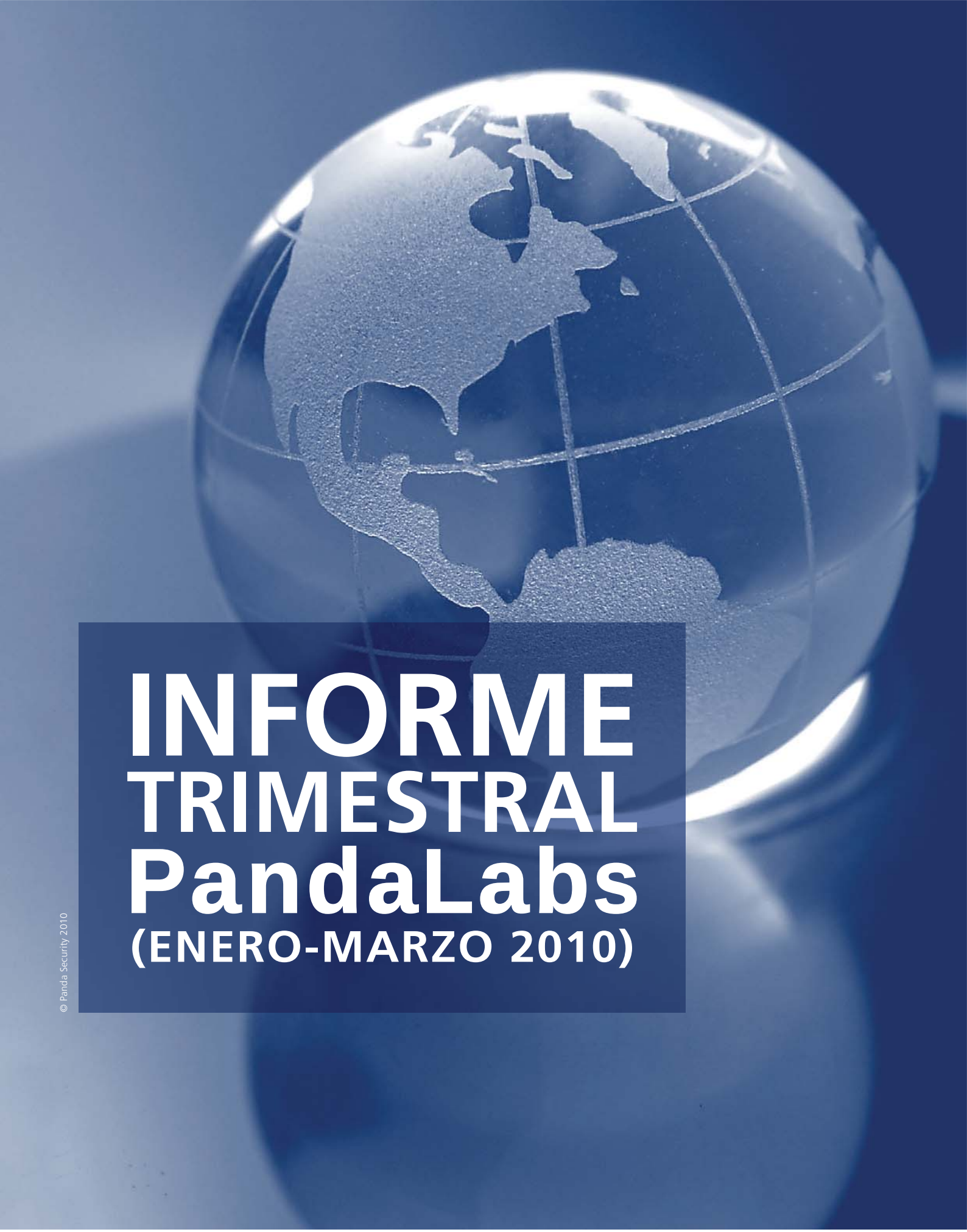

INFORME TRIMESTRAL PandaLabs

(ENERO-MARZO 2010)

PANDA SECURITY | 20 Aniversario 1990-2010

Índice

Introducción

Cuando estábamos cerrando la edición de este informe trimestral, leíamos el artículo publicado por **John Leyden** en **The Register** sobre Internet Crime Complaint Center (IC3), organismo respaldado por el FBI, que ha publicado su **informe anual** sobre el estado del delito en Internet en Estados Unidos. Es un informe parcial, pero ampliamente representativo. Entre sus principales conclusiones, comentan que han aumentado las denuncias de delitos relativos al crimen en Internet en un 22,3% respecto a 2008 y un 667%, comparado con 2001.

Las pérdidas económicas debido a delitos denunciados a través de IC3 se sitúan en 560 millones de dólares, frente a los 265 de 2008. En cuanto a la clasificación y al ranking de denuncias recibidas durante 2009, es la siguiente:

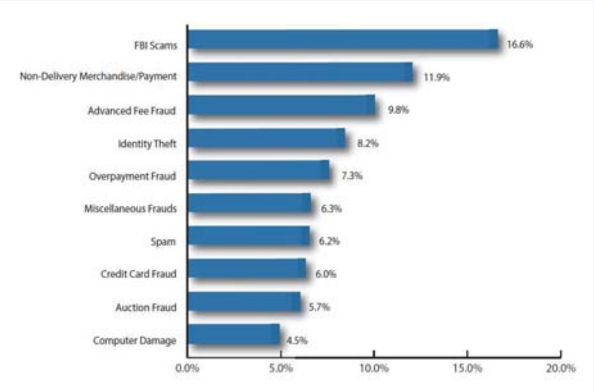

FIG.01

RANKING DE DENUNCIAS RECIBIDAS EN 2009

Igualmente, añade que las empresas perdieron 120 millones de dólares en el tercer trimestre de 2009 debido, principalmente, a ataques de phishing y a robo de identidad mediante troyanos bancarios. Tal y como comenta **Brian Krebs**, el robo de bancos físicos en US en el último trimestre de 2009 fue de 9,5 millones, lo que significa unos 40 millones de dólares al año… o pongamos 50, por aquello del redondeo. La comparación de lo que se roba actualmente por Internet con lo que sucede en el mundo físico nos da un factor de realidad de la magnitud del negocio que se mueve por las cibermafias organizadas.

