeniería social. Engañar al usuario para que sea éste el que colabore para infectar su equipo y robarle información es una tarea sencilla, ya que no existen aplicaciones de seguridad que protejan al usuario de sí mismo. En este contexto, el uso de redes sociales (Facebook, Twitter, etc.), lugares donde cientos de millones de usuarios intercambian información, en muchas ocasiones de índole personal, hace que sea el coto de caza preferido para engañar a los usuarios.

Deberemos prestar atención especial a Skype, que al sustituir a Messenger puede convertirse en un objetivo para los ciberdelincuentes.

Malware para dispositivos móviles

Android se ha convertido en el sistema operativo dominante en dispositivos móviles. Google anunció en septiembre de 2012 que habían alcanzado la escalofriante cifra de 700 millones de activaciones de Android. Si bien principalmente es utilizado en smartphones y tablets, su versatilidad y el hecho de no tener que pagar licencia para su uso va a hacer que nuevos tipos de dispositivos se sumen al uso del sistema operativo de Google. Cada vez veremos más extendido su uso, desde televisores a todo tipo de electrodomésticos, lo que abre todo un mundo aún desconocido de posibles ataques que habrá que seguir de cerca.

Ciberguerra / Ciberespionaje

A lo largo de 2012 hemos sido testigos de diferentes tipos de ataques contra naciones. Cabe mencionar Oriente Medio, donde el conflicto también está presente en el ciberespacio. De hecho muchos de estos ataques ya ni siquiera son llevados a cabo por gobiernos de sus diferentes países, sino por ciudadanos que consideran que deben defender a su nación atacando a los vecinos utilizando todos los medios a su alcance.

Además los diferentes gobiernos de las principales naciones del mundo están creando cibercomandos para prepararse tanto en la defensa como en el ataque, por lo que la "carrera ciberarmamentística" irá a más

Crecimiento de malware

El hecho de que el crecimiento de la cantidad de malware sea exponencial es algo que se ha venido repitiendo desde hace 2 décadas. Hablamos de cifras estratosféricas, con decenas de miles de nuevos ejemplares de malware apareciendo cada día, por lo que este crecimiento continuado parece que está muy lejos de llegar a su fin.

A pesar de que las fuerzas del orden de los diferentes países cada vez están mejor preparadas para luchar contra este tipo de delincuencia, se encuentran aún lastradas por la carencia de fronteras en Internet. Cada cuerpo de policía de una nación puede actuar en su territorio, mientras que un sólo ciberdelincuente puede lanzar un ataque desde un país A, robar datos a ciudadadanos de un país B, mandar los datos robados a un servidor ubicado en el país C y él estar viviendo en el país D. Esto se puede hacer con unos pocos clicks, mientras que para que la policía pueda actuar en colaboración con fuerzas del orden de otros países es una tarea que, como poco, puede llevar meses. Es por ello que los ciberdelincuentes aún están viviendo su particular edad de oro.

Malware para Mac

Casos como el de Flashback, ocurrido en 2012, han venido a demostrar que no sólo Mac no es inmune a ataques de malware, sino que se dan también infecciones masivas afectando a cientos de miles de usuarios. Si bien el número de malware para Mac sigue siendo bajo comparado con el malware para PC, esperamos que siga aumentando. El hecho de tener cada vez un mayor número de usuarios sumado a los agujeros de seguridad y a la falta de concienciación de los usuarios respecto a la seguridad (por un exceso de confianza), hace que el atractivo hacia esta plataforma siga en aumento durante el próximo año.

Windows 8

Por último, aunque no menos importante, debemos hablar de Windows 8. El último sistema operativo de Microsoft, como todos sus predecesores, también sufrirá ataques. Los ciberdelincuentes no se van a centrar sólo en él, pero se asegurarán de que sus creaciones funcionen igual de bien desde Windows XP a Windows 8, pasando por Windows 7.

Uno de los atractivos del nuevo sistema operativo de Microsoft es que puede ser utilizado tanto en PCs como en tablets o smartphones. Es por ello que si se consiguen desarrollar ejemplares de malware funcionales que permitan robar información en cualquiera que sea el dispositivo utilizado, podríamos ver un desarrollo específico de malware para Windows 8 que podría llevar los ataques un paso más allá.

05| Conclusión

Tenemos por delante un año apasionante, con nuevos retos a los que hacer frente en el campo de la seguridad:

Los usuarios de Android tendrán que hacer frente a un número creciente de ataques por parte de ciberdelincuentes que tratarán de robar información de sus víctimas.

El ciberespionaje y la ciberguerra van a ir a más, un número creciente de países está organizando sus propios comandos de ciberdefensa. Existe una gran preocupación tanto por la parte de la información que puede ser comprometida a través de ataques, como por el ataque directo a infraestructuras críticas mediante la utilización de malware.

Las empresas tendrán que extremar aún más sus medidas de seguridad para poder evitar ser víctimas del creciente número de ataques realizados por ciberdelincuentes. En este punto jugará un papel clave la protección frente a vulnerabilidades de las aplicaciones instaladas en el parque informático de las empresas, siendo Java el mayor riesgo actualmente debido a sus múltiples agujeros de seguridad.

En el blog de PandaLabs, http://www.pandalabs.com podréis tener acceso a todos los avances y descubrimientos que haremos desde el laboratorio.

06| 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.

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+
http://www.gplus.to/pandasecurityes

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

PANDA SECURITY