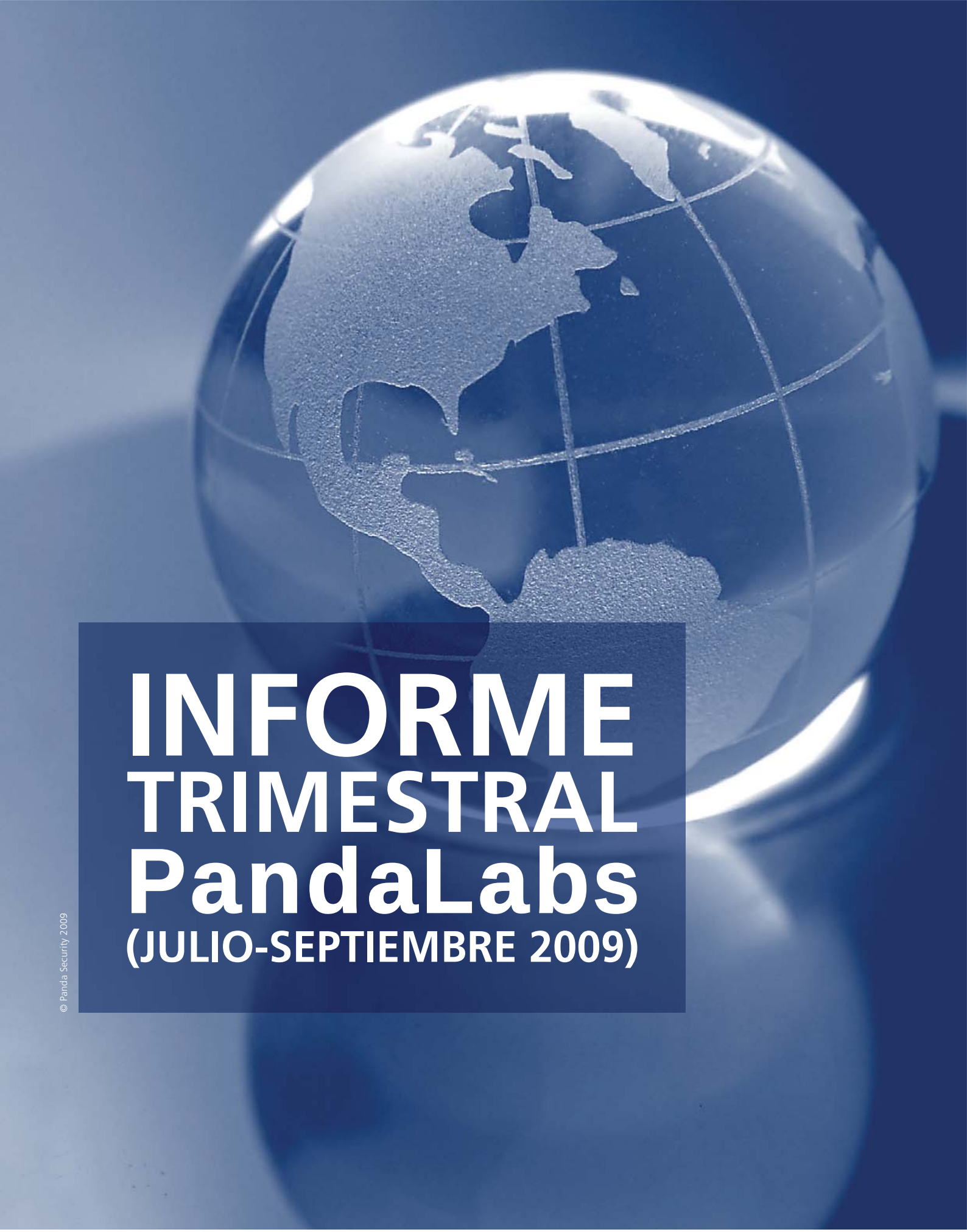

INFORME TRIMESTRAL PandaLabs

(JULIO-SEPTIEMBRE 2009)

PANDA SECURITY | 20 Aniversario 1990-2010

Índice

Introducción

El verano ya ha tocado a su fin y presentamos el tercer informe trimestral en el que analizaremos los temas más destacados de estos tres meses.

Como comentamos en anteriores informes, desde hace un tiempo los NDRs están siendo utilizados para enviar spam. En este informe analizaremos la situación actual de los NDRs y expondremos las soluciones tecnológicas disponibles para prevenir los NDRs ilegítimos.

En la ya habitual sección de Vulnerabilidades podréis consultar las que han aparecido durante estos tres meses.

Por otra parte, analizaremos las tendencias más destacadas del trimestre en lo que a malware se refiere. Este trimestre al igual que el anterior también se han producido diversas campañas de ataques utilizando técnicas BlackHat SEO con el objetivo de infectar a los usuarios.

Además, la familia Koobface, un gusano de redes sociales, ha comenzado a utilizar Twitter para propagarse mediante la publicación de enlaces maliciosos desde cuentas de usuarios infectados.

Asimismo, como en anteriores informes, presentaremos la evolución de malware activo por país durante el tercer trimestre de 2009, así como las cifras globales de malware.

Esperamos que os resulte interesante.

Resumen ejecutivo

Este trimestre el malware más detectado por los sensores de seguridad de **PandaLabs** han sido los troyanos con un 37,70%, superando el 34,37% que registró en el anterior trimestre.

Una vez más Taiwán continúa manteniendo la primera posición en cuanto a malware activo con un 28,99% seguida de cerca por Estados Unidos con un 25,62% y Reino Unido con un 25,57%.

Aprovechando la celebración del día de la independencia en Estados Unidos, los autores de Waledac –también conocido como Storm Worm– lanzaron una campaña para infectar a los usuarios.

Días más tarde apareció una nueva vulnerabilidad 0-day afectando a Microsoft Video ActiveX Control.
Unas docenas de diferentes páginas web chinas explotaban esta vulnerabilidad.

