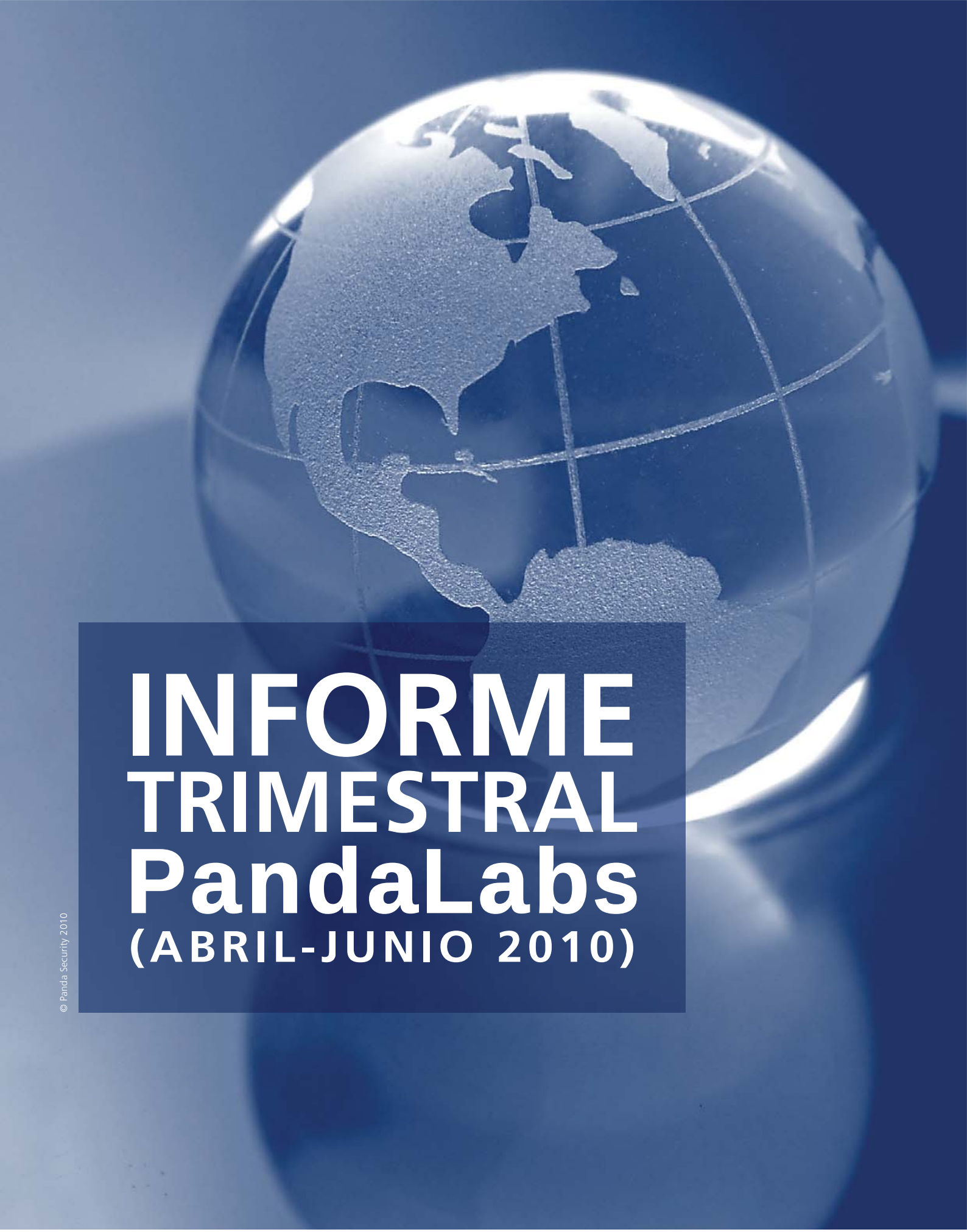


INFORME TRIMESTRAL PandaLabs

(ABRIL-JUNIO 2010)

PANDA SECURITY | 20 Aniversario 1990-2010

Índice

Introducción

Ya hemos alcanzado el ecuador del 2010, y es hora de echar un vistazo a lo ocurrido en los últimos meses. Si algo podemos destacar de lo sucedido en este segundo trimestre de 2010, es el protagonismo de las redes sociales –con Facebook y Twitter en el epicentro de este fenómeno.

Se han producido todo tipo de noticias alrededor de Facebook, muchas de ellas provocadas por la propia red social: desde un error que dejaba acceder a información de tus contactos, hasta cambios en la configuración de privacidad que provocaban que nuestros datos pudieran quedar expuestos sin nuestro conocimiento. Pero los datos expuestos no son algo exclusivo de las redes sociales, ya que hemos podido ver cómo un problema de seguridad en su sistema permitió extraer de la web de AT&T información de 114.000 compradores de iPad que habían contratado la tarifa de datos 3G con ellos. Y días más tarde, un colapso en su servicio de reservas cuando se pudo comenzar a reservar el iPhone4, provocó que usuarios pudieran acceder a la información de otros usuarios de AT&T.

Adobe ha sido el otro gran protagonista, no tanto por su "pelea" con Apple por no integrar este último compatibilidad con Flash en sus iPhone/iPod Touch/iPad, sino por la cantidad de vulnerabilidades descubiertas, algunas de ellas siendo explotadas activamente por ciberdelincuentes sin que exista un parche para solucionar el problema.

Sin más, espero que disfrutéis del informe tanto como nosotros lo hemos hecho escribiéndolo.

Ataques BlackHat SEO

Comenzamos este primer trimestre el 1 de abril, que es también el día de los inocentes en muchos países. Y cómo no, los delincuentes utilizaron esta ocasión para lanzar un nuevo **ataque BlackHat SEO**, "envenenando" los resultados de los motores de búsqueda para que sus páginas maliciosas aparezcan entre los primeros resultados cuando los usuarios busquen algún término relacionado con este día.


1. April Fools
Mar 31, 2010 ... This April 1st, the day the 2010 Census forms are officially due, the laughing you hear all around is the sound of an Obama April Fools Day ...
- 19 hours ago - Cached

2. April Fools Day Recipes
Mar 27, 2010 ... A fun menu for 6 with wacky April Fool's recipes By The Canadian Living Test . April Fool's Day recipe: Pineapple Fish Sticks. ...
- Cached

3. April Fools Jokes For Kids
Mar 31, 2010 ... What kind of pranks should you do for April Fools Day? What are good april fools day pranks for elementary school kids? ...
- 19 hours ago - Cached

4. April Fools Day Origin
Mar 31, 2010 ... The 1986 horror film April Fool's Day is themed around the day (akin to

FIG.01

RESULTADOS MALICIOSOS EN GOOGLE AL BUSCAR EL TÉRMINO "APRIL FOOLS"

Y esto sólo ha sido la punta del iceberg. Estos ciber-criminales van en busca de dinero, para lo que tienen que robarnos nuestra información y usarán todos los medios a su alcance para lograrlo.

