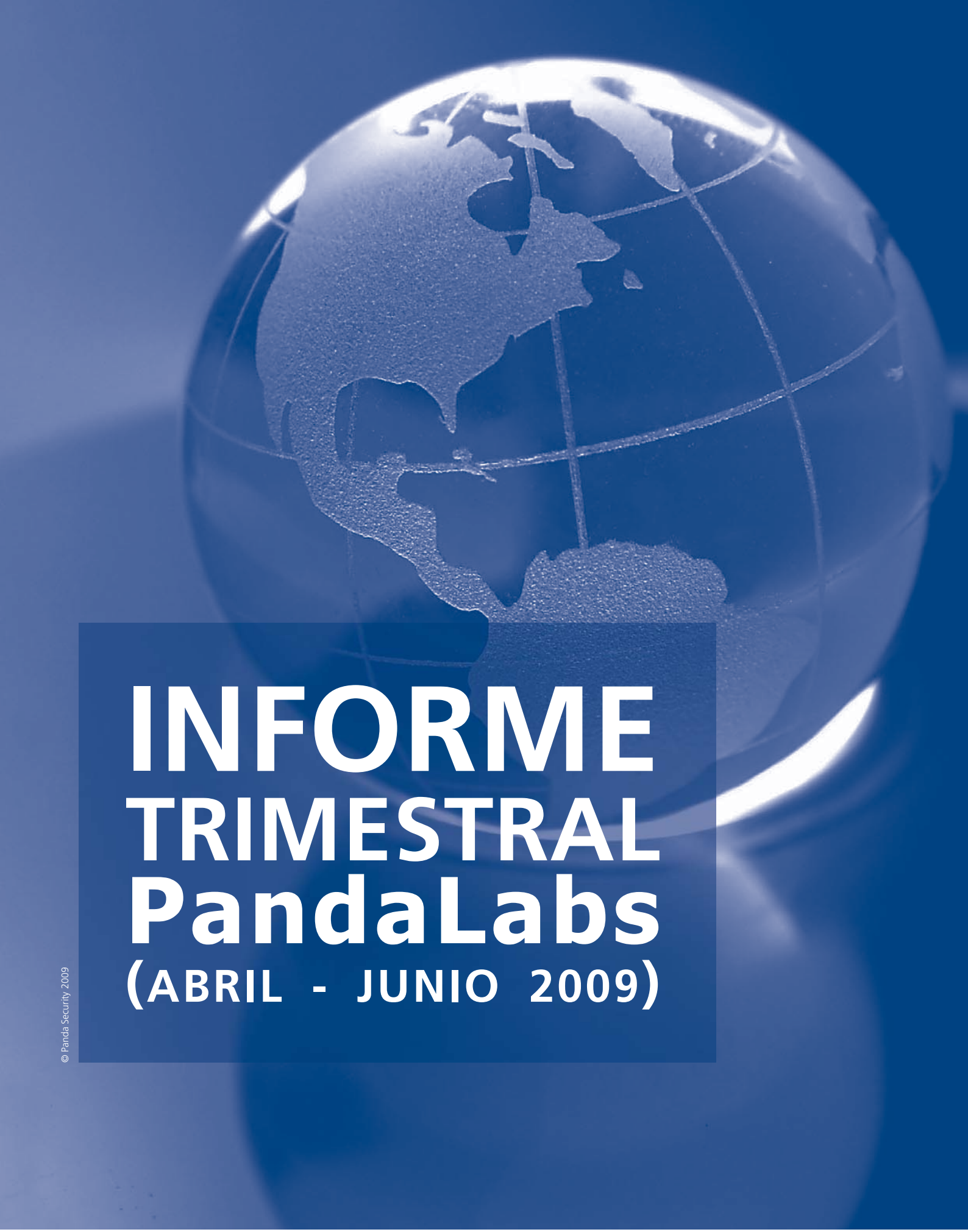

INFORME TRIMESTRAL PandaLabs

(ABRIL - JUNIO 2009)

PANDA SECURITY | *One step ahead.*

Índice

Introducción

Ya hemos alcanzado el ecuador del año 2009 y presentamos el segundo informe trimestral en el que analizaremos los temas más destacados de estos tres meses.

Durante este período hemos detectado la proliferación de dos temáticas utilizadas para distribuir spam con malware: las felicitaciones electrónicas o e-cards y las falsas notificaciones enviadas por empresas de mensajería. Analizaremos cuáles son las familias de malware que han sido distribuidas en estos mensajes.

Pero, si hay una familia capaz de adaptar la temática de los mensajes en los que se distribuye según las circunstancias, esa es la del gusano Waledac. San Valentín, la renuncia de Obama a la presidencia de EEUU y vales descuento en tiempos de crisis, son solo algunos ejemplos de los temas elegidos por esta familia.

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

Por otra parte, analizaremos las tendencias más destacadas del trimestre en lo que a malware se refiere. Las técnicas BlackHat SEO parece que cobran fuerza este trimestre. Youtube y Twitter están en el punto de mira y han sido utilizados para distribuir links maliciosos. La creciente popularidad de estos servicios no pasa desapercibida para los ciber-delincuentes.

Se cumplen dos años de la Inteligencia Colectiva. Explicaremos en qué consiste esta tecnología y lo acompañaremos con cifras que no dejan lugar a dudas de que se trata de una tecnología innovadora y adaptada a las nuevas necesidades de la lucha contra el malware.

Asimismo, como en anteriores informes, presentaremos la evolución de malware activo por países durante el primer semestre de 2009 y las cifras de malware del presente trimestre.

Esperamos que os resulte interesante.

Resumen ejecutivo

Este trimestre el adware se mantiene dentro de los niveles habituales de infección hasta situarse en un 19,62%. Aún así, la primera posición sigue siendo para los troyanos, con un 34,37%.

La media de malware activo durante este semestre asciende al 12,48%, inferior al 14,62% del año 2008.

Una vez más, Taiwán continúa siendo de forma clara el país con más malware activo, con un 33,63%. Ya por debajo del 30% nos encontramos a Turquía (28,96%) y Polonia (27,54%).

En los últimos meses dos tipos de temáticas han sido las que más han llamado la atención de los expertos en seguridad: falsos correos de empresas de mensajería y envíos de felicitaciones o postales electrónicas.

En abril se crearon más de 1 millón de links maliciosos para que los usuarios que buscaran términos relacionados con Ford acabaran en una de estas páginas maliciosas. Días después, la marca afectada fue Nissan.

En mayo se crearon cuentas de Youtube para que comenzaran a crear comentarios que incluyeran links maliciosos de forma automatizada. En total se crearon más de 30.000 comentarios con links maliciosos.

En junio Microsoft marcó una cifra récord en el número de vulnerabilidades corregidas desde que comenzó con su ciclo mensual: un total de 31.

Inteligencia Colectiva recibe 50.000 ficheros diarios, de los que 35.000 son nuevo malware. El 99,4% se procesan automáticamente por Inteligencia Colectiva con una media de 6 minutos por cada resolución.

Durante el primer trimestre de 2009, Inteligencia Colectiva procesó 4.474.350 ficheros.