También a inicios de julio hubo un ataque DDoS (Distributed Denial of Service) contra varias webs de Corea del Sur y Estados Unidos, principalmente páginas gubernamentales, militares y financieras.

A partir de agosto se han detectado incrementos de hasta un 2000% en el tráfico de NDRs, utilizados para enviar spam.

En septiembre, se ha descubierto un nuevo 0-day que afecta a los sistemas operativos Microsoft Windows desde Vista hasta Windows 2008 y que permite la ejecución remota de código.

Los ciberdelincuentes se están centrando en las vulnerabilidades y técnicas de ingeniería social, para así maximizar el número de infecciones entre los usuarios. Para conseguirlo, distribuyen malware en mensajes de spam, redes sociales y motores de búsqueda usando técnicas de Blackhat SEO.

Distribución de las nuevas amenazas detectadas

A continuación se incluye un gráfico relativo a la distribución de nuevos ejemplares de malware por tipo, detectados por **PandaLabs** durante el tercer trimestre de 2009:

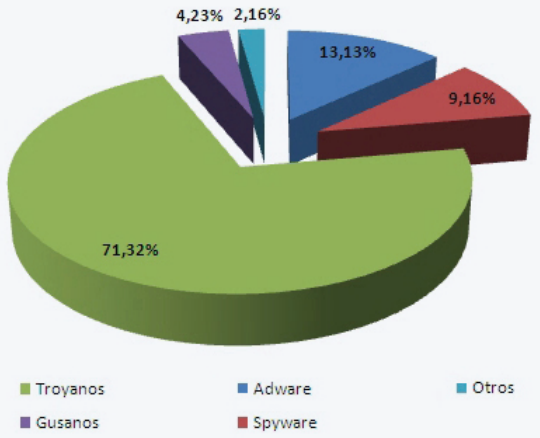

FIG.01

APARICIÓN TRIMESTRAL DE MALWARE

Según los datos del gráfico, se observa que la categoría de malware predominante sigue siendo la de los troyanos, que durante este tercer trimestre ha tenido una media del 71,32%, superior al 70,85% que se registró en el anterior trimestre.

Señalar que los backdoors se han integrado dentro de los troyanos, y los bots, según la capacidad de propagación para la que hayan sido diseñados, se han integrado en gusanos o en troyanos.

En cuanto a la categoría de los gusanos, su porcentaje ha descendido muy ligeramente hasta el 4,23%, tras el 4,40% del anterior trimestre.

Por otra parte, el spyware ha aumentado por primera vez este año y ha pasado de un 6,90% hasta un 9,16%. Respecto a la categoría de adware, sufre un ligero descenso de un 16,37% a un 13,13%, pero aún así continúa siendo la segunda categoría de malware más detectada en lo que llevamos de año.

La predisposición por parte de los ciberdelincuentes en seguir desarrollando el tipo de adware conocido como Rogue AV (falsos programas antivirus), y la efectividad de los mismos está ligada directamente a la posición de esta última categoría.

Hemos agrupado dentro de la categoría de Otros las categorías que tienen poca relevancia sobre el total.

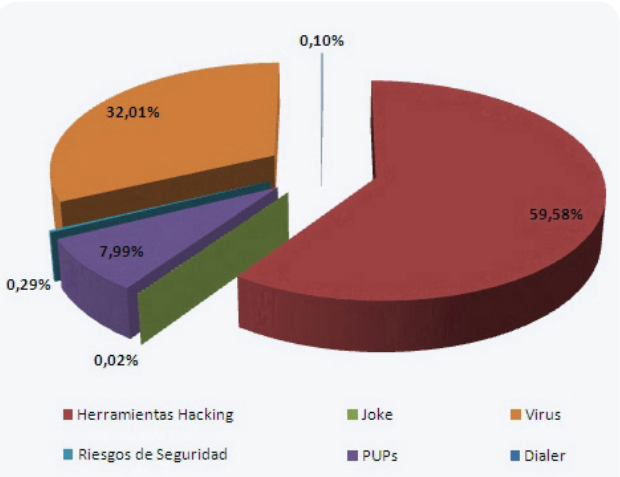

FIG.02

CLASIFICACIÓN DE LA CATEGORÍA DE OTROS

En esta sección observamos que los tipos predominantes de malware dentro de la categoría Otros corresponden a las herramientas de hacking situados con un 59,58%, seguidos de los virus, los cuales se han visto considerablemente incrementados desde un 18,16% en el segundo trimestre hasta el 32,01% actual.

Aparición de malware mes a mes

A continuación podemos ver la evolución en la aparición de nuevo malware mes a mes sobre las categorías más importantes:

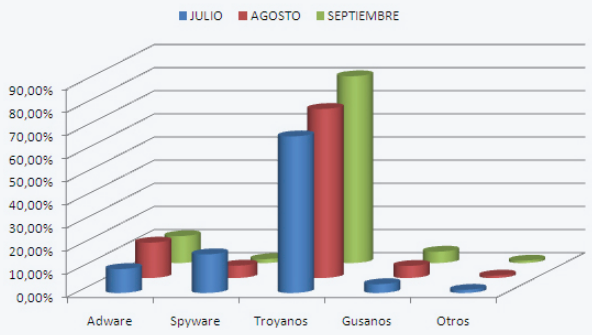

FIG.03

EVOLUCIÓN EN LA APARICIÓN DE NUEVO MALWARE

Se observa notablemente en cualquiera de los meses representados cuáles son las categorías más predominantes, que casualmente son las que más beneficios económicos reportan a los creadores de malware.

