Informe trimestral PandaLabs

Enero - Marzo 2012

01| Introducción

Bienvenidos a 2012, un año que en el mundo de la seguridad promete ser aún más apasionante que el año anterior. En este informe analizaremos las cifras que arrojan nuestros sistemas de análisis de malware desde la nube, donde veremos cómo la situación siempre es susceptible de empeorar y se baten varios récords, como el que 4 de cada 5 nuevas muestras de malware creadas durante este trimestre son troyanos.

Analizaremos diferentes ataques de los que hemos sido testigos durante estos 3 primeros meses de 2012, donde destaca la aparición de un nuevo jugador, el conocido "virus de la policía". Describiremos algunos ataques realizados a través de la red social con mayor número de seguidores, Facebook, y daremos un repaso a los últimos ataques realizados por el colectivo Anonymous. También recordaremos una de las operaciones policiales más mediáticas de los últimos tiempos, el caso Megaupload.

En el ámbito de la ciberguerra describiremos lo sucedido en Enero en Oriente Medio, cuando se vivieron una serie de incidentes de seguridad con trasfondo político.

Esperamos que disfrutéis de este informe y os sea de utilidad para estar preparados ante lo que se nos avecina.

02| El trimestre de un vistazo

Durante los últimos meses hemos sido testigos de un incremento de ataques haciendo uso de técnicas de ransomware, llegando a convertirse en una de las infecciones más "populares", incluso por encima de los falsos antivirus o rogueware.

"El virus de la policía"

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.

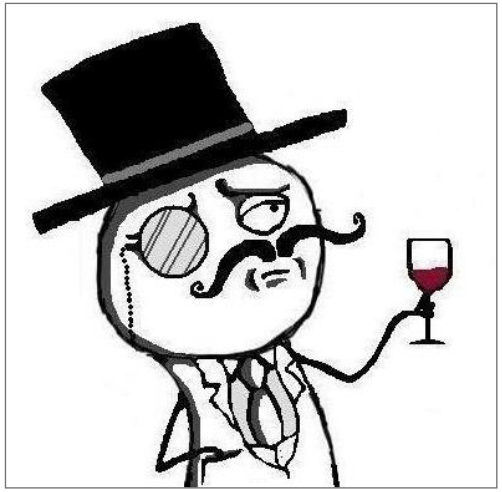


FIG.1. *ICONO UTILIZADO POR UN EJEMPLAR DEL "VIRUS DE LA POLICÍA.*

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

FIG.02. ***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.03. ***MENSAJE DEL TROYANO EN ALEMÁN.***

FIG.04. *MENSAJE DEL TROYANO EN HOLANDÉS.*

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

FIG.03. *RSA SUFRIÓ UNA INTRUSIÓN EN MARZO.*

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

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

Móviles

Como viene siendo habitual, el protagonista en esta sección es Android, el sistema operativo de Google, que ve cómo al mismo tiempo que crece su cuota de mercado aumentan las amenazas que se crean para su sistema. 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 instalarlo también instalaban un troyano que se dedicaba a enviar SMS a números Premium.

De hecho, este mismo trimestre hemos sabido que Google, cansada de los problemas con aplicaciones maliciosas en su Play Store, ha comenzado a analizar las aplicaciones antes de publicarlas, buscando comportamientos anómalos. Según ellos mismos han conseguido disminuir la descarga de aplicaciones maliciosas en un 40%.

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) fue detectado este trimestre y se hacía pasar por una aplicación legítima, pero fuera de la Play Store.

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 almacenados 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 infectarían con el gusano.

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

FIG.08. *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 trimestre, 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.09. *MENSAJE.*

Al pinchar en el enlace para ver el video, llegamos a una página que se hace pasar por Facebook, donde se nos indica que hace falta instalar un plugin para poder ver el supuesto video:

FIG.10. *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.11. *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".

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").

FIG.12. *IMAGEN QUE SE PODÍA VER AL ACCEDER A LA PÁGINA DE MEGAUPLOAD TRAS SER INTERVENIDA POR EL FBI.*

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.

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.