Las cifras del segundo 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 segundo trimestre de 2009:

APARICIÓN DE NUEVO MALWARE TRIMESTRAL

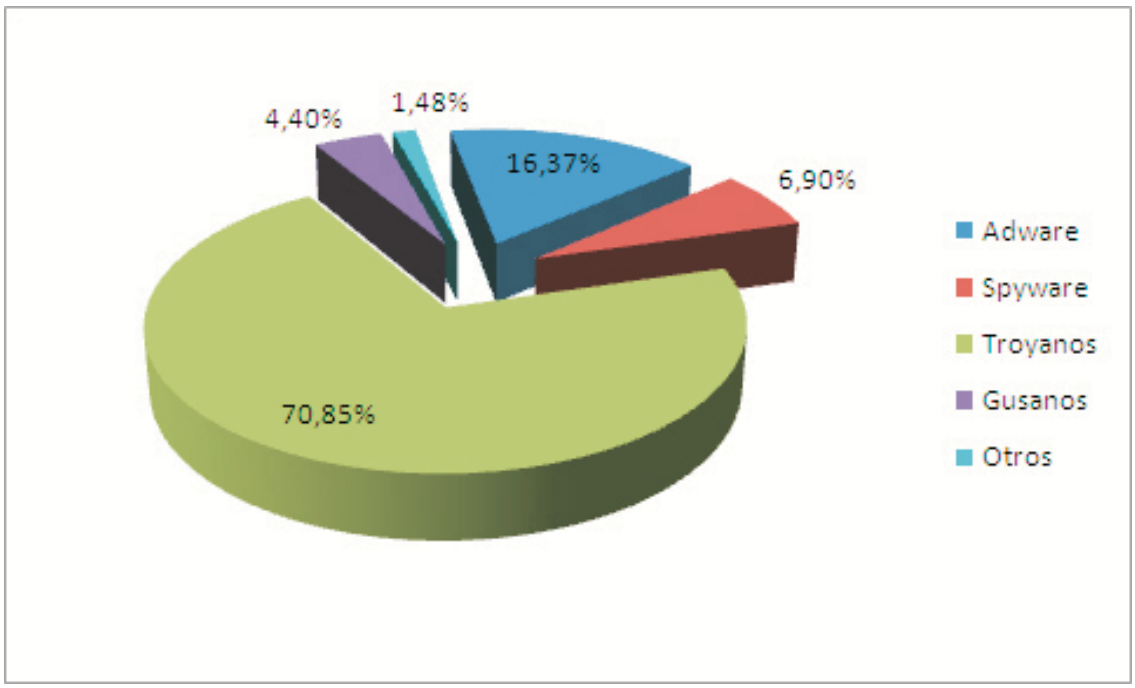

Figura 1. Aparición trimestral de malware.

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 2,97% con respecto al trimestre anterior, hasta situarse en un 70,85%.

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

En cuanto a la categoría de los gusanos, su porcentaje se ha visto incrementado ligeramente, un 1,15%, hasta suponer actualmente un 4,40% 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 segundo trimestre

Por otra parte, lo más destacable es el considerable descenso del malware tipo Spyware, un 6,25%, hasta situarse en un 6,90% del total, siendo ese descenso contrarestado por el incremento de la categoría de Adware, un 7,54%, situándose así en la segunda categoría de malware más detectada durante el segundo trimestre de 2009, con un ratio situado en el 16,37%.

La predisposición por parte de los ciberdelincuentes en seguir desarrollando el tipo de adware conocido como Rogue AV (falsos programas antivirus), y la efectividad de los mismos está ligada directamente al incremento de esta última categoría. Hemos agrupado dentro de la categoría de Otros las categorías que tienen poca relevancia sobre el total.

CLASIFICACIÓN TIPO OTROS

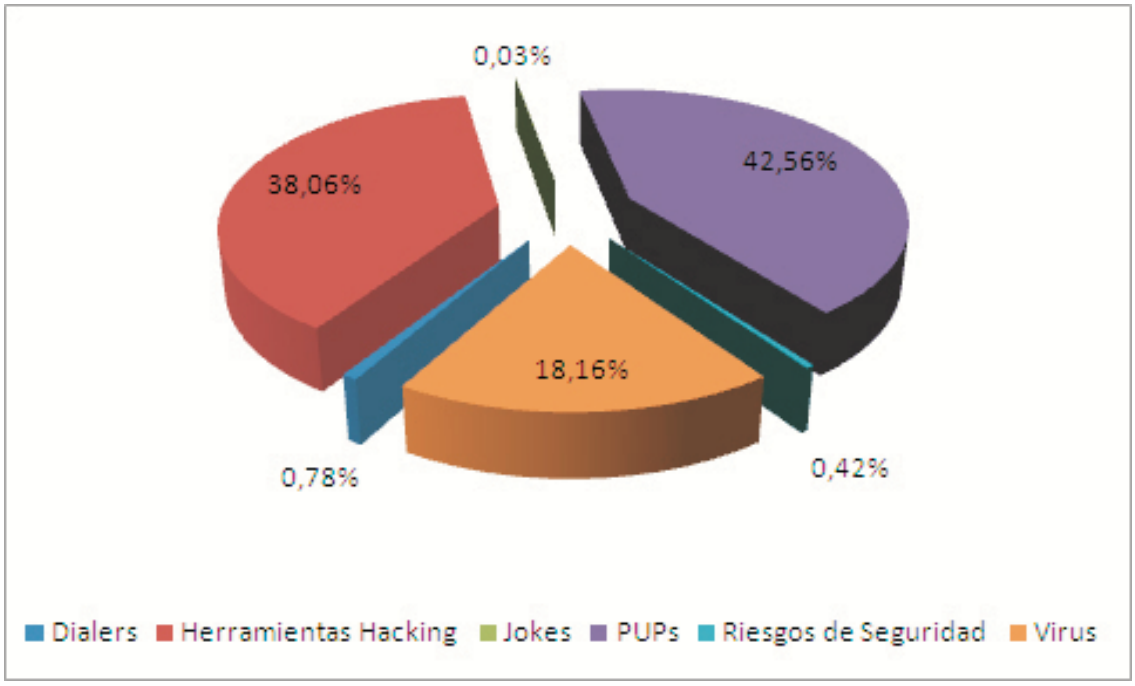

Figura 2. Clasificación de la categoría de Otros.

En esta sección observamos que los tipos de malware predominante son los PUPs y las herramientas de hacking, pese al ligero descenso que han tenido ambos a lo largo del trimestre, situándose en un 42,56% y 38,06% respectivamente.

Sin embargo cabe destacar el creciente aumento de los Virus situados en un 18,16% tras aumentar un 9,82% con respecto al anterior trimestre.

El paulatino descenso de clientes de Internet con conexión telefónica en detrimento de la banda ancha, hace que los dialers se mantengan en una cuota prácticamente imperceptible, 0,78%.