Amenazas detectadas por los Sensores PandaLabs

El siguiente gráfico muestra los niveles de infección existentes por tipos de malware a través de los sensores de seguridad de Panda Security a lo largo de este tercer trimestre:

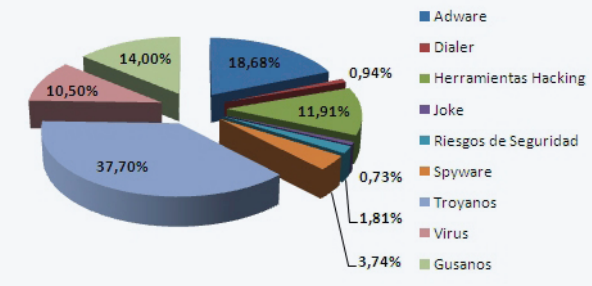

FIG.04

DISTRIBUCIÓN DETECCIONES POR SENSORES PANDALABS

En este trimestre el adware se mantiene dentro de los niveles habituales de infección hasta situarse en un 18,68% debido al gran volumen de falsos antivirus que hay en circulación actualmente, pero muy lejos de la principal amenaza detectada por nuestros sensores de seguridad que son los troyanos con un 37,70% que continúa aumentando tras el 34,37% que registró en el pasado trimestre.

A continuación se pueden observar cuáles han sido las 10 amenazas más detectadas por esos sensores:

1	Generic Trojan
2	Generic Malware
3	Trj/Lineage.BZE
4	Trj/Downloader.MDW
5	W32/AutoRun.APJ.worm
6	Adware/AccesMembre
7	Spyware/Virtumonde
8	W32/Bagle.RC.worm
9	Trj/Rebooter.J
10	Generic Worm

FIG.05

TOP TEN DE AMENAZAS DETECTADAS

Malware activo

En esta sección vamos a hablar de la evolución del malware activo durante el tercer trimestre del año 2009.

Para poder comprender qué es malware activo, es necesario definir los dos posibles estados en los que se puede encontrar: activo o latente.

El malware latente es aquel que está alojado en una máquina pero sin realizar ninguna acción. Está a la espera de ser ejecutado bien directamente por el usuario o bien de forma remota por el ciberdelincuente.

Una vez que es ejecutado, comienza a realizar las acciones dañinas para las que está programado. Por lo tanto, el estado de este malware cambiaría, y pasaría de estar latente a activo.

Hemos realizado un seguimiento sobre la evolución de malware activo mes a mes a través de nuestra herramienta online **ActiveScan 2.0**.

Gracias a este servicio, cualquier usuario puede analizar su equipo de forma on-line y gratuita, y así comprobar si su ordenador está infectado.

FIG.06

HERRAMIENTA ONLINE ACTIVESCAN 2.0

En la siguiente gráfica podemos observar la evolución del malware activo durante el tercer trimestre del año 2009:

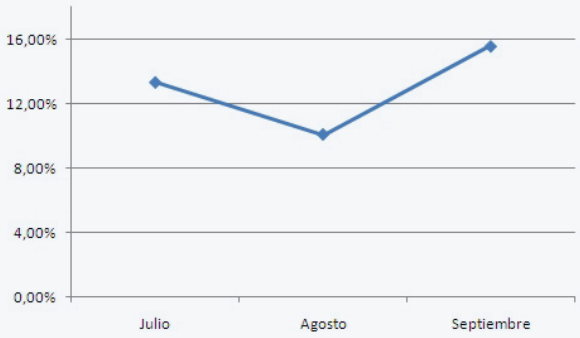

FIG.07

EVOLUCIÓN DE MALWARE ACTIVO DURANTE EL TERCER TRIMESTRE 2009

Como podemos observar en la gráfica anterior, pese a sufrir un descenso durante la época vacacional, cabe destacar que septiembre es el mes con el ratio más alto de PCs infectados con malware activo no solo durante este trimestre, sino que también de todo cuanto llevamos en el 2009, situando su punto más álgido en un 15,57%.

Malware activo

Estos datos reflejan la evolución a nivel global pero, ¿qué ocurre en cada país? En la siguiente gráfica podemos observar la infección de los países con mayor porcentaje entre los países con mayor número de análisis en ActiveScan 2.0 durante este trimestre.

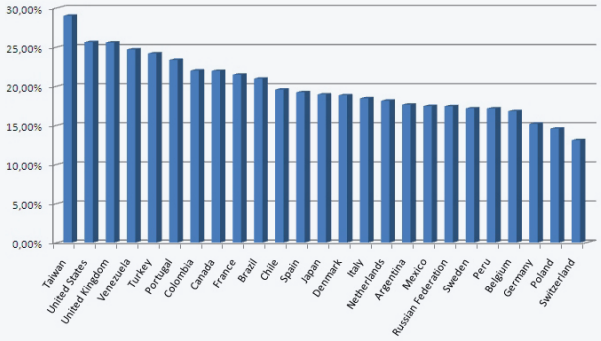

FIG.08

PAÍSES CON MAYOR PORCENTAJE DE MALWARE (JULIO-SEPTIEMBRE 2009)

Una vez más Taiwán continúa manteniendo su posición en este ranking de malware activo con un 28,99%, seguida de cerca por Estados Unidos con un 25,62% y Reino Unido con un 25,57%.

Cabe destacar nuevamente de forma positiva a Suiza quien, ya en el anterior trimestre estaba posicionado entre los países menos infectados, consigue descender aún más su ratio de malware activo, del 15% al 13,10%.

Un NDR (Non Delivery Report) es un correo electrónico automático enviado por los sistemas de correo con la finalidad de informar al emisor sobre problemas en la entrega de sus mensajes.

En **anteriores informes** ya hemos hablado de lo que son los NDRs "ilegítimos" (a partir de ahora los denominaremos simplemente NDRs) y adelantábamos que dar una solución a este tipo de amenazas era una de las prioridades en nuestras soluciones de seguridad perimetrales.

Por tanto, en este artículo nos vamos a centrar en la situación actual de los NDRs y las soluciones tecnológicas que hemos introducido en nuestros productos[1] para paliar sus efectos.

Situación Actual

En los últimos años, los NDRs han sido una amenaza habitual en gran parte como consecuencia de las técnicas DHA[2] utilizadas por los spammers para enviar spam. Pero, ha sido a partir de agosto cuando hemos visto incrementos de hasta un 2000% en el tráfico de NDRs.

