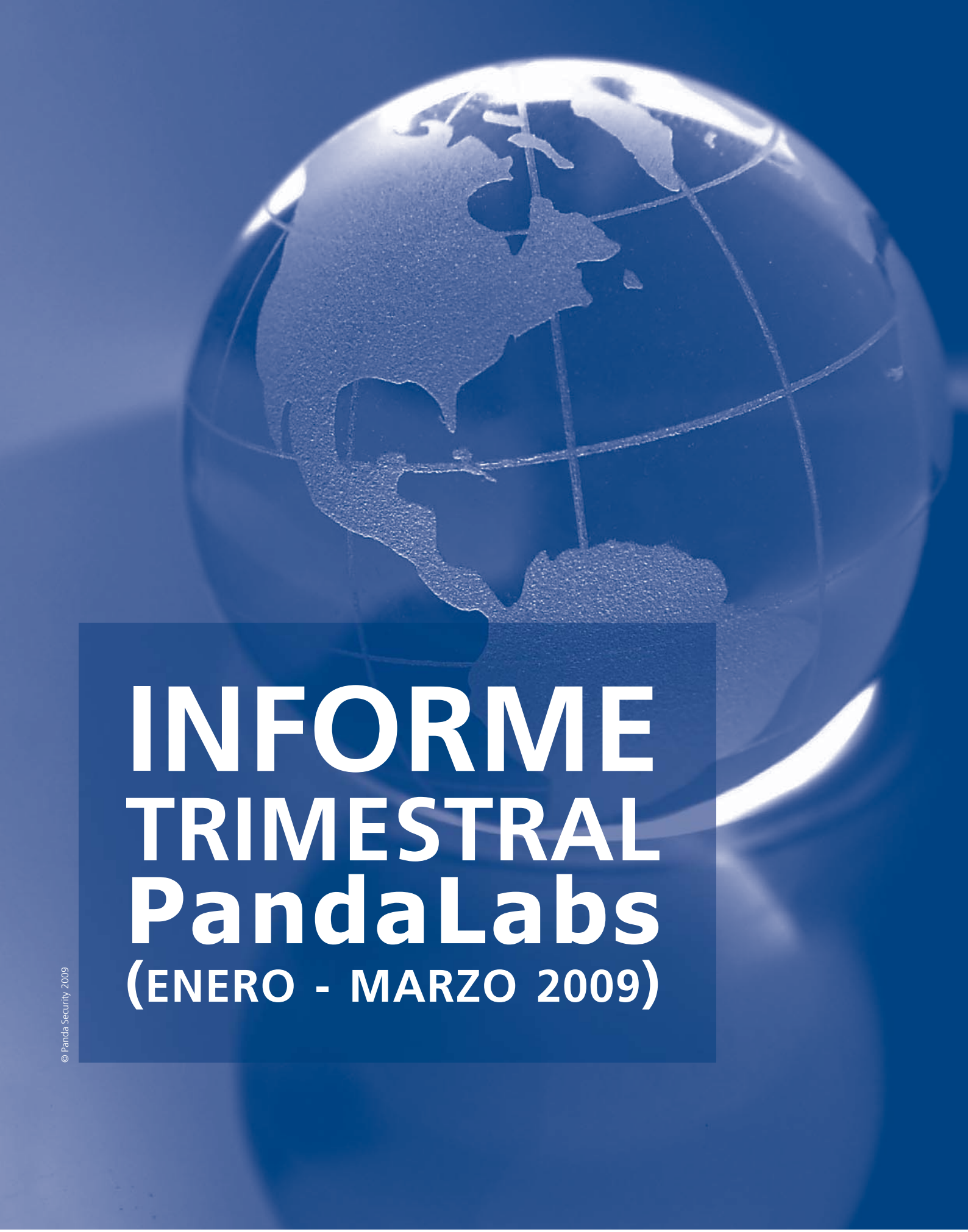

INFORME TRIMESTRAL PandaLabs

(ENERO - MARZO 2009)

© Panda Security 2009

PANDA SECURITY | *One step ahead.*

Índice

Introducción

Comienza el año 2009 y presentamos el primer informe trimestral del año en el que analizaremos los temas más destacados de estos tres meses.

Parece que los niveles de spam se han estabilizado, aunque las cifras siguen siendo elevadas. Presentamos un interesante artículo en el que nos centraremos, entre otros temas, en los focos de origen del spam. A destacar que la crisis económica también se deja notar en el spam, ya que se ha detectado una proliferación de los mensajes relacionados con temas de trabajo.

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

Este trimestre el protagonismo se lo han llevado dos gusanos: Waledac y Conficker. En cuanto al Waledac, algunos ya han afirmado que estamos ante la evolución del Storm Worm. Sea lo que fuere, lo que está claro es que Waledac desplegó todos sus medios para inundar los buzones de los usuarios de mensajes de spam relacionados con San Valentín. Por su parte, el gusano Conficker no solo ha conseguido infectar millones de ordenadores en poco tiempo sino que incluso Microsoft ofrezca una suculenta recompensa a quien capturara a su creador.

Por otra parte, analizaremos las tendencias más destacadas del trimestre en lo que a malware se refiere. Parece que vuelven los virus a la antigua usanza pero adaptándose a los nuevos tiempos. Esto se ve reflejado en el virus Sality.AO, que es capaz de distribuirse a través de la web como los ejemplares más novedosos.

Asimismo, como en anteriores informes, presentaremos la evolución de malware activo por países durante el año 2009 y las cifras de este trimestre.

Esperamos que os resulte interesante.

Resumen ejecutivo

La categoría de Spyware se incrementa un 10,57%, situándose como la segunda categoría de malware más detectada durante estos primeros meses de 2009.

Taiwán continúa siendo el país con el porcentaje más alto malware activo, superando la barrera del 30%. Turquía y Brasil ocupan el segundo y tercer puesto, desbancando a España y Estados Unidos.

La situación actual del spam en cuanto a la cantidad que circula por la red se puede decir que es estable, es decir, no se perciben variaciones considerables en los últimos meses.

A causa de la crisis económica mundial, se aprecia un incremento en el número de mensajes de spam relacionados con ofertas de trabajo o títulos académicos.

El alojamiento de las páginas web de los mensajes de spam está focalizado en Estados Unidos, Europa y China, que son los principales mercados a los que va dirigido el spam.

Alrededor de 140 dominios han sido utilizados para distribuir códigos maliciosos de la familia Waledac.

Tal ha sido la magnitud del gusano Conficker que Microsoft ha ofrecido una recompensa económica de 250.000$ a quienes proporcionen información sobre sus creadores.

La última variante conocida del gusano Conficker comenzará a generar 50.000 URLs diferentes diariamente a partir del 1 de abril.

Las cifras del primer trimestre

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 primer trimestre de 2009:

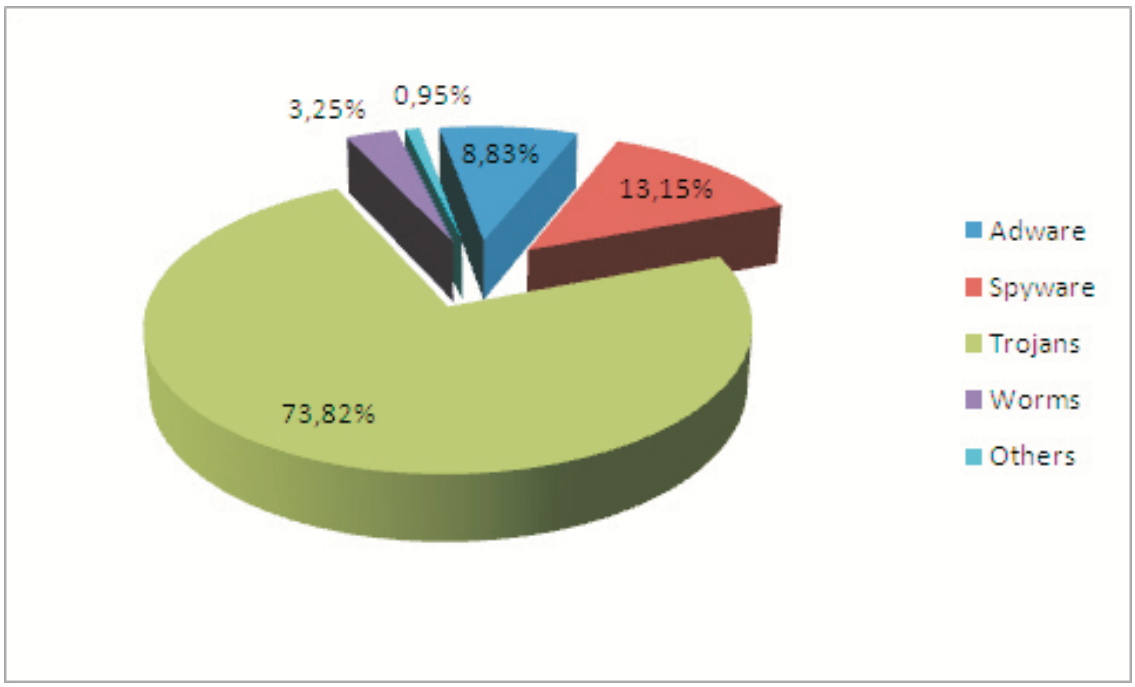

Figura 1. Aparición trimestral de malware.

