

INFORME ANUAL PandaLabs 2008

© Panda Security 2008

PANDA
SECURITY

One step ahead.

Índice

Introducción	3
Resumen ejecutivo	4
Las cifras del cuarto trimestre	5
Distribución de las nuevas amenazas detectadas	5
Aparición de malware mes a mes	8
Evolución de Malware durante el 2008	9
Amenazas detectadas por los Sensores PandaLabs	10
Malware activo	12
Informe sobre el estado actual del spam	15
Caída de McColo	15
Nuevas amenazas: NDRs	16
Vulnerabilidades Importantes del año 2008	17
Visión General	17
Vulnerabilidades destacadas	18
Métodos de Infección	21
Informe sobre troyanos bancarios	25
Principales familias	26
Vías de infección	27
Sofisticación de los troyanos bancarios	28
Crimen organizado	29
Recomendaciones	31
Los falsos antimalware en el 2008	32
Características	33
Vías de entrada habituales	37
Cifras y datos	41
Análisis a fondo: MalwareProtector2008	44
Consejos	50
Tendencias del 2008	51
Sobre PandaLabs	53

Introducción

Finaliza el año 2008 y presentamos el último informe trimestral que servirá para realizar una revisión de los acontecimientos más importantes ocurridos durante el 2008. Vamos a cerrar el año presentando los datos más relevantes correspondientes al cuarto trimestre, para posteriormente centrarnos en analizar la evolución del malware a lo largo del año.

El spam también ha dado que hablar este último trimestre. Pero en este caso de forma positiva, ya que tras la caída de McColo, el volumen de spam en circulación se vio notablemente reducido. Sin embargo, parece que se trató de una situación transitoria, ya que los niveles de spam vuelven a ser, a día de hoy, los habituales.

Una importante vulnerabilidad descubierta en el servicio RPC provocó que Microsoft se saltara su ciclo de emisión de parches habitual para solventar este fallo de seguridad. Además, esta vulnerabilidad permitió que un gusano de red se propagara en un tiempo record. Podréis ampliar la información sobre esta vulnerabilidad en la ya habitual sección de Vulnerabilidades.

Los falsos antimulware ha sido una de las amenazas que más ha crecido durante el 2008. Y es que éstos junto con los troyanos bancarios son las familias que más beneficios económicos reportan a los ciberdelincuentes. Por ello, hemos preparado dos interesantes artículos sobre estas familias tan rentables actualmente.

Para cerrar el informe, os presentamos un artículo en el que se presentan las tendencias más destacadas de este año y las que se esperan para el año que viene.

Asimismo, como en anteriores informes, presentaremos la evolución de malware activo por países durante el año 2008 y las cifras de este trimestre.

Esperamos que os resulte interesante.

Resumen ejecutivo

Los troyanos siguen siendo la categoría de malware predominante este trimestre incrementándose en un 17,96% con respecto al trimestre anterior, hasta situarse en un 77,49% del total del malware.

En cuanto al malware activo, durante el primer semestre del año, España y especialmente Estados Unidos superaron el 40% de infección aunque su media anual es del 29,17% y 24,36% respectivamente.

Durante los primeros meses del 2008, los niveles de spam supusieron entre un 60% y un 94% de todo el correo electrónico enviado a Internet.

A raíz de la caída de McColo, los niveles de spam monitorizados por Panda Security descendieron entre un 50% y un 70%.

En los primeros 8 meses de 2008, PandaLabs ya había detectado más ejemplares de malware que en todos los años de vida de Panda, con una media de 22.000 ejemplares recibidos al día.

Las cifras del cuarto 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 cuarto trimestre de 2008:

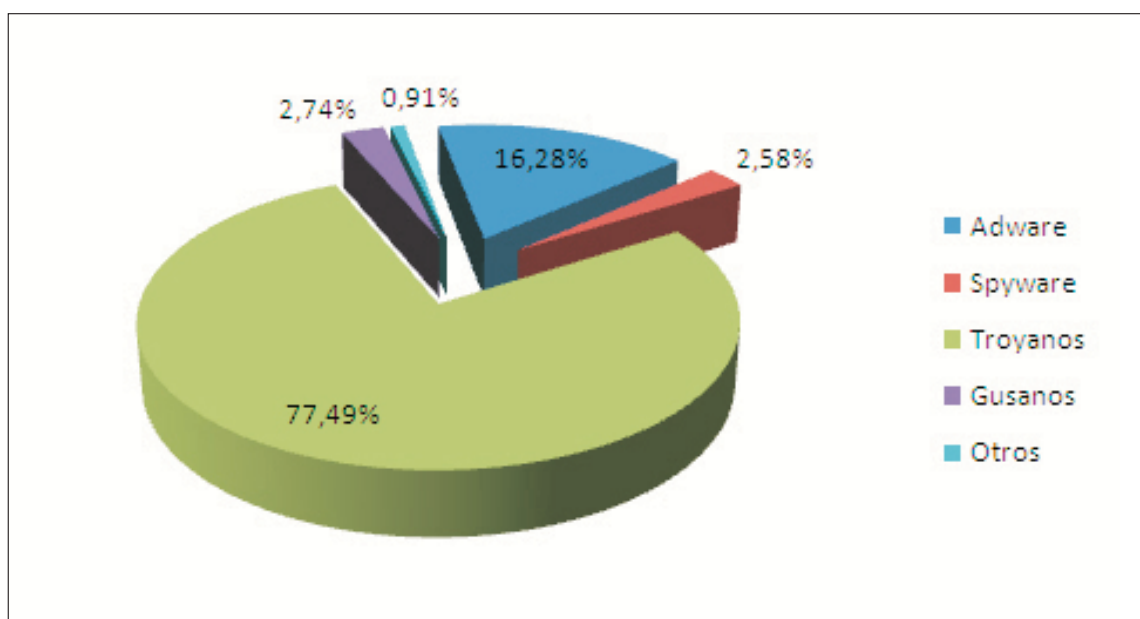


Figura 1. Aparición de malware trimestral.

Según los datos del gráfico, se observa que la categoría de malware predominante este trimestre sigue siendo la de los troyanos, incrementándose notablemente un 17,96% con respecto al trimestre anterior, hasta situarse en un 77,49%.

Tiempo atrás quedaron las grandes epidemias mediáticas en las que los ciberdelincuentes buscaban una notoriedad dentro de los círculos de creación de malware. Sin embargo en todo ese proceso de "evolución" hasta la actualidad, el único objetivo factible que hemos observado en ellos es la obtención directa de un beneficio económico por esas creaciones, siendo esta una de las razones por las que se observa tanto volumen de código malicioso relativo al tipo troyano.

Los ciberdelincuentes distribuyen miles de variantes de un mismo ejemplar con el fin de saturar a las compañías de seguridad. Sin embargo, esporádicamente, aprovechan esta situación para liberar alguna creación que realmente sí introduce una evolución en su código y que, en medio de ese volumen de variantes, podría pasar desapercibida y disponer así de una mayor vida útil.

Las cifras del cuarto trimestre

Distribución de las nuevas amenazas detectadas

A lo largo del año hemos detectado algunas de las herramientas constructor, como BitTera, YFakeCreator, Wormer y Turkojan, entre otras. Estas herramientas permiten crear nuevos códigos maliciosos simplemente marcando una serie de checks y sin que sea necesario tener conocimientos en lenguajes de programación. El grado de efectividad de esas infecciones depende de la ingeniería social y de la gran curiosidad del ser humano ante todo lo que recibimos.

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 reducido ligeramente, un 1,79%, hasta suponer actualmente un 2,74% 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.

Por otra parte, pese al "descenso" estadístico de la categoría de Adware, dentro de ellos se ha notado un crecimiento considerable del subtipo de Malware Rogue AV, del cual hablaremos más adelante.

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

Las cifras del cuarto trimestre

Distribución de las nuevas amenazas detectadas

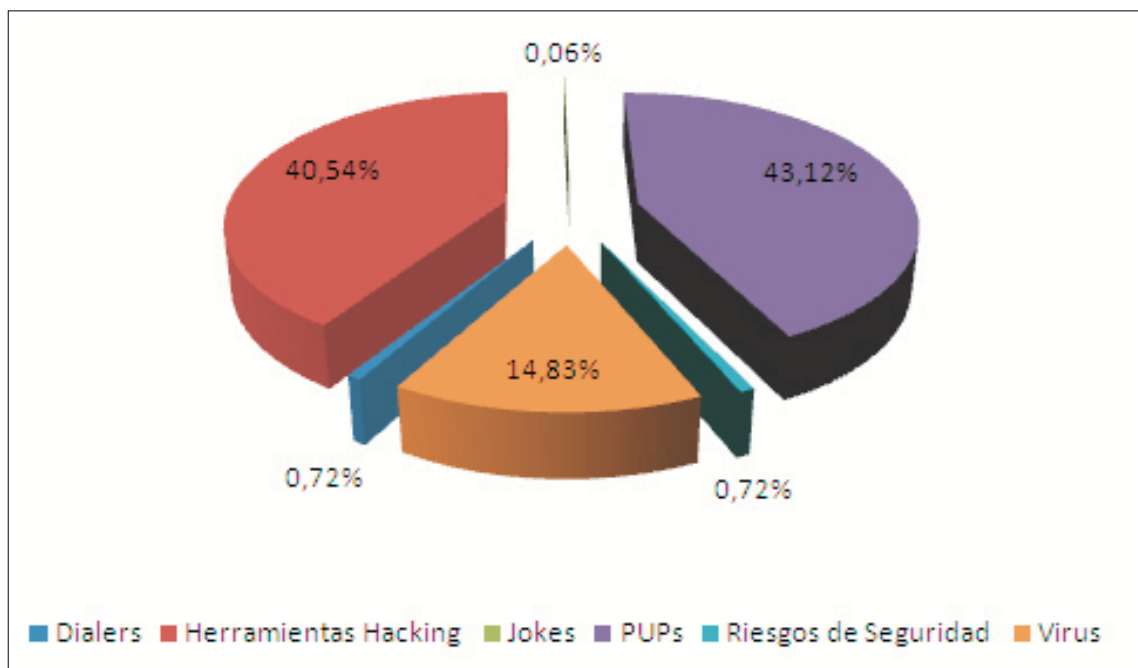


Figura 2. Clasificación de la categoría de Otros.

En esta sección observamos que el tipo de malware predominante son las Herramientas Hacking y los PUPs, situándose en un 40,54% y 43,12% respectivamente, seguido de los Virus situados en un 14,83%, después de un ligero incremento del 3,87% con respecto al anterior trimestre.

El paulatino descenso de clientes de Internet con acceso telefónico hace que los dialers se mantengan en cuotas prácticamente imperceptibles.

Las cifras del cuarto 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.

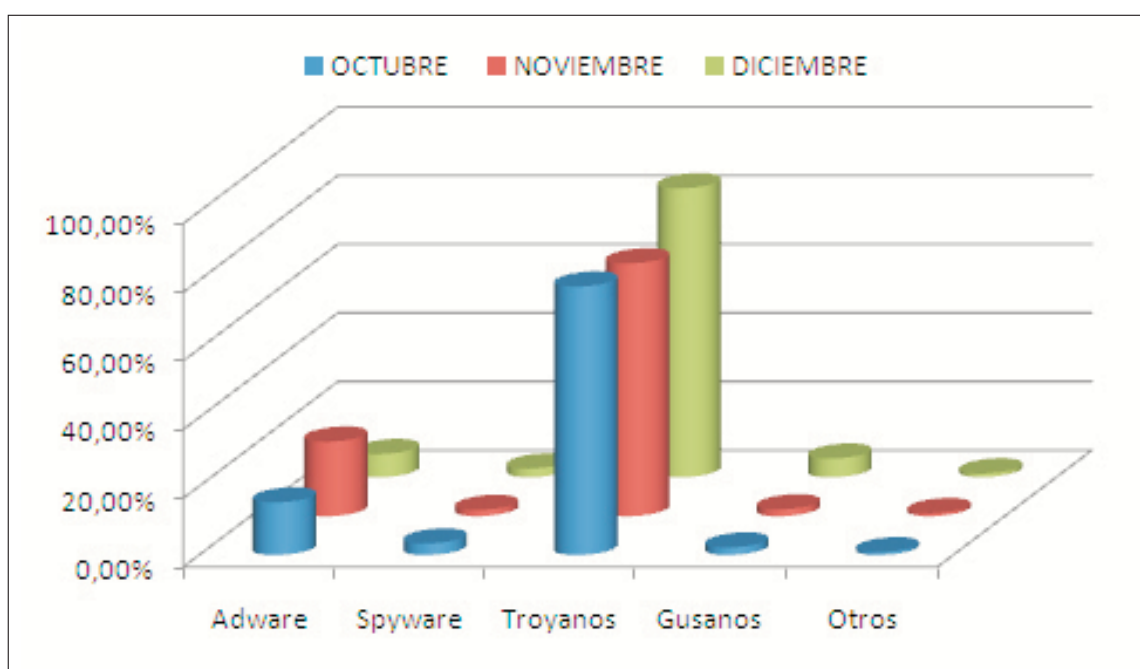


Figura 3. Evolución en la aparición de nuevo malware.