> ***"Moral" o "ética" son palabras desterradas del vocabulario de los cibercriminales, por lo que utilizan cualquier tipo de noticia, por muy trágica que ésta sea***

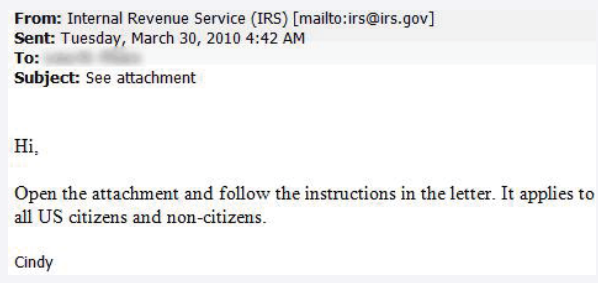
Tal es el caso de **la muerte del cantante Ronnie James Dio**, el **terremoto en Chile**, el **terremoto en China**, la **erupción del volcán Eyjafjall en Islandia** o la aparición de un **cráter en Guatemala**. No sólo se dedican a utilizar noticias trágicas, cualquier excusa es buena para tratar de infectarnos, la única condición es que exista una gran cantidad de gente interesada en buscar información: desde el final de la serie LOST, pasando por las **elecciones británicas**, un **falso positivo** de un conocido fabricante antivirus, o la celebración del **Mundial de Fútbol 2010 en Sudáfrica**.

Pero no sólo de ataques de BlackHat SEO viven los ciber-delincuentes. Como hemos explicado en otras ocasiones, utilizan principalmente 2 técnicas para infectarnos: a través de "exploits" que aprovechan agujeros de seguridad en el software instalado en nuestros equipos, y utilizando las conocidas como técnicas de ingeniería social, o lo que es lo mismo, engañando al usuario, que muchas veces es el eslabón más débil de la cadena. Sobre exploits hablaremos más adelante, aunque os puedo adelantar que Adobe ha vuelto a ser uno de los principales protagonistas, con vulnerabilidades de día-0 aparecidas en sus diferentes aplicaciones y siendo explotadas activamente por los ciberdelincuentes.

Ataques de Ingeniería Social

Respecto a la ingeniería social, los ataques no han cesado en ningún momento, utilizando todo tipo de triquiñuelas para hacernos caer y robarnos nuestros datos. Hemos visto casos de sorteos falsos, como aquel en el que supuestamente Google nos agraciaba con **1 millón de dólares**. El mejor consejo que podemos dar es que utilicemos el sentido común. Si se te aproxima una persona por la calle y te dice que te acaba de tocar un millón de dólares, ¿le creeríamos? Claro que no. Actuemos igual en Internet, y seamos siempre desconfiados.

Hay otros engaños que son más elaborados, como el que vimos en abril, coincidiendo con la campaña de la renta en Estados Unidos, donde haciéndose pasar por el gobierno nos solicitaban información. El mensaje que recibíamos era el siguiente:


From: Internal Revenue Service (IRS) [mailto:irs@irs.gov]
Sent: Tuesday, March 30, 2010 4:42 AM
To:
Subject: See attachment

Hi,

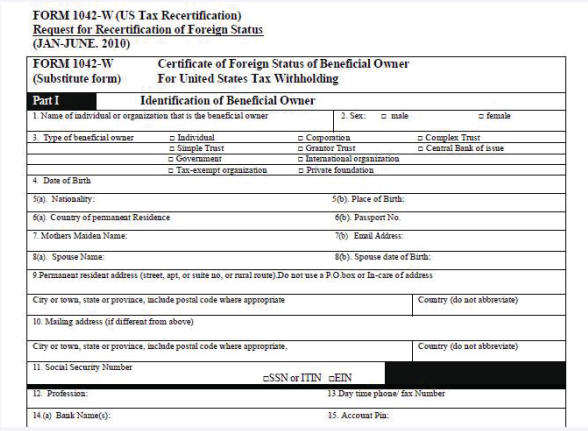
Open the attachment and follow the instructions in the letter. It applies to all US citizens and non-citizens.

Cindy

FIG.02

FALSO MENSAJE DEL IRS

Uno de los documentos falsos se trataba de un formulario falso del IRS, donde nos solicitaban todo tipo de información personal. Pedían rellenar el formulario y enviarlo a un número de fax (situado en Canadá). Evidentemente, el enviar el fax con toda nuestra información implica que puedan robar nuestra identidad.



FORM 1042-W (US Tax Recertification)
Request for Recertification of Foreign Status
(JAN-JUNE. 2010)

FORM 1042-W (Substitute form) — Certificate of Foreign Status of Beneficial Owner For United States Tax Withholding

Part I — Identification of Beneficial Owner

1. Name of individual or organization that is the beneficial owner — 2. Sex: ☐ male ☐ female
3. Type of beneficial owner — ☐ Individual ☐ Corporation ☐ Complex Trust ☐ Simple Trust ☐ Grantor Trust ☐ Central Bank of issue ☐ Government ☐ International organization ☐ Tax-exempt organization ☐ Private foundation
4. Date of Birth
5(a). Nationality: — 5(b). Place of Birth:
6(a). Country of permanent Residence — 6(b). Passport No.
7. Mothers Maiden Name: — 7(b). Email Address:
8(a). Spouse Name: — 8(b). Spouse date of Birth:
9.Permanent resident address (street, apt, or suite no, or rural route).Do not use a P.O.box or In-care of address
City or town, state or province, include postal code where appropriate — Country (do not abbreviate)
10. Mailing address (if different from above)
City or town, state or province, include postal code where appropriate, — Country (do not abbreviate)
11. Social Security Number ☐SSN or ITIN ☐EIN
12. Profession: — 13.Day time phone/ fax Number
14.(a) Bank Name(s): — 15. Account Pin:

FIG.03

FORMULARIO FALSO DEL IRS

Otro tipo de engaño muy habitual es el de imitar sitios reales, como YouTube, o el de ofrecernos vídeos que al tratar de visualizarlos nos solicitan la instalación de un códec... que finalmente se trata de un nuevo ejemplar de malware. Uno de estos casos fue el sitio malicioso llamado "Just a Tube":

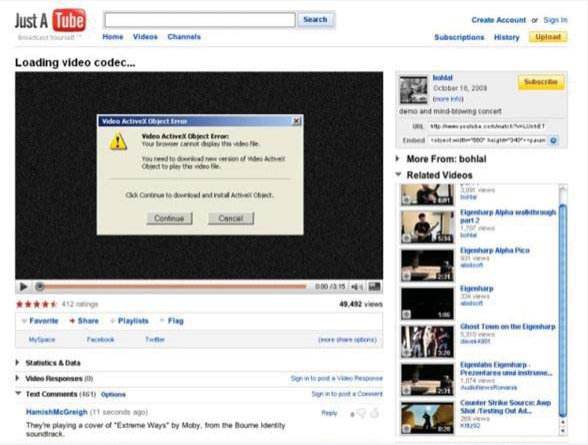


FIG.04

IMITACIÓN DE YOUTUBE CREADA PARA INFECTAR A LOS USUARIOS

Redes sociales

Y si el sitio más popular de vídeos online es imitado, Facebook no le va a ir a la zaga. En junio **publicamos un listado** con todas las diferentes páginas existentes que imitaban a la famosa red social, para tratar de robar las cuentas a los usuarios que cayeran en su trampa.