Este tipo de ataques suelen llevarse a cabo por redes de bots compuestas por ordenadores infectados. Por tanto, el coste de ancho de banda y dinero que deben soportar los spammers es muy bajo y, es por eso, que este tipo de ataques son cada vez más indiscriminados, ya que la relación aciertos/fallos no tiene impacto sobre el coste, haciendo que aumente el número de NDRs como "daño colateral".

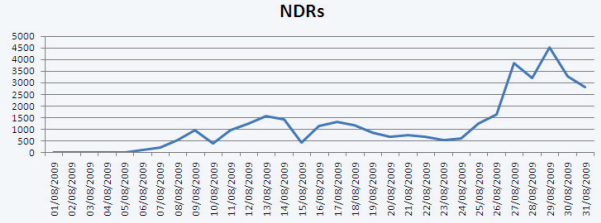

FIG.09

NÚMERO DE NDRS RECIBIDOS EN UNO DE LOS SERVIDORES DE PANDALABS

Ante este tipo de amenazas desde Panda Security hemos apostado por dos tipos de técnicas: BATV y restringir la recepción de NDRs.

BATV

BATV o Bounce Address Tag Validation es una técnica anti-NDRs basada en añadir una serie de "tags" o etiquetas en los mensajes enviados con el fin de que en caso de que nuestro correo no pueda ser entregado, el NDR generado adjunte dicha etiqueta y pueda ser reconocido como un NDR válido generado a causa de nuestro envío erróneo.

Los correos que no incluyan estas etiquetas serán considerados NDRs ilegítimos y por tanto, rechazados.

La forma de añadir este tipo de etiquetas y de asegurarnos de que estas van a incluirse en el posible NDR de respuesta puede variar según la implementación de la tecnología BATV, aunque en principio la base es la misma en todas.

Para añadir dicha etiqueta lo que se hace es, en la conexión SMTP, añadir a la dirección del emisor un tag que identifique unívocamente el mensaje y que pueda ser verificado en caso de que genere un NDR. Por tanto, en la conexión SMTP cuando en el comando MAIL FROM se envía, por ejemplo, ***sender@pandasecurity.com*** se le añade una etiqueta de la siguiente forma: ***prvs=xxxxxxx=sender@pandasecurity.com***. Donde xxxxxxx es un código generado dinámicamente que nos permitirá identificar unívocamente nuestro envío.

En caso de que el envío sea erróneo, se enviará un mensaje de respuesta a la dirección del emisor en la conexión SMTP del mensaje original, es decir, ***prvs=xxxxxxx=sender@pandasecurity.com***. Por tanto, cuando pase por nuestra solución se verificará la etiqueta ***prvs=xxxxxxx*** y se entregará el mensaje a la dirección de ***sender@pandasecurity.com***.

1 Panda Gate Defender Performa 3.2.00.

2 Directory Harvest Attack: Técnica utilizada por spammers basada en enviar correos electrónicos a combinaciones de nombre comunes y dominios válidos con la intención de descubrir cuentas de correo existentes en dicho dominio y así enviarles spam. De las combinaciones probadas por los spammers solo un pequeño porcentaje tiene éxito, por tanto, los intentos fallidos generarán un NDR. Además, teniendo en cuenta que los spammers suplantan direcciones de correo válidas, estos NDRs llegan a usuarios que no han realizado el envío realmente.

Puede surgir la siguiente pregunta: en caso de que el envío sea correcto, ¿aparecerán las etiquetas en el campo emisor del mensaje? La respuesta es no, ya que los clientes de correo obtienen la dirección del emisor del mensaje del campo "From" (en nuestro ejemplo ***sender@pandasecurity.com***), el cual no se modifica. Por tanto, la utilización de estas etiquetas no afecta al usuario.

¿Es posible que un spammer sea capaz de enviar mensajes con una etiqueta válida y nuestra solución deje pasar dicho NDR? El código incluido en la etiqueta es generado a partir de valores aleatorios además de claves que son desconocidas por los spammers, por lo que es muy difícil que los spammers puedan generar valores válidos. Además, el envío de NDRs no es la intención del spammer sino un efecto secundario de sus acciones, por tanto es poco probable que los spammers intenten explotar esta posibilidad.

A continuación vamos a exponer un ejemplo de carácter más técnico explicando cómo funciona BATV en nuestros productos. Se trata de una de las configuraciones que explicaremos más adelante y que genera más problemas de cara a la detección de NDRs.

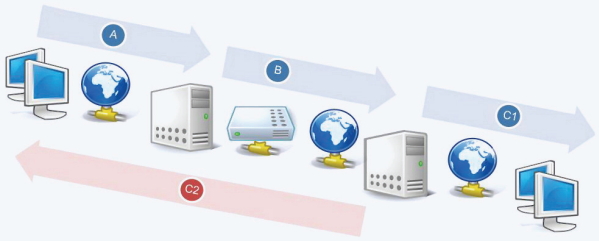

FIG.10

ESQUEMA DE TRÁFICO SMTP Y GENERACIÓN Y DETECCIÓN DE NDRS

A. Enviamos nuestro mensaje desde nuestra cuenta ***sender@pandasecurity.com*** a ***receiver@destination.com*** a través de nuestro servidor de correo.

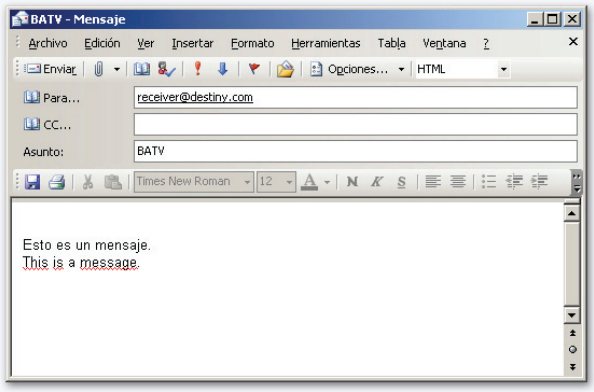

FIG.11

MENSAJE DE CORREO DE PRUEBA

B. Nuestro servidor inicia una conexión SMTP con el servidor de dominio.com. Nuestro producto (en este caso Gate Defender Performa 3.2.00) intercepta la conexión SMTP y modifica el parámetro "MAIL FROM" (ver *TABLA.01*).