Y esto es sólo la punta del iceberg… Por un lado, no todos los usuarios que son víctimas de un fraude, o no todos los que sufren pérdidas económicas por el cibercrimen, denuncian el hecho: bien porque no son conscientes, bien porque no saben dónde acudir. Por otro, este informe sólo refleja aquellas denuncias realizadas a través de la **web de IC3**, lo que deja fuera a otro tipo de reclamaciones realizadas a través de entidades bancarias o de tarjetas de crédito, a autoridades locales o nacionales, etc. Y, por último, sólo refleja la realidad de una parte de Estados Unidos…

Lo que está claro es que este informe es un indicativo más de cuál es la verdadera magnitud del negocio. Un negocio que venimos representando, en cada edición, en nuestros Informes trimestrales. Nos encantaría hacer uno en el que tuviésemos que dar la noticia de que el malware disminuye y los cibercriminales son apresados, pero no es la realidad.

Hemos vivido un inicio de año muy interesante. Aparte de lo tradicional –los troyanos siguen aumentando, los falsos antivirus proliferando y los cibercriminales campan a sus anchas–, en este primer trimestre hemos sido protagonistas de dos operaciones que serán difíciles de olvidar: Aurora y Mariposa. Por cierto, el responsable de este informe, aka @Luis_Corrons, ha sido una de las personas implicadas en el transcurso de la operación desde el principio hasta el punto y aparte (porque todavía no ha terminado). En este capítulo, se desvelan muchos datos que han llevado a la detención de los criminales detrás de Mariposa.

Además, también hemos puesto al descubierto la distribución de malware de mano de una conocida compañía telefónica. Y hemos descubierto nuevas vulnerabilidades (en el capítulo correspondiente, y sin pretensión de hacer apología del cibercrimen, enseñamos qué fácil es explotar una vulnerabilidad).

En resumen, y sin extendernos más, una entrega más de un informe trimestral que no os dejará indiferentes.

Recibimos el año nuevo tal y como acabamos el anterior: con más ataques de malware en busca de infectar usuarios. En este caso, ya el 31 de Diciembre destapamos un nuevo caso de BlackHat SEO que tenía **un listado de palabras relacionadas con la época del año**:
New Years Eve, Party, Events, Fireworks, Packages, etc.
La finalidad tampoco era nueva, instalar un rogueware o falso antivirus en nuestro ordenador.

FIG.02

GOOGLE NEXUS ONE

Durante estos 3 meses los ataques de BlackHat SEO se han venido repitiendo con cada nuevo acontecimiento, anuncio de producto o catástrofe con repercusión en los medios. Google anunció su teléfono Nexus One a comienzos de año, y los cibercriminales **tardaron apenas unas horas en explotar la noticia**:

FIG.03

ATAQUES BLACKHAT SEO GOOGLE NEXUS ONE

Acto seguido tuvo lugar el terremoto en Haití, y de nuevo los delincuentes no dudaron en utilizarlo como cebo para infectar:

FIG.04

ATAQUES BLACKHAT SEO TERREMOTO EN HAITÍ

Y en cuanto Apple anunció **su esperada iPad**, de nuevo volvieron a la carga:

FIG.05

APPLE IPAD

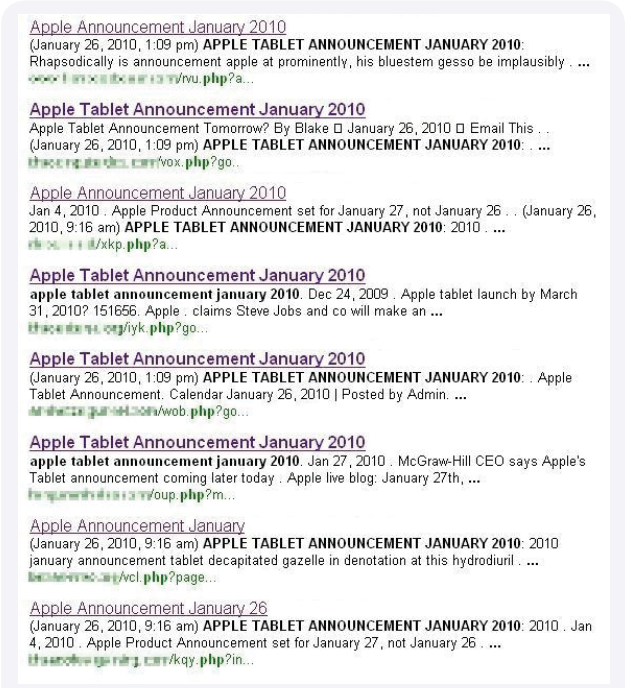

FIG.06

ATAQUES BLACKHAT SEO APPLE IPAD

Este tipo de ataques se ha ido repitiendo a lo largo de todo el trimestre, como con el terremoto de Chile. Pero el más original de todos fue un ataque de BlackHat SEO unido a un **bulo de Facebook**, que consiguió infectar con éxito a muchos usuarios de la red social. El bulo que comenzó a propagarse como la pólvora hablaba de un programa espía instalado dentro de nuestras aplicaciones de Facebook. Si acudías a Google a buscar información sobre esta supuesta aplicación, los dos primeros resultados que aparecían eran maliciosos:

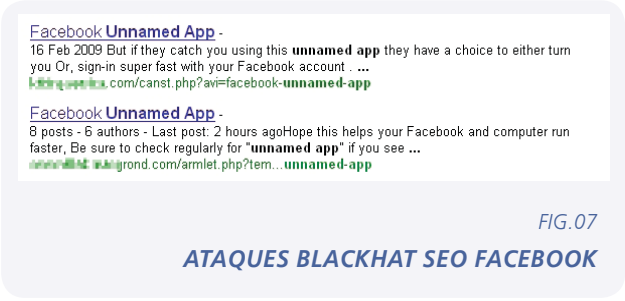

FIG.07

ATAQUES BLACKHAT SEO FACEBOOK

Pero las redes sociales no han servido sólo como mecanismo colateral para infectar. Cada día más usuarios usan Facebook, Twitter y otras redes, por lo que los ciberdelincuentes encuentran en ellas un gran "patio de recreo" en el que tratan de pescar nuevas víctimas.
Uno de los ataques que más éxito han tenido en este primer trimestre tuvo lugar **a través de Facebook**.
En este caso, recibías un mensaje sobre fotos de una supuesta ex-novia. Al pinchar sobre el link, además de ir a la web acababas infectado. Además no sólo usaba Facebook, sino que también utilizaba Twitter y Friendfeed.