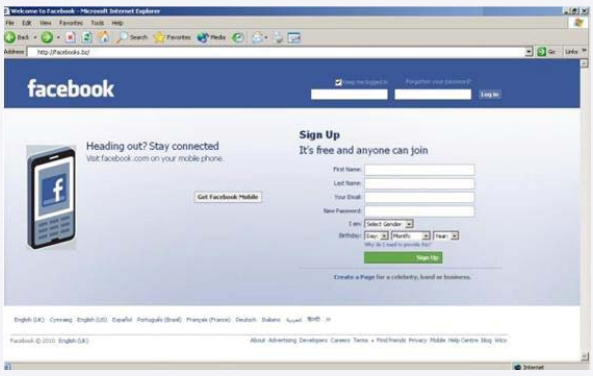


FIG.05

FALSA PÁGINA DE FACEBOOK

Y puestos a engañar a los usuarios, lo mejor es hacerse pasar por alguna de las redes sociales más populares del momento. De hecho, uno de los ataques que más éxito ha tenido este trimestre es un mensaje haciéndose pasar por el soporte de Twitter. En dicho mensaje nos informan que tenemos varios mensajes sin leer y un link para acceder a los mismos.

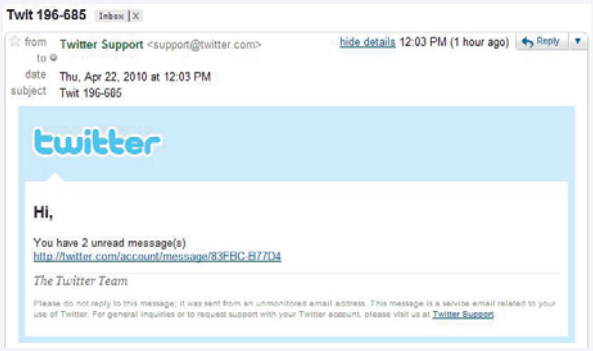


FIG.06

FALSO MENSAJE DE TWITTER

En los **primeros casos**, estos links te dirigían a páginas web de venta de productos farmacéuticos, como Viagra y otros similares. Recientemente (Fig.07) hemos visto mensajes similares cuyo propósito era directamente instalar malware en nuestro PC, advirtiendo de un falso intento de robo de nuestra cuenta de Twitter.

FIG.07

FALSO MAIL DE TWITTER PARA INFECTAR A LOS USUARIOS CON UN FALSO ANTIVIRUS

Uno de los consejos que siempre damos es que cuando recibamos un mensaje de una red social, banco, etc. donde nos dicen que ha habido un problema con nuestra cuenta y nos dan un link para solucionar el problema, no hagamos caso. Normalmente se tratará de un caso de phishing, donde nos solicitarán nuestros datos para robarnos la cuenta. En otros casos el objetivo será instalar malware, como en un falso mensaje de Facebook que fue distribuido a finales de abril, en el que nos decían que nuestra contraseña había sido cambiada y nos adjuntaban un documento donde podíamos consultar la nueva.

FIG.08

MENSAJE FALSO DE FACEBOOK

Nuestra sorpresa fue mayúscula cuando descubrimos el siguiente mensaje:

FIG.09

MENSAJE REAL DE TWITTER

Como podéis ver, se trata de un mensaje que tiene la estructura típica de cualquier phishing: mensaje supuestamente enviado por la empresa responsable del servicio, que te dice que ha habido un problema de seguridad, que han tenido que cambiarte el password y que pinches en un link para continuar con el proceso. He visto miles de mensajes de phishing con esta misma estructura. ¿Qué es entonces lo que me sorprendió en este mensaje? Que no era un phishing, era un **mensaje real**.

Volviendo al caso de mensajes falsos para distribuir malware, raro es el servicio online que no haya sido utilizado por los ciberdelincuentes: Twitter, Facebook, Amazon, UPS, iTunes, eBay, Outlook... Y cuando no se trata de un servicio online se trata de una falsa carta de felicitación, o un supuesto currículum vitae.

Las redes sociales, además de ser utilizadas como señuelo por los ciberdelincuentes, también son un medio de comunicación fantástico para todos, por lo que están siendo utilizadas para distribuir spam y malware.

Los ciberdelincuentes están utilizando las redes sociales como un medio alternativo al correo electrónico para el envío de spam y malware

Normalmente se trata de mensajes prometiéndonos un vídeo o fotos, y al pinchar en el link nos llevamos una desagradable sorpresa, ya que acabamos infectados por malware.

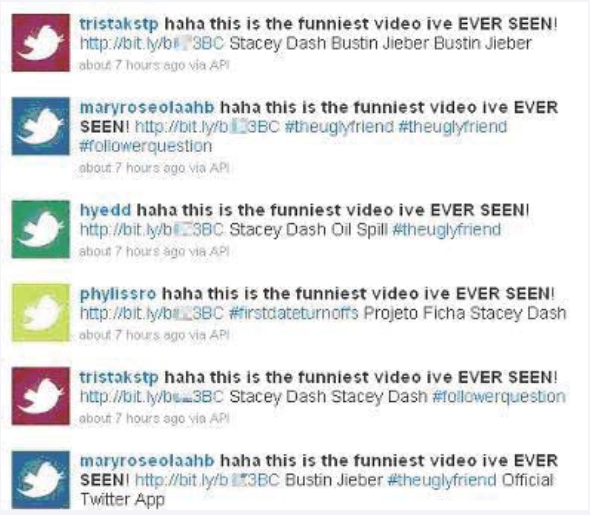


FIG.10

MENSAJES MALICIOSOS ENVIADOS POR TWITTER

¿Qué tipo de malware utilizan para infectarnos? En la mayoría de los ataques aquí descritos nos encontramos con que lo que están distribuyendo son o falsos antivirus para que los compremos o troyanos que tratan de robarnos nuestra información personal.