Las cifras del segundo 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:

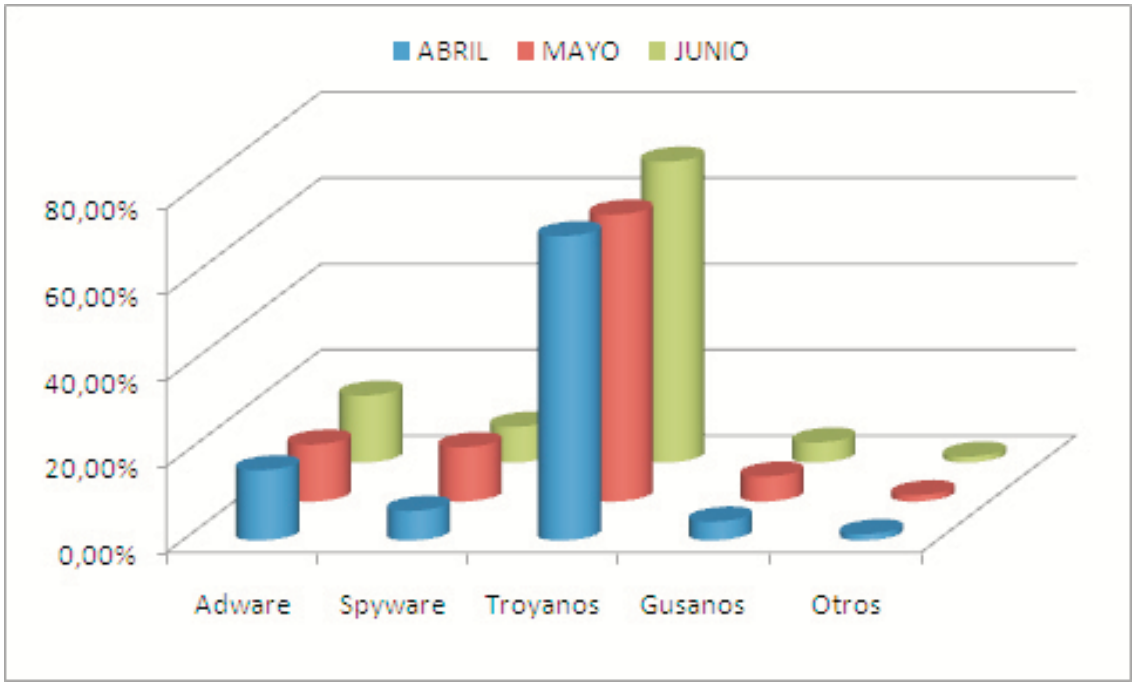

Figura 3. Evolución en la aparición de nuevo malware.

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 segundo trimestre

Amenazas detectadas por los Sensores PandaLabs

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

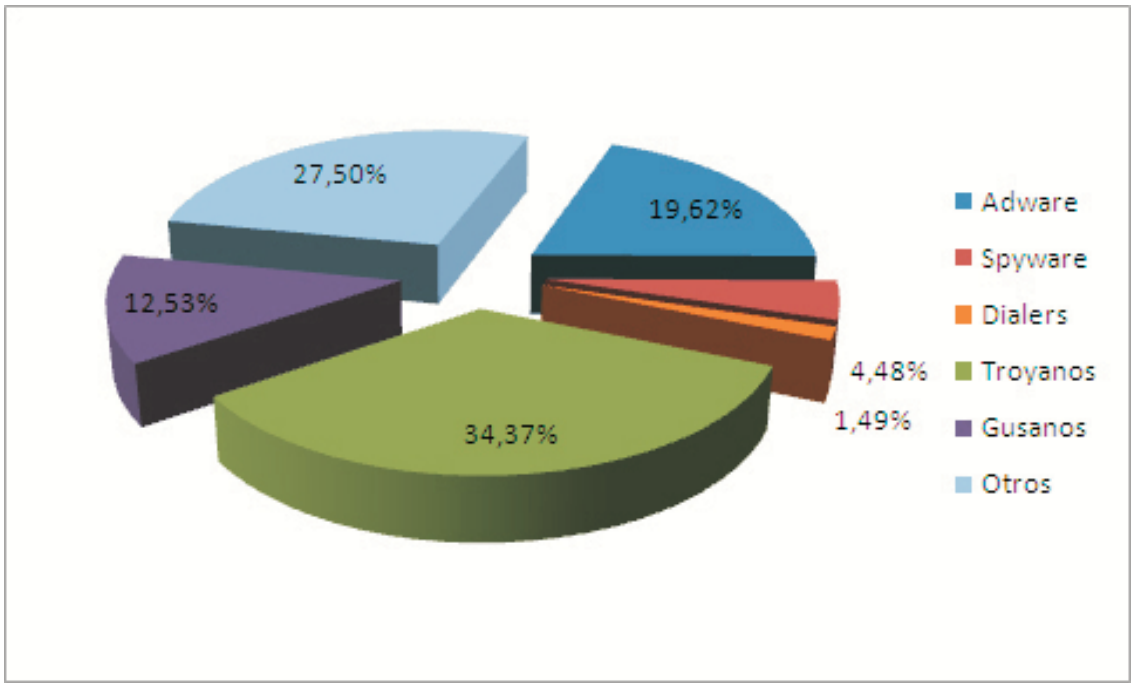

Figura 4. Distribución detecciones por sensores Pandalabs.

En este trimestre el adware se mantiene dentro de los niveles habituales de infección hasta situarse en un 19,62%, lo cual sigue dejando paso, a que la primera posición de malware predominante sigan siendo los troyanos con un 34,37%, habiéndose incrementado estos últimos un 2,86% con respecto al trimestre anterior.

Observamos también en los gusanos, un ligero crecimiento del 0,89%, manteniendo así su estatus de códigos significativos debido a la rapidez de su difusión/propagación a otros sistemas.

Los dialers, situándose en un 4,48%, siguen resistiéndose a desaparecer a pesar de la tendencia descendente que continúa durante los últimos años.

Las cifras del segundo trimestre

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

01	Trj/Downloader.MDW
02	Spyware/Virtumonde
03	Trj/Rebooter.J
04	Trj/Lineage.BZE
05	W32/Bagle.RP.worm
06	Adware/AccesMembre
07	Adware/SystemSecurity
08	W32/Waledac.AS
09	Adware/Lop
10	W32/AutoRun.DJ.worm

Figura 5. Top ten de amenazas detectadas

Malware activo

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

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

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

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

Hemos realizado un seguimiento sobre la evolución de malware activo mes a mes a través de nuestra 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 on-line 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 semestre del año 2009:

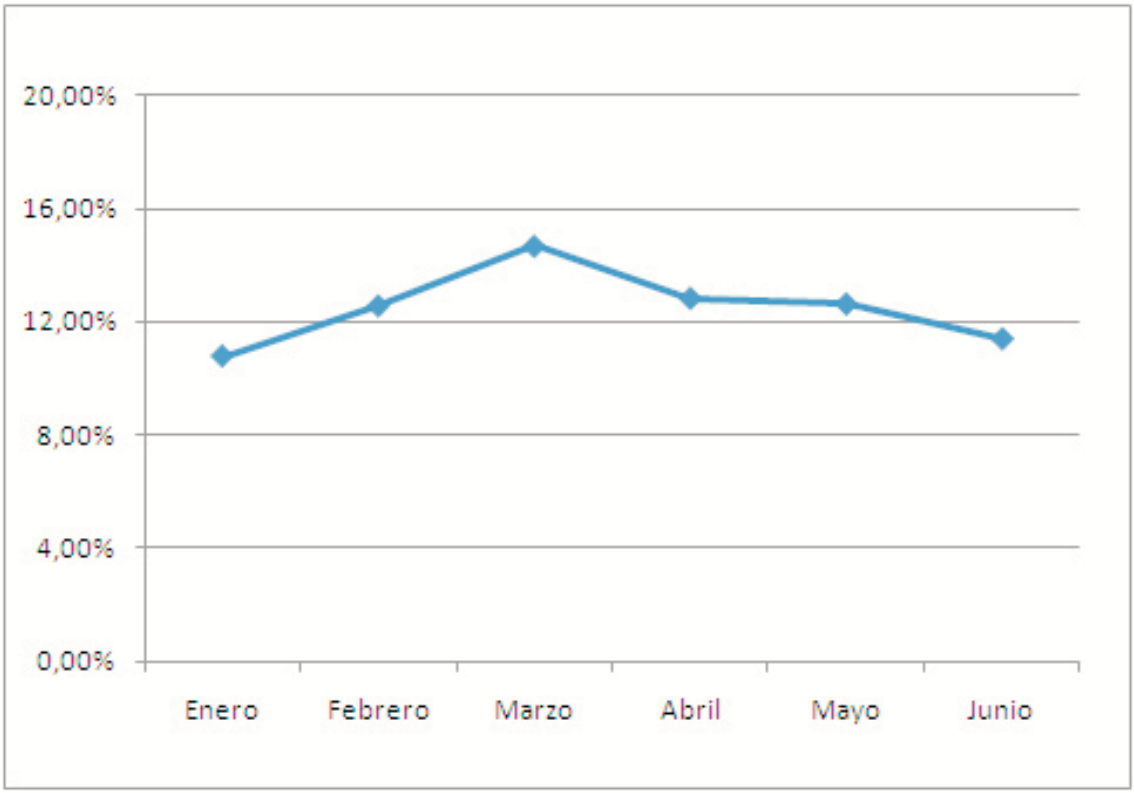

Figura 7. Evolución de malware activo durante primer semestre 2009.

Enero empezó con el ratio más bajo de todo el primer semestre de este año 2009 con el 10,78% de PCs infectados. Los siguientes dos meses fueron en aumento llegando en marzo al 14,68%, el ratio más alto de PCs infectados con malware activo de los primeros 6 meses del 2009. Marzo supuso un punto de inflexión y a partir de ahí empezó a disminuir paulatinamente hasta llegar al 11,39% registrado en junio.

La media de malware activo durante este semestre asciende al 12,48%, inferior al 14,62% de PCs infectados con malware activo durante el año 2008.

Estos datos reflejan la evolución a nivel global pero, ¿qué ocurre en cada país? En la siguiente gráfica podemos observar la infección de los países con mayor porcentaje entre los países con mayor número de análisis en Infected or Not y a través de ActiveScan 2.0 durante el primer semestre de este año 2009.

Malware activo

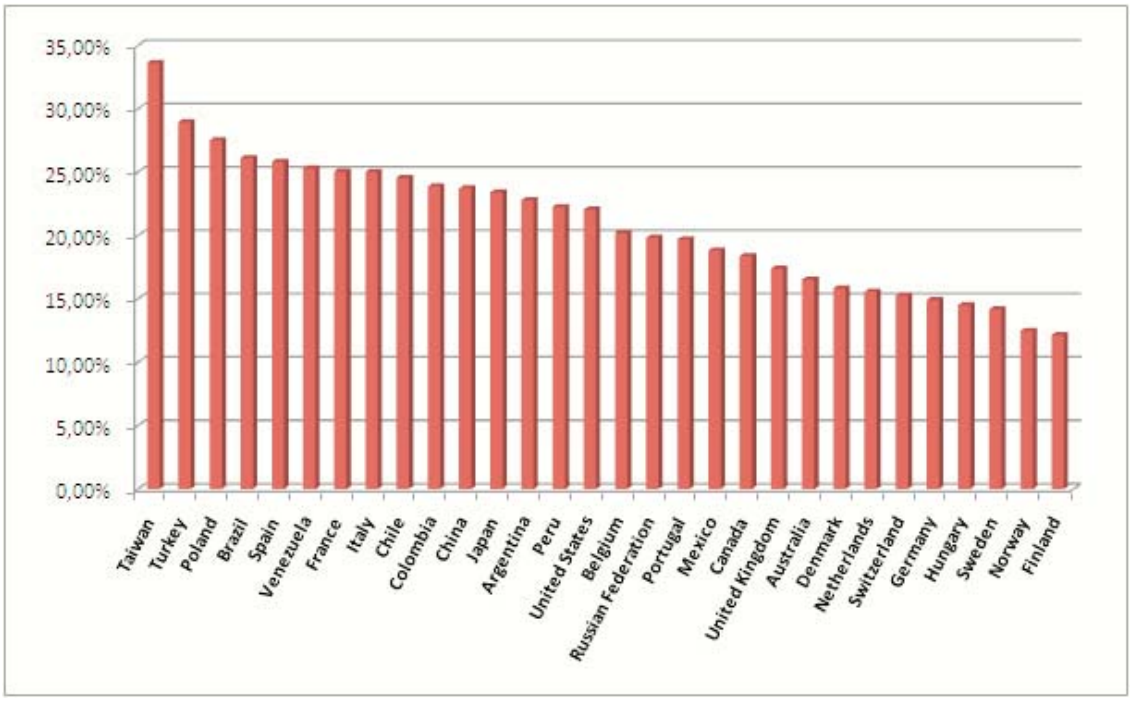

Figura 8. Países con mayor porcentaje de malware (Enero-Junio 2009).

Una vez más Taiwán continúa siendo de forma clara el país con más malware activo con el 33,63%. Ya por debajo del 30% nos encontramos a Turquía (28,96%) y Polonia con un 27,54%. A destacar también de forma positiva a los países nórdicos como Suecia (14,2%), Noruega (12,48%) y Finlandia (12,17%) como los 3 países con el menor número de PCs infectados con malware activo durante el primer semestre del 2009.

Tendencias en el envío de malware a través del spam

Cada vez surgen nuevas amenazas más sofisticadas y complejas de detectar, capaces de infectar nuestros equipos a través de vulnerabilidades muy complejas de descubrir. A pesar de ello, la ingeniería social utilizando como medio de distribución los mensajes de correo electrónico sigue siendo una de las técnicas más utilizadas, convirtiéndose en una de las principales entradas de malware en nuestros equipos.

En los últimos meses dos tipos de temas han sido los que más han llamado la atención de los expertos en seguridad: falsos correos de empresas de mensajería y envíos de felicitaciones o postales electrónicas, siendo estos últimos los que mayor tráfico han generado.

El contenido de estos mensajes suele ser corto y en texto plano. En el caso de los e-cards se nos indica que un conocido o familiar nos ha enviado una tarjeta de agradecimiento y en los casos de empresas de mensajería se nos indica que un pedido no ha podido ser entregado, por lo que nos adjuntan una hoja de seguimiento.

A continuación pueden verse ejemplos de estos mensajes:

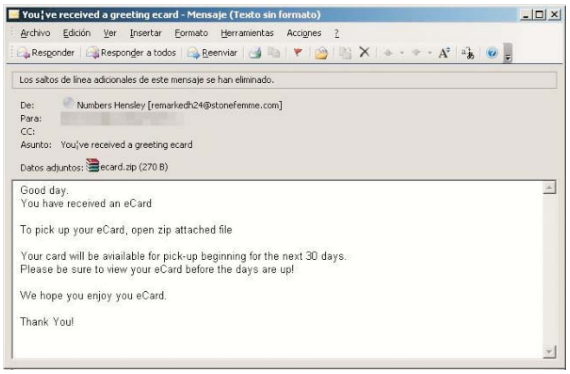

Figura 9. Mensaje tipo e-card.