C. En el tercer caso pueden ocurrir dos situaciones: 1) Que la cuenta ***receiver@destination.com*** exista y se entregue el mensaje o 2) Que la cuenta ***receiver@destination.com*** no exista y se genere un NDR.

1. El servidor dominio.com entregará el correo a ***receiver@destination.com*** con el siguiente formato:

```
Return-Path: prvs=abcdefgh=sender@pandasecurity.com
From: sender@pandasecurity.com
To: sender@destination.com
Date: Wed, 2 Sep 2009 12:49:31 +0200
Subject: BATV

Esto es un mensaje.
This is a message
```

FIG.12

FORMATO DEL CORREO ENTREGADO

Conexión SMTP Original	Conexión SMTP Modificada
220 ESMTP	220 ESMTP
helo pandasecurity.com	helo pandasecurity.com
250 mail.destination.com	250 mail.destination.com
mail from: sender@pandasecurity.com	mail from: ***prvs=abcdefgh=sender@pandasecurity.com***
250 Ok	250 Ok
rcpt to: receiver@destination.com	rcpt to: receiver@destination.com
250 Ok	250 Ok
Data	Data
354 Enter mail, end with <CRLF>.<CRLF>	354 Enter mail, end with <CRLF>.<CRLF>
From: sender@pandasecurity.com	From: sender@pandasecurity.com
Subject: BATV	Subject: BATV
Esto es un mensaje.	Esto es un mensaje.
This is a message.	This is a message.
.	.
250 ok: queued as B028343F94	250 ok: queued as B028343F94
quit	quit
221 Bye	221 Bye

TABLA.01

PROTOCOLO SMTP ORIGINAL Y MODIFICADO

Al almacenarse el correo en el servidor de destino, el parámetro MAIL FROM de la conexión SMTP se almacena como Return-Path. Como hemos comentado anteriormente, la dirección de origen que en el cliente de correo se toma como origen es la del campo FROM. El mensaje en el destino se verá de la siguiente manera:

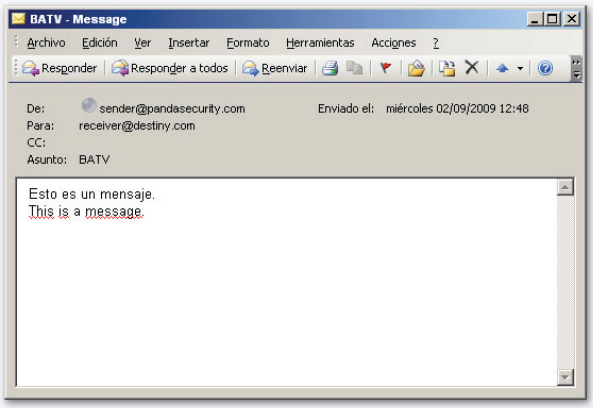

FIG.13

MENSAJE DE CORREO DE PRUEBA

Como se puede observar, los tags añadidos no afectan al envío/recepción de correos y es transparente para el usuario.

2. En el caso de que el servidor de destino acepte la conexión y luego verifique que la cuenta de correo destino no existe, enviará un aviso NDR a la dirección de correo que se identificó como origen en la conexión SMTP, es decir, al MAIL FROM.

   Por tanto el NDR se enviará de vuelta a nuestro servidor a la dirección ***prvs=abcdefgh=sender@pandasecurity.com***.

   En este caso, la conexión SMTP será analizada de nuevo por nuestro producto, restaurando la dirección original, es decir, sustituyendo ***prvs=abcdefgh=sender@pandasecurity.com*** por ***sender@pandasecurity.com***, comprobando que el valor del tag es correcto y se corresponde con un NDR generado a partir de un mensaje nuestro (ver *TABLA.02*).

   En caso de que el tag no existiera o no fuera válido, el mensaje NDR se descartaría.

Restringir la Recepción de NDRs

Esta funcionalidad integrada en nuestros productos no es tanto una técnica anti-NDRs sino una política que el usuario puede activar en caso de que lo considere oportuno. La activación de esta política supone que se descartarán todos los NDRs que no lleguen de una lista de direcciones IPs definida por el usuario. Dentro de dicha lista el usuario podrá añadir los Relays de entrada u otros servidores confiables de los que desee recibir los NDRs.

Para entender el interés de este tipo de políticas vamos a volver a explicar la generación de un NDR legítimo bajo dos configuraciones:

Configuración 1

A. El usuario envía un mensaje de correo a través de su Servidor de Correo.
B. El servidor de correo se conecta al servidor de correo donde se aloja la cuenta a la que hemos

Conexión SMTP Original	*Conexión SMTP Modificada*
220 ESMTP	220 ESMTP
helo destiny.com	helo destiny.com
250 mail.pandasecurity.com	250 mail.pandasecurity.com
mail from: postmaster@destination.com	mail from: postmaster@destination.com
250 Ok	250 Ok
rcpt to: ***prvs=abcdefgh=sender@pandasecurity.com***	rcpt to: sender@pandasecurity.com
250 Ok	250 Ok
Data	data
354 Enter mail, end with <CRLF>.<CRLF>	354 Enter mail, end with <CRLF>.<CRLF>
Subject: Message Delivery Failure	Subject: Message Delivery Failure
This is the mail system at host destiny.com.	This is the mail system at host destiny.com.
I'm sorry to have to inform you that your message could not be delivered to one or more recipients…	I'm sorry to have to inform you that your message could not be delivered to one or more recipients…
.	.
250 ok: queued as B028343F94	250 ok: queued as B028343F94
quit	quit
221 Bye	221 Bye

TABLA.02
PROTOCOLO SMTP ORIGINAL Y RESTAURADO

enviado el mail indicándole que quiere entregar un correo a dicha cuenta.

