Informe trimestral PandaLabs

Julio - Septiembre 2012

01| Introducción

Una vez más, los troyanos son los grandes protagonistas tanto en el apartado de nuevo malware creado como en el porcentaje de infecciones causadas. Los meses de julio y agosto, aunque han estado más tranquilos en otros sectores, no lo han sido en cuanto a la creación de malware. También repasamos los países con mayor porcentaje de ordenadores infectados y los más seguros. China vuelve a liderar esta tabla e Irlanda entra en el top de países menos infectados.

En el tercer trimestre hemos visto ataques que han sufrido empresas tan importantes como Dropbox, Reuters, Adobe y Blizzard, que se han visto comprometidas, ya sea a través de hackeos de sus páginas web o de robo de datos tanto de la propia empresa como de los datos de sus clientes. Aunque no todo son malas noticias, como podemos ver con el arresto del líder de TeaMp0isoN por hackear la cuenta de Toni Blair y de un estadounidense condenado por utilizar una red de bots para instalar malware.

La ciberguerra, con casos en Marruecos, China y Oriente Medio, y las infecciones para usuarios de dispositivos móviles también protagonizan este informe de PandaLabs.

02| El trimestre de un vistazo

Este trimestre hemos visto cómo numerosas empresas han sido hackeadas. 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.

Cibercrimen

En Corea del Sur, KT Corp. fue víctima del robo de datos personales de 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.1. *DROPBOX.*

FIG.2. *REUTERS.*

Blizzard, la famosa compañía de videojuegos detrás de obras como World of 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).

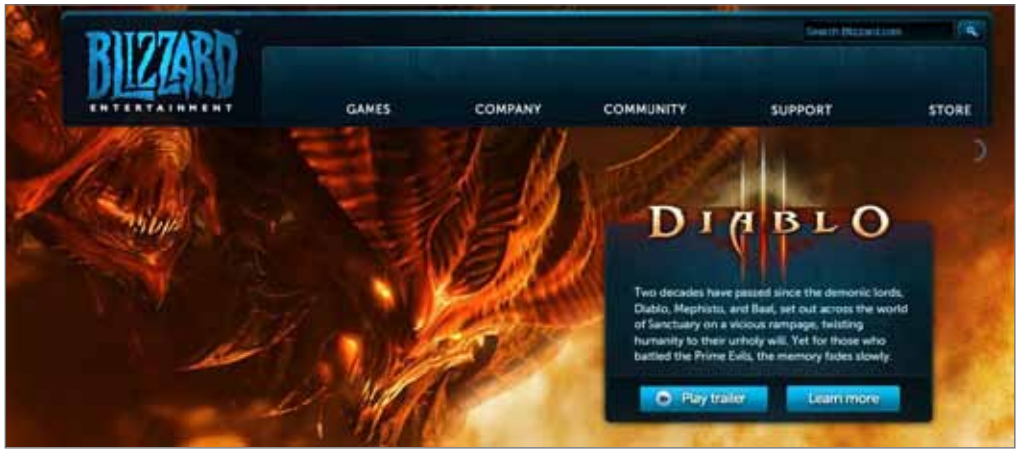

FIG.03. *BLIZZARD.*

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.

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

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.04. *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.

Ciberguerra

En este trimestre 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.05. *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.06. *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.

Móviles

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 Google Play. 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.

FIG.07. *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.

FIG.08. *ANDROID.*

Sin ir más lejos, este mismo trimestre hemos vuelto a ser testigos de otro caso en Google Play, 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.

¿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.

03| El trimestre en cifras

En el tercer trimestre de 2012 hemos recogido en el laboratorio más de 6 millones de muestras, en línea con lo que hemos visto durante la primera mitad del año. Los troyanos siguen siendo los grandes protagonistas, casi 3 de cada 4 nuevas muestras de malware creadas son troyanos. Aquí tenemos los datos en detalle:

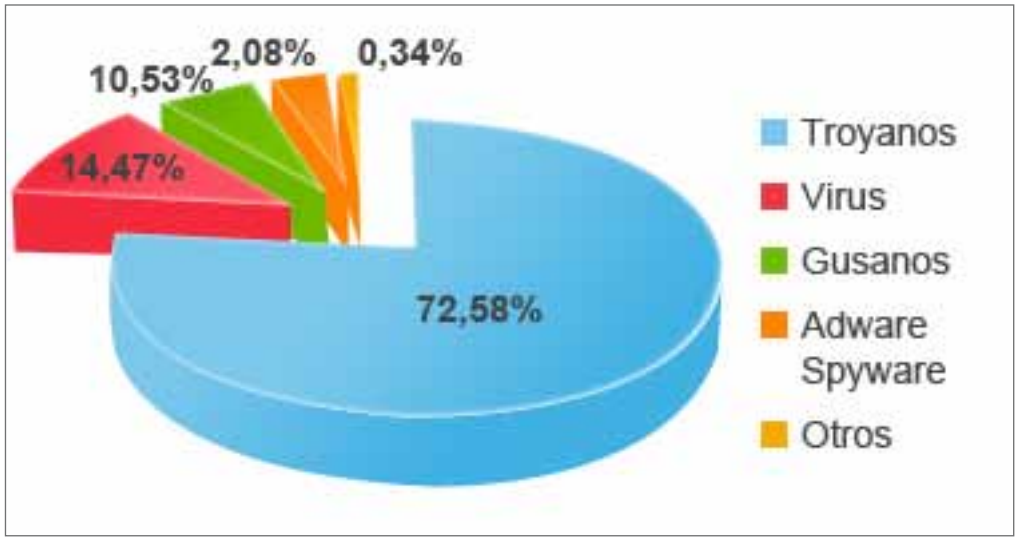

FIG.20. *NUEVO MALWARE CREADO EN EL TERCER TRIMESTRE DE 2012, POR TIPO.*

Los porcentajes recogen la cantidad de muestras creadas en el tercer trimestre de 2012, pero no siempre se traduce en los datos de infecciones reales. En la siguiente gráfica vemos lo que realmente sucede en los ordenadores de todo el mundo, recogiendo los datos obtenidos por nuestra red de sensores que forman la Inteligencia Colectiva.

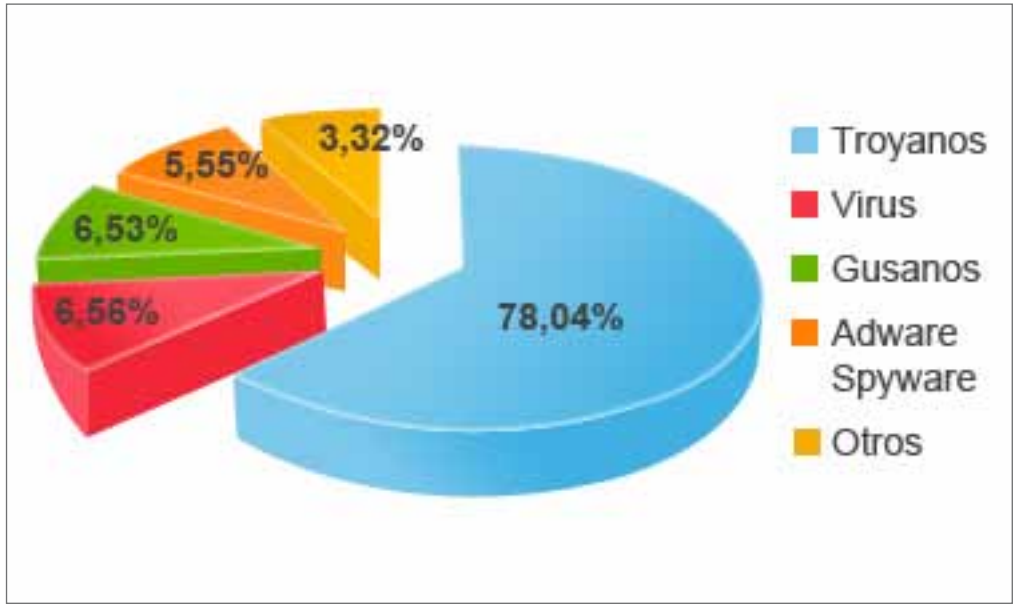

FIG.21. *INFECCIONES POR TIPO DE MALWARE EN EL PRIMER TRIMESTRE DE 2012.*

El robo de información es el motivo por el que se crean la mayoría de muestras de malware, y esto lo demuestra el resultado abrumador de los troyanos, siendo un 78,04% de todas las nuevas muestras de malware encontradas desde PandaLabs.

Otro análisis que podemos realizar es el geográfico. ¿Qué países están más infectados? ¿Cuáles están mejor protegidos? La media de PCs infectados a nivel mundial es del 30,68%, algo más baja que la del anterior trimestre de 2012. El país más infectado del mundo en este trimestre ha sido China, que tristemente suele protagonizar este ranking, con un 53,17% de PCs infectados, seguido por Corea del Sur con un 52,77%, siendo los dos únicos países del mundo que superan el 50% de ordenadores infectados. Le sigue en el ranking Turquía, con un 42,51%.