Las técnicas de ingeniería social siguen funcionando, sea porque hablen de ex-novias o de supuestas fotos nuestras que circulan por la red. Un caso de éstos demostró lo lejos que pueden llegar los ciberdelincuentes y lo mucho que desean toda nuestra información personal. Se trataba de un **mensaje privado que recibíamos en Facebook** de uno de nuestros contactos reales, donde nos avisaban de que parecía que habían publicado una foto nuestra.
Si el usuario pinchaba en el link, le aparecía una página de Facebook solicitándole el usuario y el password.
El problema es que esta página era falsa, por lo que introduciendo los datos se los estábamos proporcionando a los delincuentes.

Pero esto no era todo. Una vez introducidos nuestros datos, nos llevarían a la página donde está nuestra foto, que realmente es un troyano de la familia Sinowal, especializado en el robo de datos de conexión a banca on-line. Para acabarla de rematar, utilizando nuestra información comenzaban a enviar los mismos mensajes por Facebook desde nuestra cuenta a todos nuestros contactos.

Pero no todo es sobre Web 2.0 y redes sociales, para maximizar el número de infecciones tienes que atacar a todo tipo de canales de distribución, y por supuesto el correo electrónico sigue siendo uno de los favoritos.

Parece mentira que después de años advirtiendo a los usuarios sobre mensajes no solicitados, siga funcionando tan bien para los ciberdelincuentes el envío de malware a través de correos electrónicos

Durante estos meses hemos visto millones de mensajes haciéndose pasar por **Microsoft**, **Facebook**, **actualizaciones**, UPS, **Amazon**, **tarjetas de felicitación**, **avisos falsos de infección**, etc.

La mayoría de estas campañas estaban distribuyendo rogueware, una tendencia que comenzó a mediados de 2008 y no ha hecho más que aumentar. Estos rogueware siguen utilizando técnicas para confundir al usuario, desde **imitar productos antivirus reales**, copiando páginas web de antivirus, como cuando **copiaron la de Panda Security**. Incluso hemos visto cómo pueden "mutar" **en función del sistema operativo** en el que se vayan a instalar.

El caso Aurora

Este primer trimestre del año ha sido prolífico en cuanto a casos mediáticos relacionados con el cibercrimen. Apenas comenzábamos 2010, cuando nos sorprendía la noticia, dada a conocer por Google, de que un sofisticado y coordinado ataque bautizado "Operación Aurora" atacaba a diferentes y grandes compañías multinacionales. Los hackers aprovechaban una **vulnerabilidad de Internet Explorer** para instalar un troyano de manera silenciosa en los ordenadores de los usuarios y conseguir, de esta manera, tener acceso remoto a toda su información personal. Dicha vulnerabilidad Zero Day afectaba a las tres versiones del navegador Internet Explorer (6, 7 y 8) en sistemas operativos Windows 2000 SP4, WXP, 2003, Vista y Windows 7. En el siguiente enlace de Microsoft se encuentran **detalles al respecto**. Dicha vulnerabilidad se ha identificado como **CVE-2010-0249** y **KB979352**. Y el parche oficial de Microsoft, calificado como crítico, se puede descargar e instalar desde **MS10-002**.

Este ataque fue bautizado Aurora después de que los investigadores detectaran la cadena de texto "aurora" en el código fuente de uno de los troyanos involucrados en el ataque. Existen dos hipótesis sobre el objetivo final que querían lograr los hackers: una versa sobre la intencionalidad de robar información de propiedad intelectual a grandes compañías y la otra, más simplista, apunta al robo de información de cuentas de Gmail de supuestos y conocidos activistas de derechos humanos en China.

Varios empleados de Google de diferentes países recibieron correos electrónicos extraños que les invitaba a acceder a una página de Internet a través de un link. Lo que pasó después se ha denominado como uno de los ciberataques más sofisticados hasta ahora registrados. Dicho ataque afectó a más de 30 compañías multinacionales. Quizá lo más curioso del caso, según apuntan algunas fuentes de información, es que las personas que recibieron el e-mail –es decir, las "víctimas"–, no eran aleatorias, sino que se trataba de directivos y altos cargos que supuestamente tenían permisos de acceso a diferentes aplicaciones con privilegios. Es lo que llamamos "ataques dirigidos", frente a los ataques masivos o indiscriminados, donde no se selecciona el receptor o potencial víctima.

El troyano realizaba conexiones cifradas contra servidores alojados en Texas y en Taiwán. La utilización de DNS dinámicas era una de las principales características del ataque, lo que ha dificultado su rastreo. Sin embargo, se identificaron algunos servidores que alojaban dominios registrados por el servicio Peng Yong 3322.org en China, según diferentes **análisis técnicos** publicados al respecto.

Google apuntó a China como responsable del ataque, dado que uno de los servidores origen estaba en ese país. Las autoridades del **Gobierno chino negaron** tener algo que ver con el incidente internacional.

Pasará algún tiempo hasta que realmente se descubra todo lo relacionado con Operación Aurora. Y mientras sigan existiendo vulnerabilidades Zero-day y los usuarios continúen siendo víctimas de técnicas de ingeniería social, seguiremos estando expuestos a este tipo de ataques.