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

Las cifras del cuarto trimestre

Evolución de Malware durante el 2008

A continuación podemos ver la evolución en la aparición de nuevo malware durante el 2008, asociado a las categorías más importantes:

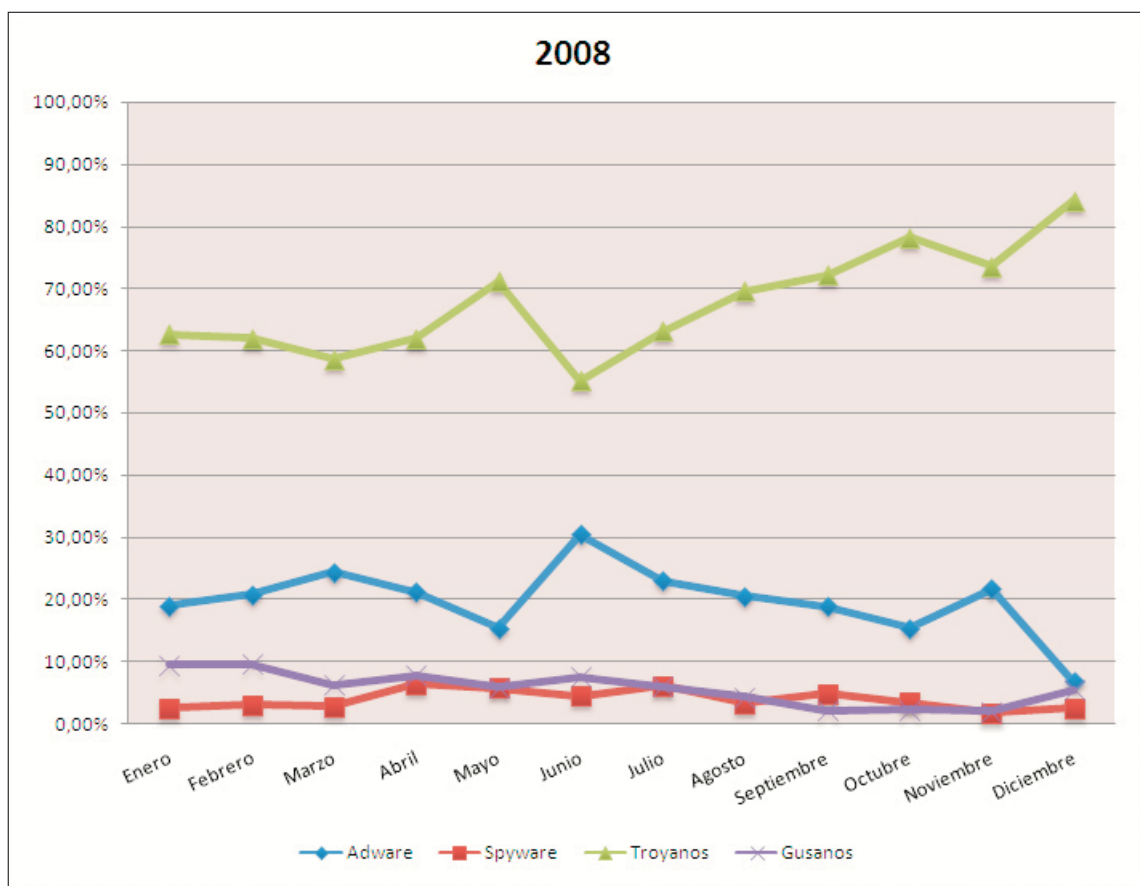


Figura 4. Evolución malware anual.

* Los datos relativos al mes de diciembre únicamente corresponden a los 10 primeros días, por lo cual la gráfica no representa el porcentaje real correspondiente a ese mes.

Esta gráfica corrobora lo anteriormente dicho sobre los troyanos: es el tipo de malware por excelencia más utilizado por los ciberdelincuentes ya que, tanto directa como indirectamente es el que más beneficios les reporta.

Las cifras del cuarto 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:

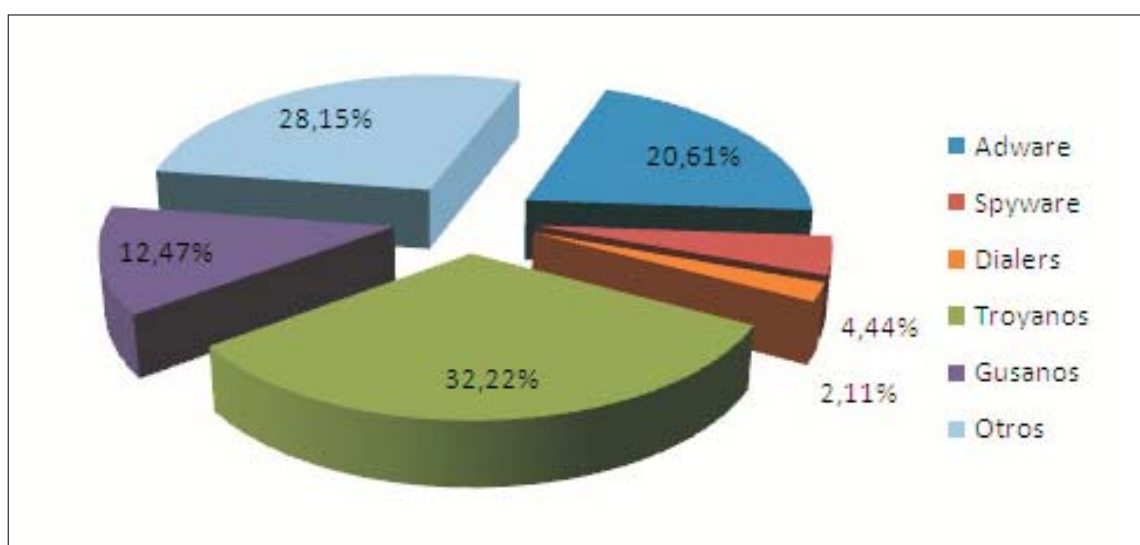


Figura 5. Distribución detecciones por sensores Pandalabs.

En este trimestre el Adware ha descendido un 16,88% hasta situarse en un 20,61%, lo cual deja paso a ocupar la primera posición a los Troyanos con un 32,22%. Éstos han tenido un ligero incremento del 3,52% con respecto al trimestre anterior, situándose así a la cabeza de los tipos de malware más detectados.

Los gusanos, pese a su ligero incremento del 0,91%, prácticamente mantienen su ratio de infecciones, situándose en un 12,47% y manteniendo así su estatus de códigos significativos debido a la rapidez de su difusión/propagación a otros sistemas.

Los dialers, situándose en un 4,44%, siguen resistiéndose a desaparecer a pesar de la tendencia descendente que continúa desde principios del año pasado.

Las cifras del cuarto trimestre

Amenazas detectadas por los Sensores PandaLabs

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

01	Trj/Rebooter.J
02	Adware/Yassist
03	W32/Bagle.RP.worm
04	W32/Gamania.gen
05	Rootkit/Nurech.BC
06	Adware/AdsRevenue
07	W32/Bagle.RC.worm
08	Adware/BaiduBar
09	W32/Puce.E.worm
10	W32/Lineage.JYT



Figura 6. Top ten de amenazas detectadas.

Malware activo

En esta sección vamos a hablar de la evolución del malware activo durante el año 2008.

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/.

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

The image shows a screenshot of the 'Infected or Not?' website. At the top, the title 'Infected or Not?' is displayed in red and blue, with the 'PANDA SECURITY' logo on the right. A central figure of a man in a suit is pointing towards a statistics box on the right that reads '23% of PCs with updated antivirus are infected* ...is yours?' and 'Scan your PC and find out!'. To the left is a navigation menu with 'Home', 'users', and 'Other antivirus users'. Below the main content are three buttons: 'SCAN IT NOW' for Enterprises, 'SIGN UP HERE' for Channel Partners, and 'SCAN YOUR PC' for Home Users. The footer includes links for 'Blog', 'Panda Security Research', 'Choose Country', and copyright information for Panda Security 2008.

Figura 7. Web Infected or Not

Malware activo

Los datos recogidos a través de Infected or not pueden ser consultados a través del Mapa mundial de Infecciones. Por defecto aparecerán los datos estadísticos del país en el que se encuentre el usuario, pero se puede consultar los datos de cualquier país pinchando en el globo que aparece sobre él y haciendo click posteriormente sobre el enlace "ver estadísticas".

En la siguiente gráfica podemos observar la evolución del malware activo durante el año 2008:

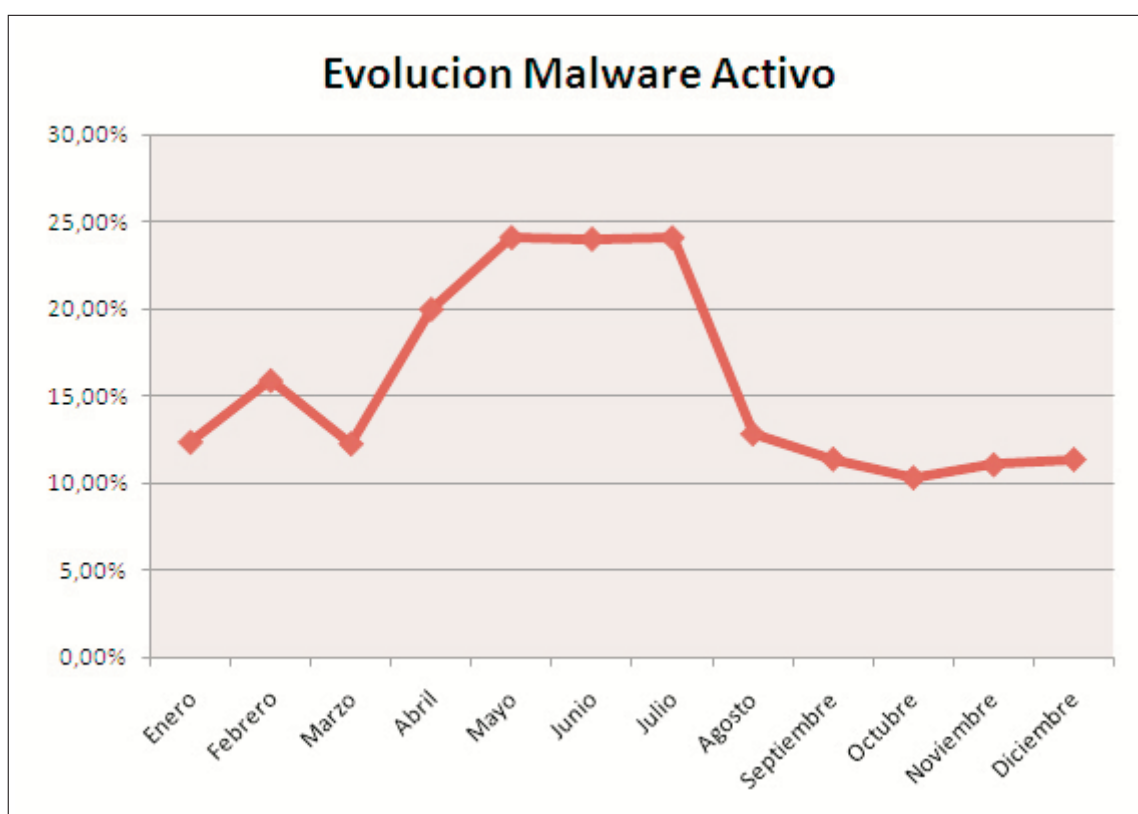


Figura 8. Evolución de malware activo durante 2008.

El primer trimestre del año fue de relativa calma, en cuanto al malware activo, pero a partir de ahí se produjo un incremento constante, llegando en los meses de mayo, junio y julio a su cota máxima, en torno al 24% de malware activo. A partir de entonces se ha producido un descenso progresivo del malware activo alcanzado el porcentaje más bajo del año en octubre 10,31% y finalizando el año en torno al 12%¹ en el mes de diciembre.

¹ Datos recogidos hasta el 10/12/2008.

Malware activo

A día de hoy la media de malware activo asciende al 15,48%. Casi un 2% menos que en los primeros 6 meses del año (17,07%).

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 de malware activo:

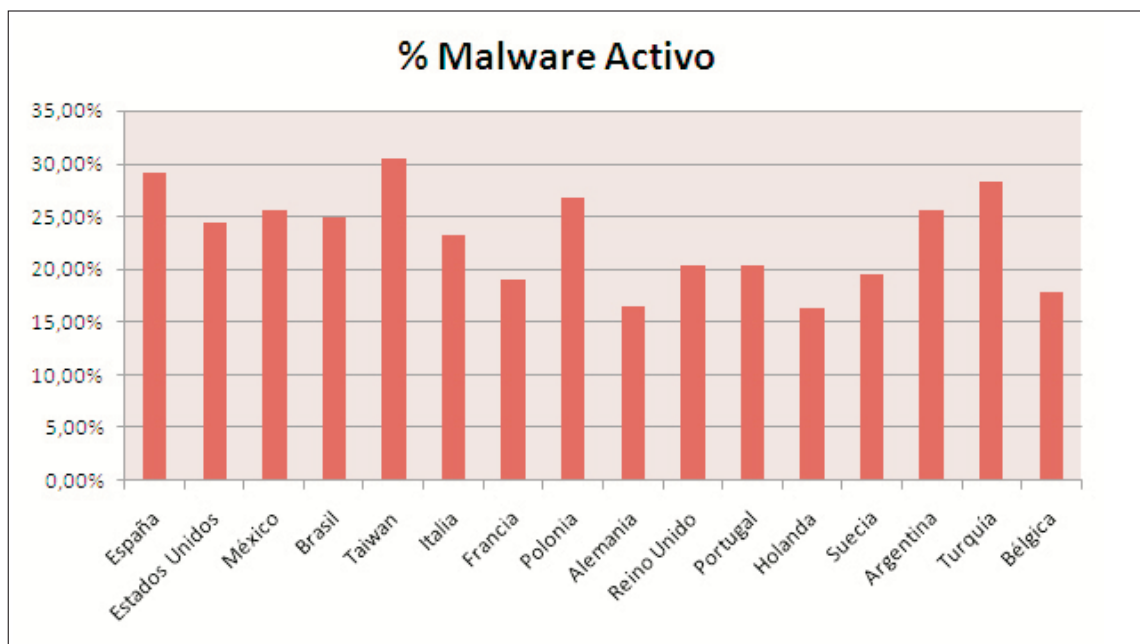


Figura 9. Países con mayor porcentaje de malware (Enero-Diciembre).

Recordemos que durante el primer semestre del año todos los países superaban el 30% de infección, llegando incluso a sobrepasar el 40% en el caso de Rusia, España y Méjico. Durante el tercer trimestre empezó una mejoría y observamos que los países con más malware activo fueron España y Estados Unidos pero con ratios de infección bastante más bajos ya que estaban en torno al 30%. Como podemos ver tras repasar la evolución del malware activo, durante este año 2008 se ha conseguido disminuir el porcentaje de infección de los países. A destacar España y especialmente Estados Unidos, que durante el primer semestre del año superaban el 40%, para finalmente acabar con una media anual del 29,17% y 24,36% respectivamente. Aunque España ha bajado considerablemente sus ratios de infección sigue siendo, junto con Taiwán y Turquía, uno de los países con el mayor porcentaje de malware activo.