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

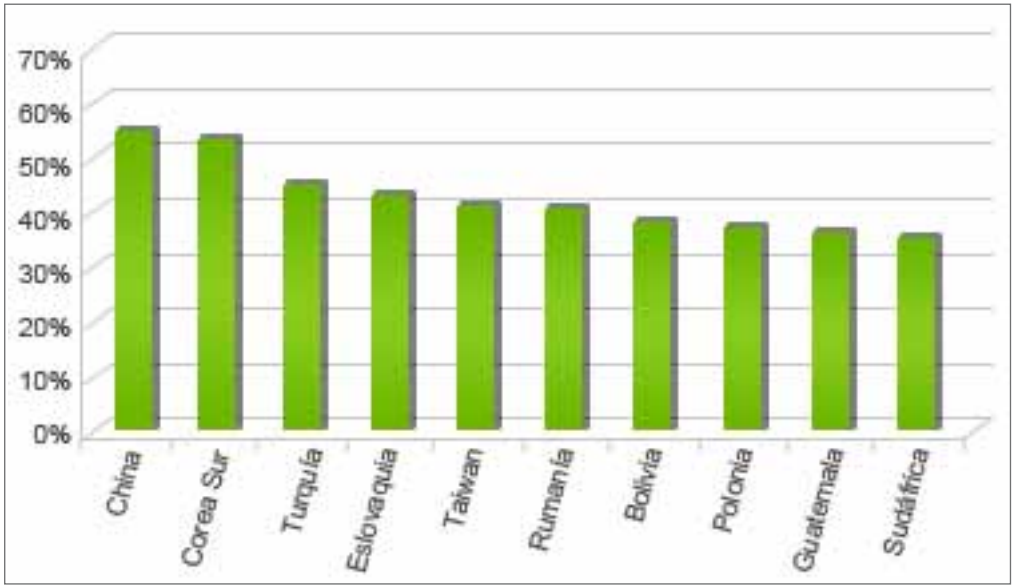

FIG.22. *PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN.*

Vemos que los países más infectados están muy repartidos geográficamente, con países asiáticos, europeos, sudamericanos e incluso africanos. Si analizamos los datos de los países mejor posicionados, aquellos cuyo índice de infección es más bajo, podemos observar que 8 de ellos son europeos, siendo Canadá y Australia los únicos países no pertenecientes al viejo continente. Irlanda se sitúa a la cabeza, con un 20% de infecciones, seguido de cerca por Noruega, con sólo un 20,16% de infecciones. En tercer lugar está Suecia, país que durante los últimos años se ha mantenido entre los menos infectados del mundo, con un 22,46% de infecciones.

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

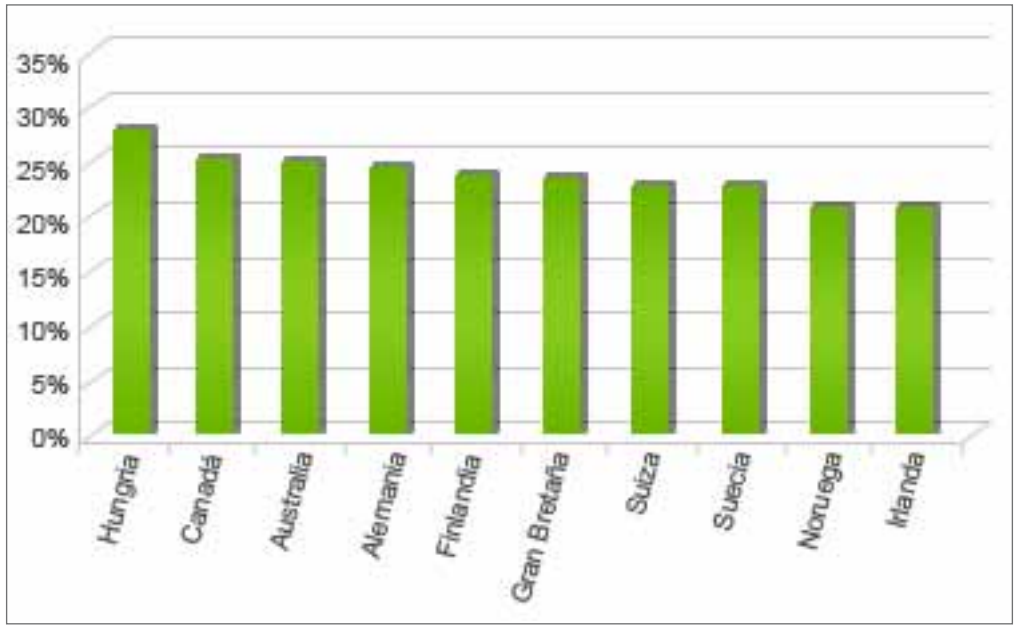

FIG.23. *PAÍSES CON MENOR ÍNDICE DE INFECCIÓN.*

04| Conclusión

Hemos visto durante este trimestre que grandes empresas han sufrido robos de datos, no sólo propios, sino también de sus clientes, poniendo en riesgo tanto a la empresa como a sus usuarios. Nos gustaría decir que el problema de robo de información se ha minimizado, pero hace falta algo más que ilusión para acabar con estos problemas. No sólo se roban datos, sino que también, como hemos visto en el caso de Adobe, se accede a los servidores para introducir firmas digitales válidas en ejemplares de malware y poder llegar a infectar a un porcentaje mayor de usuarios.

Aún nos queda buena parte del año, y debemos seguir haciendo frente a los creadores de malware y ciberdelincuentes. Aunque el número de amenazas se ha mantenido estable durante el año, alrededor de 6 millones de ejemplares, esto no quiere decir que debamos confiarnos.

Hasta aquí las noticias más destacadas del tercer trimestre de 2012. Deseamos, aunque no estamos seguros de que sea así, que el próximo número tengamos más noticias sobre la lucha contra la ciberdelincuencia y menos sobre empresas que hayan visto comprometidos sus datos. Por su bien y por el de todos nosotros.

En el próximo Informe de PandaLabs haremos un resumen de todo lo que ha sucedido durante 2012 y sacaremos nuestra bola de cristal para adelantaros las tendencias de 2013.

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 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