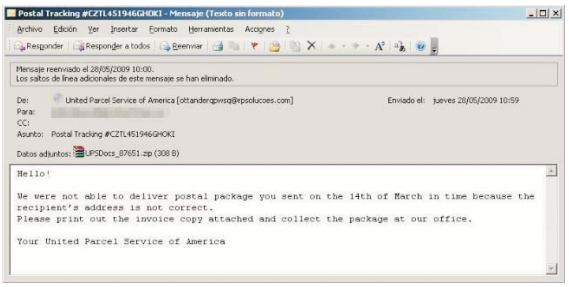

Figura 10. Mensaje tipo empresa de mensajería.

Tendencias en el envío de malware a través del spam

Para comprobar el tráfico que han generado este tipo de mensajes, hemos monitorizado un pequeño servidor de correo y en él hemos detectado diferentes picos de este tipo de mensajes:

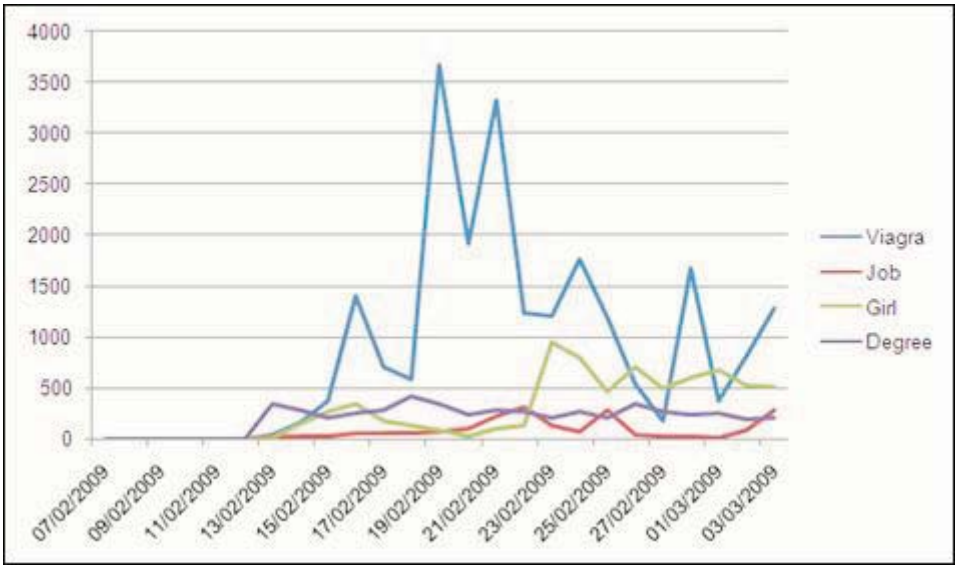

Figura 11. Número de mensajes tipo e-card/mensajería en los últimos dos meses.

Estas "oleadas" son controladas por las mafias propietarias de las redes de bots[1], encargadas de enviar este tipo de spam por lo que los envíos atienden a estrategias o necesidades de sus propietarios.

Son ataques muy localizados en el tiempo pero cuyo volumen y tamaño hace que requiera de muchos recursos de nuestros sistemas. El tipo de malware que se esconde tras estos reclamos varía tanto de familia como de variantes dentro de una misma familia. Por tanto, es necesario monitorizar este tipo de amenazas con el fin de actualizar nuestros sistemas de seguridad con las últimas versiones.

[1] Las redes de bots están compuestas por ordenadores infectados por algún tipo de malware "bot" instalado en el equipo sin el conocimiento del usuario y que son controlados de forma remota para llevar a cabo diferentes acciones, por lo general envío de spam y ataques orientados a otras máquinas.

Tendencias en el envío de malware a través del spam

A continuación detallamos mediante gráficas las principales familias que han sido enviadas mediante estos reclamos.

En el caso de la e-cards podemos encontrar más variedad de malware. Aun así, es posible diferenciar dos grandes tipos de malware: familias de spammers, como Spamta y Spamtaload, y malware bancario, como Banker y Goldun.

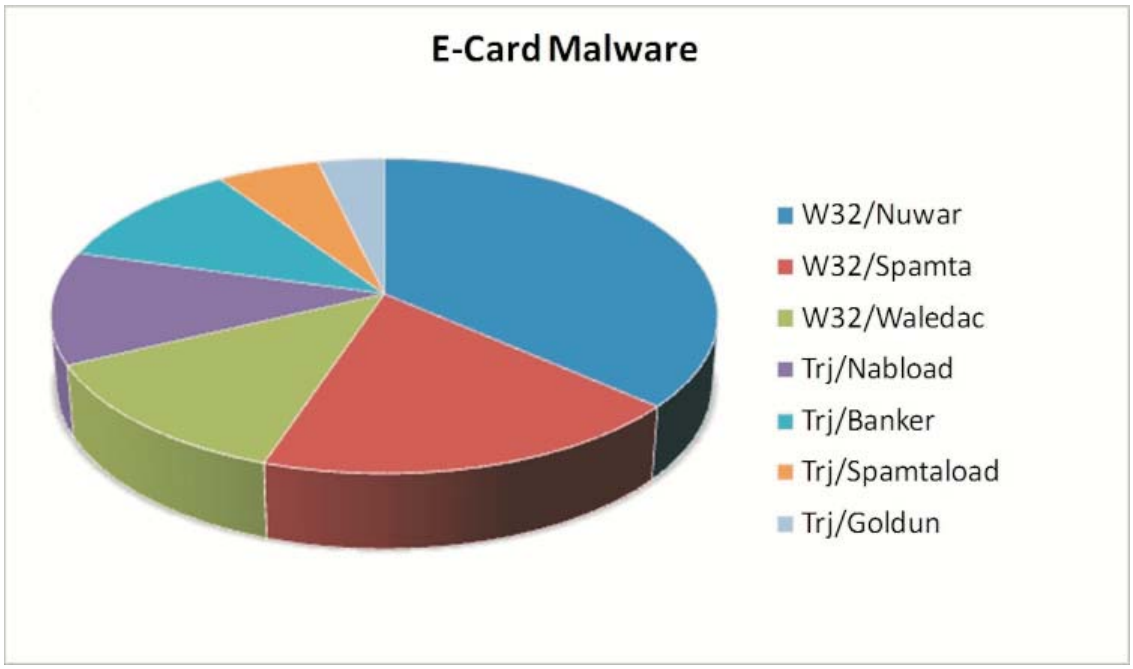

Figura 12. Distribución de tipos de malware en e-cards.

De todos modos, las nuevas oleadas de e-card indican que un nuevo tipo de malware está siendo enviado en los últimos días. Se trata del adware del tipo rogueware detectado como PrivacyCenter. No está incluido en esta gráfica, ya que el volumen de muestras recogido hasta ahora es muy bajo en comparación con muestras más antiguas.

En el caso de los mensajes de empresas de mensajería, la inmensa mayoría de malware enviado es de tipo bancario, destacando dos en particular: Sinowal y Buzus (minoritario).