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.13. *LA TIENDA DE PRODUCTOS MICROSOFT EN INDIA FUE HACKEADA.*

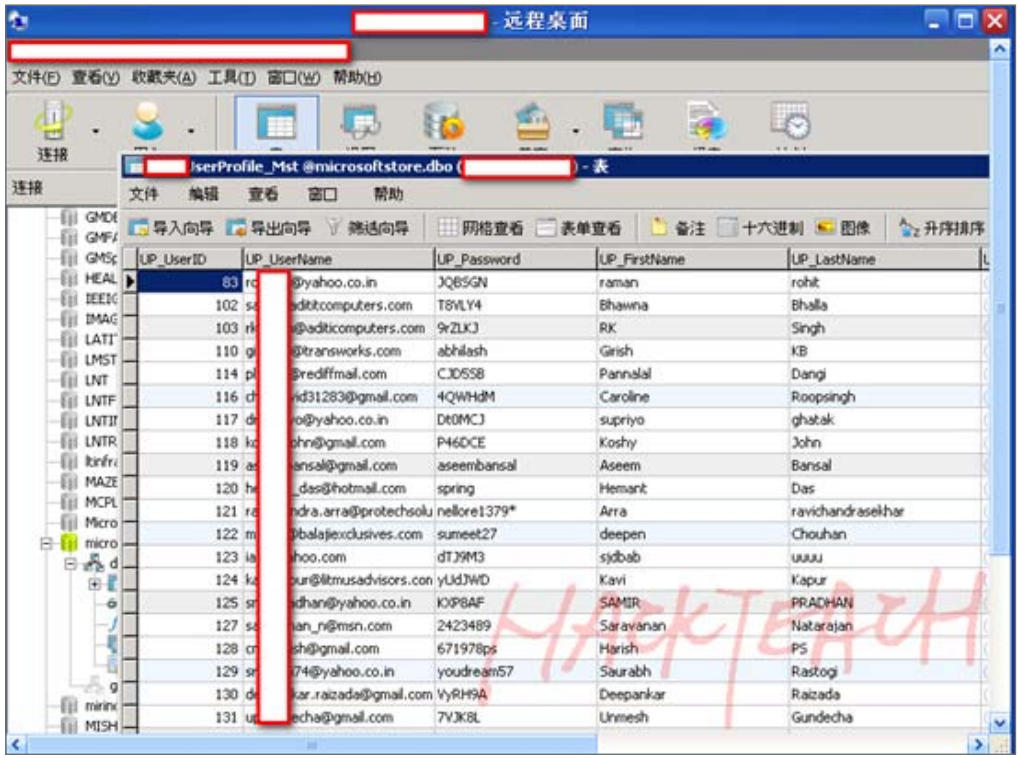
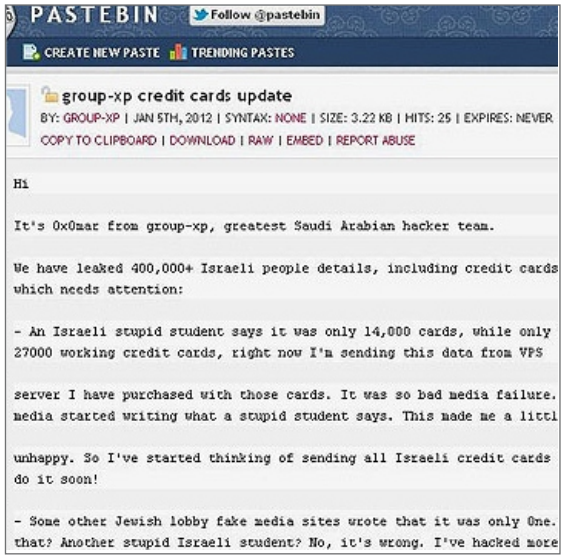


FIG.14. *CAPTURA DE PANTALLA MOSTRADA POR LOS DELINCUENTES PARA DEMOSTRAR EL ROBO DE DATOS PERSONALES DE LOS CLIENTES DE LA TIENDA DE MICROSOFT.*

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



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

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 en enero de 2013. Google eliminó todas las aplicaciones maliciosas de su tienda, y días más tarde eliminó las aplicaciones maliciosas de los móviles de los usuarios.