Según los datos del gráfico, se observa que la categoría de malware predominante este trimestre sigue siendo la de los troyanos, pese a reducirse ligeramente un 3,67% con respecto al trimestre anterior, hasta situarse en un 73,82%.

Señalar que los backdoors se han integrado dentro de los troyanos, y los bots, también se han integrado en gusanos y troyanos según corresponda.

En cuanto a la categoría de los gusanos, su porcentaje se ha visto incrementado ligeramente, un 0,51%, hasta suponer actualmente un 3,25% del total.

Seguimos observando cómo los creadores de malware perfeccionan sus creaciones de malware híbrido entre gusanos y troyanos, que recogen las funcionalidades más características de ambos, para obtener el máximo beneficio de ambas.

Las cifras del primer trimestre

Por otra parte, lo mas destacable es el considerable incremento de la categoría de Spyware, un 10,57% con respecto al trimestre anterior, situándose así en la segunda categoría de malware más detectada durante estos primeros meses de 2009, con un índice situado en el 13,15%.

En cuanto a los Adware, con un 8,83%, dentro de ellos se sigue notando una predisposición por parte de los ciberdelincuentes a seguir desarrollando el subtipo de malware conocido como Rogue AV.

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

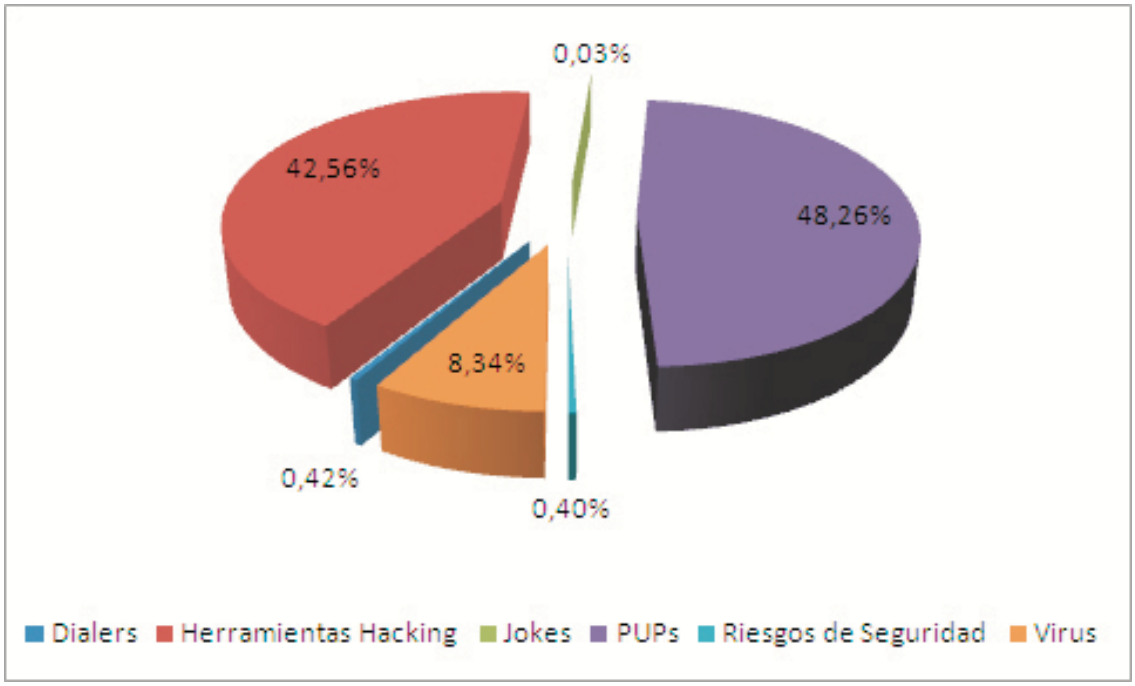

Figura 2. Clasificación de la categoría de Otros.

En esta sección observamos que el tipo de malware predominante son los PUPs y las herramientas de hacking, los cuales han incrementado situándose en un 48,26% y 42,56% respectivamente, seguido de los Virus situados en un 8,34%, después de un decremento del 6,49% con respecto al anterior trimestre.

El paulatino descenso de clientes de Internet con acceso telefónico hace que los dialers se mantengan en una cuota prácticamente imperceptible, 0,42%.

Las cifras del primer trimestre

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.

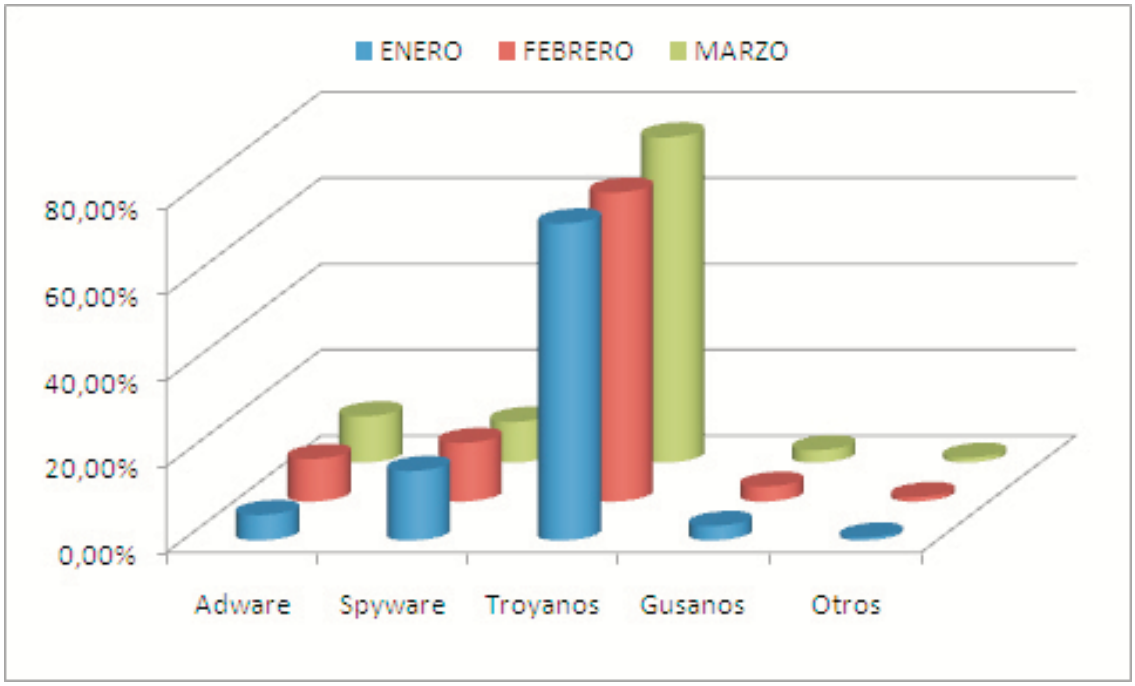

Figura 3. Evolución en la aparición de nuevo malware.

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.