Tendencias en el envío de malware a través del spam

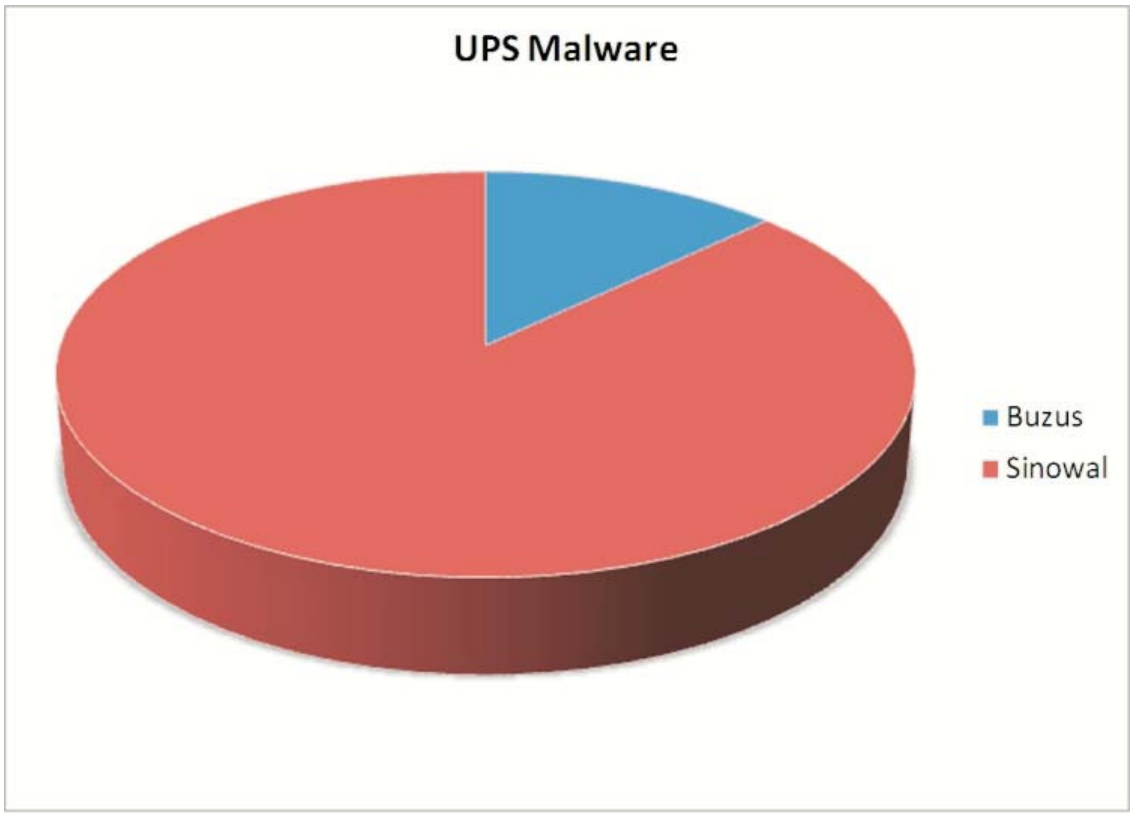

Figura 13. Distribución de tipos de malware en spam de mensajería.

El malware suele llegar comprimido con contraseña para evitar levantar sospechas y que los sistemas antivirus detecten el contenido del archivo.

Por tanto, ante este tipo de amenazas no solo es importante disponer de un buen software de seguridad en el equipo sino también de una actitud de alerta y prudente ante este tipo de ataques de ingeniería social. Sobre todo teniendo en cuenta que muchas de las amenazas que se distribuyen en estos correos son del tipo malware bancario, cuyo fin es obtener beneficios económicos mediante el robo de información bancaria.

Vulnerabilidades Q2 2009

En el mes de abril Microsoft publicó 8 boletines de seguridad, del MS09-009 al MS09-016. Como viene siendo habitual, aparecieron nuevas vulnerabilidades que afectaban al navegador web Microsoft Internet Explorer. Estas vulnerabilidades permitían la ejecución remota de código en el sistema con tan solo visitar una página web maliciosa. De esta forma tan sencilla se podría ver totalmente comprometida la máquina del usuario afectado.

Sin embargo, no sólo Internet Explorer fue castigado como navegador web, Mozilla lanzó una nueva versión de su navegador web Firefox, la 3.0.7, para solucionar 8 fallos de seguridad, de los cuales 6 eran críticos y al igual que en Internet Explorer a través de estos fallos se podía llegar a ejecutar código remoto utilizando la técnica antes comentada.

Entre los boletines publicados queremos destacar el MS09-009, una vulnerabilidad crítica en Microsoft Excel que ya estaba siendo utilizada por usuarios maliciosos para instalar malware en los sistemas vulnerables, y los boletines MS09-012 y MS09-015 que solucionaban varias vulnerabilidades que permitían a un usuario local la escala de privilegios en el sistema.

El mes abril Adobe también daba a conocer la existencia de un nuevo "0 day"[2] en sus productos Acrobat y Reader para todas las plataformas disponibles (Windows, Linux y MacOS). El fallo se encontraba en la función "getAnnots" y un atacante podía crear un PDF malicioso para aprovechar esta vulnerabilidad y de esta forma ejecutar código malicioso en el sistema de un usuario que intentase visualizar este documento PDF.

Entrando ya en el mes de mayo, Adobe corrige la vulnerabilidad crítica antes mencionada mientras que Microsoft sólo publica un boletín de seguridad, el MS09-017, dedicado a solucionar 14 vulnerabilidades que se habían descubierto en Microsoft PowerPoint. Estas vulnerabilidades también estaban siendo aprovechadas por los usuarios maliciosos nuevamente con el objetivo de instalar malware en los sistemas vulnerables. Además, la posibilidad de infección y propagación a través de estos ficheros de PowerPoint maliciosos es muy superior a la de otros ficheros.

PowerPoint, es un formato de fichero ampliamente utilizado para realizar presentaciones. No obstante, también es conocido en Internet como formato de fichero para disfrutar unos minutos leyendo historias divertidas o viendo las últimas fotos graciosas que circulan por Internet, entre otras cosas. Debido a estos factores, la mayoría de los usuarios confía en los documentos PowerPoint y además tienen la curiosidad y el deseo de querer ver el contenido de esa nueva y desconocida presentación que ha llegado a su bandeja de correo electrónico aunque no conozcan a su remitente.

En el mes de junio también se publicó una grave vulnerabilidad en el servidor web Microsoft Internet Information Server (IIS) denominada MS09-020. Las características y el método de explotación de este nuevo "0 day" hacían recordar las viejas vulnerabilidades descubiertas algunos años atrás en el servidor web de Microsoft. Por poner un ejemplo, la vulnerabilidad "Web Server Folder Traversal", descubierta en el año 2000 fue ampliamente utilizada para penetrar en numerosos servidores web.

[2] Vulnerabilidad nueva que aún no está parcheada.

Vulnerabilidades Q2 2009

La explotación satisfactoria de esta nueva vulnerabilidad permite a un usuario malicioso acceder a información privada evitando la autenticación del servidor IIS que es necesaria para acceder a dicho recurso protegido. Incluso si se dispone de los permisos adecuados también se puede dar la posibilidad de que un usuario malicioso pueda subir un fichero al servidor a través de esta vulnerabilidad. El problema radica en el protocolo WebDAV, en este caso a través de la cabecera "Translate: f" y el uso de caracteres unicode en la URI de la petición que el usuario realiza al servidor.

Para finalizar el mes con más sorpresas, el día 28 de mayo Microsoft publicó un nuevo aviso de seguridad, el 971788, donde mencionaba que se había detectado una nueva vulnerabilidad en DirectX y estaba siendo utilizada para instalar malware en los sistemas vulnerables a través de ficheros multimedia.