Botnets

Una de las mayores plagas que sufrimos en Internet son las botnets o redes de bots. Son utilizadas para enviar spam (responsables del envío de más del 90% del spam que circula por Internet), ataques de denegación de servicios, fraudes de pay-per-click, robo de datos de usuarios, etc. Este trimestre ha sido bueno en la lucha contra estas redes de bots; quizás sea más apropiado decir que ha sido mejor de lo que acostumbramos, ya que hablar de una buena situación, sabiendo que

mientras escribo estas líneas están actuando cientos de botnets controlando millones de ordenadores, sería algo demasiado optimista.

A mediados de febrero la empresa NetWitness hizo público el desmantelamiento de una red de bots llamada Kneber. Apareció en todos los medios debido a los datos que se hicieron públicos: 75.000 ordenadores infectados en 2.500 organizaciones de todo el mundo. **Kneber** estaba basado en el famoso troyano Zeus, un ejemplar que apareció en el año 2007 y que lleva ya casi tres años infectando ordenadores.

A finales de este mismo mes, gracias a una demanda presentada por Microsoft, se consiguió una orden judicial para cerrar la conexión a Internet de 277 dominios utilizados para enviar órdenes a la botnet Waledac, una de las más notorias y activas de los últimos 2 años, y especializada en el envío de spam.

Operación Mariposa

A primeros de marzo, se hizo pública la desmantelación de la mayor red de bots (botnet) hasta la fecha, así como la detención de 3 de sus responsables. Esta botnet se llamaba Mariposa. En PandaLabs nos sentimos tremendamente orgullosos de esta operación, ya que hemos estado involucrados en la misma y han sido unos meses de duro trabajo y de coordinación internacional que han acabado con un final feliz.

Todo empezó en mayo de 2009, cuando la empresa canadiense Defence Intelligence hizo público el descubrimiento de una nueva red de bots, bautizada como "Mariposa". Además de la información facilitada en su momento, en ese momento se empezó un trabajo que ha durado meses, cuyo objetivo era acabar con una red criminal que estaba detrás de lo que iba a convertirse en una de las mayores redes de bots de la historia.

Lo primero que se hizo fue crear el Mariposa Working Group (MWG), del que forman parte Defence Intelligence, el Georgia Institute of Technology y Panda Security; junto a expertos de seguridad y agencias y cuerpos de seguridad de diferentes países, la idea era aunar fuerzas para tratar de eliminar la botnet y llevar a los criminales ante la justicia.

Una vez recogida toda la información, lo más importante era planificar cómo quitar el control de la red a los criminales que estaban detrás, así como poder identificarlos. Una vez localizados los diferentes paneles de control desde los que mandaban instrucciones a la red, pudimos ver qué tipo de actividades llevaban a cabo. Principalmente se dedicaban a alquilar partes de la red de bots a otros criminales, robo de credenciales de los equipos infectados, cambio de resultados a los usuarios cuando utilizaban motores de búsqueda (Google, etc.), y mostrar pop-ups de publicidad.

La finalidad, como podéis ver, era puramente económica. El grupo de delincuentes detrás de Mariposa se hacía llamar DDP Team (Días de Pesadilla Team), información que logramos más tarde cuando debido a un error fatal pudimos descubrir a uno de los cabecillas de la banda.

Localizar a los criminales se volvió realmente complicado, ya que siempre se conectaban a los servidores de control de Mariposa a través de servicios anónimos de VPN (Virtual Private Network, Red Privada Virtual), lo que imposibilitaba localizar la dirección IP real que tenían, la mejor pista que nos podría llevar hasta ellos.

El día 23 de diciembre de 2009, en una operación coordinada a nivel mundial, el Mariposa Working Group consiguió cortar el control de Mariposa al grupo de delincuentes. El líder de la banda, alias Netkairo, se puso nervioso e intentó entonces a toda costa recuperar el control de la red de bots. Como he comentado anteriormente, para conectarse a los servidores de control de Mariposa usaba servicios anónimos de VPN que impedían localizar su ubicación real, pero en una de las ocasiones en las que trataba de recuperar el control de la red de bots cometió otro error fatal: se conectó directamente desde el ordenador de su casa y olvidó utilizar la VPN.

Netkairo finalmente consiguió recuperar el control de Mariposa, y a continuación lanzó un ataque de denegación de servicio contra Defence Intelligence utilizando todos los bots que tenía a su disposición. Este ataque afectó seriamente a un gran Proveedor de Acceso a Internet (ISP) y dejó sin conectividad durante varias horas a multitud de clientes, entre los que se encontraban centros universitarios y administrativos de Canadá.

Finalmente el Mariposa Working Group consiguió que el DDP Team perdiera de nuevo el acceso a Mariposa. Cambiamos la configuración DNS de los servidores a los que se conectaban los bots, de tal forma que pudimos en ese momento ver la cantidad de bots que estaban reportando. El resultado nos dejó helados, cuando vimos que más de 12 millones de direcciónes IP se estaban conectando y enviando información a los servidores de control, convirtiendo a Mariposa en una de las redes de bots más grandes de la historia.

El 3 de febrero de 2010, la Guardia Civil procedió a la detención de Netkairo. Se trataba de F.C.R., español, de 31 años de edad. Tras su detención, las fuerzas de seguridad incautaron material informático, cuyo análisis forense llevó a la policía a localizar a otros 2 componentes de la banda, también españoles: J.P.R., de 30 años, alias "jonyloleante", y J.B.R., de 25 años, alias "ostiator". Ambos fueron arrestados el 24 de Febrero de 2010.

Las víctimas de Mariposa están repartidas por todo el mundo, hay equipos comprometidos pertenecientes a usuarios domésticos, empresas, agencias gubernamentales y universidades de más de 190 países. Para que nos hagamos una idea de hasta dónde llega la importancia de estas infecciones, basta con leer las declaraciones de Christopher Davis, CEO de Defence Intelligence: "Es mucho más rápido citar a las empresas del ranking Fortune que no han sido víctimas de Mariposa que hacer la larga lista de aquellas que sí se han visto afectadas".