C. El servidor que aloja la cuenta receptora responde indicando que la cuenta a la que se desea enviar un correo no existe.

D. El servidor del emisor envía un NDR al usuario indicándole que el mensaje no ha podido ser enviado ya que la cuenta a la que iba dirigido el mensaje no existía.

Configuración 2 "Open Relay"

A. El usuario envía un mensaje de correo a través de su Servidor de Correo.

B. El servidor de correo se conecta al servidor de correo donde se aloja la cuenta a la que hemos enviado el mail indicándole que quiere entregar un correo a dicha cuenta.

C. El servidor que aloja la cuenta receptora acepta la conexión y recibe el correo y finaliza la conexión con el servidor del emisor. Más tarde verifica el destinatario del correo y en caso de que la cuenta no exista, envía un NDR al emisor indicando que la cuenta a la que se desea enviar un correo no existe.

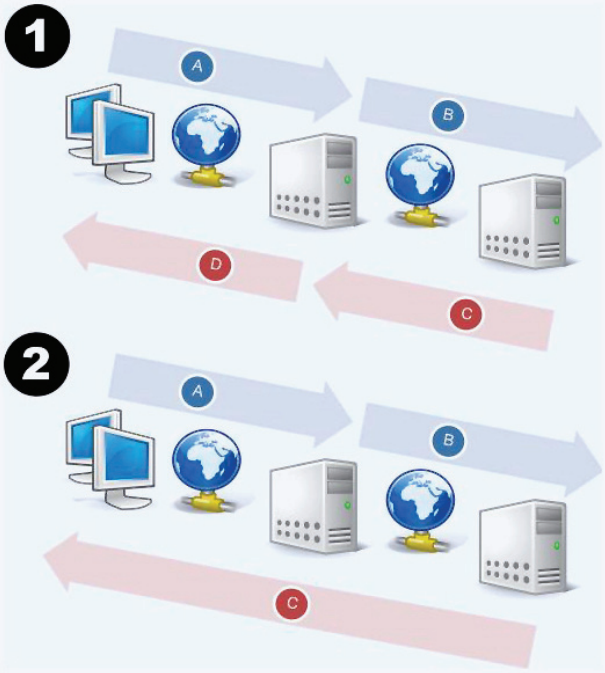

FIG.14

POSIBLES CONFIGURACIONES EN SERVIDORES DE CORREO

En la **Configuración 1**, nos encontramos una configuración estándar de un sistema de correo. Envío un correo electrónico a través de mi servidor o un relay, este se comunica con el servidor final, verifica que la cuenta a la que envío el mensaje existe y, en caso de no existir, recibo un NDR generado por mi servidor o relay.
Por tanto, según esta configuración solo debería recibir NDRs de mi servidor o relay, los cuales van a enviarme siempre NDRs legítimos. De esta manera, podría decidir descartar todos los NDRs que no provengan de mis servidores o relays.

El problema de esta política vendría con los servidores que funcionen según la **Configuración 2**, que a pesar de considerarse una configuración "no correcta" es utilizada por usuarios que buscan un mayor rendimiento, ya que es posible manejar mayores volúmenes de tráfico con el mismo equipamiento. En este segundo caso, el servidor final acepta todas las conexiones evitando hacer así la verificación de que la cuenta existe en cada envío y por tanto es él mismo quien, tras verificar más tarde que la cuenta no existe, envía el NDR indicando que la cuenta no existe. Utilizando este tipo de políticas descartaríamos los NDRs legítimos generados por estos servidores "mal"[3] configurados.

Por tanto para este segundo caso el usuario puede optar por tres opciones:

- Utilizar la política con su servidor y/o relay y asumir que es posible que se pierdan ciertos NDRs de servidores "mal" configurados.
- Utilizar la política con su servidor, relay y servidores "mal" configurados identificados de los cuales deseo recibir NDRs a pesar de que se corre el riesgo de recibir NDRs ilegítimos de estos servidores.
- Utilizar la tecnología BATV.

3 En este artículo definimos como mala dicha configuración ya que la gran mayoría de expertos desaconsejan este tipo de configuración al ser la causante en gran medida de este tipo de tráfico no deseado.

En el mes de julio, Microsoft publicó 6 boletines de seguridad, del MS09-029 al MS09-035. Como viene siendo habitual, aparecieron nuevas vulnerabilidades que afectaban al navegador web Microsoft Internet Explorer. Estas vulnerabilidades permitían la ejecución remota de código en el sistema con tan solo visitar una página web maliciosa. De esta forma tan sencilla se podría ver totalmente comprometida la máquina del usuario afectado. Además de estas vulnerabilidades, Microsoft se vio obligado a publicar 2 actualizaciones fuera de ciclo para corregir vulnerabilidades consideradas como críticas que afectaban a la librería ATL (Active Template Library), siendo las mismas las correspondientes a los boletines MS09-034 y MS09-035.

Una de las vulnerabilidades más llamativas del boletín de julio (MS09-029) es la reportada por un investigador anónimo a iDefense, que permite la ejecución remota de código arbitrario abusando de un desbordamiento del heap a la hora de procesar e interpretar archivos de fuentes. Esta vulnerabilidad era conocida por Microsoft desde el año 2008, según la información ofrecida por la mencionada compañía, filial de Verisign.

Durante este mismo mes otras compañías de software publicaron correcciones para múltiples vulnerabilidades. Adobe, por ejemplo, publicó el 30 de julio un boletín en el cual solucionaba un total de 12 vulnerabilidades remotamente explotables cubriendo productos tan extendidos como Flash Player o Acrobat Reader. De las vulnerabilidades solucionadas en este boletín, especial mención merece la vulnerabilidad CVE-2009-1869, la cual afecta a la máquina virtual de ejecución de ActionScript. Este bug, un desbordamiento numérico, afectaba a las versiones 9 y 10 de Adobe Flash Player, lo que se traduce prácticamente en la totalidad de instalaciones de Adobe Flash Player.