No obstante, esta vulnerabilidad también traía buenas noticias porque nuevamente las versiones de Windows Vista y Windows Server 2008 no eran vulnerables. En las últimas vulnerabilidades descubiertas hemos notado esta misma situación en algunas ocasiones, en estos 2 sistemas operativos la gravedad es muy inferior que en Windows XP o Windows 2000, en algunas ocasiones simplemente la vulnerabilidad no existe. Esto confirma que los esfuerzos que está realizando Microsoft por mejorar la seguridad en sus últimos sistemas operativos, Windows Vista y Windows Server 2008, no se están quedando en saco roto.

Para finalizar el resumen del trimestre, en el mes de junio, Microsoft ha publicado 10 boletines de seguridad que corrigen 31 vulnerabilidades, entre ellas la vulnerabilidad ya comentada del servidor web IIS además de 11 nuevas vulnerabilidades que afectan a Microsoft Office, 8 a Microsoft Internet Explorer, 2 a Microsoft Active Directory, 3 al servicio de cola de impresión de Windows, 4 al Kernel de Windows, 1 en Windows Search y finalmente 1 relacionada con la llamada a Procedimientos Remotos (RPC) que afecta a todas las versiones de Windows, incluidos Windows Vista y Windows Server 2008 y permite la escala de privilegios a un usuario local. No obstante y a pesar del número de vulnerabilidades que se han corregido en este mes, Microsoft no ha podido corregir la vulnerabilidad que se descubrió el 28 de mayo en DirectX.

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

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

En la variedad está el Waledac

La ingeniería social sigue siendo una de las técnicas más empleadas por el malware, y también por el gusano Waledac, para distribuirse. Se puede definir como "una colección de técnicas que se emplean con objeto de manipular a los usuarios para que realicen determinadas acciones, como el envío de información personal, la descarga de archivos, etc."

Si por algo se caracteriza la familia de los Waledac es por la diversidad de temas que han utilizado para distribuirse. La elección de los temas no ha sido casual, sino que han sido cuidadosamente seleccionados en función de:

- Acontecimientos importantes en fechas señaladas, como navidades o San Valentín.
- Noticias falsas, como la renuncia de Barack Obama a la presidencia de EEUU o explosiones en ciertas ciudades.
- Asuntos llamativos, como vales descuento o la posibilidad de espiar los mensajes de cierto número de teléfono.

Los primeros ejemplares aparecieron en navidades del año 2008 y utilizaban felicitaciones navideñas como cebo para engañar a los usuarios y distribuirse.

Renuncia de Barack Obama

En enero de 2009, comenzaron a distribuirse mensajes de correo electrónico sobre la supuesta renuncia de Barack Obama a la presidencia de Estados Unidos. Estos mensajes incluían un enlace a una página web en la que se podía consultar la impactante noticia:

Figura 14. Mensaje de correo sobre la renuncia de Obama.

En la variedad está el Waledac

Si se pulsaba el enlace del mensaje, el usuario era redirigido a una página web que imitaba a la original y en la que se podía leer la supuesta noticia, entre otras, como se puede ver en la siguiente imagen:

Figura 15. Supuesta página web oficial de Obama.

Cuando el usuario pulsaba alguno de los enlaces incluidos en la noticia, se procedía a la descarga del archivo malicioso.

San Valentín

Después de las navidades, San Valentín es la fecha más próxima que los creadores de malware aprovecharon para distribuir sus creaciones. Sin embargo, mucho antes del 14 de febrero, esta familia ya estaba distribuyendo mensajes de correo sobre el día de los enamorados.

De hecho, el 26 de enero de este año publicábamos un post en el blog de PandaLabs advirtiendo de la aparición de una oleada de Waledacs que utilizaba la temática de San Valentín para distribuirse.

En la variedad está el Waledac

En esta ocasión, llegaba en un mensaje de correo que contenía un enlace a una página en la que se mostraban unos corazones y el usuario tenía que seleccionar uno. Si el usuario pulsaba sobre cualquiera de ellos, se procedía a la descarga de un archivo bajo la previa confirmación del usuario.

Este archivo, en realidad, era una copia del gusano.

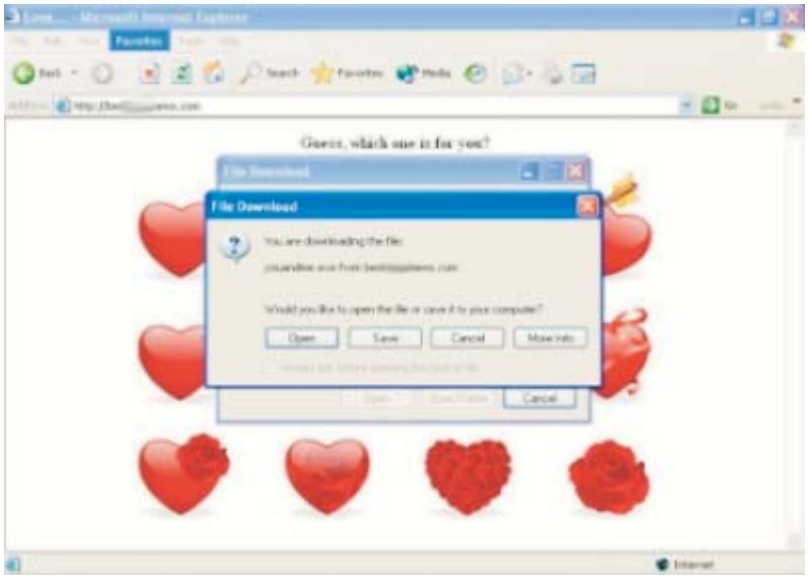

Figura 16. Página web desde la que se descarga el Waledac.

Unos días antes de San Valentín, se volvieron a distribuir mensajes de correo relacionados nuevamente con el día de los enamorados. Estos mensajes contenían un enlace a una página maliciosa que constaba de una imagen romántica y un texto en el que se ofrecía una herramienta para diseñar tarjetas para San Valentín.

El mensaje incluía varios enlaces que en teoría apuntaban a la web de descarga de dicha herramienta. Sin embargo, lo que realmente se descargaba no era una aplicación sino una variante de la familia Waledac.

Figura 17. Página web para diseñar tarjetas románticas

En la variedad está el Waledac

Vales descuento en tiempos de crisis

Los ciber-delincuentes también han querido aportar su granito de arena para ayudar a los usuarios a sobrellevar mejor la crisis económica. En este caso, los mensajes contenían enlaces que llevaban a una página web en la que se ofrecían vales descuento para numerosos establecimientos.

Figura 18. Página web desde la que se podían descargar los supuestos vales.

Si el usuario decide descargar estos vales descuento y pulsa alguno de los enlaces del mensaje, se estará descargando un archivo con nombres como couponlist.exe, coupons.exe, list.exe o print.exe. En principio, un archivo con alguno de esos nombres podría corresponder perfectamente a un listado de vales. Sin embargo, todos estos archivos ejecutables corresponden a una copia del gusano.

En la variedad está el Waledac

Explosiones

Unas semanas después, una nueva temática estaba siendo utilizada para distribuir nuevos ejemplares de Waledac. En esta ocasión, los mensajes trataban sobre una supuesta explosión y contenían un enlace a la noticia.