Estos datos son positivos, porque reflejan que la situación en cuanto a malware activo ha ido mejorando tras los alarmantes ratios registrados durante el primer semestre. Ahora, solamente Taiwán supera el 30% por lo que el balance de este año es muy satisfactorio.

Informe sobre el estado actual del spam

En Panda Security somos conscientes de la importancia que los sistemas de filtrado de spam tienen para nuestros clientes. Es por eso que desde nuestros departamentos punteros en investigación como PandaLabs se está haciendo un gran esfuerzo para que nuestras soluciones antispam estén a la altura de las necesidades de nuestros clientes y se mantengan a la cabeza de las soluciones antispam del mercado.

En el último informe del año destacamos un hecho importante en el mundo del spam como es la caída de los sistemas de la empresa de hosting McColo y sus consecuencias en el perfil del spam actual. Asimismo, destacamos el trabajo que desde Panda Security se está realizando para hacer frente a las nuevas amenazas como son los NDRs ilegítimos (también conocidos como Backscatter).

Caída de McColo

Comentamos en el informe del segundo trimestre que durante los primeros meses del 2008 los niveles de spam supusieron entre un 60% y un 94% de todo el correo electrónico enviado a Internet. Además, también comentamos que las redes de bots eran el método más frecuente de distribución de spam.

Dicha situación ha cambiado drásticamente en el último trimestre. El pasado 11 de noviembre las autoridades norteamericanas clausuraron la empresa de hosting McColo, empleada por gran número de cibercriminales, y desde cuyos dominios se controlaban redes de bots, se distribuía malware y se enviaba spam (directa o indirectamente mediante las redes de bots).

Como consecuencia de ello, a partir de ese día descendió notablemente la cantidad de spam que circulaba por la red. Los niveles de spam monitorizados por Panda Security descendieron entre un 50% y un 70%.

Además del descenso en los niveles de spam, también se pudieron observar cambios sustanciales en la naturaleza del spam. Hasta el pasado 11 de noviembre la distribución de spam en nuestros sistemas de monitorización era de un 50% solo texto (tanto plano como HTML) y el otro 50% correos con adjuntos de los cuales una parte eran malware.

A partir del 11 de noviembre, el perfil del spam ha cambiado hacia un predominio del contenido exclusivamente de texto. De esto se deduce que McColo no era solo una importante fuente de spam sino también de distribución de malware, y es que a partir de esa semana descendió ligeramente la distribución de determinadas familias de falsos antimalware.

Informe sobre el estado actual del spam

En cualquier caso, en PandaLabs no dudábamos de que se trataría de un descenso transitorio y de que se emplearían empresas de hosting alternativas para continuar con las actividades maliciosas. En el tiempo que ha transcurrido desde entonces, hemos podido comprobar cómo los niveles de spam se han ido recuperando.

La siguiente gráfica refleja los niveles de spam en circulación durante el mes de noviembre:

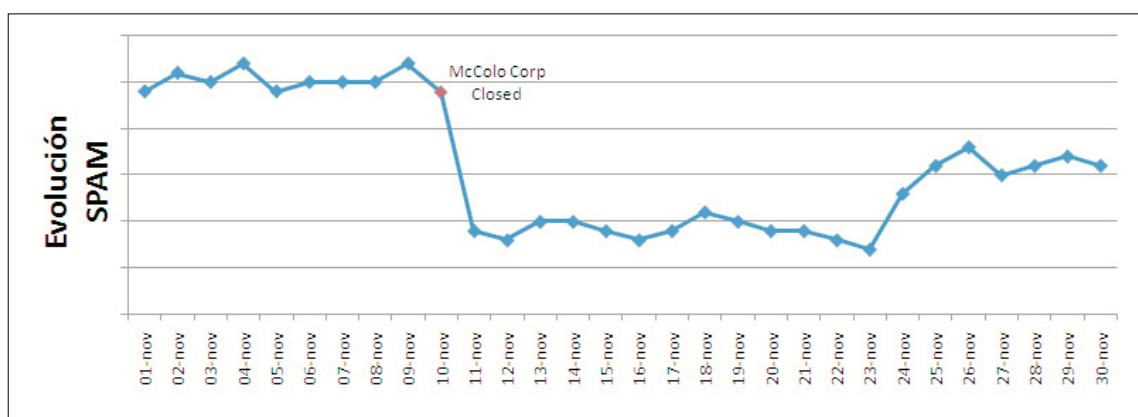


Figura 10. Volumen de spam durante noviembre.

Nuevas amenazas: NDRs

Gran parte de nuestros esfuerzos este año se han centrado en mejorar nuestros sistemas de detección de Correo No Deseado, tanto spam como NDRs ilegítimos (también conocidos como Backscatter). Nuestros niveles de detección de spam siguen siendo óptimos en cuanto a ratios de detección se refiere y en esa línea seguimos investigando y mejorando nuestras soluciones de cara a detectar más y que nuestros sistemas de detección sean más estables ante posibles oleadas de spam o incidencias puntuales.

Por otro lado, durante este año hemos hablado en numerosas ocasiones de los NDRs o Non Delivery Reports y hemos explicado su origen y funcionamiento. Los NDRs ilegítimos son correos electrónicos no solicitados que no podemos considerarlos spam como tal, ya que como comentamos en el anterior informe trimestral, son correos generados por sistemas de correo legítimos. En este sentido, seguimos trabajando y probando diferentes tecnologías con el objetivo de implantar en nuestros productos sistemas que permitan diferenciar de una forma fiable NDRs legítimos (es decir, generados a partir de un correo enviado por el usuario) de los NDRs ilegítimos (generados a partir de un correo enviado por un spammer).

Durante el próximo año dichas mejoras irán viendo la luz permitiendo a nuestros clientes disponer de un servicio aún mejor.

Vulnerabilidades Importantes del 2008

En esta sección haremos un resumen de las vulnerabilidades más importantes de este año. Posteriormente, explicaremos los métodos de infección que más se han utilizado para distribuir malware a través de estas vulnerabilidades durante el transcurso del año 2008.

Visión general

Durante el año han ido apareciendo diferentes vulnerabilidades que afectaban a la suite ofimática de Microsoft Office; algunas de estas han sido encontradas "in-the-wild", es decir, antes de que la vulnerabilidad se hiciese pública. Este tipo de vulnerabilidades vienen siendo habituales año tras año junto con las vulnerabilidades que afectan a los navegadores web como Internet Explorer, Firefox, Safari y Opera.

Una novedad dentro de este grupo de aplicaciones fue el lanzamiento de Chrome, el navegador de Google en su versión beta. El hecho de que unos días después de su aparición se detectaran numerosas vulnerabilidades en esta aplicación puso en entredicho el modelo de seguridad que Google había planeado para su navegador web. Habrá que esperar a ver qué ocurre cuando lancen la versión final.

Este año también le ha llegado el turno a Vista y han salido varias vulnerabilidades explotables de forma remota. Algo destacable es la aparición de dos nuevas vulnerabilidades que afectan a Internet Information Server (IIS). Durante algún tiempo no se habían publicado vulnerabilidades que afectasen al servidor web de Microsoft, pero durante el mes de febrero aparecieron dos vulnerabilidades que permitían la elevación de privilegios y la ejecución remota de código.

No obstante, Microsoft no ha sido la única compañía castigada gravemente; Adobe se ha visto afectada por múltiples vulnerabilidades en sus productos. Algunas de estas son de carácter muy grave y permiten la ejecución de código en el sistema con sólo visitar una página maliciosa que contenga un flash que permite explotar la vulnerabilidad.

La última vulnerabilidad detectada afecta a los productos Adobe Acrobat y Adobe Reader. Esta vulnerabilidad permite la ejecución de código en el sistema afectado debido a un parseo erróneo en la función javascript util.printf() que se puede utilizar en la composición de ficheros PDF.

Vulnerabilidades Importantes del 2008

Vulnerabilidades destacadas

A continuación destacamos las 3 vulnerabilidades que consideramos más importantes de este año 2008.

Vulnerabilidad en Servicio de DNS

Todos los que nos movemos en el mundo de la seguridad estaremos de acuerdo en que la vulnerabilidad descubierta en el servicio de DNS, que permite a los usuarios maliciosos redirigir cualquier página web o dominio a un sistema controlado por dicho usuario, es una de la más graves descubiertas este año.

Tras varios meses de investigación, Dan Kaminsky descubrió una vulnerabilidad que utilizaba las 2 características del protocolo DNS: Predicción de puerto origen e ID de transacción y algunos registros adicionales de recursos, que permitían a un usuario atacante controlar todo el tráfico dirigido a un dominio.

81 fabricantes fueron alertados en el advisory de CERT. Se dice que esta ha sido la mayor actualización sincronizada de seguridad en toda la historia de Internet. Esta era la primera vez en la que muchos de los principales fabricantes como Cisco y Microsoft, entre otros, se han coordinado para garantizar la seguridad de los usuarios en el menor tiempo posible. Para más información sobre esta vulnerabilidad se puede consultar el [informe trimestral de PandaLabs](#) correspondiente al tercer trimestre.

ClickJacking, una nueva amenaza

La vulnerabilidad fue descubierta por los investigadores Jeremiah Grossman y Robert Hansen, actualmente dos de los principales investigadores en seguridad de navegadores web. Su presentación en la OWASP APPSEC USA'08 en Nueva York fue pospuesta a petición de los fabricantes de los navegadores web y de la empresa Adobe, debido a las consecuencias que podría tener.

Esta vulnerabilidad se debe a errores de diseño ya conocidos y que no han sido tenidos en cuenta en los navegadores web. Esta técnica viene a decir que un usuario malicioso puede utilizar el "clic" de ratón sobre una página de navegación del usuario para realizar otras acciones a las que dicho "clic" no iba destinado.

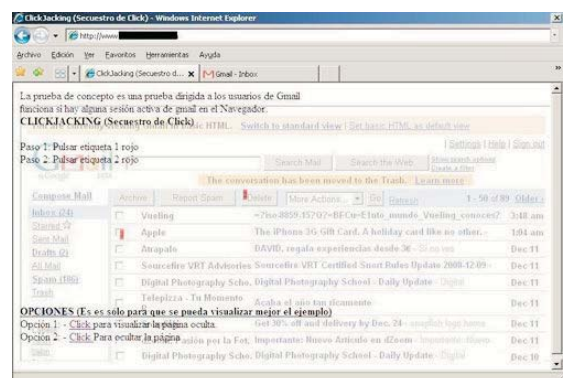
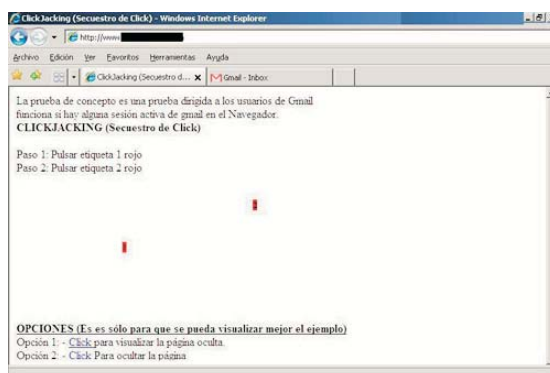
Vulnerabilidades Importantes del 2008

Vulnerabilidades destacadas

Uno de estos ataques consiste en crear un iframe invisible que cargue una página privada del usuario donde este pueda tener una sesión activa, como puede ser el correo electrónico, almacén de fotos online, etc. Un usuario malicioso podría crear una página web y obligar al usuario a realizar ciertos "clics" de ratón estratégicos. El usuario sin saberlo estaría siendo víctima de un ataque de clickjacking y estaría realizando las acciones en la página invisible cargada desde el iframe de la página maliciosa. Por ejemplo, sin darse cuenta un usuario podría estar haciendo público su perfil de usuario de myspace, mostrando sus fotos privadas de flickr o más grave aún eliminando reglas del cortafuegos.

Una de las acciones que más preocupó a la empresa Adobe, era que utilizando esta técnica, un usuario podría activar la cámara y el micrófono y grabar video y audio sin que el usuario que sufre el ataque pudiera darse cuenta de ello.

En el laboratorio de PandaLabs creamos un ejemplo para verificar esta técnica y vimos la sencillez del ataque. La prueba simplemente consistía en que un usuario podría estar jugando a un supuesto "juego" en el que se le requería hacer clic en ciertas zonas de la página. Sin embargo, lo que estaba haciendo realmente era eliminar mensajes de la bandeja de entrada de su correo web sin darse cuenta en 2 clics de ratón, como se puede ver en las siguientes imágenes:



Figuras 11 y 12. Prueba de concepto de clickjacking.

Vulnerabilidades Importantes del 2008

Vulnerabilidades destacadas

Microsoft MS08-067 y el gusano Conficker

Esta vulnerabilidad junto con la de DNS han sido las dos más importantes que han aparecido este año. Para solventar esta vulnerabilidad en el menor tiempo posible Microsoft tuvo que saltarse su ciclo de emisión de parches periódico, que realiza el segundo martes de cada mes.

La vulnerabilidad se debe a que el servicio no trata correctamente las solicitudes RPC especialmente diseñadas. Un atacante que aprovechara esta vulnerabilidad podría lograr el control completo de un sistema afectado.

La vulnerabilidad afecta a todos sus sistemas operativos, lo que incluye a Vista y 2008 Server llegando a provocar en ambos una denegación del servicio. Sin embargo, en los sistemas operativos Windows 2000, Windows XP y Windows 2003, la vulnerabilidad ha sido clasificada como crítica.

El motivo de esta clasificación es que sin ningún tipo de autenticación la vulnerabilidad proporciona acceso al sistema a través de los recursos compartidos, permitiendo la ejecución de código en el mismo de forma remota. Esto ha permitido en un tiempo record la creación del gusano [Conficker.A](#) que se propaga utilizando esta nueva y peligrosa vulnerabilidad aún activa para aquellas máquinas que no hayan sido parcheadas.

Microsoft menciona en su web que si se siguen los procedimientos recomendados relativos al uso de cortafuegos y de las configuraciones de seguridad predeterminadas estas pueden contribuir en la seguridad de los sistemas frente a estos ataques. Microsoft también recomienda que los sistemas conectados a Internet deben tener expuestos la cantidad mínima de puertos.