Facebook Clickjacking

Facebook es la mayor de las redes sociales, y a pesar de diversas polémicas sobre la (falta de) privacidad de la información, no deja de crecer. Una de las acciones más sencillas que permite es poder decir que "Me gusta" algo. Cuando estamos en la red social, basta con pinchar en el icono correspondiente para que digamos que nos gusta la foto de un amigo, un comentario, una aplicación... y también se puede decir que te gusta algo sin estar en Facebook directamente. Muchas páginas web han implementado esto, de tal forma que puedes decir que algo te gusta, mientras estemos logueados en Facebook, haciendo un solo click.

Lo mejor es verlo con un ejemplo; existe un juego de rol online de vampiros llamado **Blood Wars**, que no tiene nada que ver con Facebook. Sin embargo, recientemente han añadido la opción de poder decir en Facebook que te gusta desde la página principal del juego:

FIG.11

OPCIÓN "ME GUSTA" EN BLOOD WARS

Al pinchar en el link que te dan, automáticamente se actualiza tu estado en Facebook, indicando que te gusta Blood Wars:

FIG.12

ESTADO ACTUALIZADO DE FACEBOOK

Está bien, es cómodo para los usuarios de Facebook, para las empresas es genial porque permite que se hable de ellas o sus productos de forma más fácil... entonces, ¿cuál es el problema? Pues que estamos hablando de páginas web y sencillo código en javascript que nos permiten "pervertir" el uso original que se le había dado a esta funcionalidad.

Imaginad que añadimos al blog de PandaLabs un icono para que digas que te gusta PandaLabs. Pensarás que en tu cuenta aparecerá que te gusta PandaLabs... pero, ¿y si hemos cambiado el código para que diga "Saber que es tonto"? Entonces en Facebook aparecería así: **"A Luis le gusta saber que es tonto"**. Bien, esto no es tan grave, sólo se trata de una broma. Podríamos hacerla más interesante, podríamos poner un link prometiendo que si pincháis en él, entráis en el sorteo de un iPad, y en cambio al hacer click aparecerá en Facebook LO QUE YO QUIERA.

Pero pongámonos en la mente de un cibercriminal, que busca dinero. Puede querer ganar dinero haciendo que visites una página que tenga publicidad, por ejemplo. O aún peor, que distribuya malware y nos infecte con un falso antivirus, un troyano, etc. De momento no hemos visto ningún caso de distribución de malware, pero sólo es cuestión de tiempo.

En las últimas semanas no han dejado de aparecer casos donde se utilizan ganchos como "101 Hottest Women in the World", "Farmville" o "Sexo en Nueva York 2", prometiéndonos acceder a contenido sobre la temática de la página, ver un video, etc. y lo único que pasa es que se "propaga" apareciendo en Facebook y haciendo caer en la trampa a todos nuestros amigos que pinchen en el link. Un buen consejo para estos casos es ser desconfiados y desactivar javascript en vuestros navegadores.

Nuevas Técnicas de Phishing (Tabnabbing)

Hay un dicho informático que probablemente tengan muy presente a la hora de planear sus ataques las mafias que están detrás de las amenazas que combatimos día a día. La frase dice así: "*El virus informático más destructivo se encuentra entre el teclado y la silla.*"

¿Para qué diseñar complejos algoritmos y dedicar horas de esfuerzo para descubrir errores de programación cuando el punto más vulnerable de un ordenador es el propio usuario? Eso es lo que piensan muchas mafias y cada día encuentran maneras más originales de hacernos caer en su trampa.

Es un nuevo concepto de phishing que apareció documentado en mayo de 2010. Desconocemos si realmente se ha utilizado o si simplemente es una prueba de concepto, pero es muy interesante para comprobar cómo nuestros hábitos como usuario pueden ser analizados.

El *tabnabbing* se basa en aprovechar el sistema de navegación por pestañas o "tabs" para hacer creer al usuario que está en una página de un servicio conocido como Gmail, Hotmail, Facebook... y así robar sus contraseñas.

Muchos de nosotros estamos acostumbrados a tener múltiples pestañas abiertas en nuestros navegadores, tantas que a veces hasta perdemos la cuenta e incluso tenemos la misma página abierta en más de una pestaña.

FIG.13

VISTA DE UN NAVEGADOR CON VARIAS PESTAÑAS ABIERTAS

Cuando queremos volver a una página nos guiamos por el *favicon*, o icono de la página, además de su título, y no solemos prestar atención a la dirección que aparece en la barra de navegación.

Este comportamiento puede ser explotado para que accedamos a una página falsa y así comprometamos nuestras contraseñas.

El modus operandi es bastante sencillo.

1. Conseguir que el usuario acceda a tu web. Aquí las posibilidades son múltiples; desde el clásico spam, a mensajes a través de redes sociales, foros, etc.

2. Mediante JavaScript detectar cuándo tu página ha perdido el foco (es decir, ya no es la página que se está visualizando porque el usuario está en otra pestaña, programa o navegador). Unos segundos después (para asumir que el usuario se ha olvidado de esta pestaña), también mediante JavaScript es posible cambiar el *favicon*, el título y el contenido de tu página para que simule que es una página de un servicio conocido, en este caso usaremos como ejemplo Gmail.

3. El usuario tras navegar por otras páginas y haber abierto un gran número de pestañas quiere volver a visitar, por ejemplo, su correo electrónico de Gmail, y comprueba que existe una pestaña de este servicio abierta, en este caso se trata de la página falsa de Gmail. El usuario no se acuerda de cuándo ha accedido a esta página y al ver el formulario de acceso asume que hace mucho tiempo que la abrió y que seguramente ha caducado la sesión.

4. Al introducir su usuario y contraseña, la falsa página guarda estos datos y redirecciona al usuario a la página original del servicio.

El usuario no es consciente de que su usuario y contraseña han sido comprometidos y seguramente puedan ser usados por las mafias para fines delictivos.

No queremos causar una gran alarma, pero sí hay que estar alerta en nuestro día a día y sospechar de todo aquello que nos parezca raro y que supongamos fruto de nuestra olvidadiza cabeza. Sólo con una actitud alerta y unas políticas de uso correctas podremos utilizar nuestros ordenadores con seguridad de no ser estafados mediante trucos de ingeniería social.

También muchos especialistas apuntan a que el sistema de login mediante usuario y contraseña está obsoleto y que son los propios navegadores los que tienen que liderar una migración hacia sistemas más seguros, como el "Account Manager" propuesto por Mozilla Labs hace unos meses.

Los smartphones se hacen querer

Hemos comentado en muchos de nuestros informes que la aparición de malware en una plataforma viene condicionada por la rentabilidad. Por tanto, para que aparezca malware en una plataforma, ésta debe de ser predominante o por lo menos abarcar un volumen de usuarios que hagan rentable la inversión en I+D por parte de las mafias.