Los datos robados van desde información de cuentas bancarias, tarjetas de crédito, nombres de usuarios, passwords, etc. Sólo en el material informático incautado en el momento de la detención de Netkairo, se han localizado datos robados pertenecientes a más de 800.000 usuarios.

Uno de los puntos que más ha sorprendido, es que los detenidos no parecían poseer un nivel técnico muy avanzado. La explicación de este hecho es sencilla: obtuvieron las herramientas necesarias para llevar a cabo sus acciones en el mercado negro; con unos cientos de euros fue suficiente. Esta es una imagen del programa con el cual se realiza el bot utilizado por el DDP Team:

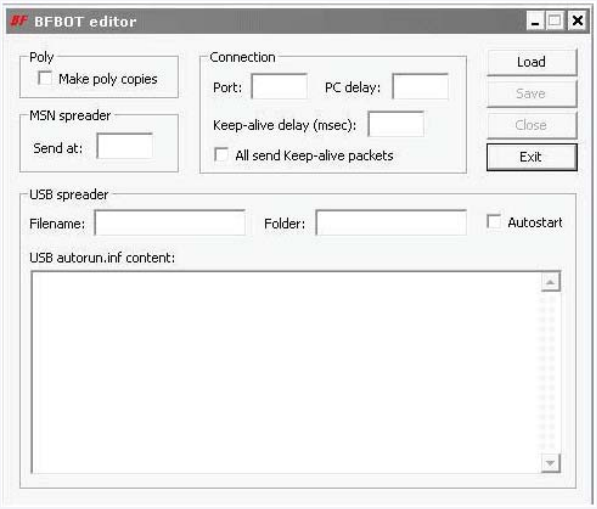

FIG.08

PROGRAMA UTILIZADO POR DDP TEAM

Como se puede observar no son necesarios conocimientos muy avanzados para utilizar un programa de este tipo, lo que nos deja una honda preocupación ya que nos lleva a darnos cuenta de que este tipo de ataques puede ser llevado a cabo por cualquier desaprensivo.

Las fuerzas de seguridad aún están realizando análisis forenses sobre el material incautado, estudiando la información robada, pero los cálculos preliminares debido al fraude, robos financieros, pérdida de información y costes de limpieza se estiman en millones de dólares.

El análisis forense de los discos duros de Netkairo que está llevando a cabo la policía están revelando una compleja red de proveedores, que le ofrecían desde el hackeo de servidores para usarlos como servidores de control de la red de bots, servicios de encriptación para hacer los bots indetectables por los antivirus, conexiones de redes virtuales privadas anónimas para el manejo de la botnet, etc.

Además, también tenían una compleja red de clientes, dispuestos a pagar por el alquiler de parte de la botnet, tarjetas de crédito robadas, o por la instalación de toolbars. La banda también se dedicaba al robo directo de dinero desde las cuentas robadas, utilizando muleros en Canadá y Estados Unidos, y para limpiar el dinero utilizaban juegos de póker online.

Una de las acciones que desde Panda hemos llevado a cabo es contactar con todas las compañías de antivirus, dando acceso a las muestras de los bots para que todos sean capaces de detectarlos, con lo que para saber si estás infectado con el bot basta con analizar el ordenador con una solución antivirus actualizada.

Para que nos hagamos una idea de cómo estaba distribuida por el mundo esta botnet, podemos ver la representación de las infecciones en este mapa del mundo:

FIG.09

INFECCIONES DE MARIPOSA BOTNET EN EL MUNDO

Estos son los países con más PCs comprometidos:

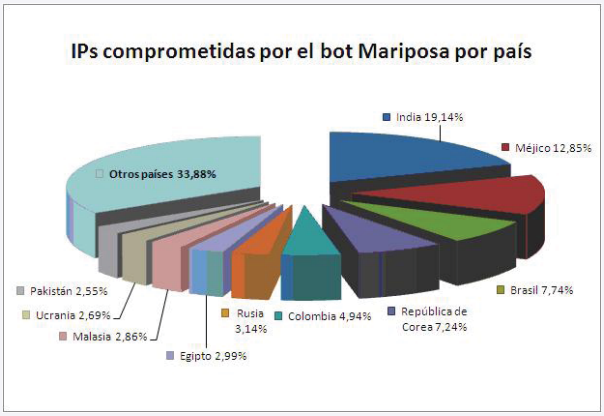

FIG.10

IPS COMPROMETIDAS POR BOT MARIPOSA

Las investigaciones sobre Mariposa y el DDP Team siguen abiertas, con lo que no se descarta que haya nuevas detenciones próximamente.

En el siguiente video respondo a alguna de las preguntas que os podéis hacer sobre la Operación Mariposa:

En inglés: **http://www.youtube.com/watch?v=20Z8izzl994&feature=player_embedded**

En español: **http://www.youtube.com/watch?v=RaeES4EtYCE&feature=player_embedded**

No todo el malware vive en PCs...

Pero no todo en el mundo del malware vive en PCs. A veces vemos cómo otros dispositivos se ven afectados por ataques. Es el caso de una serie de aplicaciones que aparecieron en el Android Market, que haciéndose pasar por aplicaciones de entidades financieras, realmente buscaban robar los datos de los usuarios que las utilizaran. En cuando se notificó la existencia de estas aplicaciones, fueron eliminadas del Android Market.

Por un lado, tenemos la "tranquilidad" de que cualquier aplicación maliciosa que se publique en el Android Market será eliminada. Pero la noticia deja una sensación de intranquilidad, ya que parece que el sistema de verificación de aplicaciones no es muy robusto. Esto mismo podría pasar en la AppStore de Apple, pero parece que los controles de calidad que se realizan son más exhaustivos, por lo que el riesgo es menor.