No obstante, se recomienda encarecidamente actualizar el parche publicado por Microsoft sobre la vulnerabilidad [MS08-067](#).

Vulnerabilidades Importantes del 2008

Métodos de Infección

En esta sección vamos a explicar los diferentes métodos de infección que hemos visto a lo largo de este año. Aunque estos métodos no son nuevos, siguen siendo eficaces como medios por los cuales el malware llega a infectar un sistema.

Método A: A través de técnicas de Ingeniería Social

Este método de distribución se realiza por lo general a través de envíos masivos de correo electrónico, aunque también se pueden utilizar otros medios, como foros y blogs. Las vulnerabilidades que se utilizan para esta vía de infección por lo general se deben a errores no controlados en una aplicación al parsear (proceso de interpretar los datos que hay en el fichero) el fichero, normalmente de tipo ofimático.

Este método de infección requiere de una interacción por parte del usuario, como por ejemplo, abrir un documento. Para conseguirlo, el usuario malicioso utiliza técnicas de ingeniería social que aprovechan la curiosidad innata del usuario y por lo tanto es engañado e infectado. Por este motivo, cientos de miles de máquinas quedan infectadas cada vez que circula por la red un documento malicioso que hace referencia a alguna noticia importante. No es difícil de entender por qué actualmente hay infecciones de malware que utilizan temas relacionados con la victoria histórica del nuevo presidente de los Estados Unidos, Barack Obama.

Todos estamos expuestos a este tipo de ataques cada día, y si no somos conscientes de la gravedad que puede suponer abrir un fichero adjunto de origen desconocido, tarde o temprano podemos llegar a estar infectados por un fichero malicioso. Hay que resaltar que la mayor peligrosidad recae al abrir ficheros de la suite ofimática de Microsoft, ficheros PDF de Adobe y ficheros multimedia.

La tecnología TruePrevent disponible en nuestra gama de Antivirus 2009 está especialmente diseñada para prevenir este tipo de ataques desconocidos.

Aquí mostramos algunas de las vulnerabilidades que se han utilizado este año para infectar a los usuarios a través de este método.

- Microsoft Word Smart Tag Invalid Length Processing Vulnerability (CVE-2008-2244)
- Microsoft Access Snapshot Viewer ActiveX Control Vulnerability (CVE-2008-2463)
- Microsoft code ejecución Vulnerability (CVE-2008-1091, CVE-2008-1434)
- Microsoft Word File Information Block Memory Corruption (CVE-2008-0109)
- Microsoft Excel Multiple Vulnerabilities (CVE-2008-3471, CVE-2008-3477, CVE-2008-4019, CVE-2008-3003, CVE-2008-3004, CVE-2008-3005, CVE-2008-3006)
- Microsoft Excel Multiple code Execution Vulnerability (CVE-2008-0081, CVE-2008-0111, CVE-2008-0112, CVE-2008-0114, CVE-2008-0115, CVE-2008-0116, CVE-2008-0117)
- Adobe Reader/Acrobat Javascript Method Handling Vulnerability (CVE-2008-2641)
- Adobe Acrobat/Reader Multiple Vulnerabilities (CVE-2008-2549, CVE-2008-2992, CVE-2008-4812 a CVE-2008-4817).

Vulnerabilidades Importantes del 2008

Métodos de Infección

Método B: Infección a través de páginas legítimas en Internet

Se suele decir que si un usuario no navega por páginas sensibles o de dudosa reputación, su sistema no tiene peligro de ser infectado. [Durante el segundo trimestre](#) de este año esta idea ha cambiado debido a que millones de páginas "seguras" han sido infectadas con código malicioso y han sido las causantes de infectar cientos de miles de sistemas.

Al principio se pensaba que las incidencias que estaban ocurriendo eran debido a una vulnerabilidad de "día cero" que podría afectar a los servidores Microsoft Internet Information Server y Microsoft SQL Server. Esta idea fue desmentida por el propio Microsoft y finalmente se descubrió el motivo. Las aplicaciones web de los servidores infectados eran vulnerables a ataques de SQL Injection² convirtiéndose estas en el talón de Aquiles de un servidor aunque este estuviese completamente parcheado.

Estos ataques fueron realizados con herramientas especialmente diseñadas cuyo objetivo era modificar el contenido de las páginas web del aplicativo atacado incluyendo en ellas un iframe que apuntaba a un servidor que contenía exploits para diversas vulnerabilidades de los navegadores web de los usuarios: MS06-014, MS07-004, MS07-018, MS07-033 y MS07-55. Esta acción fue aprovechada para distribuir diferentes ejemplares de malware.

El ataque normalmente automatizado comienza por la búsqueda de aplicativos web que pueden ser vulnerables a ataques de SQL Injection utilizando el motor de búsquedas de Google³. Una vez localizado uno o varios servidores vulnerables, la herramienta lanza diversos ataques para identificar el diseño de la base de datos que hay tras el aplicativo web. Una vez descubierto este diseño, se lanza el ataque final, que consiste en modificar el contenido de los campos de texto de las tablas de la bases de datos del servidor atacado.

Como resultado, el aplicativo web además de contener información legítima, contiene código malicioso que se ejecuta cuando el usuario carga las páginas HTML del aplicativo Web infectado. Este código tiene como objetivo instalar un malware en el sistema sin que el usuario se percate de ello. Como hemos comentado, para esta acción utiliza vulnerabilidades que afectan a los navegadores web o a los componentes instalados en estos.

Este método a parte de ser muy efectivo, abarata los costes para los ciberdelincuentes al no tener que contratar, por ejemplo, servicios de distribución de spam. Además, es el usuario quien tiene la iniciativa de acceder a la página "segura". Es esta misma acción la que hace que se oculte aún más el método y el origen de la infección. Si, además se trata de una página que recibe muchas visitas, el ciberdelincuente se asegurará un número mayor de infecciones.

² Técnica que consiste en inyectar sentencias SQL en la consulta SQL real que se van a ejecutar en el servidor de base de datos

³ La técnica de utilizar el motor de Google para este tipo de operaciones es conocida como Google Hacking

Vulnerabilidades Importantes del 2008

Métodos de Infección

A principios del 2007 cientos de miles de usuarios quedaron infectados por un malware al acceder a la web de la SuperBowl⁴. Este mismo año la web de TrendMicro fue comprometida⁵ y miles de usuarios y visitantes fueron infectados con un troyano que se instalaba en los equipos de los usuarios que visitaban la web de la empresa antivirus.

Estos u otros ejemplos nos hacen ver que incluso visitando páginas seguras, un usuario puede terminar infectado. La gravedad es aún mayor si estos ataques van dirigidos a aplicaciones web de banca o compra por Internet. El usuario malicioso puede diseñar un malware a medida haciéndolo más efectivo al poder seleccionar sus víctimas.

Método C: Gusano de Red

De todos los métodos de infección sin lugar a dudas los gusanos de red son los más peligrosos y los que más repercusión han tenido en los últimos años. Aunque el 2008 parecía un año tranquilo en cuanto a este tipo de infecciones, en el mes de octubre Microsoft publicó el boletín de seguridad MS08-067, que hacía referencia a una vulnerabilidad de "día cero" que afectaba a toda las versiones de sus sistemas operativos.

Aunque Windows Vista ha mejorado en seguridad y es la versión más segura de este sistema operativo hasta el momento, también ha sucumbido ante esta grave vulnerabilidad, aunque en este sistema y en 2008 Server sólo permite realizar una denegación de servicio, mientras que en los sistemas con Windows XP y 2000 es posible la ejecución de código de forma remota. Este tipo de explotación da paso a la aparición de nuevos gusanos de red como es el caso del W32/Conficker.A.worm.

Este método no necesita la interacción del usuario; una vez que ha infectado un sistema, el gusano se aprovecha de otras máquinas vulnerables y se propaga a través de la red de forma automática utilizando dicha vulnerabilidad para introducirse en los sistemas.

Por otra parte, este tipo de infecciones no son totalmente transparentes ya que es usual detectar infecciones de gusanos al observar un funcionamiento anómalo en el tráfico de la red y detectar fallos en sistema operativo debido a un consumo excesivo de memoria o de CPU y a errores producidos en los servicios de Windows como el svchost.

⁴ http://www.infoworld.com/article/07/02/02/HNdolphinssiteshacked_1.html

⁵ <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9068478>

Vulnerabilidades Importantes del 2008

Métodos de Infección

En Resumen

Independientemente del método utilizado para distribuir el malware, una vez más se demuestra cómo los ataques informáticos y la distribución de malware aporta sustanciosos beneficios económicos, ya que el malware distribuido está principalmente orientado al robo de datos bancarios.

Como otras veces, los creadores de malware, con el fin de conseguir un mayor impacto y duración de la explotación de la vulnerabilidad descubierta en productos de la empresa Microsoft, esperan al segundo miércoles de cada mes para explotar las vulnerabilidades de "día cero".

De esta manera, cuentan en principio con una ventana de un mes hasta la siguiente actualización de Microsoft. No obstante, en varias ocasiones Microsoft ha tenido que saltarse esta rutina de publicación y lanzar una actualización urgente para solucionar el fallo de seguridad descubierto debido a la gravedad e impacto de la vulnerabilidad, como ha sido en el caso de la vulnerabilidad de MS08-067.

Desde Panda Security, aconsejamos tener actualizado siempre su aplicación antivirus y tener activado el cortafuegos. Adicionalmente, para incrementar la seguridad en el sistema siempre se deben aplicar las últimas actualizaciones de seguridad del sistema operativo, navegadores web y aplicaciones instaladas. A los usuarios de Windows XP también aconsejamos la instalación del Service Pack 3 publicado ya por Microsoft y la actualización que corrige la vulnerabilidad MS08-067, ya que ésta es posterior al Service Pack 3.

Informe sobre troyanos bancarios

Los troyanos bancarios siguen suponiendo una gran amenaza para los usuarios y es que, a pesar de que las entidades bancarias han ido aumentando las medidas de seguridad de sus páginas web, también los troyanos bancarios se han ido sofisticando e incluyendo nuevas funcionalidades.

Una de las mayores preocupaciones de los usuarios en cuanto a los riesgos de Internet es el robo de información confidencial, como contraseñas y más aún si se trata de datos bancarios. Esto convierte a los troyanos bancarios en uno de los tipos de malware más peligrosos para los usuarios, ya que están diseñados precisamente para robar ese tipo de información.

Los troyanos bancarios junto con los falsos programas antivirus, sobre los que también hablamos en este informe, parecen haberse proclamado como las categorías más rentables para los ciberdelincuentes.

La ingeniería social sigue siendo uno de los métodos más utilizados por los ciberdelincuentes para introducir este tipo de malware en los ordenadores de los usuarios. Aunque no siempre es imprescindible la intervención del usuario, ya que otra manera habitual de introducir malware en los ordenadores es través de páginas web infectadas.

Una vez instalado en el ordenador, el principal objetivo de estos troyanos es conseguir los datos bancarios de los usuarios afectados. Normalmente, los troyanos se quedan residentes en memoria y solo se activan cuando el usuario accede a la página web de ciertas entidades bancarias. Para ello, los troyanos cuentan con una lista de bancos a los que atacar.

Para los ciberdelincuentes es relativamente sencillo obtener estos programas maliciosos, ya que existe todo un mercado de venta de troyanos diseñados a la carta y de los denominados kits bancarios, que permiten no solo crear troyanos con múltiples funcionalidades sino controlarlos y enviarles nuevas instrucciones.

En este artículo resumiremos las principales familias de troyanos bancarios, explicaremos cuáles son las vías de entrada habituales, analizaremos el complejo entramado que hay detrás de este negocio tan lucrativo y ofreceremos una serie de recomendaciones para mantenerse protegido frente a estas amenazas.

Informe sobre troyanos bancarios

Principales familias

A pesar de que existen diversas familias de troyanos bancarios, a continuación destacamos los 3 tipos donde se pueden englobar las familias más activas:

1) Troyanos bancarios brasileños (Banbra, Bancos).

Estos troyanos están diseñados principalmente para robar contraseñas de entidades bancarias brasileñas y portuguesas, aunque también es posible encontrar entidades españolas en variantes de la familia Bancos. Suelen enviar la información obtenida a través de correo electrónico o por FTP.

La diferencia entre ambas familias reside en su lenguaje de programación. Las variantes de la familia Banbra están programadas en Delphi, mientras que las de la familia Bancos en Visual Basic.

A diferencia de otras familias, no se crean con kits generadores de troyanos sino que son programados por completo.

2) Troyanos bancarios rusos 1.0 (Cimuz, Goldun...)

Existen numerosas variantes de estas familias, ya que se suelen diseñar a través de herramientas de creación de troyanos. Sin embargo, las variantes creadas con estas herramientas presentan diferencias mínimas entre ellas, ya que se trata de kits que no se han actualizado durante los últimos años.

A consecuencia de ello, las nuevas variantes de estas familias de troyanos no implementan nuevas funcionalidades y su detección es relativamente sencilla desde el punto de vista del programa antivirus.

3) Troyanos bancarios rusos 2.0 (Sinowal, Torpig, Bankolimb).

Actualmente algunas de estas familias son las más activas y por lo tanto las más peligrosas, ya que cambian y se actualizan constantemente. Esto dificulta bastante su detección, además van añadiendo nuevas funcionalidades para robar credenciales de diferentes entidades.

Todos ellos tienen una forma común de funcionamiento: la lista de entidades a monitorizar para robar las credenciales la obtienen de un fichero de configuración, que puede estar bien junto al troyano o en un servidor aparte controlado por el ciberdelincuente, de tal forma que no tienen que modificar el troyano para añadir una nueva entidad. También utilizan diferentes técnicas de ocultamiento y polimorfismo que complican su detección y eliminación.