Las cifras del primer trimestre

Amenazas detectadas por los Sensores PandaLabs

El siguiente gráfico muestra la distribución de las detecciones realizadas por los sensores de seguridad Panda Security, a lo largo de este cuarto trimestre:

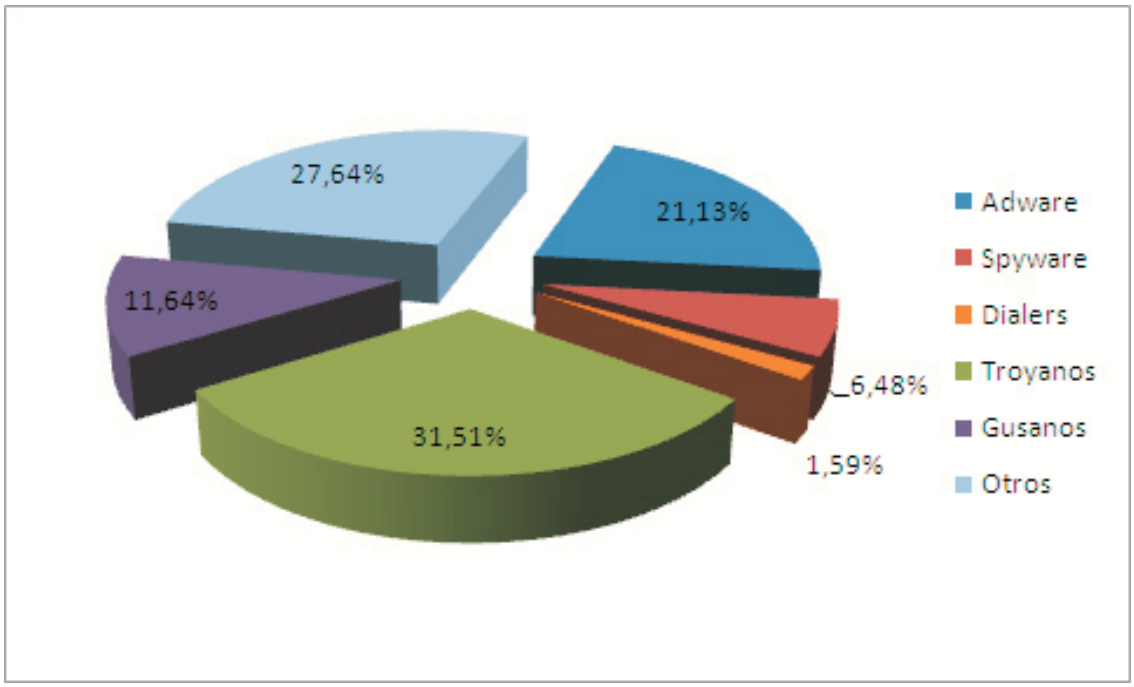

Figura 4. Distribución detecciones por sensores Pandalabs.

En este trimestre el Adware se ha incrementado ligeramente un 0,52% hasta situarse en un 21,13%, lo cual deja paso a ocupar la primera posición a los Troyanos con un 31,51%. Estos también han descendido con respecto al trimestre anterior, pero aun así siguen situándose a la cabeza de los tipos de malware mas detectados.

Los gusanos, también se suman a las categorías de malware en descenso con un decrecimiento del 0,83%, aunque prácticamente mantienen su ratio de infecciones, situándose en un 11,64% y manteniendo así su estatus de códigos significativos debido a la rapidez de su propagación a otros sistemas.

Los dialers, situándose en un 1,59%, siguen resistiéndose a desaparecer a pesar de la tendencia descendente que continúa durante los últimos años.

Las cifras del primer trimestre

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

01	Spyware/Virtumonde
02	Trj/Rebooter.J
03	Adware/Yassist
04	Adware/Antivirus2009
05	W32/Bagle.RP.worm
06	Adware/AccesMembre
07	W32/Bagle.RC.worm
08	W32/Conficker.C.worm
09	W32/AutoRun.DJ.worm
10	W32/Gamania.gen

Figura 5. Top ten de amenazas detectadas

Malware activo

En esta sección vamos a hablar de la evolución del malware activo durante el 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 web: www.pandasecurity.com/infected_or_not/ y a través de nuestra herramienta online ActiveScan 2.0.

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

Figura 6. Herramienta online ActiveScan 2.0

Malware activo

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

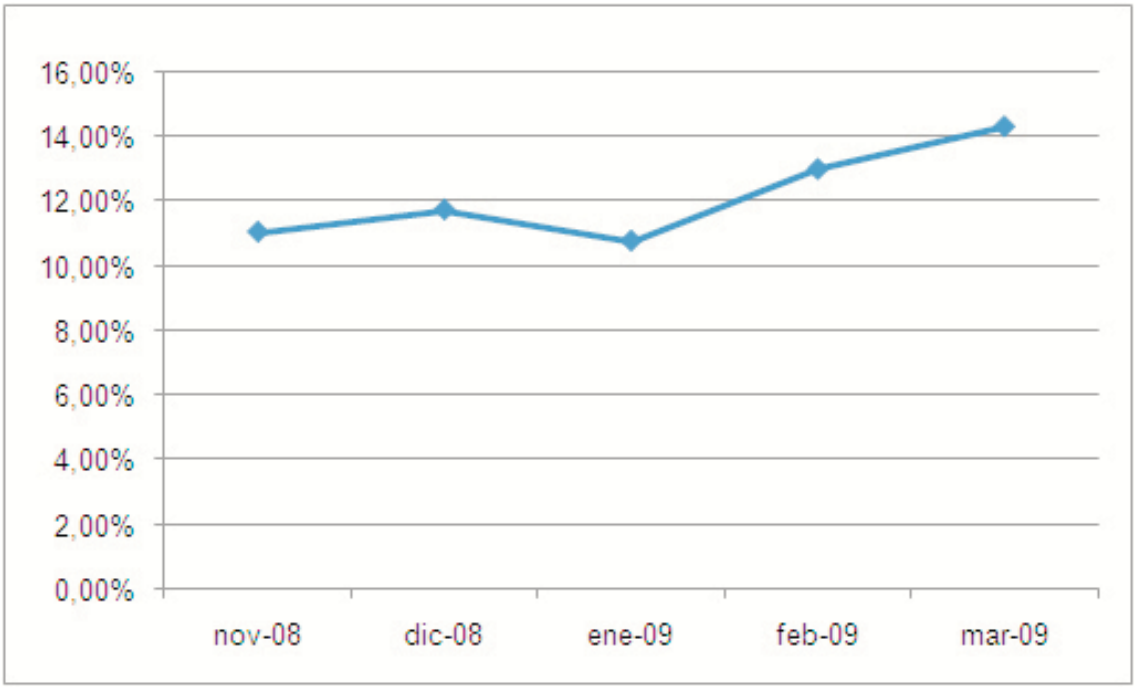

Figura 7. Evolución de malware activo durante primer trimestre 2009.

Hemos incluido los dos últimos meses del 2008 para tener una mejor perspectiva de la evolución del malware activo.

Enero empezó con el ratio más bajo de este primer trimestre con el 10,78% de PCs infectados. A partir de ahí se ha producido un incremento progresivo hasta llegar al 14,33%, siendo el porcentaje más alto de malware activo desde agosto del 2008.

La media de malware activo durante este trimestre asciende al 12,67%, porcentaje inferior al 14,62% correspondiente al año 2008. Pero los datos no engañan y los porcentajes de este trimestre son más elevados que el último trimestre del 2008, por lo que si esta tendencia continúa, el porcentaje se incrementará en el próximo trimestre.

stos datos reflejan la evolución a nivel global pero, ¿qué ocurre en cada país? En la s iguiente gráfica podemos observar el porcentaje de infección de los países con mayor n úmero de análisis[1] en Infected or Not y a través de ActiveScan 2.0

[1] Países ordenados por número de análisis realizados.

Malware activo

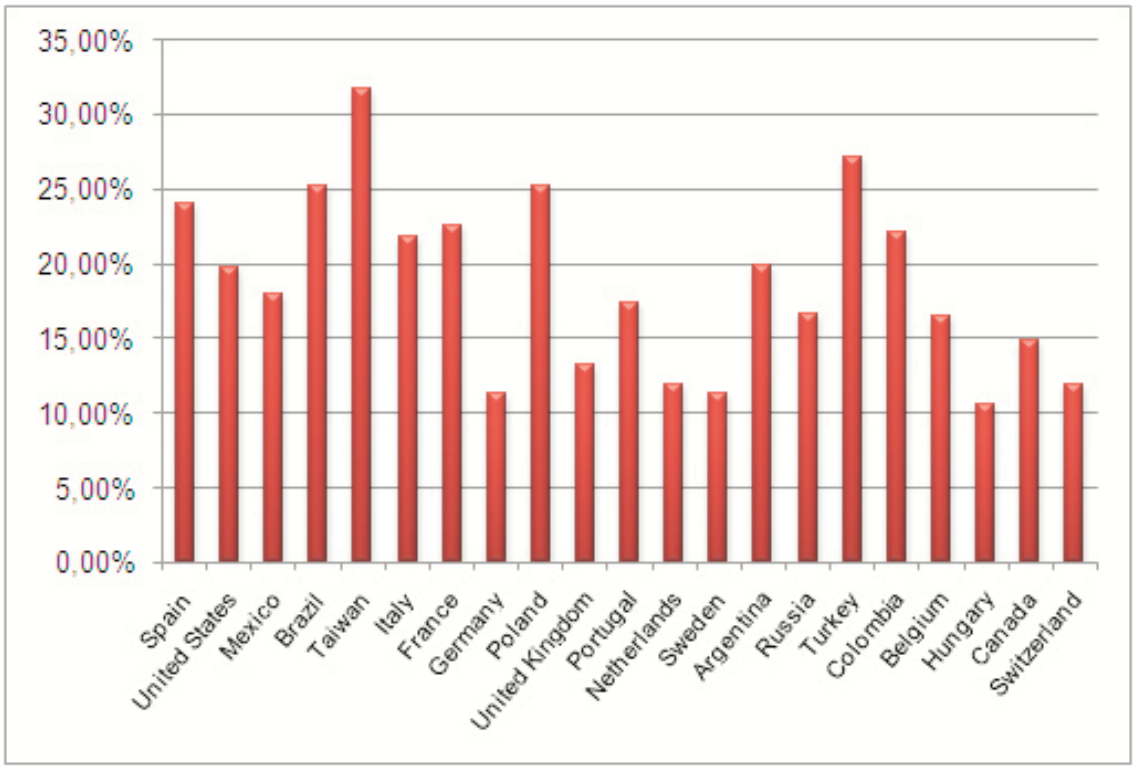

Figura 8. Países con mayor porcentaje de malware (Enero-Marzo 2009).