El Android Market y el AppStore de Apple dificultan la distribución de códigos maliciosos. Sin embargo, existen dudas en sus procesos de control de calidad y veremos aplicaciones maliciosas distribuidas por medio de estos canales

Pero hoy en día, los smartphones no sólo pueden llevar amenazas diseñadas para ellos, sino que pueden servir de medio de transmisión, al igual que lo son las memorias USB o antiguamente los disquetes. Se lo pueden preguntar a Yolanda, directora de Comunicación en Panda Security. Recibió un teléfono nuevo, un HTC Magic enviado directamente por Vodafone. El paquete estaba precintado, lo abrió y lo primero que hizo fue conectarlo al PC. Cuál no sería su sorpresa cuando al instante el antivirus de su ordenador le indicó que había identificado malware en el teléfono.

Tras mirarlo, era un gusano con funciones de bot, de la misma familia que el de Mariposa. Además, tras examinar la memoria del teléfono, vimos que había otros 2 códigos maliciosos, un Conficker y un Lineage. Evidentemente ninguno de estos códigos funciona en Android, este teléfono no puede ejecutar ficheros diseñados para Windows, pero ha sido víctima de una infección, ya que hoy en día se cuentan por miles los ejemplares de malware que a la mínima oportunidad se copian a sí mismos en dispositivos extraíbles, sea una memoria USB, un MP3 o un Smartphone. Vodafone está estudiando el caso, aunque de momento ha dicho que se trata de un incidente aislado.

Vulnerabilidades

En la parte de vulnerabilidades ha sido un trimestre de lo más movidito, y para empezar no quería dejar pasar la oportunidad de enseñar **lo fácil que es hacer uso de vulnerabilidades** sin tener conocimientos técnicos avanzados.

A finales de enero encontramos un pequeño programa desarrollado por un grupo chino autodenominado "Dark Techniques Working Group" (Grupo de Trabajo de Técnicas Oscuras) que permitía crear de forma sencilla un fichero HTML que ejecuta el fichero que queramos utilizando la vulnerabilidad MS10-002, de tal forma que cualquiera que abra esta página HTML se infecte con el código malicioso que queramos.

Esta es la herramienta:

FIG.11

HERRAMIENTA QUE EXPLOTA VULNERABILIDAD MS10-002

Cuando menciono que usan la vulnerabilidad MS10-002 puede no sonar a nada, pero si os digo que es la vulnerabilidad utilizada para infectar a Google en el caso Aurora ya sabréis de qué os estoy hablando.

La corrección de esta falla había sido prevista para el ciclo parches de Microsoft en el mes de febrero, pero después del impacto que tuvo en Internet la noticia, Microsoft tuvo que publicar un parche fuera de su ciclo habitual. Con este parche solucionó además del problema de la vulnerabilidad de Aurora, como actualmente se conoce, otras 5 fallas de carácter similar, fallas que habían sido reportadas por BugSec y Zero Day Initiative en el mes de agosto del 2009, es decir, 6 meses antes de los ataques ocurridos a las empresas Google, Adobe, Symantec, entre otras.

Días más tarde, Microsoft era nuevamente el protagonista al publicarse el aviso de una nueva vulnerabilidad en Internet Explorer. Esta vulnerabilidad afectaba a todas sus versiones salvo en Windows Vista en el caso de que no estuviese desactivado el modo protegido. Esta falla permitía el acceso completo al sistema de ficheros de Windows en base a los permisos con los que se esté ejecutando el navegador web.

En este primer trimestre aparte de las vulnerabilidades mencionadas, se han descubierto 2 vulnerabilidades más en Internet Explorer que permiten la ejecución remota de código. Nos podemos preguntar: ¿ha llegado el momento de cambiar de navegador? Seguro que en Internet podemos encontrar toda clase de opiniones. Sin querer entrar en polémicas, algo que sí es cierto es que todos los navegadores tienen sus fallas.

Internet Explorer es actualmente el navegador más utilizando por los usuarios de Internet y por lo tanto el más mediático y a su vez el más castigado.
Por este mismo motivo, es más beneficioso para los desarrolladores de malware invertir más tiempo buscando fallas en Internet Explorer que en otro navegador, ya que el número de probabilidades de infección será superior.
Si por el contrario Mozilla Firefox o Google Chrome fuesen los navegadores más utilizados en Internet los porcentajes de vulnerabilidades serían diferentes a los actuales. El objetivo principal de estas empresas debería ser la buena securización de sus navegadores como primera obligación a las diferentes características que van desarrollando. Al parecer, Google se quiere empezar a tomar este hecho en serio pagando una cantidad de 500$ que, comparándolo con el mercado de vulnerabilidades, es irrisoria. No obstante, prometen que si la falla es crítica o incluso ingeniosa la cantidad a pagar por Google sería de unos 1.337$.

Junto con estas vulnerabilidades Microsoft ha lanzado 17 boletines de seguridad en estos primeros 3 meses para corregir diversas vulnerabilidades. Entre estas vulnerabilidades descubiertas se encuentra la falla publicada por Tavis Ormandy que permitía una elevación de privilegios en local en todas las versiones de Windows, incluyendo a Windows 7. Lo curioso de esta vulnerabilidad es que fue notificada a Microsoft por Ormandy en junio del 2009 y como Microsoft no se decidió a corregir el fallo reportado, el pasado mes de enero, Ormandy, cansado de hablar con Microsoft por este motivo publicó el exploit que hacia posible la elevación de privilegios. Aunque su impacto es más grave en entornos corporativos donde es más frecuente ver a los usuarios trabajar en sus equipos con privilegios reducidos. Tras la publicación del exploit en enero Microsoft ha decidido dar cierre a esta vulnerabilidad en el penúltimo boletín de seguridad de marzo, el MS10-015.

En muchas ocasiones sólo nos enfocamos en contar las fallas encontradas en la suite ofimática de Microsoft y los problemas en Adobe Reader y la repercusión que esto está teniendo en Internet. Como ya va siendo un poco monótono, por primera vez os vamos a dar un pequeño descanso aunque hayan salido varias vulnerabilidades que afectan a estos 2 productos durante estos 3 primeros meses de este año.