Informe sobre troyanos bancarios

Vías de infección

La ingeniería social sigue siendo la técnica más habitual para introducir este tipo de amenazas en los ordenadores de los usuarios. Para ello, se suelen distribuir en mensajes de spam que pueden ser de dos tipos:

1) Spam con un archivo adjunto. Normalmente se trata de archivos adjuntos comprimidos, con extensión zip, que contienen un archivo ejecutable. Sin embargo, para engañar a los usuarios y hacerles pensar que se trata de archivos inofensivos, utilizan las siguientes técnicas:

- **Icono inofensivo:** Presenta un icono relacionado con el tipo de archivo que pretende ser, es decir, si se trata de una imagen tendrá el siguiente icono:



Figura 13. Icono de una imagen.

- **Doble extensión:** Normalmente, el archivo ejecutable tiene doble extensión, en primer lugar tiene la extensión del archivo por el que se hace pasar, por ejemplo en este caso que se trata de una imagen, la extensión sería jpg y después la extensión exe. Es habitual que entre la primera extensión y la segunda haya espacios libres para que el usuario no se percate de que la extensión real es exe. Aunque no siempre es necesario añadir una extensión "inofensiva". Si el archivo tiene un icono aparentemente inofensivo para el usuario, puede que la extensión del archivo pase desapercibida para el usuario.

Lo más habitual en estos casos es que el archivo que ejecuta el usuario se trate de un troyano de tipo Downloader. Estos archivos son de pequeño tamaño y su única función es conectarse a una página web para descargar el troyano bancario.

2) Spam que contienen enlaces a una página web. Se trata de mensajes de correo electrónico que contienen un enlace a una página web. Normalmente, se suele utilizar como cebo un video. Cuando el usuario pulsa el enlace para ver el video, solicita la instalación de algo, puede tratarse de un códec o de una actualización flash, etc.

Una vez descargado el supuesto códec o actualización, hay ocasiones en las que el usuario es redirigido a una página web en la que puede ver un video para evitar que sospeche o simplemente no se muestra ningún video, lo que podría alertar al usuario.

Sin embargo, no hay que olvidar una técnica que se empezó a utilizar a comienzos de este año: la infección de páginas web legales. Para ello, se inserta en dichas páginas una llamada a un servidor malicioso con el objetivo de conseguir información sobre el sistema, como versión del sistema operativo, navegador y actualizaciones instaladas, para introducir malware, que pueden ser troyanos bancarios, intentando explotar alguna vulnerabilidad existente en el sistema.

Informe sobre troyanos bancarios

Sofisticación de los troyanos bancarios

Las entidades bancarias han reaccionado ante la amenaza que suponen los troyanos bancarios para la privacidad y confidencialidad del usuario y han mejorado la seguridad y la autenticación de los clientes. Y como consecuencia de ello, se ha producido una sofisticación de los troyanos bancarios. Las técnicas que utilizan para robar la información han ido mejorando a medida que los bancos, conscientes de la amenaza que suponen estos troyanos, han aumentado las medidas de seguridad en sus páginas web. Por ejemplo, la implantación de los teclados virtuales para el registro de los usuarios, supuso un importante avance en la seguridad de estas páginas web. De esta manera, un keylogger no podría capturar los datos introducidos por el usuario.

Sin embargo, los creadores de malware desarrollaron nuevas funcionalidades para los troyanos bancarios, haciéndoles capaces de registrar los movimientos realizados con el ratón e incluso realizar capturas de pantalla o de vídeo, como es el caso de [Trj/Banbra.DCY](#).

Algunos ejemplares como los pertenecientes a la familia BankoLimb tienen un archivo con una lista de URLs de bancos objetivo. Cuando el usuario infectado con un BankoLimb accede a alguna página web cuya dirección coincida con la de su lista, el troyano se activará e inyectará código html extra en la página del banco.

Esto implica que además de los campos habituales que tiene que rellenar el usuario para registrarse, tendrá que proporcionar más información. El usuario está en la página legítima, pero ligeramente modificada. Por eso es importante que si un usuario está navegando y accede a la página de su banco y le solicitan más información de la habitual, no confíe y no introduzca ningún dato en dicha página, porque posiblemente su ordenador esté infectado con algún troyano bancario y toda la información que introduzca será capturada. Otras veces, los troyanos superponen la página falsa sobre la original para que el usuario no se de cuenta o directamente redirigen al usuario a una página falsa que imita a la original. Una vez que el usuario se registre en dicha página falsa puede mostrar una página de error o incluso podría redirigir al usuario de nuevo a la página original del banco para evitar que el usuario sospeche.

Algunas variantes de la familia del Sinowal son realmente sofisticadas, ya que son capaces de modificar datos "on the fly", es decir, al vuelo. Por ejemplo, si un usuario está realizando una transferencia a través de la página web de su banco, estas variantes pueden modificar los datos del receptor de dicha transferencia una vez enviada la petición. Además el resultado que se le devuelve al usuario sería con los datos originales, por lo que el usuario no se daría cuenta de la estafa.

Otras variantes consultan al servidor para saber si deben realizar alguna acción en función de las páginas que el usuario está visitando. De esta forma no depende de un fichero de configuración y el ciberdelincuente puede ampliar o modificar la lista de sitios web de los que quiere robar información, inyectar código, etc. Una vez que roban la información, suele enviarla a través de correo electrónico o se sube a un servidor FTP.

Informe sobre troyanos bancarios

Crimen organizado

En contra de lo que se puede pensar que el ciberdelincuente que crea el troyano bancario es el que roba la información confidencial de los usuarios para posteriormente robarles el dinero, la realidad es bien distinta y el entramado que hay detrás de este negocio es bastante complejo.

El siguiente gráfico ilustra de forma esquemática el proceso más habitual que hay detrás de este negocio tan lucrativo:

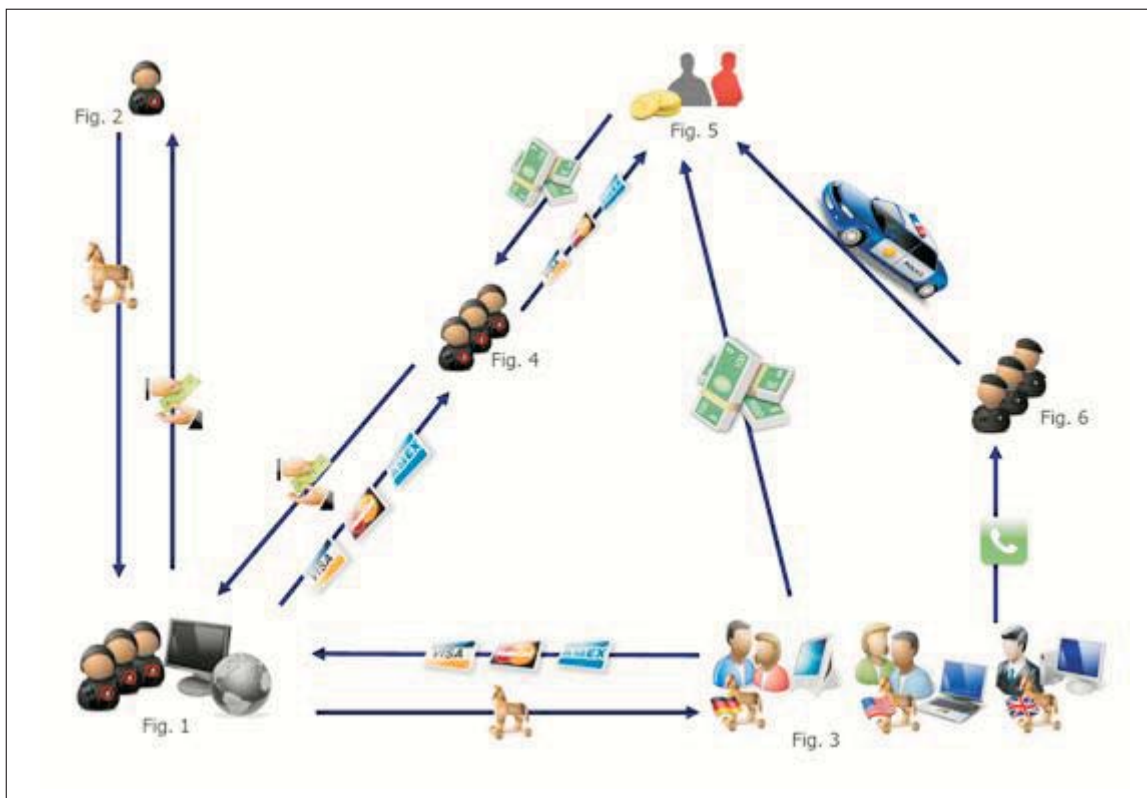


Figura 14. Representación del crimen organizado.

Informe sobre troyanos bancarios

Crimen organizado

Como se puede observar, no se trata de una única persona la que distribuye un troyano bancario para conseguir los datos bancarios de los usuarios y así robarles el dinero. Es mucho más complejo que todo eso y hay todo un negocio detrás de ello.

Vamos a explicar en qué consiste este entramado.

En primer lugar, un grupo de ciberdelincuentes (figura 1) solicita/encarga en foros especializados o en el propio mercado del malware (figura 2) un troyano diseñado a la carta con determinadas características e incluso también podría alquilar toda la infraestructura necesaria para distribuir ese troyano, bien mediante spam o mediante servidores de malware que infectan por el método conocido como drive-by-download. Esta técnica permite la descarga automática de un fichero sin conocimiento del usuario aprovechando posibles vulnerabilidades en el ordenador.

Una vez que tienen el troyano, lo distribuyen a los usuarios con el objetivo de conseguir sus datos bancarios (figura 3). Para ello, los métodos más habituales de distribución de los troyanos son los mensajes de spam o bien infectando páginas web.

Esta técnica de infección de páginas web legítimas consiste en modificar el código fuente de dichas páginas web, añadiendo una referencia de tipo iframe que apunta a un servidor malicioso.

Estos ciberdelincuentes no roban directamente el dinero a los usuarios sino que les roban los datos bancarios y se ponen en contacto con otros ciberdelincuentes (figura 4) a los que les ofrecen los datos a cambio de dinero. De esta manera, hacen negocio pero evitan que les puedan seguir el rastro.

Todos los datos robados se venden en el mercado del malware. Sin embargo, tampoco los que compran los datos bancarios robados son los que roban el dinero a las víctimas. Para evitar que se pueda seguir la pista de los ciberdelincuentes, contratan otras personas como intermediarios, se trata de los muleros (figura 5), Estas personas son contratadas bajo el pretexto de ofertas de trabajo desde casa.

El dinero robado se transfiere a las cuentas de los muleros, ellos se quedan con un porcentaje de ese dinero, normalmente en torno al 3-5% y después de sus cuentas se transfieren a través de un sistema de pago o de envío de dinero anónimo, para pasar a manos de los ciberdelincuentes. Utilizan un sistema de pago/de envío de dinero anónimo para que no puedan ser localizados.

En caso de que las víctimas del robo denuncien los hechos a la policía y se inicie la investigación, en principio los únicos que han dejado un rastro son los muleros.

De esta manera todos salen ganando excepto los propios usuarios afectados y los muleros, ya que en caso de que la policía investigue, serán los que figuren como los ladrones.

Informe sobre troyanos bancarios

Recomendaciones

Los mensajes de spam continúan siendo una asignatura pendiente para los usuarios a la hora de evitar la instalación de malware en sus ordenadores. En ocasiones, el contenido de ciertos mensajes que por ejemplo utilizan logotipos conocidos puede llevar a los usuarios a no desconfiar de los mismos.

Sin embargo, muchos otros mensajes presentan una serie de características como faltas de ortografía o información incoherente, que debería frenar la tentación de los usuarios de ejecutar archivos o pinchar enlaces.

En el caso de los mensajes que contienen archivos adjuntos es importante que antes de ejecutarlos, el usuario lo analice con una solución antivirus para comprobar si contiene malware.

Si se trata de enlaces a páginas web, antes de pulsar el enlace, es recomendable situar el cursor sobre el enlace para comprobar si el enlace que se indica a través del cursor es el mismo que el proporcionado en el mensaje. Y es que en muchas ocasiones, los enlaces que se incluyen en los mensajes están camuflados y en realidad apuntan a una dirección maliciosa desde la que se descargaría el malware.

Por otra parte, los ciberdelincuentes utilizan la infección de páginas web legales para introducir troyanos bancarios en los sistemas de los usuarios. Para ello, es importante tener los sistemas correctamente actualizados y parcheados para evitar que se pueda explotar alguna vulnerabilidad en sus ordenadores.

Los falsos antimalware en el 2008

En los últimos meses han ganado protagonismo los llamados falsos antimalware, también conocidos como "rogue antimalware". Este tipo de programas no son novedosos, pero su gran actividad durante este último semestre ha hecho que hablar de ellos sea indispensable en el Informe anual de PandaLabs.

Últimamente se han detectado numerosos mensajes de spam que distribuyen este tipo de molestos programas. Utilizan la ingeniería social para engañar a los usuarios y los temas más habituales siguen siendo las noticias de actualidad o temas morbosos, y los videos de famosos.

Estos programas se caracterizan por mostrar mensajes alarmistas de manera continuada para acabar con la paciencia de los usuarios y que acaben registrando el producto y por tanto reembolsando una cierta cantidad de dinero.

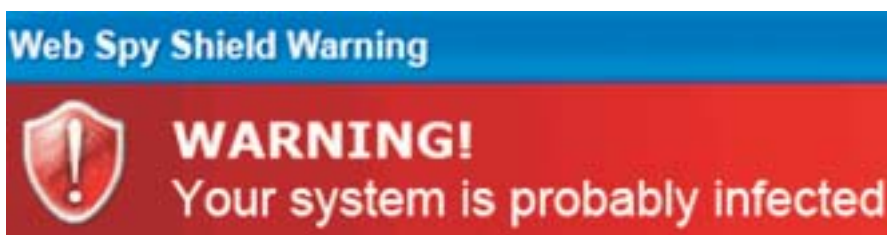


Figura 15. Falso mensaje de infección.

Además, los ciberdelincuentes se aprovechan de que la máxima preocupación de los usuarios en cuanto a los riesgos de Internet es el robo de contraseñas, datos bancarios o información personal del usuario. Por tanto, no hay nada mejor para asustarle que mostrar mensajes alertando de que su información personal corre peligro porque su ordenador está infectado con un troyano ladrón de contraseñas.

Por lo tanto, es importante que los usuarios puedan reconocer este tipo de programas engañosos y así evitar caer en la trampa. Aunque muchos de estos programas tienen interfaces y funciones muy parecidas a los programas auténticos, los métodos que utilizan no son muy ortodoxos.