Ciberguerra

El primer trimestre de 2012 ha sido muy activo en este campo. El 2 de Enero tuvo lugar el robo de datos de miles de tarjetas de crédito de ciudadanos israelís. 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.

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 israelís 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.

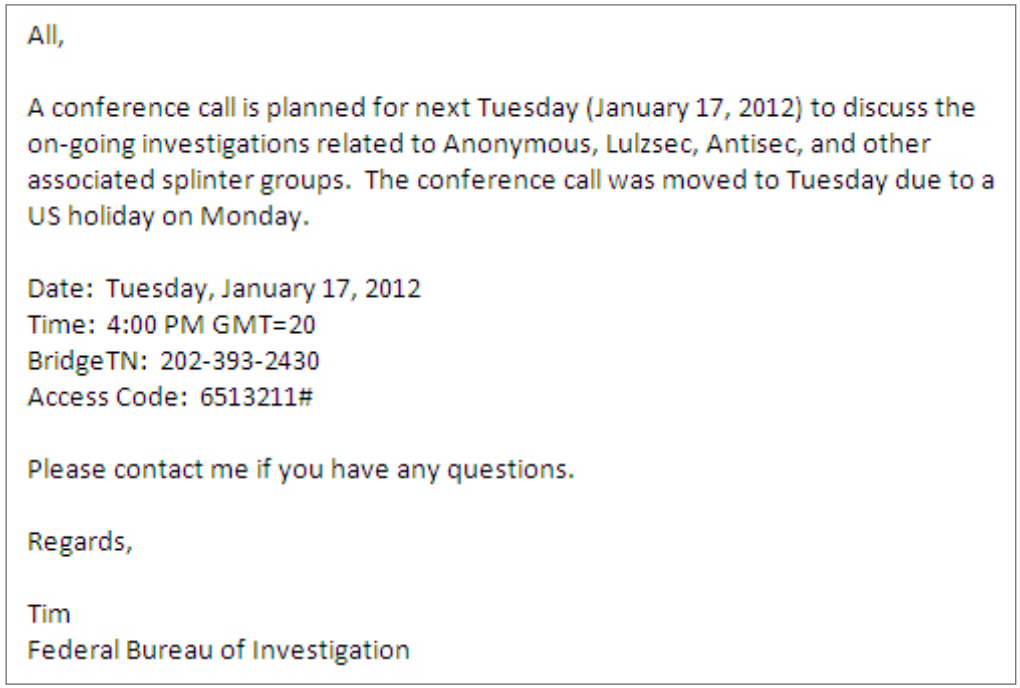
Sin dejar China, supimos también que desde ese país se había estado espiando a la empresa Nortel, tras comprometer las credenciales de 7 ejecutivos de la compañía, incluido su CEO. Al menos desde el año 2000 habrían estado accediendo a información interna de la empresa.

Anonymous

Tanto el grupo Anonymous como LulzSec han estado muy activos durante estos tres meses.

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.17. *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.