Taiwán continúa en el Top1 con el porcentaje más alto (31,70%) de malware activo, siendo el único que supera la barrera del 30%. A destacar también Turquía y Brasil, que ocupan el segundo y tercer puesto respectivamente, desbancando a España y Estados Unidos. Polonia tiene el mismo porcentaje de malware activo que Brasil, pero ocuparía el cuarto puesto, ya que tiene menor número de análisis. También debemos resaltar la mejoría de México (17,95%) que ha perdido casi un 10% en comparación al 24,87% de media de malware activo durante todo el año 2008.

Informe Trimestral de Spam

En este documento se va a analizar la situación del spam actual. Gracias a los sistemas de monitorización de spam que disponemos en PandaLabs podemos obtener datos estadísticos de la cantidad de spam que llega a nuestros SpamTraps[2], ratios de detección de nuestros productos, origen del spam, etc.

Tráfico de Spam

Para analizar el tráfico de spam hemos tomado como referencia una de nuestras fuentes, de la que obtenemos actualmente unos 43.000 correos diarios de spam, llegando a picos de 68.000 correos diarios. Esta cantidad de spam nos permite obtener estadísticas bastante fiables de la situación actual del spam.

La situación actual del spam en cuanto a la cantidad que circula por la red se puede decir que es estable, es decir, no se perciben variaciones considerables en los últimos meses.

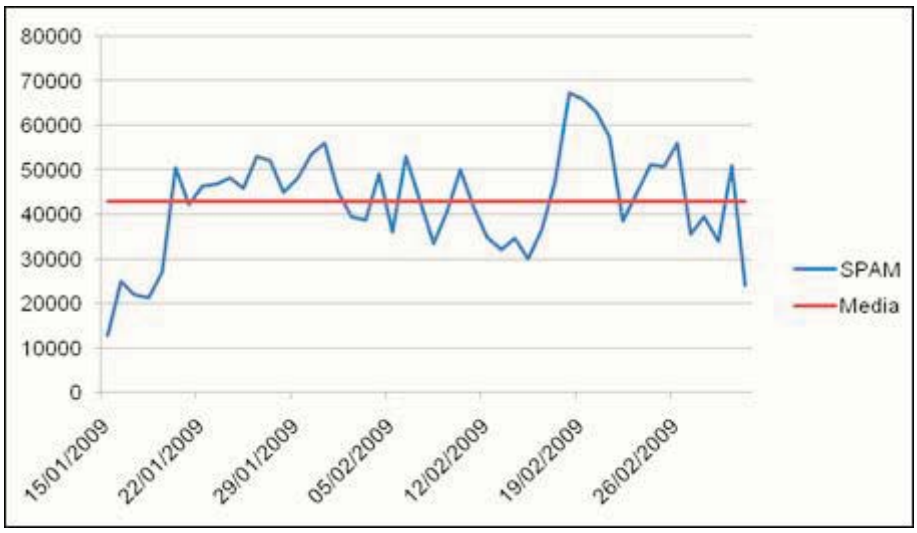

Figura 9. Volumen de Spam en circulación (Enero-Febrero 2009).

[2] SpamTrap es un servidor de correo accesible desde Internet al se le han asociado ciertos dominios para los que no existen cuentas. Está configurado de tal forma que acepte todos los correos enviados a este servidor. La intención de este servidor es la de recoger spam enviado por spammers. Existen diferentes técnicas y configuraciones para favorecer la recepción de spam.

Informe Trimestral de Spam

En cuanto a la temática de los mensajes, a causa de la crisis económica mundial, se puede apreciar un incremento en el número de mensajes relacionados con ofertas de trabajo o títulos académicos.

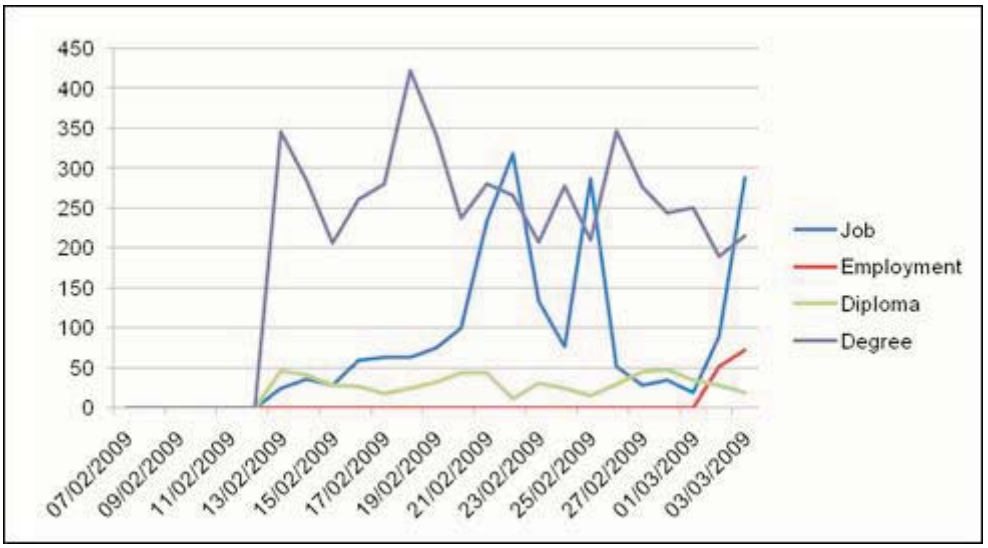

Figura 10. Temática de los mensajes de Spam.

De todas maneras, los mensajes con contenido sexual o relacionado con venta de fármacos siguen siendo claramente dominadores como se puede ver en el siguiente gráfico.

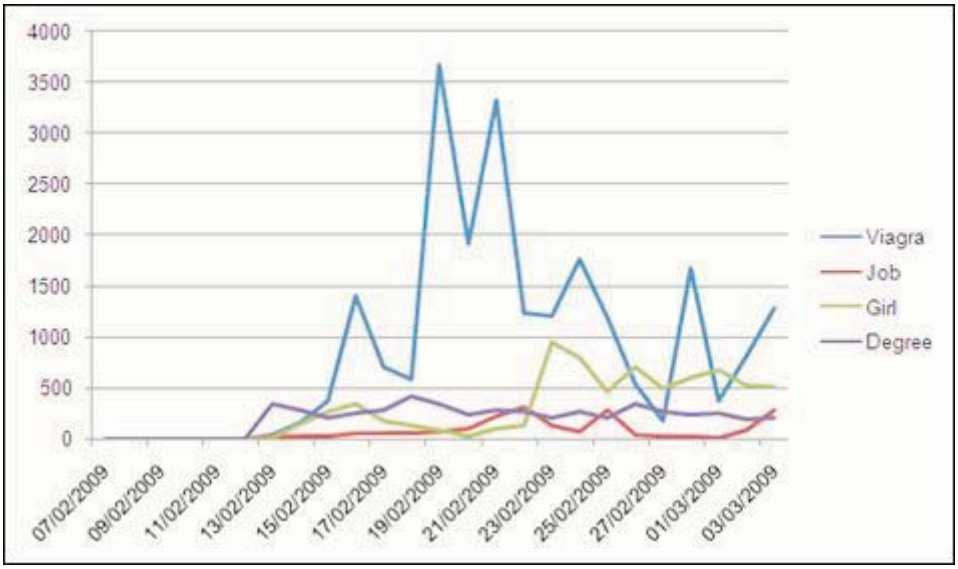

Figura 11. Comparativa entre las temáticas principales del Spam

Informe Trimestral de Spam

Origen del Spam

En cuanto al origen del spam, antes de sacar cualquier conclusión hay que tener en cuenta cuáles son las posibles fuentes de spam:

- SPAMMERS
- REDES DE BOTS (Malware)

Es decir, por un lado, tenemos ISPs que albergan máquinas dedicadas al rastreo de direcciones y envío masivo de spam a dichas direcciones. Y, por otro lado, tenemos máquinas de usuarios infectadas con malware controlado de forma remota para el envío de spam.