En este artículo explicaremos en qué consisten estos programas, cuáles son las vías de entrada habituales y cómo actuar ante este tipo de amenazas. Asimismo, podrá comprobar a través de una serie de gráficas el notable aumento de este tipo de amenazas que afectan directamente al bolsillo de los usuarios.

Los falsos antimalware en el 2008

Características

En líneas generales, se trata de aplicaciones que informan de una falsa infección en el equipo y que ofrecen una supuesta solución para eliminar dicha infección. Para ello, el usuario debe registrarse y pagar un importe determinado.

A pesar de que, en un principio, este tipo de herramientas se ofertan como gratuitas, a la hora de registrarse el usuario tiene que pagar un determinado importe. Ofrecen análisis online gratuitos pero los resultados son engañosos, bien porque alertan sobre amenazas inexistentes o bien porque esas amenazas son instaladas por las propias herramientas. Además, muestran mensajes continuos y molestos advirtiendo de que el ordenador está infectado.

Después de analizar numerosos ejemplares de este tipo de malware, los datos confirman que tienen un comportamiento muy similar, no solo en cuanto al tipo de mensajes que muestran sino también en cuanto a modificaciones en el sistema.

A continuación, enumeramos las características comunes de este tipo de programas:

- Avisos de alertas falsas a través de ventanas emergentes, notificaciones en la barra de tareas, modificación del salvapantallas.
- Diseño y funciones similares a las de los verdaderos antivirus.
- Finalizan el análisis completo del equipo en un tiempo muy reducido.
- Las infecciones que muestran hacen referencia a ficheros inexistentes en el equipo o que han sido descargados por ellos mismos.
- Todos solicitan registrar previamente el producto para poder realizar la desinfección, y este registro siempre conlleva un gasto económico para el usuario.

Respecto a los efectos que producen en el equipo, podemos señalar que realizan numerosas modificaciones en el registro de Windows con el objetivo de hacer creer al usuario que está realmente infectado.

Estas modificaciones tienen las siguientes consecuencias:

- Modifica el fondo de escritorio.
- Establece un salvapantallas diseñado por el propio adware.
- Oculta la pestaña Escritorio y la pestaña Protector de pantalla de las Propiedades de Pantalla. De esta manera, el usuario no puede modificar ni el fondo de escritorio ni el salvapantallas.

Los falsos antimalware en el 2008

Características

Habitualmente, el fondo de escritorio y el salvapantallas que establece el adware contienen mensajes en los que se alerta al usuario de que el ordenador está infectado.

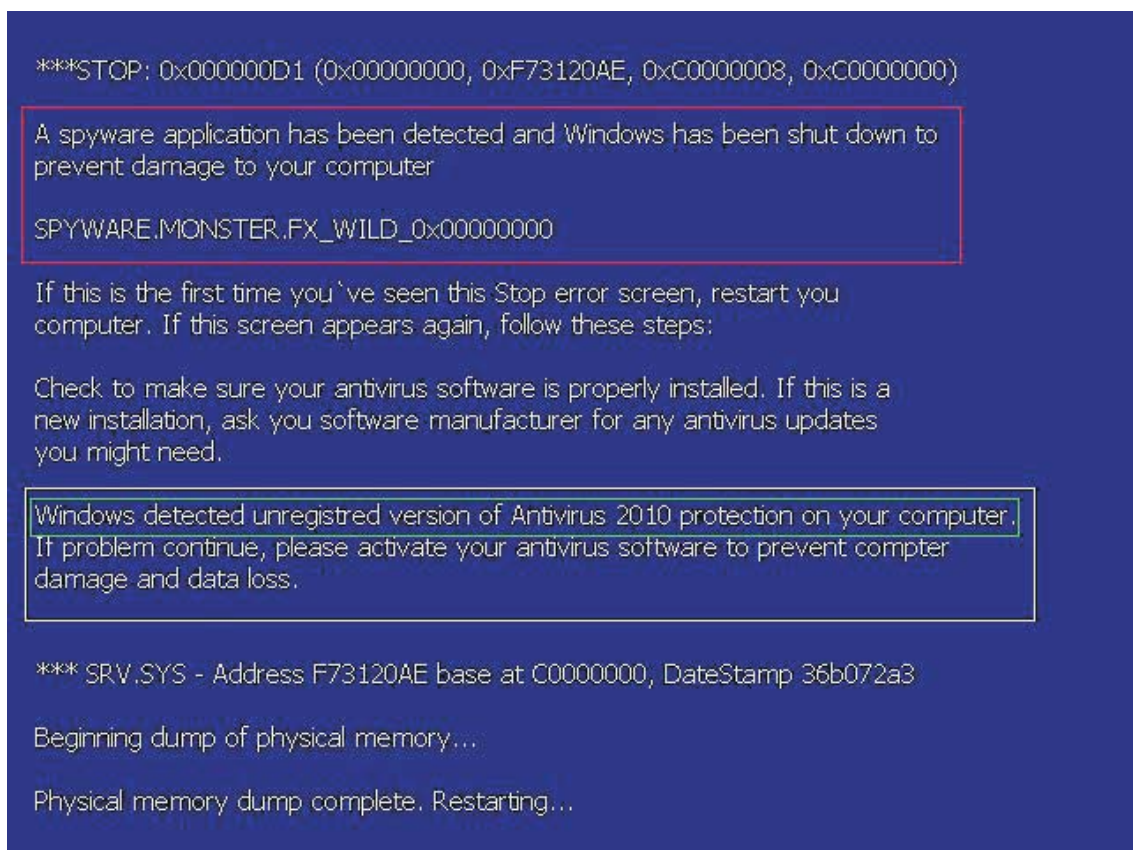


Figura 16. Ejemplo de salvapantallas establecido por los Rogue AVs.

Habitualmente, el fondo de escritorio y el salvapantallas que establece el adware contienen mensajes en los que se alerta al usuario de que el ordenador está infectado.

Los falsos antimalware en el 2008

Características

El objetivo que se persigue con estas técnicas es terminar con la paciencia de los usuarios para que acaben registrándose y abonando la cantidad solicitada. Finalmente, lo que en principio parecía ser gratis, acaba saliendo caro.

Se valen de la falsa percepción de que un programa de seguridad que detecta algo que otro no lo hace es mejor, es decir, cuanto más detecte una solución de seguridad, mejor. Pero nada más lejos de la realidad; el hecho de que detecte más no quiere decir que sea mejor, ya que como ocurre en estos casos, muchas veces lo que detecta es falso o inexistente. El objetivo de este tipo de programas es puramente económico, conseguir que los usuarios adquieran la licencia correspondiente.

En la siguiente imagen podemos observar un diagrama que muestra los diferentes elementos relacionados con la distribución de rogue AVs y la obtención de información personal de los usuarios:

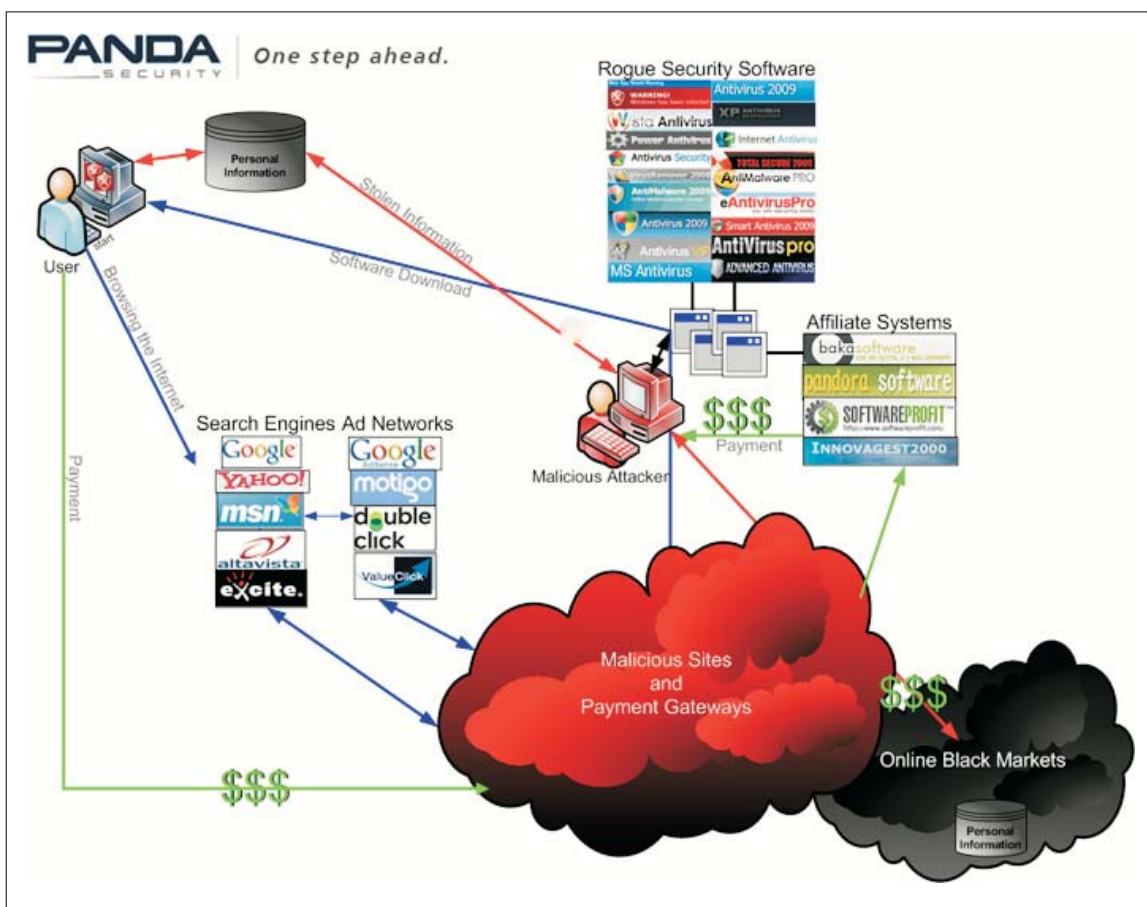


Figura 17. Diagrama distribución de rogue AVs.

Los falsos antimalware en el 2008

Características

Las referencias para el diagrama son:

- Paso 1: Las líneas azules muestran el proceso por el que un usuario es redirigido a una página web infectada.
- Paso 2: Las líneas rojas muestran el camino que sigue la información recogida desde el usuario hasta el mercado negro.
- Paso 3: Las líneas verdes muestran los pagos que realizan los usuarios a través de páginas web maliciosas.

Puedes consultar más información sobre el este diagrama en el [blog de PandaLabs](#).

Los falsos antimalware en el 2008

Vías de entrada habituales

Uno de los posibles medios de entrada de estos programas en nuestros ordenadores es a través de la visita de ciertas páginas web de dudoso contenido, como páginas web de contenido para adultos, entre otras. Para ello, utilizan la técnica conocida como Drive by download para descargar archivos. Esta técnica permite la descarga automática de un fichero sin conocimiento del usuario aprovechando posibles vulnerabilidades en el ordenador. También se suelen utilizar banners publicitarios que ofrecen descargas gratuitas.

Otro medio de distribución de estos programas es a través de las páginas web de software pirata. Utilizan técnicas de ingeniería social para engañar a los usuarios, ya que renombran los ficheros con nombres atractivos para que los usuarios los descarguen pensando que se trata de cracks, seriales...

Sin embargo, los ciberdelincuentes son conscientes de la rentabilidad que supone este negocio y no dudan en poner todos los medios a su alcance para asegurar una buena distribución de estos programas. Así, ya no solo se pueden descargar desde páginas de dudosa reputación, sino también desde páginas web legítimas. En julio publicamos un interesante artículo, [Webs legales en jaque](#), que trata el tema de infección de páginas web legales.

Ahora solo falta conseguir que los usuarios visiten estas páginas web; pero, ¿cómo se consigue esto? A través del spam.

Algunas familias de troyanos como los Exchanger y los Spammer están diseñados para enviar masivamente mensajes de spam.

Este tipo de mensajes adjuntan el propio adware o incluyen un enlace que apunta a una página web desde donde se descarga el fichero mediante el método Drive by download mencionado previamente.

Los mensajes de spam se utilizan para distribuir cualquier tipo de malware, pero hasta ahora lo más habitual era que estos mensajes estuvieran diseñados para distribuir troyanos, sobre todo de tipo ladrón de contraseñas. Sin embargo, en los últimos meses, se ha detectado un cambio en el tipo de malware distribuido a través de spam y ahora son estos falsos antimalware los más utilizados.

Los temas estrella que utilizan para engañar a los usuarios siguen siendo los mismos: noticias de actualidad y videos de famosos.

Los falsos antimalware en el 2008

Vías de entrada habituales

Las siguientes imágenes corresponden a mensajes de correo electrónico utilizados para distribuir estos programas:



Figura 18. Mensajes de spam para distribuir Rogue AV.

Por último, otra vía habitual de entrada de estos programas es a través de malware. Existen ciertas familias de malware que descargan este tipo de programas. Tal es el caso de la familia de los Nuwar, o incluso algunas familias de adware que a su vez descargan otros ejemplares de adware, como es el caso de Adware/Bravesentry.

El último método de ingeniería social que están usando los distribuidores de falsos antivirus consiste en saltarse la infección a través de la cuál nos engañan para que compremos estas falsas aplicaciones y directamente intentan engañarnos indicándonos que tenemos que activar nuestro antivirus.