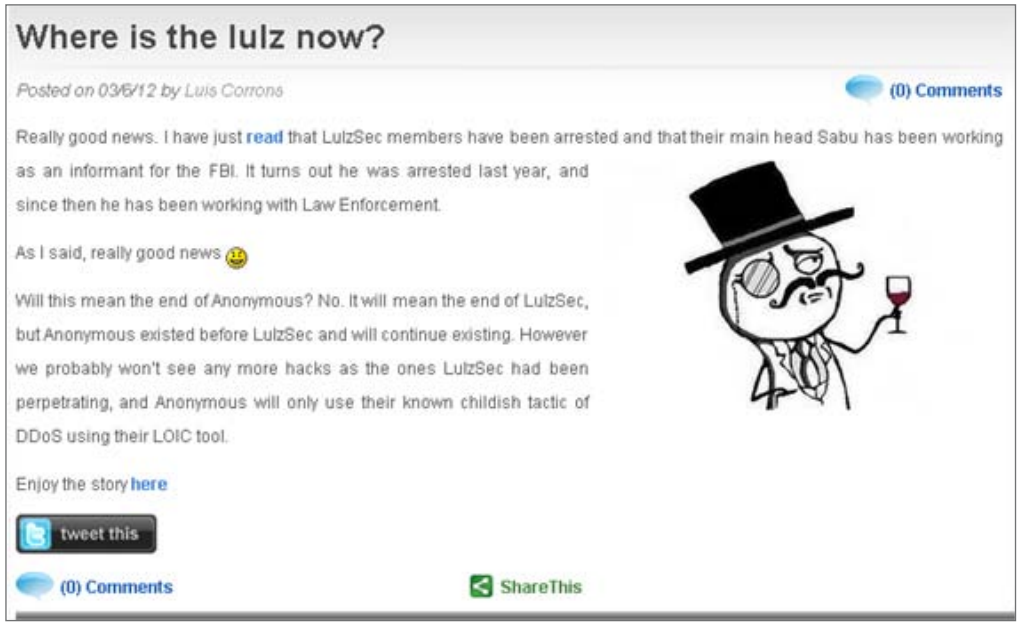


FIG.18. *ARTÍCULO EN EL BLOG DE PANDALABS HACIÉNDOSE ECO DEL ARRESTO DE MIEMBROS DE LULZSEC.*

FIG.19. *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 .

03| El trimestre en cifras

En los primeros 3 meses de 2012 hemos recogido en el laboratorio más de 6 millones de muestras, siguiendo la tónica imparable de los últimos años. Además se bate un nuevo récord, ya que 4 de cada 5 nuevas muestras de malware creadas son troyanos. Viene a reafirmarse la tendencia de los últimos meses, en el que aumentaba la proporción de troyanos creados.

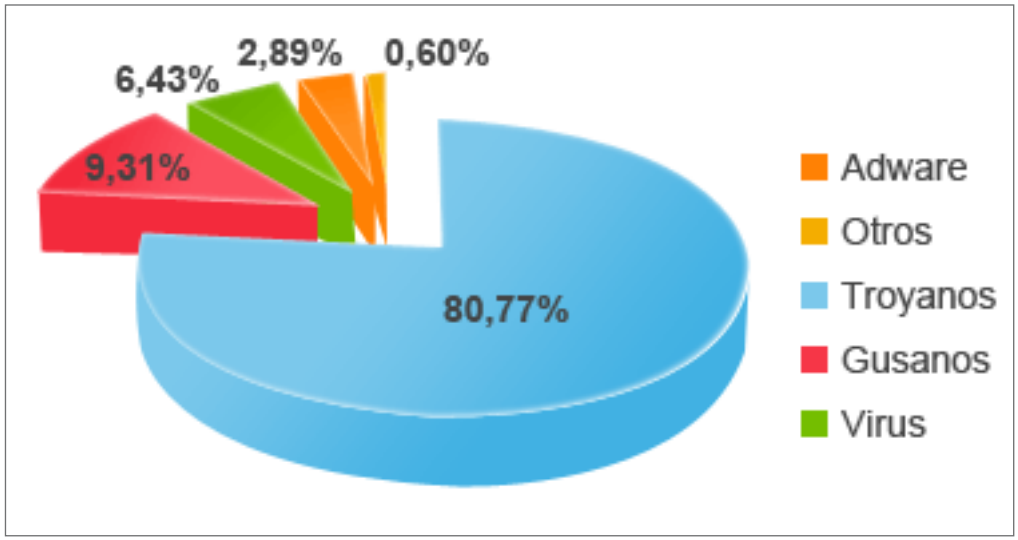


FIG.20. *NUEVO MALWARE CREADO EN EL PRIMER TRIMESTRE DE 2012, POR TIPO.*

Uno de los causantes del aumento en la creación de troyanos es el conocido "virus de la policía", del que podéis encontrar más información en la sección de "El Trimestre de un vistazo".

Veamos cuántas infecciones ha causado cada tipo de malware en el mundo. Una de las características de los troyanos es que no se replica, 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:.

