Informe trimestral PandaLabs

Abril - Junio 2012

01 | Introducción

Hoy en día ya nadie duda de la dependencia tecnológica que tenemos. Toda la información la tenemos en formato digital. Atrás quedó la época del álbum de fotos, con recuerdos de nuestra familia que se guardaban como oro en paño. Ahora tenemos miles de fotografías en formato digital, música, películas, documentos de trabajo, extractos bancarios… toda nuestra vida está intrínsecamente ligada a la red.

Pero va aún más allá, utilizamos ordenadores para todo, desde nuestro aparato de televisión hasta los electrodomésticos. Y no se queda aquí, se utilizan para controlar los semáforos, el alumbrado público, la distribución de agua y electricidad… se usan en centrales eléctricas de todo tipo, se utilizan para controlar armamento…

Esto explica en gran medida la revolución que estamos viendo desde nuestra atalaya en el laboratorio, con oleadas de decenas de miles de ejemplares de malware llegando cada día. Todas las oportunidades que la red nos brinda para mejorar nuestra vida, son también oportunidades para los amigos de lo ajeno, aquellos que se aprovechan de los usuarios para robar su información y comerciar con ella, o directamente para obtener su dinero. Su ansia de ganancia no disminuye, por lo que los ataques son cada vez más virulentos.

En este informe podremos ver y analizar las nuevas estrategias que están urdiendo los ciberdelincuentes para maximizar sus ganancias. También veremos nuevos casos de ciberguerra, algo que ha dejado de ser una posibilidad para convertirse en una realidad donde gobiernos como el de EEUU reconocen abiertamente participar en hackeos de páginas web, y analizaremos el caso **Flame**, un ataque de ciberespionaje ligado a Stuxnet.

02| El trimestre de un vistazo

En el pasado informe os comentamos cómo uno de los ataques más prevalentes llevados a cabo por ciberdelincuentes es el del conocido como "Virus de la Policía". Durante el segundo trimestre de 2012 los ataques han evolucionado. 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.

El auge del ransomware – Virus de la Policía "Reloaded"

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"). Este trimestre encontramos una nueva variante, que curiosamente activaba la cámara web del equipo infectado. ¿Para qué?: Han modificado la típica página de advertencia que venían utilizando hasta ahora:

FIG.01. *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.02. *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.

Cibercrimen

Continúa la "edad de oro" del cibercrimen, con cientos de casos de todo tipo de robos. Destacamos a continuación algunos de los casos acaecidos durante este trimestre, para que nos podamos hacer una idea de cómo está la situación.

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.

FIG.03. *USUARIOS AFECTADOS POR UN COMPLEMENTO MALICIOSO DEL NAVEGADOR CHROME HAN VISTO CÓMO LAS PÁGINAS DE WIKIPEDIA SE LLENABAN DE PUBLICIDAD.*

En muchas ocasiones hemos comentado cómo los ciberdelincuentes se han profesionalizado y siempre intentan mejorar. Un caso muy llamativo que ha sucedido este trimestre 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.

Y estos son sólo algunos de los pocos casos que hemos conocido durante este trimestre. Sin embargo no todo son malas noticias, ya que poco a poco las fuerzas del orden van mejorando en la lucha contra el cibercrimen.

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.04. *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.

Móviles

Android sigue siendo la plataforma móvil con más crecimiento, y por lo tanto la que más ataques recibe. Durante este trimestre hemos visto diferentes troyanos, todos ellos con 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.

Es por ello que la aparición de la siguiente noticia ha llamado mucho la atención: Boeing, el gigante aeroespacial, va a sacar este mismo año un smartphone super-seguro basado en Android. Pero antes de que nos lancemos todos a reservar uno, hay que aclarar que se trata de un teléfono diseñado principalmente para agencias gubernamentales, por lo que el precio será muy alto. Aún no han revelado los detalles, pero incluirá el cifrado de las comunicaciones.