También hay que tener en cuenta que en el caso de los spammers, estos suelen albergar sus máquinas en ISPs de países donde las leyes y el control sobre el spam son débiles o simplemente no existen.

A continuación, se muestran una serie de gráficas que representan la distribución del origen del spam a nivel mundial:

País	%
EEUU	11,61
Brasil	11,5
Rumania	5,8
India	5,76
Turquía	5,35
Polonia	4,91
Corea	4,82
Rusia	3,81
Vietnam	2,84
GB	2,61
España	2,43
Alemania	2,38
Colombia	2,24
Italia	1,94
Argentina	1,93
China	1,92
Tailandia	1,82
Ucrania	1,36
Israel	1,26
Australia	1,11
Chile	1,08
Méjico	1,04
Otros	20,48

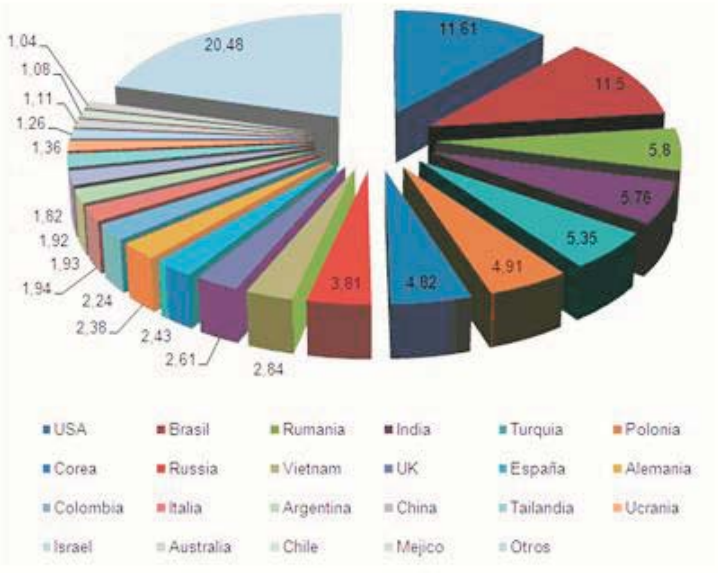

Figura 12. Origen del Spam a nivel mundial.

Informe Trimestral de Spam

Figura 13. Distribución del Spam mundial (cuanto más intenso sea el color mayor será el nivel de spam).

A continuación se muestra una gráfica que representa la localización de las principales regiones desde las que se envía spam atendiendo a la IP de origen. En verde se representan las fuentes moderadas, en naranja las moderadas-altas y en rojo las fuentes altas.

Figura 14. Origen del Spam en función de la IP

Informe Trimestral de Spam

Destacan del mapa, dos IPs: la 58.211.75.8 con más de 1.000 correos enviados y situada en Beijing, y la 211.234.119.69 con casi 3.400 correos situada en Seúl.

Como se puede apreciar en la siguiente imagen, los puntos destacados también presentan circunferencias concéntricas de diferentes colores. Esto nos indica que en esas mismas ciudades están situados otros orígenes importantes de spam.

Figura 15. Otros orígenes importantes de Spam.

Si comparamos las gráficas de origen del spam por países con la de origen de spam por IPs, se puede observar que muchos países no tienen grandes fuentes de spam a pesar de ser el origen de gran parte del spam. Esto es debido a que se trata de países donde existen estrictas normas para neutralizar a los spammers y donde el acceso a Internet esta muy generalizado en los hogares. Son, por tanto, países donde existe una gran implantación de las redes de bots, que son controladas por las mafias para el envío de spam.

En estos países algunos ISPs están planteando el bloqueo del puerto SMTP para conexiones domésticas y así mitigar el efecto de estas redes de bots.

Informe Trimestral de Spam

En el caso de Europa se puede apreciar que es en los Países del Este donde más se concentra el origen del spam.

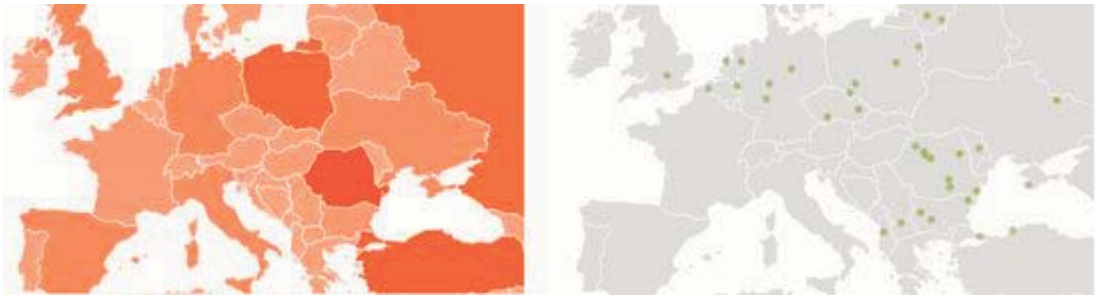

Figura 16. Origen del Spam en Europa.

URLs del Spam

Tras analizar el origen del spam ahora analizaremos dónde están albergadas las páginas a las que apuntan dichos mensajes. Como hemos mencionado previamente, el envío de spam está penado en algunos países e incluso en el caso de Estados Unidos se han dictado condenas en este sentido. Por el contrario, las páginas a las que apunta el spam no tienen ninguna responsabilidad ni se puede demostrar que son quienes están detrás de dicho spam. Es por eso que el mapa de distribución de orígenes cambia considerablemente en lo que respecta a Occidente.

Informe Trimestral de Spam

El alojamiento de las páginas está focalizado en Estados Unidos, Europa y China, que son los principales mercados a los que va dirigido el spam.

Figura 17. Alojamiento de URLs del Spam.

Conclusión

La conclusión que se puede obtener a partir de los datos expuestos es que las políticas antispam puestas en marcha por algunos gobiernos y sobre todo por los ISPs hace que los sistemas de bots sean los más utilizados por los spammers, debido a que son fuentes de baja intensidad, por lo cual no llaman la atención y tienen menos riesgo de ser listados en DNSBLs[3], además de que eximen de cualquier responsabilidad al spammer.

Destacar que la caída de McColo, el ISP que controlaba la mayor red de bots, a principios de noviembre del año pasado hizo que el tráfico de spam decayera hasta en un 75%. Por tanto, es muy importante concienciar a los usuarios de la necesidad de mantener sus sistemas libres de malware, ya que no solo repercutirá en la integridad de su sistema y sus datos sino que también ayudará en gran medida a disminuir las posibles fuentes de spam.

[3] DNSBL son listados de posibles IPs desde las cuales nos podrían enviar spam; bien porque alguna red de SPAMTRAPs ha recibido spam desde estas IPs, bien porque los usuarios han recibido spam desde estas direcciones y las han reportado o bien porque se consideran IPs desde las que no se deberían enviar correos electrónicos (conexiones domesticas), estas IPs son recopiladas y actualizadas por organismos como SpamHaus y utilizadas por numerosos servidores de correo para rechazar los correos enviados desde dichas IPs.

Vulnerabilidades Q1 2009

MS09-001, el primer boletín de seguridad de Microsoft para el año 2009. En este boletín Microsoft publicó varias actualizaciones críticas que afectaban a todos los sistemas Windows. Estas actualizaciones resolvían 3 vulnerabilidades, 2 privadas y 1 pública descubiertas en el protocolo del Servidor de Mensaje de Bloque de Microsoft (SMB). La explotación satisfactoria de la vulnerabilidad permitía, y permite para los sistemas Windows que todavía no estén actualizados, que un usuario atacante ejecute código en una máquina remota. De esta forma, la máquina de la víctima quedaría completamente comprometida.

En el segundo boletín del año, el MS09-002, pudimos ver nuevamente varias vulnerabilidades que afectaban a Internet Explorer. Posiblemente este navegador sea la aplicación más castigada de Microsoft en lo que se refiere a vulnerabilidades descubiertas.