En su día parecía que Symbian era la única y más estable candidata a dominar el mercado de los terminales inteligentes y fue en esta plataforma en la que empezó a aparecer malware.

Con la aparición de nuevas plataformas como iPhone o Android la popularidad de Symbian decayó y con ella, la aparición de malware para esta plataforma

Además, a partir de la versión 9 de Symbian, las políticas de seguridad eran más estrictas, lo que dificultaba no sólo la creación de malware, sino también el desarrollo "HomeBrew" (software casero). Estos motivos son los que han hecho que Symbian deje de ser el objetivo principal de las mafias.

Por todo esto, parece claro que los principales objetivos serán Android e iPhone, pero lo que no sabemos aún es por qué plataforma se decantarán, y eso lo decidirá, como hemos comentado anteriormente, la rentabilidad. Los argumentos para apostar por uno u otro son varios: Apple o Google, público "techie" o generalista, control en el Market/Store...

A pesar de que en Asia y África Symbian es aún dominador en el mercado de terminales inteligentes, es interesante valorar los datos a nivel mundial y más concretamente el mercado estadounidense, ya que al fin y al cabo es uno de los mercados más importantes en términos de volumen, además de que nos puede indicar las tendencias que seguirán el resto de países en un futuro próximo.

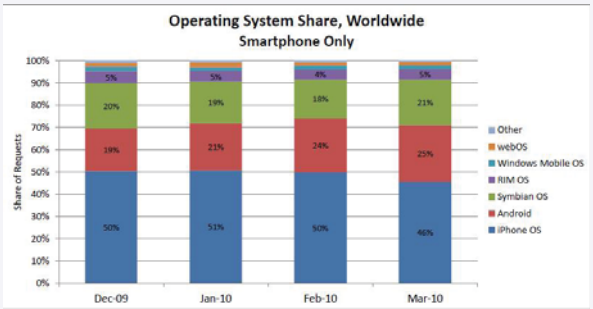


FIG.14

DISTRIBUCIÓN DE SO PARA MÓVILES. FUENTE: adMob.

Como vemos, a nivel mundial iPhone es claro dominador del mercado ya que en mayor o menor medida está presente en los principales países consumidores de terminales inteligentes. Pero como hemos comentado anteriormente, es interesante observar el mercado estadounidense por separado, ya que nos puede indicar hacia dónde puede dirigirse el mercado mundial.

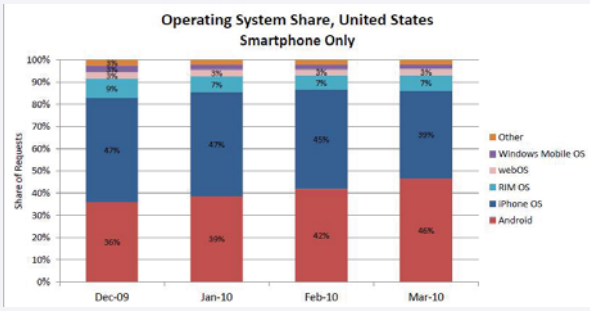


FIG.15

DISTRIBUCIÓN DE SO PARA MÓVILES EN EE.UU. FUENTE: adMob.

Como se puede ver en la gráfica, el tráfico generado por terminales Android ya superaba al de los terminales iPhone en Estados Unidos. Teniendo en cuenta que la distribución de los terminales Android está siendo desigual a nivel mundial (aún no están disponibles en muchos países) y que en los países asiáticos los terminales inteligentes basados en Linux o plataformas más abiertas han tenido bastante éxito, podemos deducir que Android puede convertirse en el terminal inteligente "mainstream" por excelencia.

Por supuesto, esto son tan solo conjeturas y el tiempo nos dirá qué plataforma será el objetivo de las mafias; aun así, debemos estar alerta y vigilantes de cara a estar *one step ahead*.

Vulnerabilidades

El mes de abril comenzaba con una actualización para corregir la vulnerabilidad descubierta en el navegador Firefox durante el concurso *Pwn2Own* que tiene lugar en la conferencia de seguridad **CanSecWest** en Vancouver.

Este mismo mes, Apache publicaba una noticia donde comentaba que sus infraestructuras habían sido comprometidas a través de la explotación de una vulnerabilidad desconocida en su software de gestión de errores e incidencias, JIRA. El informe comenta que los atacantes se aprovecharon de una vulnerabilidad de XSS para comprometer varias sesiones de usuarios, entre las que se incluían varias cuentas con privilegios de administración. Parece ser, que para realizar el ataque se ocultó el enlace malicioso a través de los servicios de acortamiento de URL que se utilizan comúnmente en las redes sociales para no sobrepasar el espacio máximo en la creación de mensajes utilizados en servicios como Twitter o Facebook. ¿Qué esconde la siguiente URL? **http://tinyurl.com/yd5dm77**.

En cuanto a redes sociales, podemos decir que tampoco están seguras en cuanto a fallos de diseño y programación. En una **noticia** leíamos cómo era posible que cualquier usuario de Facebook pudiera visualizar las conversaciones de sus amigos con otras personas en tiempo real. Nuevamente estos fallos de seguridad nos recuerdan que hay que ser precavidos con la información que comentamos en este tipo de redes. Horas más tarde la organización lanzó el siguiente comunicado:

"For a limited period of time, a bug permitted some users' chat messages and pending friend requests to be made visible to their friends by manipulating the "preview my profile" feature of Facebook privacy settings. When we received reports of the problem, our engineers promptly diagnosed it and temporarily disabled the chat function. We also pushed out a fix to take care of the visible friend requests which is now complete. Chat will be turned back on across the site shortly. We worked quickly to resolve this matter, ensuring that once the bug was reported to us, a solution was quickly found and implemented."

En este comunicado se menciona que la incidencia había estado presente durante un período corto de tiempo. Pero, realmente ¿desde hace cuándo se ha estado utilizando este fallo? ¿Cuánto tiempo se ha podido ver comprometida nuestra privacidad? ¿Sigue siendo vulnerable?

Pasemos ahora al mundo de las bases de datos, el gigante en este campo, Oracle, comenzó este segundo trimestre del año corrigiendo 47 vulnerabilidades, de las cuales sólo 19 podían ser explotadas si el atacante estaba autenticado. Es decir, 28 vulnerabilidades podían ser explotadas por un usuario sin previa autenticación. Entre las aplicaciones y servicios afectados por vulnerabilidades sin autentificar están *Oracle Fusion Middleware*, *Oracle Collaboration Suite*, *Oracle E-Bussines Suite*, *Oracle PeopleSoft Enterprise*, *JID Edwards EnterpriseOne* y *Oracle Industry Suite*.