Los falsos antimalware en el 2008

Vías de entrada habituales

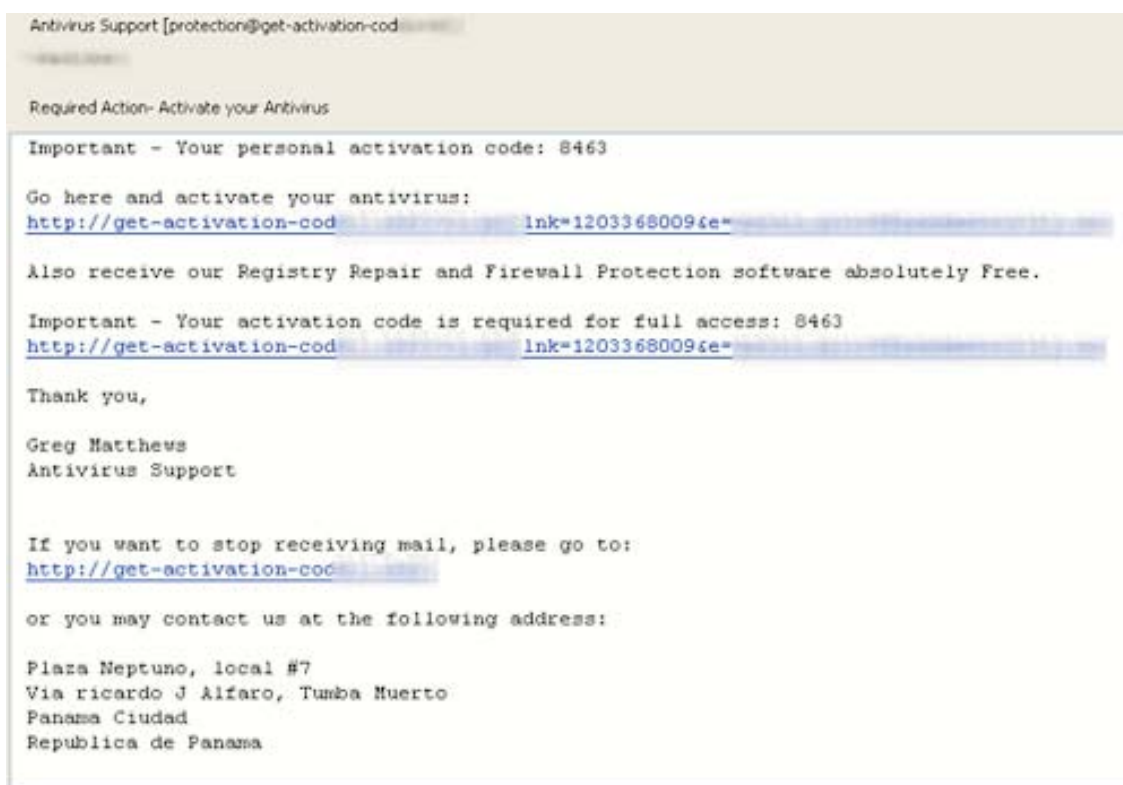


Figura 19. Mensaje de spam para distribuir Rogue AVs.

De esta manera recurren únicamente a la ingeniería social para engañar al usuario y no a través de la falsa infección del ordenador.

Los falsos antimalware en el 2008

Vías de entrada habituales

The screenshot shows a registration page for a fake anti-malware product. The header features the text 'AntiVirus Protection' and 'The Best AntiVirus Online' in blue, with a 'HACKER SAFE' logo in the top right corner. A progress bar below the header has three steps: '1. General Information', '2. Membership Choices' (highlighted in yellow), and '3. Instant Access!'. On the left, there is a 'SAVE 30%' badge with a '2 DAY PROMO ENDS' timer showing '14:08:33'. Below this is a 'Special Features' list: 'Official latest version', 'Easy to install and use', 'Fastest download time', 'Automatic free updates', 'Tutorials and guides', 'Millions of satisfied users', and '24/7 expert support'. The main content area is titled 'Membership Options and Features' and lists several benefits: '7 day Money Back Guarantee', '24/7 Expert Customer Support (Toll-free phone, email and chat)', and 'This is a flat fee with no additional costs.' It offers three membership options: '3 Year Unlimited VIP Membership & Support for ONLY €32.95 (€7.97/year (best value!))', '2 Year Full & Unlimited Access for only €11.27/year', and '1 Year Unlimited Access for only €1.57/month'. A checked checkbox offers to 'Supercharge my Internet connection with the award winning Download Accelerator for only €8.95 and download up to 300% faster!'. At the bottom, there is a 'Payment Method' section with logos for Mastercard, VISA, and a 'CreditCard' button. A small note indicates 'All funds are in Euro' with a Euro symbol.

Figura 20. Página para registrar el falso antimalware.

Los falsos antimalware en el 2008

Cifras y datos

En el tercer informe trimestral ya mencionamos el importante incremento que se había producido en la categoría de los adware, debido principalmente a estos programas de falsos antimalware. Esto produjo que durante ese trimestre el 37,49% detectado a través de los sensores de Pandalabs fuera de tipo adware, comparado con el 22,03% que se registró durante el segundo trimestre del año.

En la siguiente gráfica se puede observar la evolución de las detecciones de rogue AVs durante el año 2008.

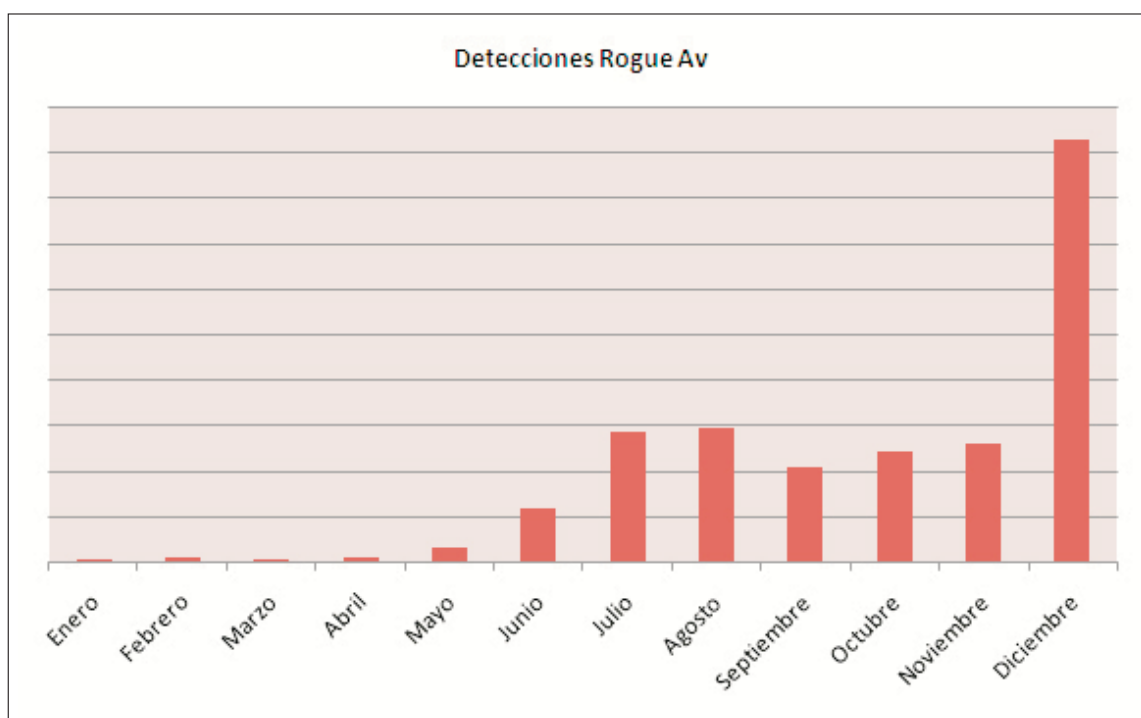


Figura 21. Detecciones de Rogue AVs durante 2008.

Se puede observar que el auge de los falsos antivirus comenzó en junio y se mantuvo muy activo durante los siguientes meses hasta el mes de diciembre donde se disparó, llegando a triplicarse el número de detecciones comparándolo con agosto, que hasta ese momento era el mes con el mayor número de detecciones de estos falsos antivirus durante el año 2008.

Los falsos antimalware en el 2008

Cifras y datos

¿Y a qué se debe ese aumento tan significativo durante el mes de diciembre? En la siguiente gráfica obtendremos la respuesta:

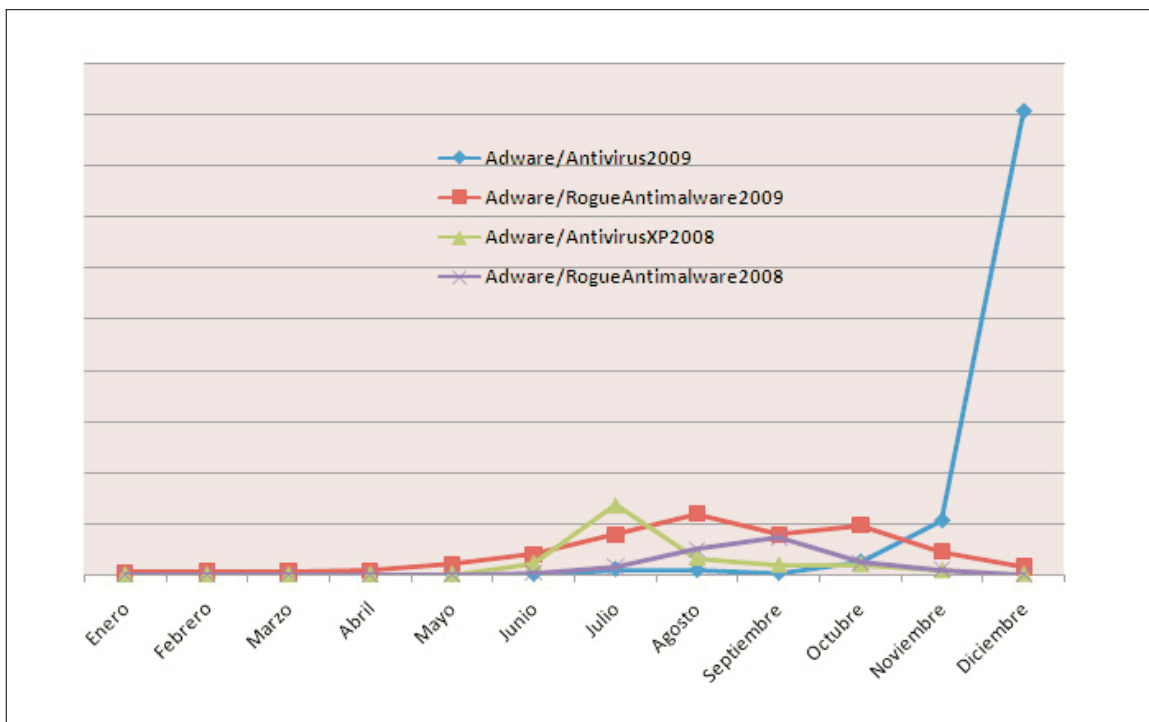


Figura 22. Rogue AVs más activos durante 2008.

Como se puede observar el culpable es el Adware/Antivirus2009 que es, sin duda, alguna el rogue AV más activo durante este año 2008.

Los falsos antimalware en el 2008

Cifras y datos

A continuación podemos observar la distribución de los rogues AVs durante el año 2008:

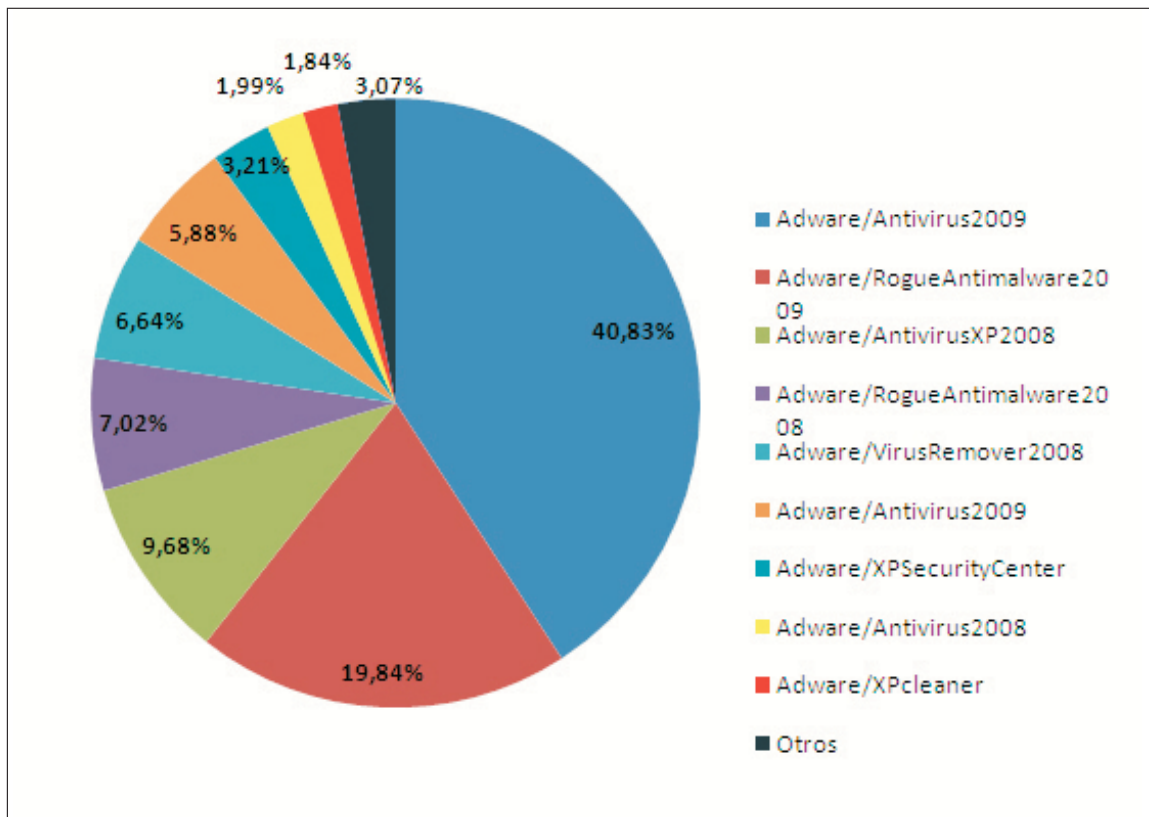


Figura 23. Distribución de los rogue AVs.

Los falsos antimalware en el 2008

Análisis a fondo: MalwareProtector2008

Entre los ejemplares que hemos analizado en estos meses, hay uno que no ha destacado por ser el más activo, pero sí por utilizar un salvapantallas un tanto curioso para asustar al usuario: unas cucarachas comiéndose el escritorio.