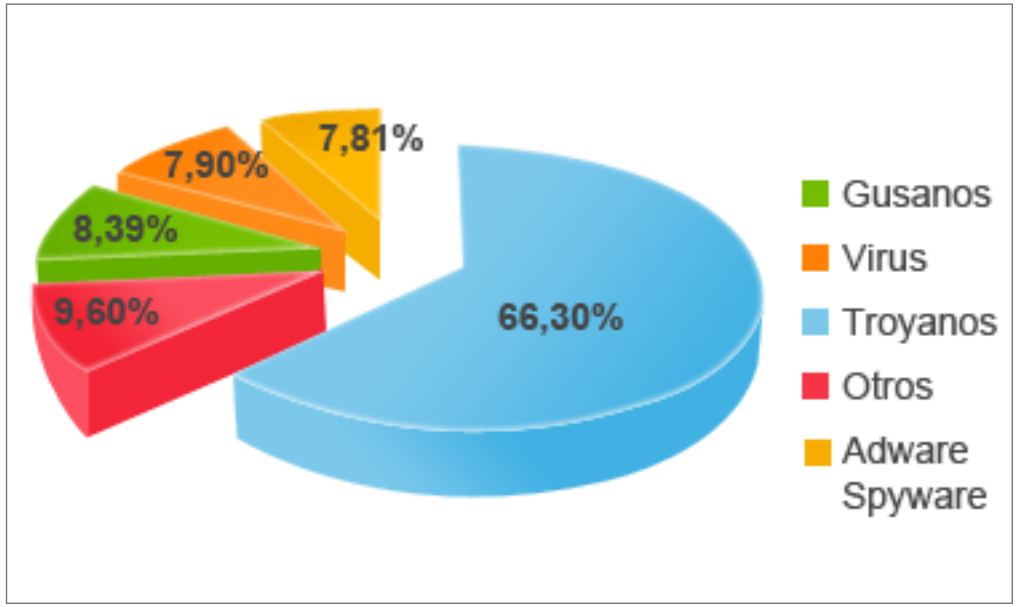


FIG.21. *INFECCIONES POR TIPO DE MALWARE EN EL PRIMER TRIMESTRE DE 2012.*

Si bien el mayor causante de infecciones es el troyano, como cabía esperar, llama la atención la relativa "poca" cantidad de PCs infectados por gusanos, que es menor a la proporción de nuevas muestras de gusanos detectadas en estos tres meses. En cualquier caso este dato viene a corroborar cómo la época de las grandes epidemias masivas de gusanos ha dejado lugar a una masiva epidemia silenciosa de troyanos.

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 35,51%, más de 3 puntos por debajo de la media de 2011. El país más infectado del mundo en este trimestre ha sido China, con un 54,10% de PCs infectados, siendo el único país del mundo que supera el 50% de ordenadores infectados. Le siguen en el ranking Taiwán, con un 47,15% y Turquía (42,75%). A continuación podemos ver los 10 países con mayor índice de infección:

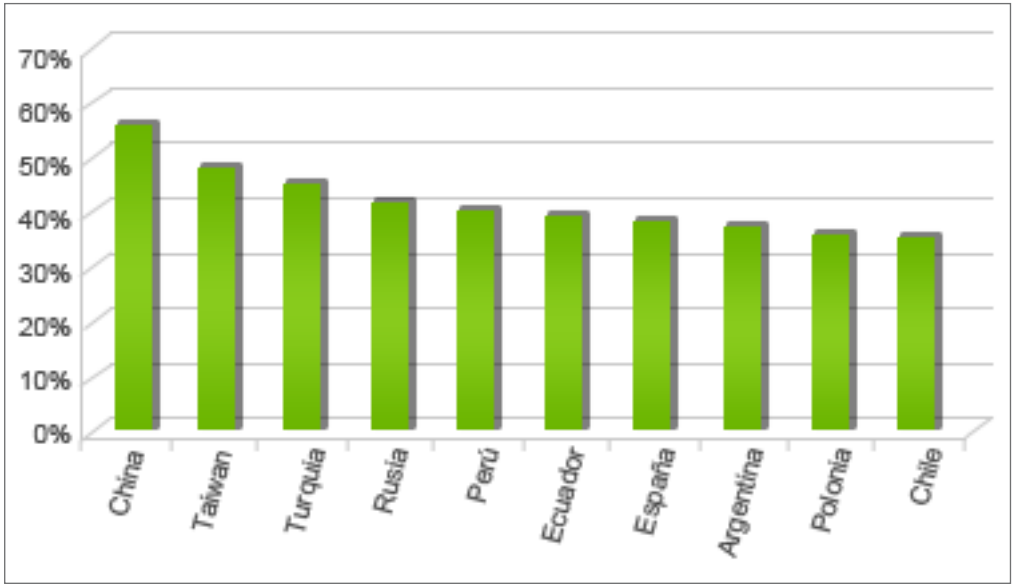


FIG.22. *PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN.*

Vemos que los países más infectados están repartidos geográficamente. Si analizamos los datos de los países mejor posicionados, aquellos cuyo índice de infección es más bajo, vemos que excepto Japón el resto son europeos, siendo Suecia el que ostenta el lugar más alto del podio con un porcentaje que no llega al 20%, batiendo otro récord, aunque en esta ocasión muy positivo:

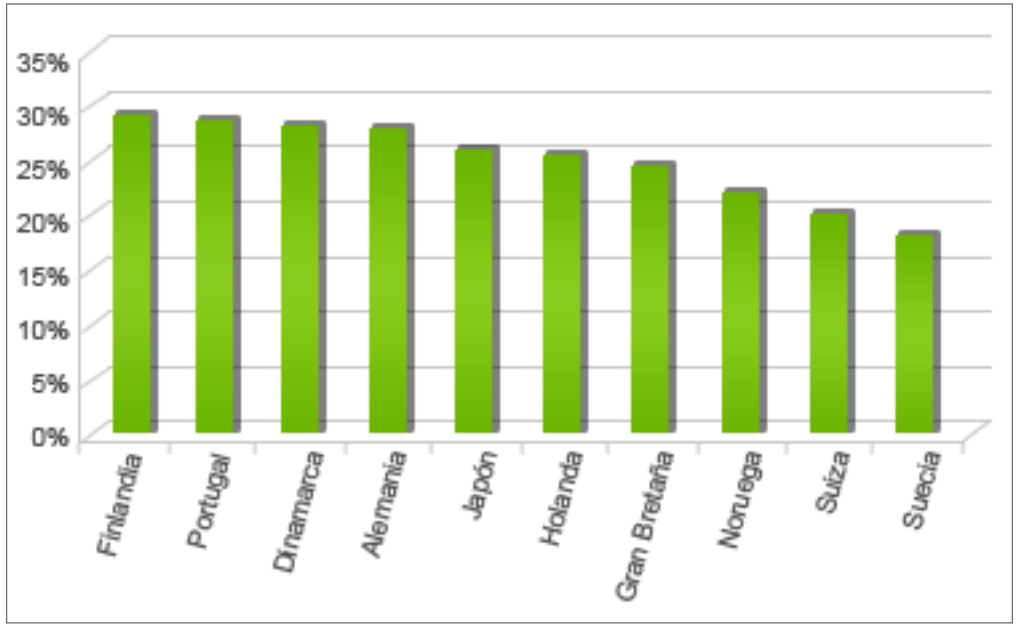


FIG.23. *PAÍSES CON MENOR ÍNDICE DE INFECCIÓN.*

04| Conclusión

Aún nos queda por delante la mayor parte del año 2012, donde parece que no nos vamos a aburrir, mientras seguimos haciendo frente a los ciberdelincuentes dispuestos a robar todo tipo de información para enriquecerse a costa de los ciudadanos.

Anonymous seguirá dando que hablar, tanto por los ataques que protagonizará como por las diferentes acciones policiales en su contra. En cualquier caso habrá que seguir muy de cerca cuál es su evolución tras la detención de los principales miembros de LulzSec.

En el ámbito de la ciberguerra seguiremos viendo casos que nunca dejan de sorprendernos. Nos vemos dentro de 3 meses para contaros las últimas novedades.

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