Igualmente tenemos a Microsoft publicando sus boletines de seguridad cada segundo martes de mes. Entre las vulnerabilidades publicadas, queremos destacar las que se mencionan en el boletín **MS10-020**, que corregía 5 vulnerabilidades que permitían la ejecución remota de código a través de una respuesta SMB malformada afectando a todas las versiones del sistema operativo Microsoft Windows.

La vulnerabilidad corregida en el boletín **MS10-026** permitía la ejecución si un usuario abre un archivo con formato AVI que contiene una pista de audio en formato MP3 diseñada para explotar la vulnerabilidad. El problema residía en el códec MP3 de Microsoft. Esta vulnerabilidad, sin embargo, no afectaba a la última versión de Microsoft, Windows 7.

Como dato curioso en este ciclo de parches, señalar que Microsoft se vio obligado a publicar nuevamente el boletín **MS10-025**, al no proteger de forma adecuada la vulnerabilidad que afectaba al servicio *Windows Media Unicast Service* en un sistema Windows 2000 con Service Pack 4.

El boletín de seguridad **MS10-040** corregía una vulnerabilidad de ejecución remota de código en la que un atacante autenticado podría llegar a ejecutar código de forma remota en IIS6 e IIS7 instalado en los sistemas Windows Server 2003, Windows Vista y Windows Server 2008. Esta vulnerabilidad se produce cuando el servidor web de Internet Information Services no asigna correctamente la memoria al analizar la información de autenticación específica recibida del cliente. La ejecución de estos comandos sería bajo los derechos de la identidad de proceso de trabajo (WPI), que, de forma predeterminada, está configurada con privilegios de cuenta de servicio de red. No obstante, si hay servidores IIS cuyos grupos de aplicación estén configurados con una WPI que use una cuenta con privilegios administrativos, estos pueden verse más gravemente afectados.

Microsoft aún dispone de una vulnerabilidad no parcheada que ha sido descubierta por el conocido investigador de Google Tavis Ormandy. El día 9 de junio publicó una vulnerabilidad que afecta a Windows Help. Ésta permite la ejecución de comandos en un sistema Windows XP y Windows 2003. Microsoft **comenta** que el investigador de Google no les ha dejado suficiente tiempo para poder corregir dicha vulnerabilidad y así poder dar protección a sus clientes. También añade que la solución propuesta por Google es incompleta y es fácilmente eludible.

"Without giving us time to resolve the issue for our potentially affected customers, makes broad attacks more likely and puts customers at risk."

"While this was a good find by the Google researcher, it turns out that the analysis is incomplete and the actual workaround Google suggested is easily circumvented."

A pesar de todo, Microsoft ha publicado una **solución provisional** para poder mitigar la amenaza en los sistemas vulnerables, lo que no ha evitado que aparezcan los primeros ataques funcionales por parte de ciberdelincuentes.

En este trimestre Adobe tampoco ha quedado al margen, no sólo las aplicaciones Reader y Acrobat han tenido su ración de vulnerabilidades, sino también Adobe Photoshop, la aplicación de retoque fotográfico por excelencia en sus versiones CS3 y CS4, que son vulnerables debido a un tratamiento incorrecto del formato de imagen TIFF. Esta vulnerabilidad permite la ejecución remota de código en entornos Windows y Macintosh.

Para finalizar queremos hacer mención a la última **vulnerabilidad crítica** que se ha reportado en los programas Adobe Reader y Adobe Acrobat que está siendo explotada actualmente en Internet. El problema reside en la versión de Adobe Flash Player 10.0.45.2, así como en versiones anteriores junto con la versión de la librería autoplay.dll que viene incluida en Adobe Reader y Acrobat 9.x. Esta vulnerabilidad permite la ejecución de código en los sistemas afectados.

Como solución temporal, Adobe recomienda eliminar o renombrar la librería *autoplay.dll* en sistemas Windows, la *libauthplay.so.0.0.0* en sistemas Linux y Solaris y finalmente la librería *AuthPlayLib.bundle* en sistemas Macintosh. Adobe menciona que es posible que se produzcan ciertos errores no explotables y mensajes de error si se intenta visualizar un fichero PDF que contengan contenido SWF.

Adobe pretende solucionar esta incidencia el día 29 de junio. No obstante gracias a TruPrevent los usuarios que tengan instaladas las soluciones antivirus de PandaSecurity disfrutan nuevamente de protección frente a este nuevo "0 day".

Nuestro compañero Sean-Paul Correll ha preparado un video demostrativo donde se puede observar cómo la nueva versión de nuestro antivirus **Panda Cloud Antivirus** equipado con la tecnología TruPrevent ya estaba protegiendo a nuestros clientes frente a este "0 day" incluso antes de su aparición y antes de que el fabricante proporcione una solución real a la vulnerabilidad. La solución propuesta por Adobe resta funcionalidad al producto mientras que Panda Cloud Antivirus permite ejecutar esta funcionalidad y bloquea aquel PDF que sea malicioso.

Que cada vez hay más malware en circulación es un hecho que ya nadie pone en duda. Cuando hace algunos años comenzamos a hablar de un crecimiento exponencial de las amenazas, los usuarios miraban con desconfianza. Hoy, no sólo es un hecho probado, sino que la escalada de cibercrimen sigue en aumento. Y no sólo aumentan los nuevos ejemplares de malware, sino las variantes de ejemplares ya existentes para intentar burlar las medidas de seguridad que las compañías antivirus colocamos en los principales vectores de infección.

Esto no nos debería sorprender teniendo en cuenta los servicios que ofrecen las cibermafias para que incluso los usuarios sin conocimientos avanzados puedan crear malware con todo tipo de funcionalidades, entre ellas, la de asegurar que no va a ser detectado por las compañías antivirus.

Existen herramientas que permiten a usuarios sin conocimientos avanzados crear malware.

Ese es el caso de un portal de Internet de venta de **bots "indetectables"** descubierto en mayo, que además estaba especializado sobre todo en redes sociales. Aquí tenemos la combinación perfecta: malware indetectable + redes sociales.