Los servidores Microsoft Exchange y Microsoft SQL Server también estuvieron en el punto de mira en el mes de febrero. Para el servidor Microsoft Exchange se descubrieron 2 vulnerabilidades críticas, y 1 vulnerabilidad para el servidor Microsoft SQL Server. Esta última, afectaba al procedimiento almacenado sp_replwritetovarbin y aunque fue descubierta en el mes de diciembre del año 2008, ha sido solucionada por Microsoft en febrero de este mismo año. Para corregir estas 3 vulnerabilidades se publicaron los boletines de seguridad MS09-003 y MS09-004 respectivamente.

Los investigadores de seguridad tampoco se han querido olvidar de las aplicaciones ofimáticas. En febrero se dio a conocer una vulnerabilidad 0 day en Microsoft Excel que estaba siendo utilizada para instalar malware en organizaciones gubernamentales de la zona de Asia. A día de hoy, Microsoft aún no ha publicado ningún parche para dar solución a esta nueva vulnerabilidad. No obstante ha mencionado algunas recomendaciones en su Advisory número 968272 . En el blog de PandaLabs hemos publicado un post sobre esta vulnerabilidad donde mencionamos cómo nuestro antivirus ya estaba protegiendo a nuestros clientes desde el primer día en el que aparecieron los primeros documentos xls vulnerables gracias a las tecnologías TruPrevent.

Además de Microsoft Excel, también se descubrieron varias vulnerabilidades que afectaban al programa Microsoft Office Visio. No obstante, en esta ocasión Microsoft publicó en su boletín de seguridad MS09-005 las actualizaciones que corregían las 3 vulnerabilidades descubiertas y que permitían la ejecución de código en la máquina afectada.

Vulnerabilidades Q1 2009

También se han descubierto varias vulnerabilidades críticas que afectan al formato de fichero PDF y por lo tanto las aplicaciones Adobe Acrobat y Adobe Reader eran vulnerables. Además de estas 2 aplicaciones, en esta ocasión también tenemos que añadir la aplicación gratuita Foxit Reader, en la que se ha encontrado una vulnerabilidad de carácter similar a las anteriores. Esto puede ser debido a que cada vez más usuarios están utilizando esta aplicación gratuita para visualizar ficheros PDF y para los desarrolladores de malware esto puede suponer un porcentaje de infección atrayente.

Por último, en este mes de marzo Microsoft ha publicado varias vulnerabilidades con sus respectivas actualizaciones en los boletines de seguridad MS09-006, MS09-007 y MS09-008. La vulnerabilidad descrita en el boletín MS09-006 se produce por una incorrecta validación de la información pasada a través del componente GDI del kernel desde el modo usuario del sistema operativo. Esta vulnerabilidad es muy crítica y afecta a todas las versiones de Windows. Las 2 vulnerabilidades restantes son de tipo spoofing. La primera de ellas, reflejada en el boletín MS09-006, afecta al paquete de seguridad Secure Channel (SChannel). La otra vulnerabilidad afecta a los servidores WINS y DNS de Microsoft. En el blog de PandaLabs hemos publicado un post que muestra un estudio realizado en el laboratorio sobre la actualización provista por Microsoft para corregir esta vulnerabilidad en el servidor de DNS de Windows.

En Panda Security estudiamos día a día las mejoras de nuestros productos para proteger a nuestros clientes de estas nuevas vulnerabilidades. 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.

Amenazas más destacadas del Q1

Conficker

El gusano Conficker es la amenaza de malware más importante que hemos observado a lo largo de este primer trimestre, estimándose el número de ordenadores afectados en unos 10 millones. Su difusión ha sido de tal alcance que hasta sistemas de organismos militares de Gran Bretaña y Francia se vieron afectados.

Tal ha sido su magnitud que hasta Microsoft ha ofrecido una recompensa económica de 250.000$ a quienes proporcionen información sobre los creadores de esta familia de malware.

Figura 18. Noticia publicada por Microsoft ofreciendo una recompensa.

Hasta el momento, las tres variantes descubiertas de este gusano estaban preparadas para explotar la vulnerabilidad MS08-067 como método de propagación. No obstante, los ciberdelincuentes han ido implementando nuevas mejoras con respecto a las variantes anteriores que les permitan una mayor expansión.

Una de las características más destacables de dicha familia es que roba contraseñas e información confidencial, y a su vez se propaga infectando dispositivos de almacenamiento extraíbles haciendo uso de la copia de un fichero autorun.inf, el cual permite al malware ser ejecutado nada más conectar el dispositivo en un nuevo sistema.

Otra de las vías de propagación utilizada es la de efectuar una conexión contra el recurso compartido ADMIN$ del resto de los ordenadores conectados en la misma red que el sistema infectado. En el caso de no conseguirlo, utiliza la lista de usuarios del sistema infectado, junto con una lista de más de 200 contraseñas comunes, con intención de poder efectuar una conexión válida con esos equipos.

La utilización de una lista de contraseñas comunes o débiles, no es novedoso; sin embargo, sigue demostrándose una y otra vez la efectividad de estos códigos maliciosos en explotar sistemas que no están protegidos con contraseñas rígidas (formadas por combinaciones de números, letras, etc).

Amenazas más destacadas del Q1

Estos son algunos ejemplos de contraseñas comunes: 123456, qwerty, admin., password, login, default, etc.

Entre otras de las acciones maliciosas que efectúa en el sistema infectado, este gusano no solo monitoriza los procesos activos del sistema para eliminar los correspondientes a aplicaciones de seguridad para poder reducir el nivel de protección del ordenador, sino que además, como podemos ver en la lista a continuación, también impide el acceso web a los dominios de software y foros de seguridad más relevantes:

```
seg000:00888114 9C 24 87 00                 dd offset aGrisoft          ; "grisoft"
seg000:00888118 90 24 87 00                 dd offset aHackerwatch      ; "hackerwatch"
seg000:0088811C 84 24 87 00                 dd offset aHacksoft         ; "hacksoft"
seg000:00888120 7C 24 87 00                 dd offset aHauri            ; "hauri"
seg000:00888124 74 24 87 00                 dd offset aIkarus           ; "ikarus"
seg000:00888128 6C 24 87 00                 dd offset aJotti            ; "jotti"
seg000:0088812C 60 24 87 00                 dd offset aK7computing      ; "k7computing"
seg000:00888130 54 24 87 00                 dd offset aKaspersky        ; "kaspersky"
seg000:00888134 58 26 87 00                 dd offset aKido             ; "kido"
seg000:00888138 4C 24 87 00                 dd offset aMalware          ; "malware"
seg000:0088813C 44 24 87 00                 dd offset aMcafee           ; "mcafee"
seg000:00888140 38 24 87 00                 dd offset aMicrosoft        ; "microsoft"
seg000:00888144 30 24 87 00                 dd offset aMirage           ; "mirage"
seg000:00888148 24 24 87 00                 dd offset aMsftncsi         ; "msftncsi"
seg000:0088814C 1C 24 87 00                 dd offset aMsmvps           ; "msmvps"
seg000:00888150 14 24 87 00                 dd offset aMtc_sri          ; "mtc.sri"
seg000:00888154 00 24 87 00                 dd offset aNetworkassocia   ; "networkassociates"
seg000:00888158 F8 23 87 00                 dd offset aNod32            ; "nod32"
seg000:0088815C F0 23 87 00                 dd offset aNorman           ; "norman"
seg000:00888160 E8 23 87 00                 dd offset aNorton           ; "norton"
seg000:00888164 E0 23 87 00                 dd offset aOnecare          ; "onecare"
seg000:00888168 D8 23 87 00                 dd offset aPanda            ; "panda"
seg000:0088816C D0 23 87 00                 dd offset aPctools          ; "pctools"
seg000:00888170 C8 23 87 00                 dd offset aPrevx            ; "prevx"
seg000:00888174 BC 23 87 00                 dd offset aPtsecurity       ; "ptsecurity"
seg000:00888178 B0 23 87 00                 dd offset aQuickheal        ; "quickheal"
seg000:0088817C A8 23 87 00                 dd offset aRemoval          ; "removal"
seg000:00888180 A0 23 87 00                 dd offset aRising           ; "rising"
seg000:00888184 98 23 87 00                 dd offset aRootkit          ; "rootkit"
seg000:00888188 8C 23 87 00                 dd offset aSafety_live      ; "safety.live"
seg000:0088818C 7C 23 87 00                 dd offset aSecurecomputin   ; "securecomputing"
seg000:00888190 70 23 87 00                 dd offset aSecureworks      ; "secureworks"
seg000:00888194 68 23 87 00                 dd offset aSophos           ; "sophos"
seg000:00888198 5C 23 87 00                 dd offset aSpamhaus         ; "spamhaus"
seg000:0088819C 54 23 87 00                 dd offset aSpyware          ; "spyware"
seg000:008881A0 4C 23 87 00                 dd offset aSunbelt          ; "sunbelt"
seg000:008881A4 40 23 87 00                 dd offset aSymantec         ; "symantec"
seg000:008881A8 38 23 87 00                 dd offset aTechnet          ; "technet"
seg000:008881AC 30 23 87 00                 dd offset aThreat           ; "threat"
seg000:008881B0 20 23 87 00                 dd offset aThreatexpert     ; "threatexpert"
seg000:008881B4 14 23 87 00                 dd offset aTrendmicro       ; "trendmicro"
seg000:008881B8 0C 23 87 00                 dd offset aTrojan           ; "trojan"
seg000:008881BC 04 23 87 00                 dd offset aVirscan          ; "virscan"
seg000:008881C0 FC 22 87 00                 dd offset aVirus            ; "virus"
seg000:008881C4 EC 22 87 00                 dd offset aWilderssecurit   ; "wilderssecurity"
seg000:008881C8 DC 22 87 00                 dd offset aWindowsupdate    ; "windowsupdate"
```