Redes sociales

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. Suelen suceder muchos de estos casos, y este trimestre no ha sido la excepción. 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:

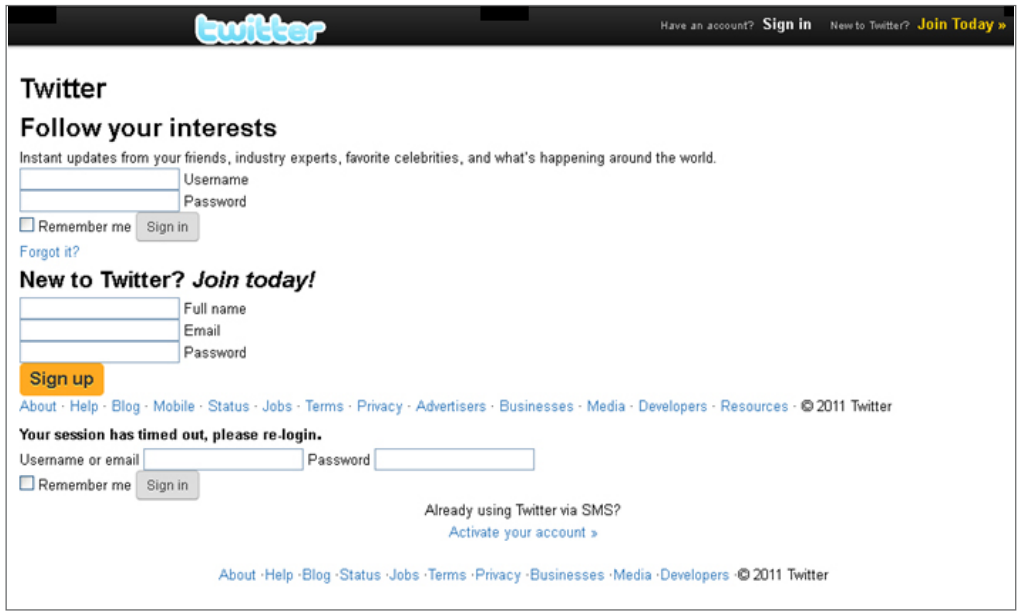

FIG.05. *PÁGINA DE PHISHING UTILIZADA PARA ROBAR CREDENCIALES DE USUARIOS DE TWITTER.*

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.06. *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.07. *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.

Ciberguerra

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 trimestre, 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.

03| El trimestre en cifras

En el segundo trimestre de 2012 hemos recogido en el laboratorio más de 6 millones de muestras, cifra similar al primer trimestre de este año. El tipo de malware aparecido también es similar al del trimestre anterior, con un 78,92% de troyanos: casi 4 de cada 5 nuevas muestras de malware creadas son troyanos. Aquí tenemos los datos en detalle:

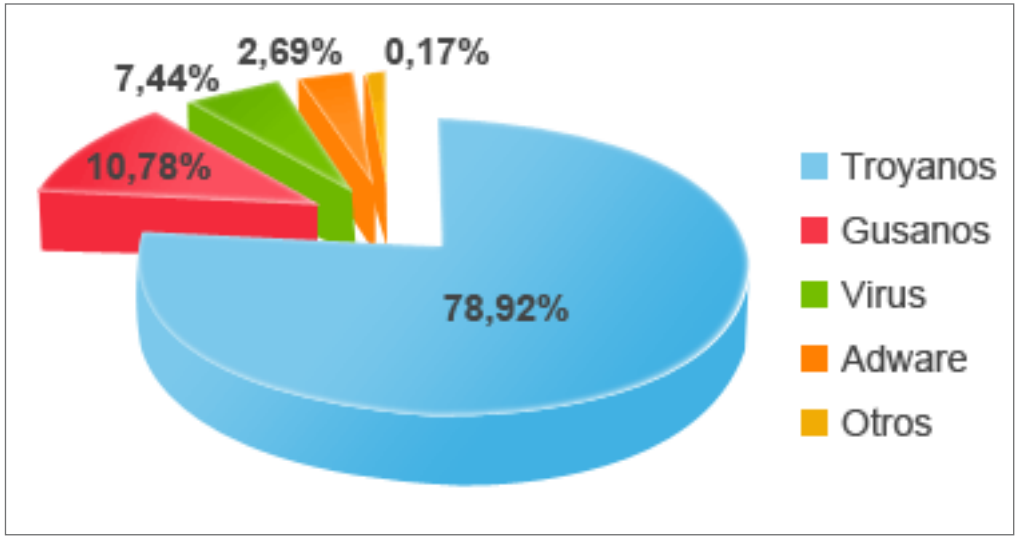

FIG.08. *NUEVO MALWARE CREADO EN EL SEGUNDO TRIMESTRE DE 2012, POR TIPO.*

Si analizamos las infecciones causadas por el malware en el mundo, gracias a los datos aportados por la Inteligencia Colectiva, vemos que también están protagonizadas por los troyanos: de cada 4 infecciones que han tenido lugar durante este trimestre, 3 eran de troyanos. Veamos cómo se reparten las infecciones:

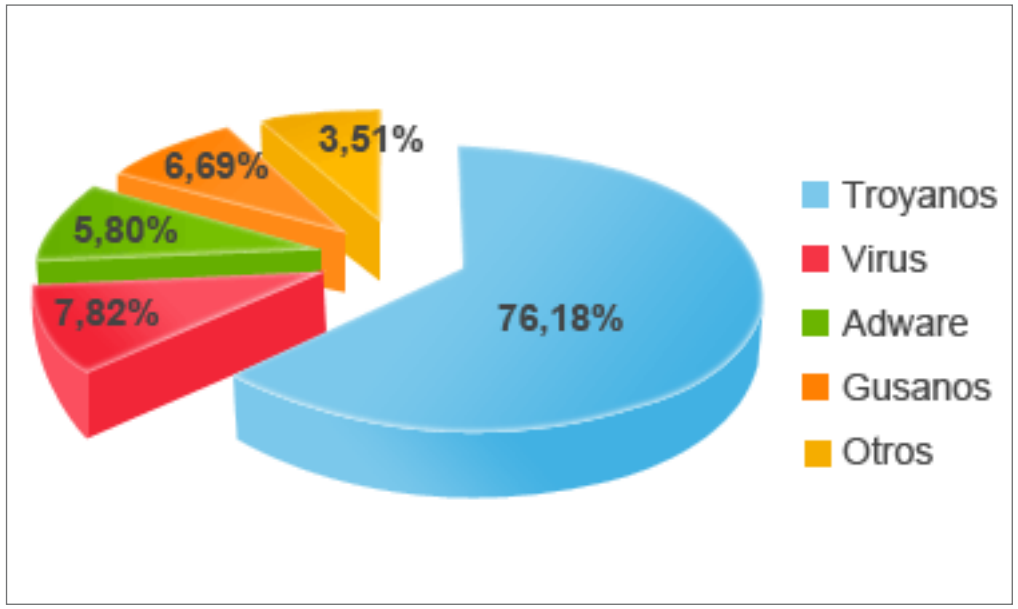

FIG.09. *INFECCIONES POR TIPO DE MALWARE EN EL SEGUNDO TRIMESTRE DE 2012.*

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 la invasión de los troyanos, teniendo como protagonistas a troyanos bancarios y al infame "Virus de la policía".