También afectada por un desbordamiento numérico, la máquina virtual de Java tuvo que ser actualizada para corregir la vulnerabilidad CVE-2009-2675, en el mes de agosto, la cual permitía a un atacante remoto la ejecución arbitraria de código simplemente visitando una página web maliciosa.

En el mes de agosto, Microsoft publica 8 boletines de seguridad, del MS09-036 al MS09-042. Toda una variedad de productos de dicha compañía recibieron actualizaciones de seguridad: Microsoft Office, Media Player, Microsoft Active Template Library (ATL), ASP.NET, etc.

Este mismo mes, Adobe corrige más vulnerabilidades en Adobe Flash Player, muchas de ellas reportadas por compañías como iDefense y Tipping Point. La mayoría de estas permitían la ejecución arbitraria de código con tan solo visitar una página web maliciosa.

En el momento de escribir este artículo, ya en septiembre, se ha producido un pequeño susto con la aparición de un nuevo 0-day que afecta a los sistemas operativos Microsoft Windows desde Vista hasta Windows 2008 (ambos inclusive). El único de estos sistemas operativos que no se ve afectado (según Microsoft) es la versión retail de Windows 7, siendo vulnerables, no obstante, las versiones betas del producto.

La vulnerabilidad fue reportada por Laurent Gaffié el día 7 de septiembre en la popular lista de seguridad informática "Full Disclosure". La persona que encontró dicha vulnerabilidad la consideró erróneamente como una simple denegación de servicio (un fallo que únicamente supone una molestia y no un problema real). Sin embargo, el investigador Rubén Santamarta, tras analizar dicho bug, se dio cuenta de que el mismo permite la ejecución de código arbitrario. Actualmente esta vulnerabilidad carece de solución, a excepción de una temporal: deshabilitar SMB2 (la nueva versión del protocolo para compartir archivos e impresoras de Microsoft Windows). De todos modos, la complejidad para explotar dicho bug, a nivel de kernel, reduce en gran medida el riesgo de que el mismo pueda ser utilizado por malware en el futuro como una vía de propagación, tal y como hizo en el pasado **Conficker** con la vulnerabilidad MS08-067.

Para la protección contra este tipo de vulnerabilidades aún sin corregir por el fabricante, nuestros productos disponen de las tecnologías de protección contra amenazas desconocidas, que se encargan de proteger al usuario frente a estos nuevos ataques desconocidos.

En Panda Security estudiamos día a día cómo mejorar nuestros productos para proteger a nuestros clientes de estas nuevas vulnerabilidades. No obstante, recomendamos siempre la instalación urgente de los parches de seguridad publicados en los boletines de seguridad de Microsoft, así como otras actualizaciones de seguridad que puedan afectar a otros productos instalados en el mismo sistema, como pueden ser: Adobe, Mozilla, Google y Microsoft Office.

Como viene siendo habitual todos los años, el verano no es una época en la que dejen de aparecer nuevas amenazas.

A inicios de julio, y aprovechando la celebración del día de la independencia en Estados Unidos, los autores de **Waledac** –también conocido como Storm Worm– lanzaron una campaña para infectar a los usuarios, tratando de engañarlos a través de una página falsa de YouTube con un supuesto video de la celebración del 4 de julio. Como es habitual en estos casos, al tratar de visualizar el falso video nos muestra un mensaje diciendo que para reproducirlo necesitamos instalar en el ordenador unos codecs, que realmente son el gusano Waledac. Una vez infectado, nuestro equipo comenzará a enviar mensajes de spam para que otros usuarios caigan en la trampa:

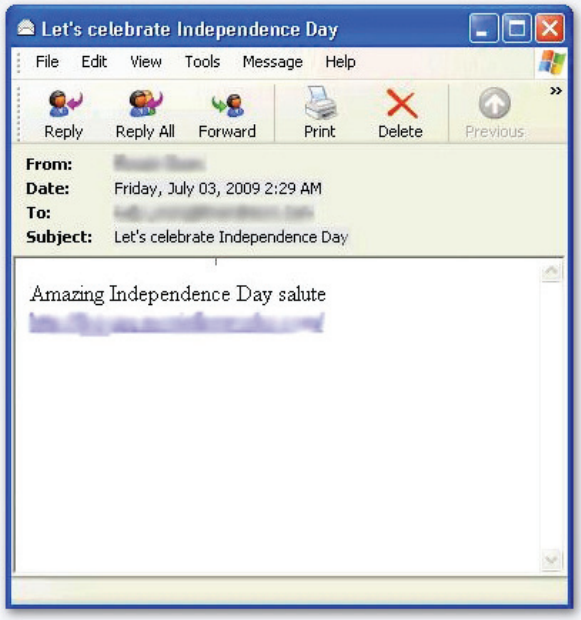

FIG.15

EMAIL SOBRE EL DÍA DE LA INDEPENDENCIA

Unos días más tarde apareció una **nueva vulnerabilidad 0-day** afectando a Microsoft Video ActiveX Control. Descubrimos unas docenas de diferentes páginas web chinas que explotaban esta vulnerabilidad. En muy poco tiempo Microsoft publicó un parche para evitar que dicha vulnerabilidad pudiera ser explotada.

En este **video** mostramos cómo la vulnerabilidad es utilizada por los ciberdelincuentes para ejecutar código y cómo puede ser bloqueada proactivamente gracias a las tecnologías TruPrevent sin necesidad de tener instalado el parche.

También a inicios de julio hubo un **ataque DDoS** (Distributed Denial of Service) contra varias webs de Corea del Sur y Estados Unidos, principalmente páginas gubernamentales, militares y financieras. Un gusano Mydoom, que además tenía diferentes componentes que instalaba en el equipo infectado, es el que ordenaba a los ordenadores realizar este ataque. Aunque se especuló que el ataque podría haber sido realizado por Corea del Norte no se pudo probar.