Figura 19. Listado de nombres de direcciones relativos a compañías de seguridad

Amenazas más destacadas del Q1

Además, deshabilita servicios como Windows Automatic Update, Windows Security Center, Windows Defender y Windows Error Reporting, dejando al sistema a merced de otros códigos maliciosos.

Precisamente otra de las acciones del Conficker es verificar la fecha actual del sistema, contrastándola con webs como google.com, yahoo.com, ask.com, entre otras, y si esta es posterior al 1 de enero u otra predefinida, genera con un algoritmo dependiendo de la fecha actual del sistema para acceder a una web para descargarse otros códigos maliciosos en el sistema.

Este malware además habilita el acceso remoto mediante una puerta trasera con funcionalidad de "Autoactualización", lo cual le permite mantenerse al día de las instrucciones que desee su creador.

Pese a la existencia de un parche de seguridad catalogado como crítico, que de no tenerlo instalado permitiría que un código malicioso pudiera introducirse libremente en un sistema, existe una ventana de tiempo desde que se libera el parche, hasta que este es aplicado mayoritariamente por los usuarios. Y ese es el tiempo que aprovechan los ciberdelincuentes para poder recopilar toda la información confidencial de los sistemas infectados. Incluso cuatro meses después de la publicación del parche por parte de Microsoft, aun siguen existiendo evidencias de equipos infectados totalmente desprotegidos debido al descuido de sus propietarios o administradores.

Amenazas más destacadas del Q1

Waledac en San Valentín

A lo largo del año existen fechas señaladas, como Navidad, Año Nuevo o San Valentín, en las que los spammers incrementan su actividad bombardeando nuestros buzones de correo con mensajes no solo molestos, sino que también muchos de ellos ocultan intenciones maliciosas.

Durante los dos últimos años, el spam enviado en dichas fechas provenía mayoritariamente de la red de bot conocida como Storm worm. Sin embargo, actualmente la familia Waledac se ha convertido en la protagonista del día de San Valentín.

Haciendo uso de diversas técnicas de ingeniería social, los spammers distribuyeron los primeros mensajes maliciosos relacionados con San Valentín mucho antes de la fecha del día de los enamorados, siendo el resultado de su acción más molesto que malicioso. Sin embargo, el mero hecho de visualizar su contenido reporta suficientes beneficios económicos como para que los ciberdelincuentes sigan motivados a seguir con sus acciones maliciosas..

A continuación podemos visualizar un ejemplo del contenido de la página web a la que nos redirigen los enlaces que contienen los primeros mensajes de spam de San Valentín:

Figura 20. Web a la que redirigen los primeros spam de San Valentín.

Amenazas más destacadas del Q1

Sin embargo, no solo se han distribuido mensajes considerados como "inofensivos", ya que los ciberdelincuentes, bajo esta temática, han distribuido múltiples códigos maliciosos de la familia Waledac a través de esos correos con urls maliciosas.

El funcionamiento sigue siendo similar al de los primeros mensajes de spam que publicitaban ciertos productos farmacéuticos, puesto que su distribución es a través de correo electrónico con asuntos relacionados con la temática de San Valentín, en el que nos informarán que alguien decidió enviarnos una tarjeta virtual. Para poder visualizar la tarjeta, el mensaje contiene un enlace que nos redirigirá al dominio malicioso.

A continuación, podemos visualizar un ejemplo de dichos dominios maliciosos:

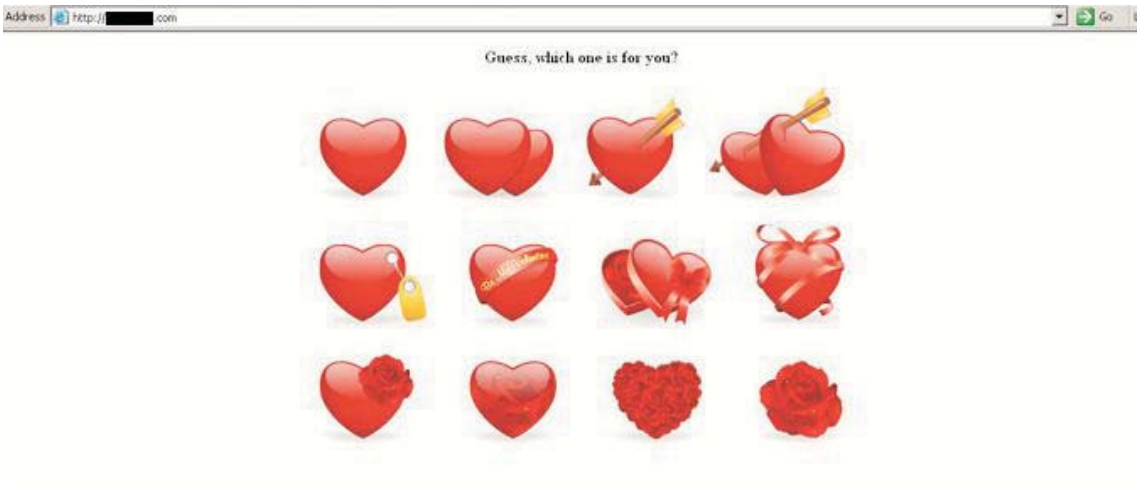

Figura 21. Dominio malicioso de Waledac.

Amenazas más destacadas del Q1

A continuación, bien por interacción del usuario o de forma automática, se efectúa la descarga del gusano en el ordenador. No obstante, requiere la confirmación del usuario para que la descarga se realice con éxito:

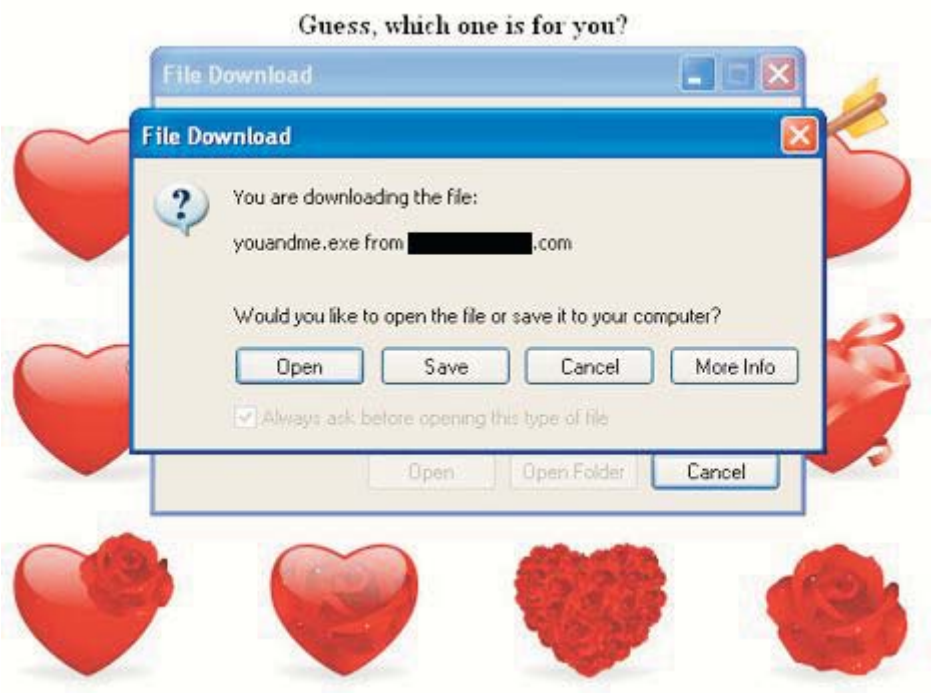

Figura 22. Proceso de descarga del archivo malicioso.