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 31,63%, casi 4 puntos por debajo del anterior trimestre de 2012. El país más infectado del mundo en este trimestre ha sido, por primera vez desde que elaboramos este ranking, Corea del Sur, con un 57,30% de PCs infectados, seguido por China con un 51,94%, siendo los dos únicos países del mundo que superan el 50% de ordenadores infectados. Le sigue en el ranking Taiwán, con un 42,88%. En el caso de China llama la atención cómo algunas de sus regiones más desarrolladas, cuentan con un ratio de infección realmente bajo respecto al resto del país; es el caso por ejemplo de Hong Kong, donde el ratio de infección es de únicamente un 23,36%. A continuación podemos ver los 10 países con mayor índice de infección:

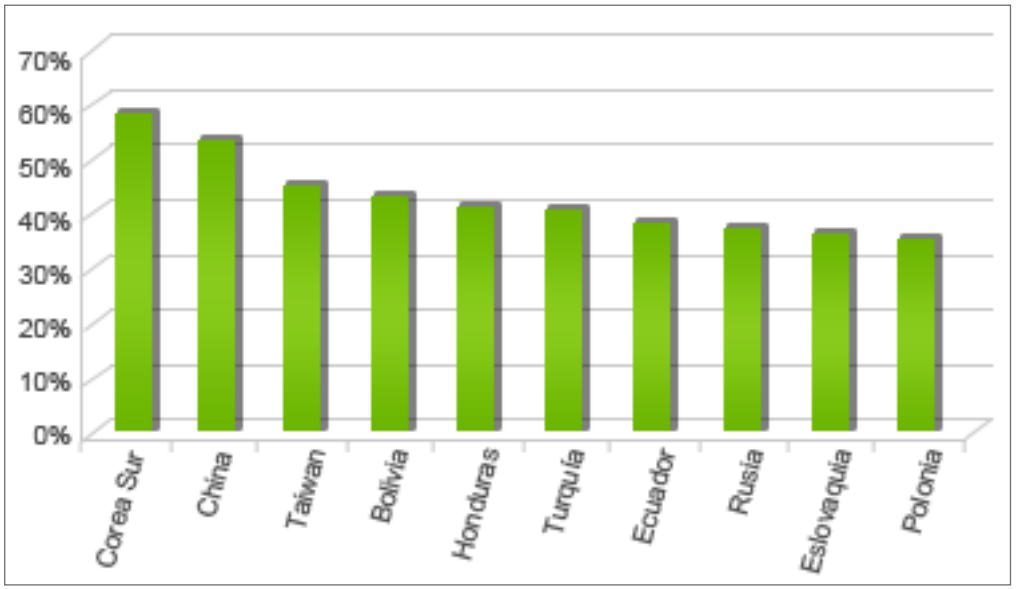

FIG.10. *PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN.*

Vemos que los países más infectados están repartidos geográficamente, aunque las primeras posiciones están copadas por países asiáticos. Si analizamos los datos de los países mejor posicionados, aquellos cuyo índice de infección es más bajo, podemos observar que ninguno de ellos supera el 25% de infección. También hay que resaltar que el palmarés está dominado principalmente por países europeos (Uruguay es el único país dentro del top 10 con menos infecciones que no es europeo), con Suiza de líder con sólo un 18,40% de infecciones, seguido muy de cerca por Suecia con un 19,07%, siendo éstos los únicos países que bajan del 20% de infecciones:

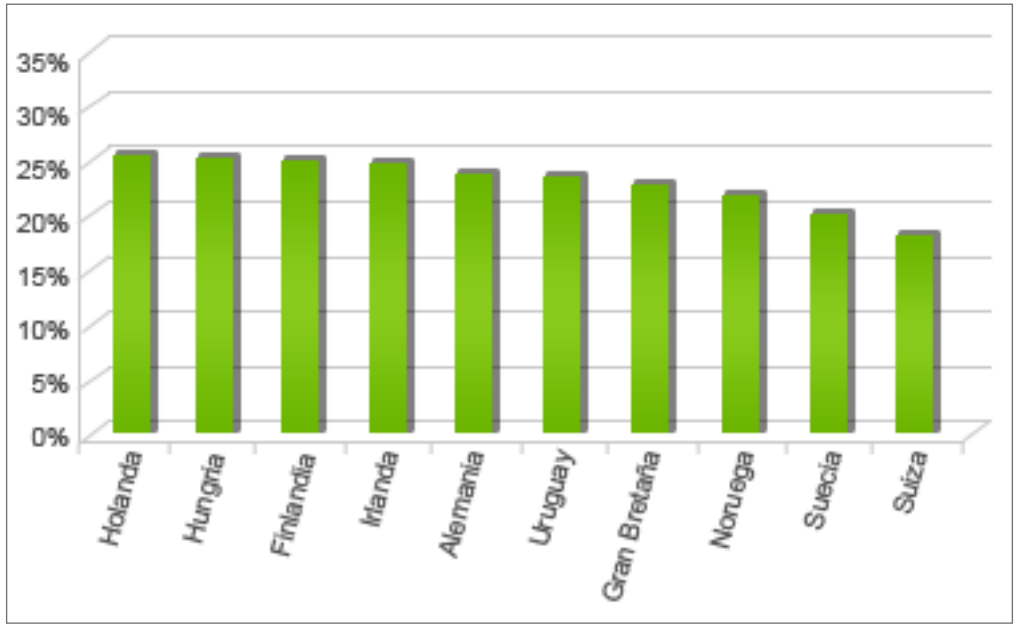

FIG.11. *PAÍSES CON MENOR ÍNDICE DE INFECCIÓN.*

Llama la atención que en el ranking de países menos infectados aparezcan en su mayoría países muy desarrollados tecnológicamente. ¿Se trata de una tendencia real? Para analizarlo hemos decidido analizar los datos de los países pertenecientes a la OCDE (Organización para la Cooperación y Desarrollo Económico). El resultado es el siguiente:

ÍNDICE DE INFECCIÓN DE PAISES MIEMBROS DE LA OCDE

Corea del Sur	**57,30%**
Turquía	**39,29%**
Eslovaquia	**36,09%**
Polonia	**35,74%**
España	**33,35%**
República Checa	**32,31%**
Chile	**31,94%**
Estados Unidos	**30,03%**
México	**30,00%**
Italia	**29,82%**
Australia	**29,56%**
Eslovenia	**28,86%**
Dinamarca	**28,42%**
Francia	**28,40%**
Portugal	**27,56%**
Japón	**26,99%**
Bélgica	**26,23%**
Austria	**26,18%**
Canadá	**24,89%**
Holanda	**24,74%**
Hungría	**24,54%**
Finlandia	**24,02%**
Irlanda	**23,64%**
Alemania	**22,61%**
Reino Unido	**21,01%**
Noruega	**20,50%**
Suecia	**19,07%**
Suiza	**18,40%**

Sí parece haber una relación entre el desarrollo tecnológico y el ratio de infección. Bien es cierto que hay muchos otros factores que influyen en estas cifras, pero aún así podemos ver que sólo los 7 primeros países tienen un ratio de infección mayor a la media mundial, mientras que el resto, desde Estados Unidos a Suiza, tienen un ratio de infección menor que la media.

04| Conclusión

Todo indica que seguirá creciendo el número de amenazas a las que nos tenemos que enfrentar los usuarios, así que ahora más que nunca debemos estar bien protegidos: contar con una buena solución de seguridad, tener actualizado todo el software que utilicemos para cerrar posibles agujeros de seguridad y siempre utilizar el sentido común para evitar caer en las trampas de ingeniería social que tan peligrosamente tienden los ciberdelincuentes.

Comenzamos la época veraniega con la llegada de las Olimpiadas 2012 en Londres, por lo que podemos asegurar que veremos ataques utilizando está temática como gancho para engañar a los usuarios. Lo dicho, utilicemos el sentido común y evitaremos ser víctimas de estos ataques.

Tenemos por delante la segunda mitad del año 2012, donde seguiremos al pie del cañón informando de todas las novedades que se produzcan en el mundo de la seguridad, así como peleando constantemente contra todo el malware y sus creadores.

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