Estas son algunas de las páginas web que sufrieron el ataque:

www.president.go.kr
www.whitehouse.gov
www.faa.gov
www.dhs.gov
www.defenselink.mil
www.nasdaq.com
finance.yahoo.com
www.usbank.com
www.ftc.gov
www.nsa.gov
www.amazon.com
www.washingtonpost.com

Durante este trimestre también han aparecido **nuevas variantes del gusano Koobface**. Como principal novedad, las nuevas variantes no sólo utilizan Myspace y Facebook, sino que han comenzado a utilizar Twitter para propagarse, publicando enlaces maliciosos desde cuentas de usuarios infectados:

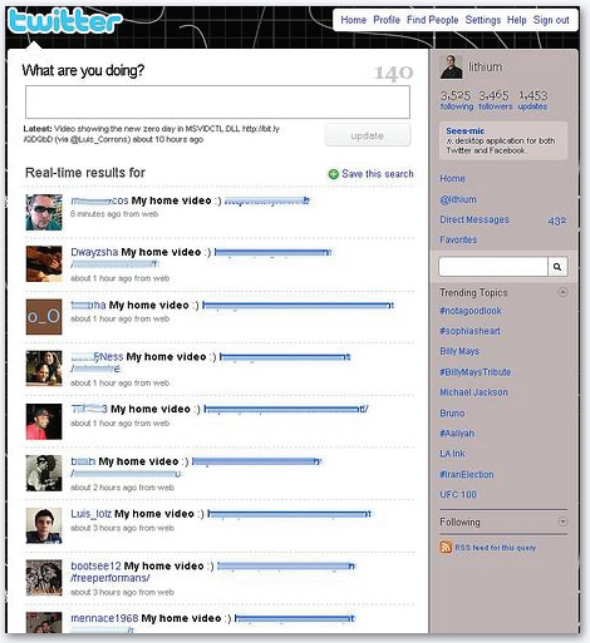

FIG.16

ENLACES MALICIOSOS PUBLICADOS EN TWITTER

Además de la propagación, esta variante del Koobface instala en los equipos infectados el falso antivirus InternetAntivirusPro para así poder obtener un beneficio económico directo. El uso de la ingeniería social para engañar e infectar a los usuarios es una técnica muy utilizada por parte de los cibercriminales. Por ello, se utilizan cada vez más todo tipo de noticias para captar la atención de los usuarios. Durante este trimestre hemos visto que ya no sólo utilizan grandes noticias de repercusión mundial, sino que también usan noticias muy locales, haciendo los ataques más personalizados. Como ejemplo, el caso de un pequeño incendio que tuvo lugar en **Angeles Crest National Forest**. Al buscar información en Google sobre dicho lugar, podemos observar cómo mediante técnicas de Blackhat SEO[4] en los primeros resultados aparecían páginas creadas por los ciberdelincuentes para infectar a los usuarios:

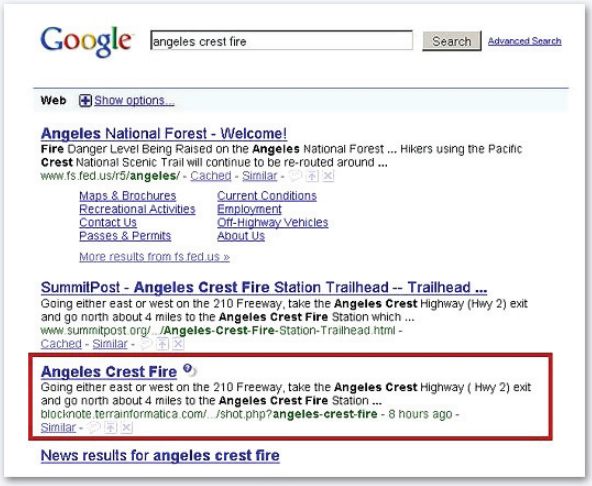

FIG.17

RESULTADOS MOSTRADOS UTILIZANDO TÉCNICAS DE BLACKHAT SEO

Estos ataques se han venido repitiendo de forma masiva. Tan sólo unos días después de este ataque en concreto vimos cómo realmente sólo era la punta del iceberg y que realmente pertenecía a una campaña más amplia de ataques. En la siguiente imagen podemos observar una serie de términos de búsqueda sobre los que este grupo de ciberdelincuentes había creado campañas de Blackhat SEO:

4 SEO son las siglas en inglés de Search Engine Optimization (*optimización para motores de búsqueda*), y básicamente se refiere a las técnicas utilizadas para conseguir que las páginas web mejoren su posicionamiento en los resultados de los motores de búsqueda (Yahoo, Google, etc.). BlackHat SEO se refiere al uso que los ciberdelincuentes hacen de las técnicas SEO para conseguir que sus páginas aparezcan en estas primeras posiciones.

FIG.18

PALABRAS DE BÚSQUEDA UTILIZADAS PARA CAMPAÑAS DE BLACKHAT SEO

En septiembre **este tipo de ataques** han continuado; este es un listado de los términos de búsqueda más utilizados por los ciberdelincuentes durante este mes:

- Obama Speech
- GM group enterprises
- Apple
- Beatles
- America
- White House
- Jon Gosselin
- Live Interview
- School Season

Como hemos visto, los ciberdelincuentes se están centrando en las vulnerabilidades y técnicas de ingeniería social, para así maximizar el número de infecciones entre los usuarios. Para conseguirlo, distribuyen malware en mensajes de spam, redes sociales y motores de búsqueda usando técnicas de Blackhat SEO. Por esto es muy importante que tengamos siempre todo el software de nuestros equipos actualizado, para evitar infecciones a través de vulnerabilidades, así como tener mucha precaución a la hora de pinchar en enlaces cuya procedencia desconozcamos.

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/*