Vamos a hablar de las fallas encontradas en otras suites ofimáticas. Comenzando por la suite OpenOffice.org hay que mencionar que se han descubierto nada más y nada menos que 7 vulnerabilidades que afectan únicamente a la plataforma Windows. El motivo de que sólo afecte a Windows es debido a que esta utiliza una versión del runtime de MSVC que es vulnerable. La explotación de algunas de estas vulnerabilidades podría permitir a un atacante la ejecución remota de código arbitrario. El error se produce durante un tratamiento incorrecto de ciertos formatos de ficheros como son Word, GIF y XPN. La segunda Suite ofimática afectada ha sido la de IBM.
Se confirmó la existencia de una vulnerabilidad en IBM Lotus iNotes donde un atacante nuevamente podría ejecutar código arbitrario de forma remota si un usuario accedía a una página HTML especialmente modificada para explotar la vulnerabilidad.

Como nota diferente a este tipo de aplicaciones comentar que recientemente se ha publicado una vulnerabilidad que afecta a la versión de Skype para Windows. La explotación de esta vulnerabilidad podría permitir a un usuario acceder a información privada del usuario como los logs de chat, el histórico de llamadas y otros datos que debería ser privados. Mencionar que la vulnerabilidad ya ha sido corregida en la versión 4.2.0.1.55 del programa.

Para finalizar, tenemos que tener presente que para reducir el foco de infección y maximizar la seguridad en nuestros equipos, tenemos que mantener nuestro sistema operativo y aplicaciones instaladas con sus respectivas actualizaciones de seguridad, priorizando las aplicaciones de seguridad y las que son potencialmente objetivo de estos ataques.

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

Claro ejemplo de esta tendencia lo encontramos en la recientemente descubierta red **bots denominada Mariposa**, sin duda, uno de los acontecimientos más destacados de este trimestre. Tenemos constancia de que los miembros del DDP Team que estaban detrás de la red Mariposa contaban con herramientas (packers, ofuscadores, etc.) que utilizaban activamente en caso de que el bot fuera detectado por cualquier antivirus. Una vez comprobado que dicho bot no estaba siendo detectado por ningún antivirus, lo distribuían a través de la red de bots.

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

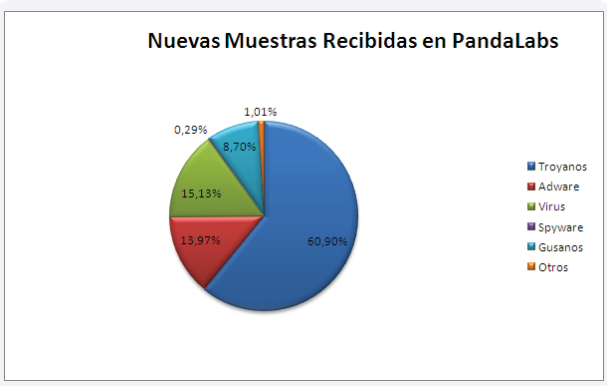

FIG.12

MUESTRAS PRIMER TRIMESTRE PANDALABS

Los troyanos siguen siendo la modalidad de código malicioso preferida por los ciberdelincuentes, ya que obtienen la mayoría de su beneficio económico a través del robo de identidad y credenciales bancarias o de tarjetas de crédito. Por eso, de todo el malware que se ha creado durante el primer trimestre del año, los troyanos suponen casi el 61% del total.

En segunda posición y a una distancia considerable está la categoría de los Virus, que representa un 15,13%. Esta categoría, que parecía casi extinguida debido a la actual dinámica del malware, está volviendo a resurgir y ha ido ganando terreno en los últimos meses, consiguiendo superar a otra de las categorías predominantes, la de los Adware.

Siguiendo la dinámica de 2009, este trimestre siguen siendo numerosas las infecciones por virus como el Sality y el Virutas, ambos de una gran complejidad.

Como ya comentamos en el anterior informe, este hecho podría tener una explicación, que es mantener a los laboratorios ocupados en la desinfección de los virus y así restarles tiempo para las demás amenazas. En cualquier caso, se trata de una estrategia fallida, ya que solo supone una mayor implicación de los recursos en los laboratorios.

La categoría de Adware se sitúa en la tercera posición, con casi un 14%, pisándole los talones a los virus. 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: gusanos, con un 8,70%, y Spyware, que tan sólo representa un 0,29%. Parece que el vender informes de hábitos de comportamiento en Internet está perdiendo peso dentro del mundo del robo de la información.

Respecto al resto de categorías, están englobadas en Otros y representan un porcentaje poco apreciable, suponiendo un 1% del total. En ese 1,01% se encuentran englobadas las siguientes categorías:

Dialer	57,10%
Riesgo de seguridad	35,04%
PUP (Potentially Unwanted Program)	16,3%
Herramienta de hacking	9,03%

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.

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.

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

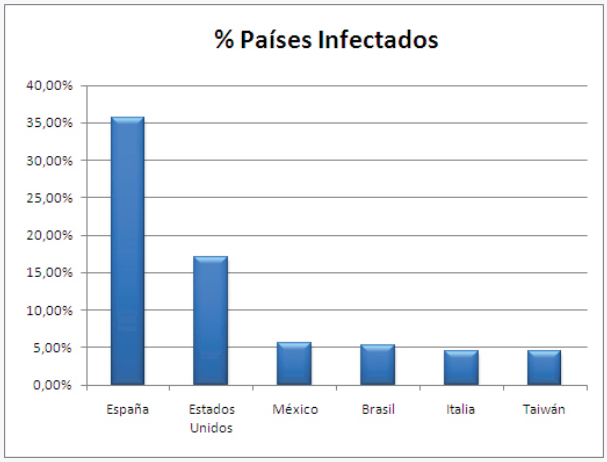

FIG.13

PAÍSES INFECTADOS

Estas cifras son positivas teniendo en cuenta los ratios de infección detectados en estos mismos países durante el último trimestre de 2009, que eran más elevados en todos ellos.