El malware que hemos recibido en el laboratorio a lo largo del segundo trimestre de 2010 está distribuido de la siguiente manera:

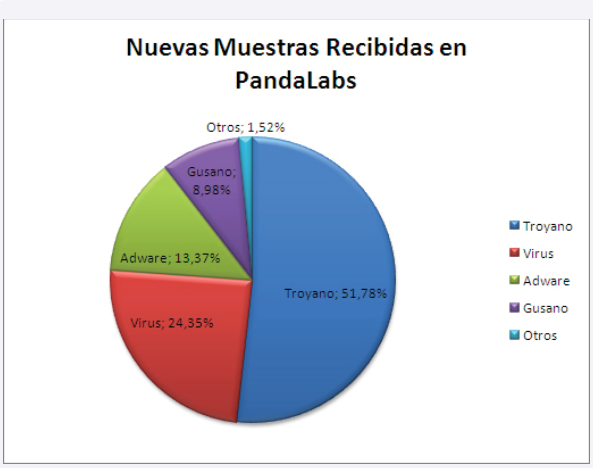


FIG.16

NUEVAS MUESTRAS RECIBIDAS EN PANDALABS

Los troyanos siguen siendo la modalidad de código malicioso preferida por los ciberdelincuentes, ya que la mayoría de su beneficio económico lo obtienen del robo de identidad y credenciales bancarias o de tarjetas de crédito. Por eso, de todo el malware que se ha creado durante el segundo trimestre del año, los troyanos suponen casi el 52% del total. En segunda posición y a una distancia considerable está la categoría de los Virus, que representa un 24,35%. Si comparamos estos datos con el trimestre anterior (15,13%), vemos que la categoría de virus ha ido ganando terreno en los últimos meses.

Este aumento podría hacernos pensar que vuelve el malware "tradicional", pero no es así. Debemos tener en cuenta que éstas son las muestras recibidas, y lo que sucede es que ha aumentado el número de muestras recibidas de tipo virus, lo que no significa que haya aumentado el número de virus distintos que han aparecido en este período. Otra forma de comprobar esto, incluso más efectiva, es ver la incidencia de infecciones, donde podemos comprobar que el número de PCs infectados por troyanos, por ejemplo, es varias veces mayor que el de PCs infectados por virus, como veremos más adelante.

La categoría de Adware mantiene posiciones respecto al trimestre anterior y continúa en la tercera posición, con un 13,37%. Dentro de esta categoría están englobados los conocidos como rogueware o falsos antivirus, que desde su proliferación hace ya dos años no han parado de crecer y su tendencia es que continúe siendo así. Al igual que con el caso de los troyanos, la motivación que hay detrás de los rogueware o falsos antivirus también es puramente económica. A continuación nos encontramos con otros sospechosos habituales, los gusanos, rozando el 9%.

Parece que el vender informes de hábitos de comportamiento en Internet está perdiendo peso dentro del mundo del robo de la información. A partir del primer trimestre de 2010, la categoría Spyware comenzó una caída en picado, ya que tan sólo suponía un 0,29% del total. Este trimestre la situación es incluso peor, ya que representa un 0,16%. Por esta razón, esta categoría ha sido relegada a la categoría de Otros.

En esta categoría están englobadas aquellas amenazas que representan un porcentaje poco apreciable, ya que suponen un 1,52% del total. En ese porcentaje se encuentran englobadas las siguientes categorías:

Dialer	30,53%
PUP (Potentially Unwanted Program)	28,45%
Herramienta de hacking	17,36%
Riesgo de seguridad	13,08%
Spyware	10,58%

Incidencia del malware en el mundo

En el anterior apartado hemos comentado la distribución de las principales categorías de malware teniendo en cuenta las muestras que hemos recibido en PandaLabs.

En este apartado, nos centraremos en la incidencia del malware analizando la situación en varios países del mundo. En primer lugar, veamos en la siguiente gráfica la distribución de infecciones en el mundo por tipo de malware:

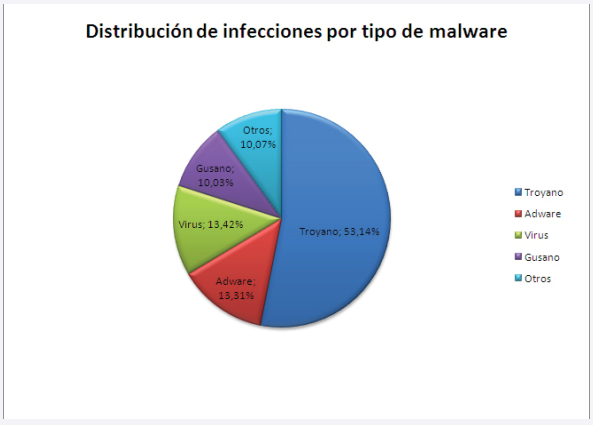


FIG.17

DISTRIBUCIÓN DE INFECCIONES POR TIPO DE MALWARE

Los triunfadores son los troyanos, como era previsible, ya que son la principal herramienta utilizada por los ciber-delincuentes para el robo de información.

Más de la mitad de los ordenadores infectados han sido víctimas de troyanos. En cambio, los virus y gusanos, que por su naturaleza (están diseñados para propagarse) podría suponerse que son los que más infecciones causan, ni siquiera generan la mitad de infecciones que los troyanos.

Los datos reflejados en la siguiente gráfica se han obtenido gracias a los análisis realizados a través de la herramienta online **ActiveScan 2.0**. Se trata de un servicio que permite a cualquier usuario analizar su equipo de forma online y gratuita, y así comprobar si su ordenador está infectado.

Estos datos no sólo tienen en cuenta el malware activo, es decir, aquel que está en ejecución en el momento de realizar el análisis, sino también el malware latente, que es aquel que está alojado en el ordenador pero que aún no ha sido ejecutado. Puede ser ejecutado por el propio usuario o puede estar a la espera de ser ejecutado remotamente.

En la siguiente gráfica podemos observar los países con mayor porcentaje de infección:

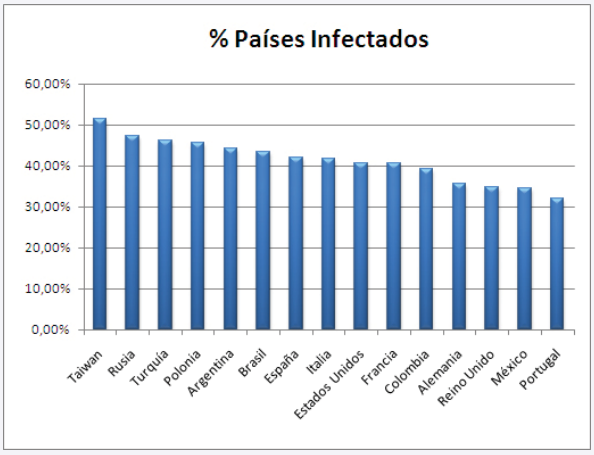


FIG.18

PAÍSES CON MAYOR PORCENTAJE DE INFECCIONES DURANTE ESTE TRIMESTRE

En cuanto a cuáles son las amenazas más prolíficas en algunos de estos países, la categoría estrella es en todos ellos la de los troyanos:

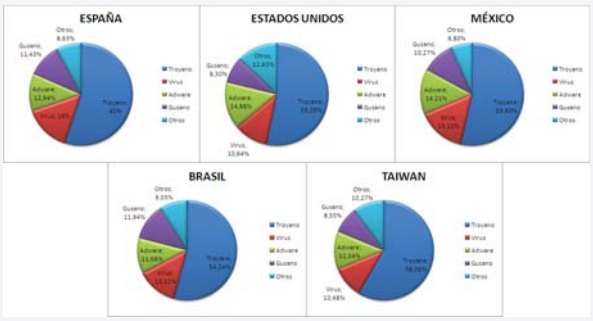


FIG.19

INFECCIONES POR PAÍS

En todos estos países el porcentaje de troyanos supera el 50%, una cifra nada desdeñable, que demuestra una vez más la preferencia de los ciberdelincuentes por distribuir malware de este tipo, principalmente destinado al robo de información.