Los ciberdelincuentes crearon múltiples dominios dedicados exclusivamente a distribuir ficheros maliciosos del gusano Waledac, todos ellos con nombres aparentemente inofensivos, como card.exe, ecard.exe, love.exe, loveyou.exe, meandyou.exe, etc.

Alguno de dichos dominios incluso estaba preparado para modificar el fichero a descargar, de tal forma que no se difundiera únicamente un código malicioso para evitar poner en alerta a las empresas de seguridad a través de epidemias silenciosas, generando múltiples pero pequeñas infecciones.

Tan grande ha sido la repercusión de esos dominios que distribuían códigos maliciosos del Waledac, que incluso algunos gozaban de una buena posición en los buscadores. Esto podía provocar que un usuario que intentara localizar tarjetas virtuales pudiera llegar a dar por casualidad con alguno de los dominios maliciosos.

Amenazas más destacadas del Q1

A continuación se pueden observar ejemplos de algunos dominios maliciosos relacionados con tarjetas virtuales de San Valentín:

Figura 23. Ejemplos de dominios maliciosos relacionados con San Valentín.

Amenazas más destacadas del Q1

No solo el Waledac ha estado activo antes y durante el día de San Valentín, sino que incluso semanas más tarde los dominios que habían sido utilizados para distribuir malware, ahora ofertaban cupones descuento exclusivos.

Figura 24. Web que oferta cupones descuento

Amenazas más destacadas del Q1

Evidentemente dichos cupones también se correspondían al Wadelac, pero bajo nombres diferentes: couponlist.exe, coupons.exe, list.exe o print.exe; es decir, el mismo perro con distinto collar.

En estos momentos nos consta que han sido utilizados alrededor de 140 dominios para distribuir códigos maliciosos de la familia Waledac.

Como hemos podido observar, el Wadelac no solo ha estado presente en temas relacionados con San Valentín, sino que también en otros eventos importantes como ha sido la campaña de elecciones a la presidencia de los Estados Unidos. Los ciberdelincuentes sabían en todo momento que atraería la atención de los usuarios conocer a través de mensajes de correo la renuncia a la presidencia de Barack Obama.

Figura 25. Email sobre la renuncia a la presidencia de Barack Obama.

Figura 26. Web que muestra la noticia falsa sobre Barack Obama.

Amenazas más destacadas del Q1

Independientemente de la artimaña utilizada por los ciberdelincuentes para hacernos llegar estos códigos maliciosos a nuestros sistemas, estas son algunas de las acciones mas significativas que realizan cuando se introducen en ellos:

- Modifica entradas del registro del sistema, permitiendo su ejecución tras efectuarse el próximo reinicio del sistema.
- Encripta la información substraída de direcciones capturadas, almacenadas en un archivo de nombre aleatorio y remitiéndolas a diferentes direcciones preparadas para la recogida de dicha información.
- El sistema adquiere la funcionalidad de propagar nuevos mensajes de spam para ampliar el número de posibles infectados.
- Su componente Backdoor abre un puerto TCP de comunicación que permite a usuarios remotos conectarse y ejecutar comandos arbitrarios en los sistemas infectados.

En la actualidad aún existen algunas discrepancias en cuanto a si el Waledac es una evolución o el mismo Storm worm, puesto que presentan muchas similitudes en cuanto a su distribución y efectos maliciosos sobre el sistema. No obstante, lo que sí se puede constatar es que junto con el gusano Conficker es uno de los códigos maliciosos más destacables del trimestre.

Tendencias Q1 2009

Si hacemos bien nuestro trabajo, el apartado de tendencias de este informe debería, al menos en parte, confirmar lo que en el último informe augurábamos para todo el año 2009. Y de hecho así es, empezando por el resurgimiento de los virus que vaticinábamos y que se ha hecho realidad con la aparición del Sality.AO.

Sality.AO

Sality.AO utiliza técnicas que hace años que no se veían como EPO o Cavity. Ambas son técnicas relacionadas con el modo en que se lleva a cabo la modificación del fichero original para infectarlo, haciendo más difícil de detectar esa modificación así como la posterior desinfección. Así, la técnica EPO permite la ejecución de parte del fichero legal antes de que comience la infección, lo que dificulta la detección del ejemplar. Por su parte, la técnica Cavity consiste en la utilización de los espacios en blanco del código del fichero legal para insertar el código malicioso del virus.

Estas técnicas están muy alejadas de las que se logran con las herramientas de creación automática de malware, causantes en gran medida del notable aumento de amenazas en los últimos años, y requieren técnicas más artesanales y un gran conocimiento de programación de códigos maliciosos. Además, Sality.AO añade funcionalidades extra como la posibilidad de conectarse a un canal IRC para recibir órdenes de su creador, pudiendo éste tomar el control de la máquina.

Igualmente, no se limita a la infección de ficheros como los viejos ejemplares de virus, sino que también busca distribuirse a través de la web como los ejemplares más novedosos. Para ello, infecta los archivos PHP, ASP y HTML que encuentre en el equipo con un tag iFrame. Debido a esto, cuando alguno de esos ficheros es ejecutado, el navegador es redirigido, sin que el usuario se dé cuenta, a una página maliciosa en la que se lanza un exploit contra el equipo, con el fin de descargar en él nuevos ejemplares de malware.

La historia no termina aquí; si alguno de esos ficheros infectados son subidos a una página web –y las extensiones de los archivos infectados son las típicas de archivos que se suben a la web-, los usuarios que los descarguen desde ellas o que visiten las páginas formadas por esos códigos quedarán infectados igualmente.

El archivo que se descarga a través de esta técnica es un troyano que a su vez está infectado con un virus, una variante más antigua del propio Sality. El troyano, además, cuenta con funcionalidades downloader para seguir descargando nuevos ejemplares de malware en el equipo.

Tendencias Q1 2009

Redes Sociales

Las compañías de seguridad llevamos tiempo hablando del cuidado que hay que tener con las redes sociales, desde el punto de vista de nuestra intimidad y la información personal que puede ser accedida por terceros, así como medio utilizado para propagar malware.

Si bien a lo largo de 2008 vimos que había sucesos aislados que afectaban a redes sociales, durante el primer trimestre de 2009 vemos que es algo que realmente ha tomado un ritmo frenético. Además del típico malware, como Boface (también conocido como Koobface), que utiliza redes sociales para propagarse, lo que más estamos viendo es el uso de las redes sociales para poner enlaces que llevan a malware en forma de comentarios, tratando de engañar a los usuarios para que se infecten.

No podemos decir que hayan inventado la rueda, la verdad es que el algo que llevan haciendo desde siempre: utilizar la curiosidad de los usuarios para engañarles y llevar a que se infecten o a sitios publicitarios. La única novedad es que lo están comenzando a hacer de forma masiva en determinadas webs muy populares hoy en día: digg.com, YouTube, Facebook, Twitter...

Conficker

Mirando todo lo sucedido en este primer trimestre de 2009 no podemos dejar de mencionar al gusano Conficker, que ha conseguido generar millones de infecciones en un corto plazo de tiempo. Aunque actualmente la situación podríamos decir que está controlada, una de las características que tiene el gusano es la capacidad de generar URLs a las que se conecta para poder descargar código malicioso. La última variante conocida comenzará a generar 50.000 URLs diferentes diariamente a partir del 1 de abril, por lo que es de esperar que utilicen esta vía para infectar con nuevas variantes del Conficker o con otros códigos maliciosos.

USB VACCINE

Los dispositivos extraíbles se han convertido en un importante recurso para garantizar la propagación del malware, ya que actualmente cada vez se utilizan más las llaves USB o los discos duros portátiles para compartir información, no solo en los entornos domésticos sino también en los corporativos.

Todas las empresas actualmente tienen protegido su perímetro (firewall, etc.), pero aún así nada impide que un trabajador llegue con su llave USB de casa, lo conecte a la estación de trabajo y extienda ese código malicioso por toda la red. Debido a la proliferación de malware con estas funcionalidades, en Panda Research hemos desarrollado una utilidad gratuita que permite a los usuarios proteger sus dispositivos extraíbles del malware: USB vaccine.

Tendencias Q1 2009

AMTSO

En mayo tendrá lugar en Budapest la próxima reunión del AMTSO, donde validaremos una serie de documentos en los que venimos trabajando los últimos meses; en el próximo informe hablaremos de ellos en detalle.

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/.