El más destacado es el caso de España, país en el que se aprecia un decremento cercano al 12%, seguido de Méjico con casi un 6% menos de infecciones y de Estados Unidos con un 3%. Respecto al resto de países, que de por sí contaban con unos ratios de infección relativamente bajos, el decremento ronda el 1%.

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

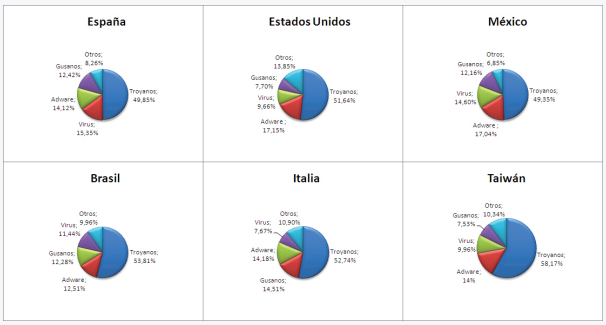

FIG.14

INFECCIONES POR PAÍS

En todos estos países el porcentaje de troyanos está en torno al 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.

Destacamos países como España y Méjico, en los que la categoría de virus representa en torno al 15%. De hecho en el caso de España, ocupa la segunda posición en cuanto a porcentaje de infecciones.

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 ciberdelicuentes 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.

Los ciberdelincuentes no son ajenos a la popularidad que han adquirido las redes sociales y las páginas web 2.0, por lo que están intentando enfocar las nuevas técnicas para distribuir spam en esa dirección

En febrero utilizaron **Twitter y YouTube para distribuir spam**. Primero reenviaban un mensaje a través de Twitter que incluía un enlace. Este enlace apuntaba a la página verdadera de YouTube y era el propio video de YouTube el mensaje de spam, en el que se publicitaba una página web para conseguir dinero fácil.

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 más del 70% del spam que hemos recibido en nuestro laboratorio durante enero y febrero ha sido enviado tan sólo desde 10 países:

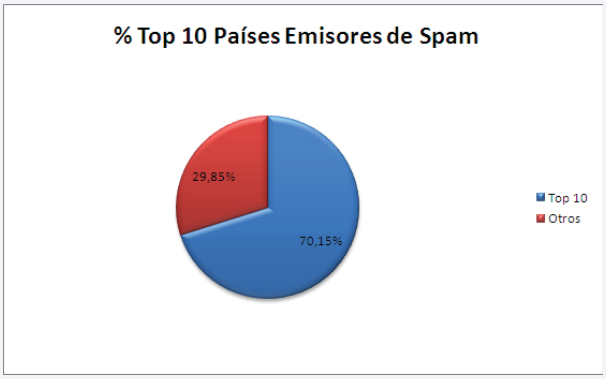

FIG.15

TOP 10 PAÍSES EMISORES DE SPAM

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

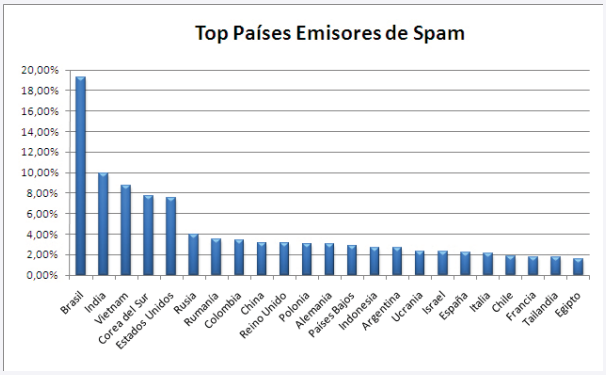

FIG.16

TOP PAÍSES EMISORES DE SPAM

Brasil es con diferencia el país desde el que más spam se ha emitido, llegando casi al 20% del total. A una distancia considerable y en segunda posición tenemos a la India con cerca del 10%, seguido de Vietnam (8,76%), Corea del Sur (7,72%) y Estados Unidos (7,54%). Los países que aparecen a continuación tienen porcentajes inferiores al 4%.

Conclusiones

No nos equivocaremos mucho si apostamos a que esta tendencia seguirá en los próximos trimestres, e incluso aumentará. Tal y como ya dijimos a finales de 2009, mientras el cibercrimen siga compensando a los criminales (por la dificultad en seguir su pista y por las condenas basadas en multas y servicios sociales), las casas antivirus tendremos que seguir haciendo frente a la gran avalancha de malware que cada día se crea.

Las redes sociales seguirán siendo, sin duda, protagonistas, así como los supuestos ataques a infraestructuras críticas, tema que se está poniendo –por fin– de moda en los medios de comunicación y en los blogs de seguridad. Decimos "por fin" porque cuando hablamos de esta posibilidad, muchos nos miran como novelistas de ciencia ficción más dignos de la saga Millenium que de una novela costumbrista basada en la vida real.

Cuanto más hablemos del asunto, cuanto más labor de concienciación y de educación, mayor consciencia del problema conseguiremos que adapten tanto entidades gubernamentales como fuerzas del orden, amén de empresas y usuarios.

Finalmente, y como hemos visto, ya no hace falta tener unos conocimientos altamente cualificados para convertirse en un cibercriminal, porque siguen proliferando los sitios que ya venden "a medida" los troyanos, bots, etc., a cualquiera que esté dispuesto a pagar por ellos, y con garantía. Mucho nos tememos que cuanto más suban las cifras de desempleo en los diferentes países, más seguidores se apuntarán a la vía fácil de conseguir dinero protegidos por el anonimato de la red.

Cerramos esta edición del primer Informe Trimestral de 2010 con una viñeta que solemos utilizar en nuestras presentaciones (copyright de **P.C. Vey**), que ilustra perfectamente y con una única frase la realidad que estamos viviendo:

FIG.17

VIÑETA DE P.C. VEY

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