Cuando se ejecuta, el adware modifica el fondo de escritorio estableciendo el siguiente:



Figura 24. Fondo de escritorio establecido por MalwareProtector2008.

Los falsos antimalware en el 2008

Análisis a fondo: MalwareProtector2008

En el mensaje se puede leer lo siguiente:

¡Aviso! ¡Spyware detectado en su ordenador! Instale un antivirus o un antispysware para desinfectar su ordenador.

De esta manera tan llamativa, consigue hacer creer al usuario que su ordenador está infectado.

Posteriormente, muestra un mensaje en el que se alerta al usuario de que su ordenador contiene un adware diseñado para robar contraseñas o información bancaria:

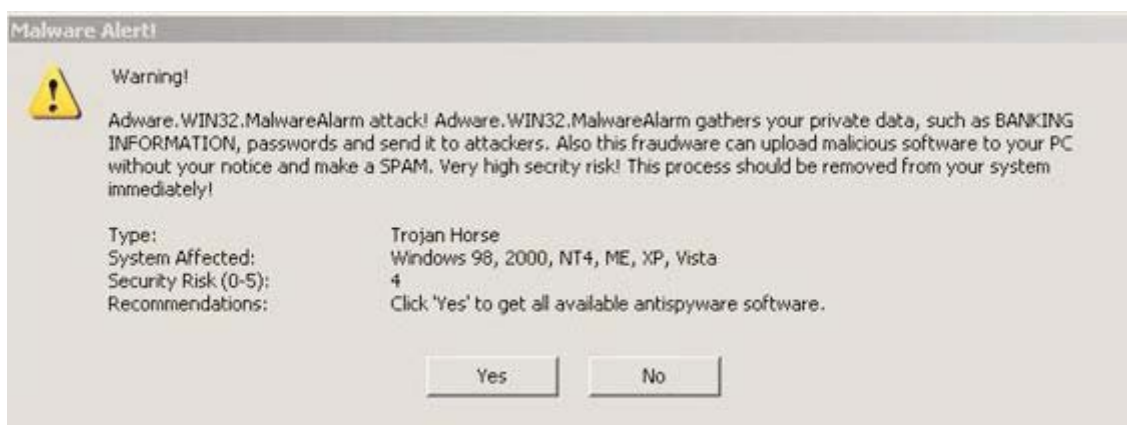


Figura 25. Mensaje de alerta mostrado por MalwareProtector2008.

Los falsos antimalware en el 2008

Análisis a fondo: MalwareProtector2008

Además, se le insta a que elimine dicha amenaza del sistema lo antes posible. Para ello, se le ofrece un software antispyware que desinfectará el ordenador:

En el caso de que no aceptemos el mensaje, se ejecutará cada cierto tiempo un salvapantallas que simula unas cucarachas comiéndose el escritorio:



Figura 26. Salvapantallas mostrado por MalwareProtector2008.

Los falsos antimalware en el 2008

Análisis a fondo: MalwareProtector2008

Esta es otra de las técnicas utilizadas para conseguir que el usuario acabe aceptando el mensaje y descargando un falso programa antivirus.

Si se acepta el mensaje, se procederá a la descarga del falso programa antimalware. Una vez descargado, el programa comenzará a realizar un análisis del ordenador en busca de posible malware.

El resultado del análisis es engañoso y muestra una serie de amenazas que supuestamente han infectado el ordenador:

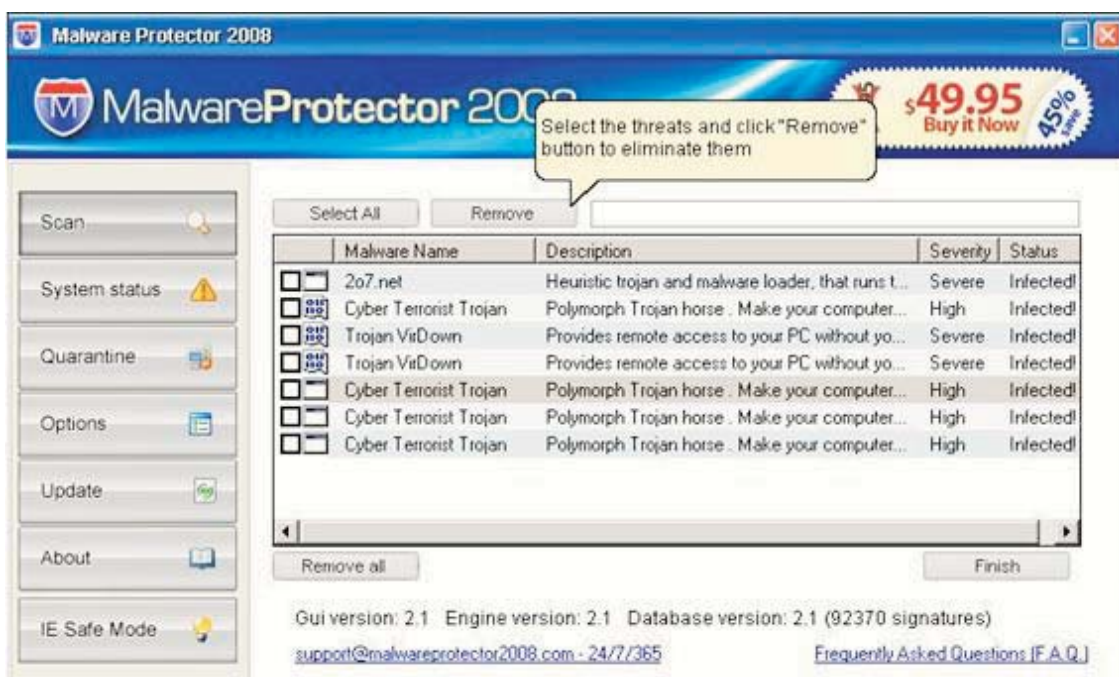


Figura 27. Resultado del análisis realizado por MalwareProtector2008.

Los falsos antimalware en el 2008

Análisis a fondo: MalwareProtector2008

Si seleccionamos la opción de eliminar el malware, se mostrará una ventana indicando que el ordenador está infectado con adware y spyware y que es aconsejable registrarse para eliminar dichas amenazas y estar protegido:



Figura 28. Interfaz del MalwareProtector2008.

Los falsos antimalware en el 2008

Análisis a fondo: MalwareProtector2008

Para poder registrarnos, deberemos abonar la cantidad que se indica en la página web a la que se nos redirige al pulsar el botón para obtener el modo completo de la aplicación:



Figura 29. Página web del MalwareProtector2008.

Una vez nos hayamos registrado y abonado la correspondiente cantidad, el ordenador continuará desprotegido y vulnerable frente a otro tipo de amenazas.

Las características de este adware son muy similares a las del resto de falsos antimalware: los mensajes de alerta que muestra, la interfaz de la aplicación, el modo de actuación...por lo que este análisis detallado facilitará a los usuarios la identificación de este tipo de programas.

Los falsos antimalware en el 2008

Consejos

El spam es el medio habitual utilizado para distribuir este tipo de programas, por lo tanto hay que tener especial precaución con los mensajes de correo electrónico que recibimos con noticias o asuntos llamativos. En estos emails se invita al usuario a seguir un enlace para poder ver el vídeo o las imágenes de esa falsa noticia. Por lo tanto, no debemos hacer clic en los enlaces incluidos en este tipo de mensajes, ya que en tal caso podríamos estar descargando en el ordenador uno de estos falsos antimalware.

Desconfía de aquellos programas que no recuerdas haber instalado y que comienzan a mostrar falsas infecciones o ventanas emergentes en los que se te invita a comparar algún tipo de antivirus. Lo más seguro es que en tu equipo se haya instalado alguno de estos programas maliciosos.

Es importante mantener actualizados todos los programas. Un programa no actualizado puede ser un programa vulnerable. Por ello, conviene mantener actualizados todos los programas que se tengan instalados en el equipo, ya que muchos de estos códigos maliciosos utilizan vulnerabilidades existentes en los ordenadores para introducirse en éstos e infectar el equipo.

Es conveniente analizar cada cierto tiempo el equipo con un antivirus de confianza, de modo que si alguno de estos ejemplares está residente en el equipo, pueda ser detectado y eliminado.

Sin duda los falsos antimalware o rogue AVs se han convertido en uno de los principales protagonistas de este año 2008. Esta nueva familia está reportando cuantiosas cantidades de dinero a sus creadores y podemos asegurar que aún no ha llegado a su fin. El mes de diciembre ha sido el más activo para estos falsos antivirus, triplicando en número de detecciones a su predecesor, por lo que no nos augura que en el comienzo del 2009 mejore la situación. Esperemos que en el primer informe trimestral del 2009 tengamos que rectificar estas palabras.

Tendencias del 2008

Durante 2008, una de las amenazas que más ha crecido han sido los falsos antivirus. Se trata de un tipo de adware que se hace pasar por una solución de seguridad y que, una vez ejecutado en un ordenador, hace creer al usuario que está infectado con decenas de ejemplares de malware distintos para, a continuación, intentar venderle la versión de completa del antivirus que soluciona ese falso problema. El objetivo, por supuesto, es obtener beneficios económicos con las infecciones. Según nuestros datos, estos ciberdelincuentes estarían obteniendo más de diez millones de euros al mes.

Por otro lado, distintos estudios que hemos realizado han demostrado cómo la crisis económica que experimentan diversos países a nivel mundial se ha convertido en un arma para los ciberdelincuentes. En 2008 hemos podido comprobar cómo a cada bajada de la bolsa le seguía una subida de los nuevos ejemplares de malware aparecidos y cómo a cada subida del paro le seguía un aumento en el envío de spam, especialmente, del relacionado con las falsas ofertas de trabajo y destinados a captar muleros (personas destinadas a mover el dinero procedente de acciones ilegales de una cuenta a otra para blanquearlo).

Los ciberdelincuentes aprovechan la necesidad de trabajo de la gente para intentar captarlos con ofertas suculentas. En otras ocasiones, esas ofertas son de otro tipo como falsas hipotecas o créditos que, en realidad, persiguen que el usuario proporcione sus datos bancarios a los ciberdelincuentes.

El uso cada vez más extendido de las redes sociales ha causado que éstas sean también cada vez más utilizadas por los ciberdelincuentes para distribuir sus creaciones.

La infección de páginas web legales o no, mediante ataques de inyección de SQL, ha sido otra de las tendencias en alza durante 2008.

La utilización de virus de boot (que sustituían el Master Boot Record o disco cero original por uno falso) para ocultar troyanos ha sido otra de las nuevas técnicas crecientes en 2008 y que seguirá en aumento el próximo año. Realmente esta es una técnica muy antigua que fue muy popular al principio de los años 90, pero en los últimos años prácticamente había desaparecido hasta que ha sido rescatada este año. Lo más probable es que a lo largo de 2009 veamos ésta y otras técnicas que aun siendo antiguas pueden ser muy eficaces para ocultar malware.

Por último, el aumento del malware, que ya vaticinamos en 2007, ha sido otro de los aspectos destacados en 2008. Con una media de 22.000 ejemplares recibidos al día en nuestros laboratorios, en los primeros 8 meses de 2008 ya habíamos detectado más ejemplares de malware que en todos los años de vida de Panda, lo que supone un crecimiento impresionante de las nuevas amenazas, del que muchos usuarios parecen no tener conciencia.

Para 2009, se espera que esas cifras continúen en aumento. Respecto a las formas de distribución, las redes sociales serán cada vez más explotadas, y ya no sólo por gusanos que se propagan de un usuario a otros, sino por códigos maliciosos diseñados para llevar a cabo acciones más dañinas como el robo de datos confidenciales. Igualmente, la distribución de malware utilizando los ataques de inyección SQL seguirá en aumento.

Tendencias del 2008

Una tendencia que comenzará a tomar notoriedad en 2009 será el uso de packers y ofuscadores más personalizados. Este tipo de herramientas son utilizadas desde hace años para tratar de evitar que los antivirus detecten las muestras de malware. En principio han utilizado versiones de estas herramientas existentes en el mercado, pero cada vez se están decantando más por desarrollar versiones "privadas" de tal forma que las compañías antivirus tengamos más dificultades a la hora de poder acceder al código malicioso original.

Parecida razón tendrá el rebrote de códigos maliciosos clásicos como los virus que prevemos para 2009. El uso de tecnologías de detección cada vez más sofisticadas, como nuestra Inteligencia Colectiva, capaces de detectar incluso ataques de bajo nivel y las técnicas de malware más novedosas, provocará que los ciberdelincuentes comiencen a hacer uso de viejos códigos, pero adaptados a las nuevas necesidades. Es decir, ya no serán virus destinados a evitar el buen funcionamiento del sistema o la apertura de archivos, como hace una década, sino que servirán, por ejemplo, para ocultar troyanos destinados al robo de información bancaria.

Para finalizar el informe, destacar una de las iniciativas más importantes que se han llevado a cabo este año. En enero de 2008 tuvo lugar el nacimiento oficial de AMTSO (AntiMalware Testing Standards Organization). Panda fue la empresa anfitriona que organizó este evento en Bilbao. Allí se fijaron las bases sobre las que iba a trabajar el grupo, y a lo largo de 2008 celebramos nuevas reuniones en Holanda, organizado en este caso por Norman, en Seattle, organizado por Microsoft y en Oxford, organizado por Sophos. En esta última reunión finalizamos dos documentos en los que habíamos estado trabajando durante todo el año.

Por un lado, el "Fundamental Principles of Testing", con las principales recomendaciones de cómo realizar tests de soluciones antimalware que deben ser seguidas tanto por testers, editores y fabricantes.

Por otro lado, el "Best Practices for Dynamic Testing", con la recomendación de las mejores prácticas a la hora de probar la eficacia de productos antimalware ante un ataque real.

En 2009 ya tenemos planificadas las dos próximas reuniones: a principios de febrero nos reuniremos en Mountain View, Estados Unidos, para trabajar en los nuevos documentos que estamos preparando. Esta reunión está organizada por Symantec. En mayo tendrá lugar una nueva reunión en Budapest, organizada en esta ocasión por VirusBuster.

En la web de AMTSO (www.amtso.org) se pueden descargar los dos documentos arriba comentados y consultar todas las noticias relativas a esta organización.

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/>