Si comparamos estos datos con los del trimestre anterior, se aprecia un incremento en todos los países en todas las categorías en general con la excepción de los gusanos, categoría que sufre un ligero descenso. Aunque, sin duda, la subida es especialmente destacable en la categoría de los troyanos. Así por ejemplo, en el caso de España ha pasado de no superar el 50% en el primer trimestre a alcanzar el 60% en este último trimestre.

En la siguiente gráfica se puede observar la evolución de esta categoría durante los dos primeros trimestres del año 2010:

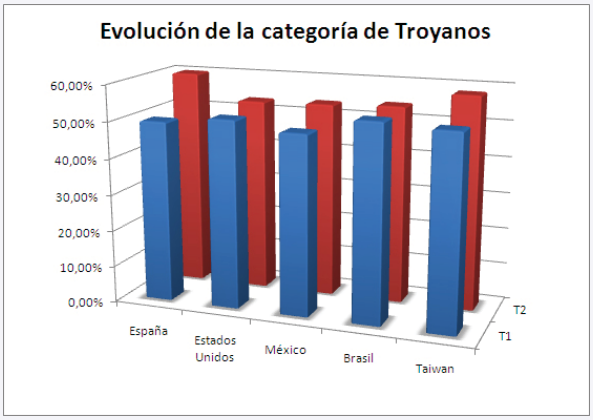


FIG.20

EVOLUCIÓN DE LA CATEGORÍA DE TROYANOS DURANTE EL T1 Y T2

Datos de Spam

Todos los días vemos spam, mensajes de correo no deseado inundan nuestros buzones. Puede llegar de diversas maneras, texto plano, HTML, imágenes, documentos pdf, incluso en mp3.

Aún así, es algo a lo que los usuarios estamos acostumbrados, por lo que cada vez nos cuesta menos distinguir qué mensaje es spam y cuál no. Y si a eso le sumamos los mejorados filtros antispam con los que cuentan los servicios de correo, el cerco al spam parece bastante cerrado.

Sin embargo, los ciberdelincuentes no se quedan atrás e idean nuevas formas no sólo de saltarse los filtros antispam, sino también las capacidades de los usuarios para reconocer spam.

A pesar de ello, los mensajes de spam "tradicionales" siguen siendo elevados, y el volumen de spam global arroja unas cifras de miles de millones de mensajes cada día.

La mayoría del spam está generado a través de redes de bots. Los ordenadores que conforman esas redes de bots están distribuidos por todo el mundo. Pero, ¿en qué países se concentra la mayor parte de ese spam?

En la siguiente gráfica se puede observar que poco más de la mitad del spam que hemos recibido en nuestro laboratorio durante los meses de marzo, abril y mayo ha sido enviado tan sólo desde 10 países:

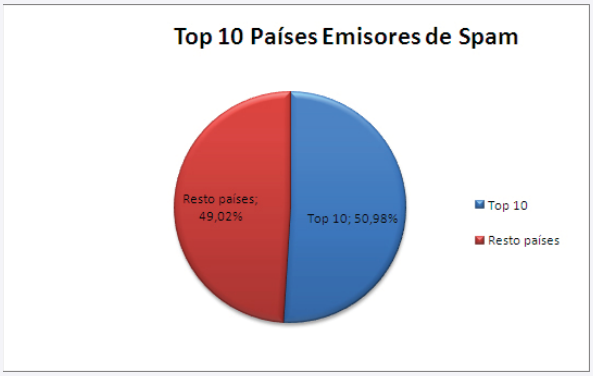


FIG.21

TOP 10 PAÍSES EMISORES DE SPAM

En la siguiente gráfica se puede ver con detalle qué países están detrás de estos datos:

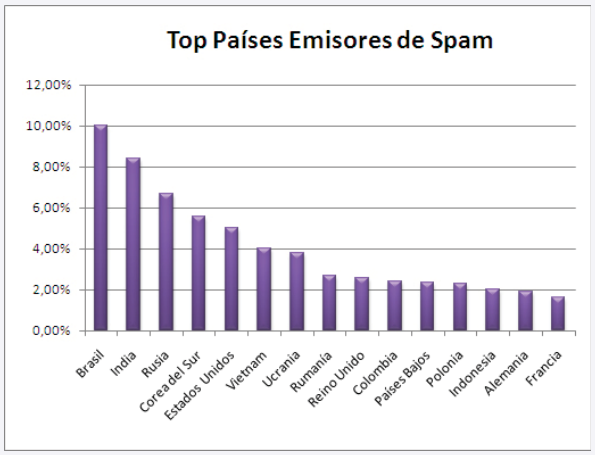


FIG.22

TOP PAÍSES EMISORES DE SPAM

Brasil continúa siendo el país desde el que más spam se ha emitido, superando el 10% del total; el trimestre anterior casi un 20% del spam fue enviado desde este país. En segunda posición tenemos a la India con poco más del 8%, seguido de Rusia (6,64%), Corea del Sur (5,54%), Estados Unidos (5%) y Vietnam (4,02%). Los países que aparecen a continuación tienen porcentajes inferiores al 4%.

Conclusiones

Como habéis podido leer, ha sido un trimestre de lo más animado, y eso que sólo hemos recogido algunos de los hechos más importantes. Antes de nada, pidamos un deseo: que Adobe espabile y dé a la seguridad la importancia que se merece, o seguirán siendo responsables, aunque sea indirectos, de muchas infecciones.

Durante los próximos meses las grandes protagonistas seguirán siendo las redes sociales, ya que los ciber-criminales no dejan de estudiar nuevas formas de sacar partido para poder llegar a los usuarios. Por otra parte, los usuarios debemos exigir que las opciones que nos permitan mantener nuestra privacidad sean claras, y aún más importante es no tolerar que si se añade una nueva opción de compartir información, ésta venga activada por defecto. Un error que Facebook ha cometido demasiadas veces.

La segunda mitad del año nos va a traer tablet PC basados en Android y Windows 7, lo que traerá al mundo de la seguridad nuevos retos.

Permaneced atentos a **nuestro blog**, donde comentaremos las principales novedades en el mundo del malware y la seguridad.

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 en el blog de **PandaLabs** en: **http://pandalabs.pandasecurity.com/**.