Si el usuario pulsaba el enlace, era redirigido a una página web en la que podía leer la noticia y además se mostraba un vídeo sobre el suceso. Para no levantar las sospechas de los usuarios, se utilizó la imagen de la agencia Reuters.

Sin embargo, para visualizar el video, se requiere que el usuario descargue una actualización del Flash Player, que no es otra cosa que la copia del gusano.

Espía de sms

La temática más reciente utilizada por el Waledac ha sido hacerse pasar por una aplicación para espiar los sms de otros teléfonos móviles.

Esta técnica consiste en ofrecer un servicio que permite a los usuarios leer los sms recibidos en un teléfono movil. Con el pretexto de poner a prueba a tu pareja o por simple curiosidad, ofrecen un programa que permite acceder a información privada sin que la víctima se percate de ello.

Sin embargo, detrás de este mensaje no hay ningún programa espía, sino un código malicioso de la familia Waledac.

Si el usuario decide descargar y ejecutar el supuesto programa, el ordenador quedará afectado por este gusano.

Figura 19. Página de descarga programa espía.

Tendencias Q2 2009

Este trimestre se ha caracterizado por el gran impulso que los ciberdelincuentes han dado a la distribución de malware a través de técnicas BlackHat SEO y el uso de los servicios de la web 2.0 más conocidos, desde Youtube hasta Twitter, en combinación con vulnerabilidades tanto en estos servicios como en aplicaciones muy utilizadas por los usuarios, como Microsoft PowerPoint o Adobe Acrobat Reader.

Vulnerabilidades

Ya el 2 de abril Microsoft publicó un aviso de seguridad fuera de su ciclo habitual con la publicación de un parche para PowerPoint debido a un agujero de seguridad que afectaba a sus versiones para Windows y Mac. A lo largo de este trimestre hemos visto un número creciente de vulnerabilidades que afectaban a diferentes fabricantes. Cabe destacar la publicación de los boletines de seguridad de Microsoft en junio, que han marcado una cifra récord en el número de boletines publicados desde que Microsoft comenzó con su ciclo mensual; estos boletines corrigen un total de 31 vulnerabilidades.

Técnicas BlackHat SEO

Los ataques de BlackHat SEO no son algo nuevo, aunque sí que hemos visto un incremento importante en el segundo trimestre de 2009. SEO son las siglas en inglés de Search Engine Optimization (optimización para motores de búsqueda), y básicamente se refiere a las técnicas utilizadas para conseguir que las páginas web mejoren su posicionamiento en los resultados de los motores de búsqueda (Yahoo, Google, etc.). BlackHat SEO se refiere al uso que los ciberdelincuentes hacen de las técnicas SEO para conseguir que sus páginas aparezcan en estas primeras posiciones.

En abril desde PandaLabs descubrimos un nuevo caso de BlackHat SEO; en esta ocasión era especialmente interesante ya que estaban utilizando una marca en concreto (el fabricante americano de coches Ford). Crearon más de 1 millón de links maliciosos para que los usuarios que buscaran términos relacionados con Ford acabaran en una de estas páginas maliciosas. Días después, repitieron la jugada pero esta vez la marca afectada fue Nissan. En ambos casos se trataba de lo mismo: una vez accedía a la página maliciosa, se solicitaba al usuario la instalación de un supuesto códec que realmente es un falso antivirus llamado Adware/MSAntiSpyware2009.

Desde entonces han seguido apareciendo más casos haciendo uso de diferentes temáticas. Es necesario subrayar la importancia que los ciberdelincuentes están dando a este tipo de técnicas. Utilizan siempre temáticas muy actuales, haciendo uso de herramientas como Google Trends para saber qué tipo de términos son más usados por los internautas, y están atentos a cualquier noticia que tenga especial relevancia, como la gripe porcina (Swine Flu), etc.

Tendencias Q2 2009

Para ilustrar esta situación, el día 1 de junio Microsoft anunció en el E3 su "Project Natal", un nuevo sistema que permite interactuar con su consola Xbox 360 sin necesidad de mandos. Este anuncio causó mucho revuelo y apareció en todas las noticias. Menos de 24 horas después, al realizar una búsqueda en Google con las palabras "Youtube Natal" el primer resultado que aparecía en la búsqueda era una página maliciosa. Buscando páginas creadas por los mismos ciberdelincuentes nos encontramos con las siguientes páginas tratando diferentes temas:

16,000 links "**TV Online**"
16,000 links "**YouTube**"
10,500 links "**France**" (Airline Crash)
8,930 links "**Microsoft**" (Project Natal)
3,380 links "**E3**"
2,900 links "**Eminem**" (MTV Awards/Bruno Incident)
2,850 links "**Sony**"

Por si esto no fuera suficiente, otra forma de tratar de infectar a los usuarios ha sido a través de Youtube. Básicamente, Youtube permite a los usuarios registrados añadir comentarios sobre los videos que ven, de tal forma que puedan servir a los usuarios que van a ver estos videos. En este caso los delincuentes crearon cuentas para que comenzaran a crear comentarios de forma automatizada; estos comentarios incluían links a sitios maliciosos para infectar a los internautas. En total crearon más de 30.000 comentarios con links maliciosos.

Uso malicioso de Twitter Trends

Otro objetivo de los delincuentes ha sido Twitter. En abril apareció un gusano que utilizando una técnica de cross-site scripting infectaba a los usuarios cuando visitaban los perfiles de usuarios infectados. El gusano infectaba el perfil del usuario, para seguir así con su propagación. Aparecieron nuevas variantes, y se supo quien era su creador, un joven llamado Mikey Mooney, que aparentemente quería atraer usuarios a un servicio competidor de Twitter.

A principios de junio comenzaron a aparecer ataques en Twitter utilizando otras técnicas: básicamente han adoptado el BlackHat SEO para los usuarios de Twitter. Twitter tiene una característica llamada "Twitter Trends", básicamente es un listado de los temas más tratados en Twitter, y cuando accedes a ellos, obtienes un listado de todos los tweets que hay publicados sobre ese tema. Estos temas son finalmente los que más gente lee, por lo que realmente es un objetivo muy valioso para los delincuentes.

Tendencias Q2 2009

Básicamente lo que estos delincuentes están haciendo es escribir tweets sobre los temas que aparecen en Twitter Trends con links maliciosos a webs para instalar malware a quien las visite. El primer ataque se centraba en sólo uno de los temas, pero días más tarde ampliaron su campo de acción y absolutamente todos los temas tenían links maliciosos. Cuando el actor David Carradine falleció, en unas pocas horas ya había cientos de tweets maliciosos, y lo mismo está sucediendo con todos los temas más populares de Twitter.

Para acabar este apartado de tendencias, no podemos olvidar que en este segundo trimestre de 2009 se cumple el segundo aniversario de Inteligencia Colectiva.

Dos años de Inteligencia Colectiva

En 2007 Panda Security lanzó al mercado la Inteligencia Colectiva: un conjunto de tecnologías capaces de analizar, clasificar y desinfectar de forma automática todos los ficheros recibidos diariamente en PandaLabs. Cuando se celebra su segundo aniversario, esta decisión estratégica de la compañía nos ha permitido posicionar a Panda como The Cloud Security Company al ofrecer al mercado la primera solución de seguridad en proteger desde la nube: Panda Cloud Antivirus.

La existencia de un negocio con grandes beneficios económicos orquestados por mafias ciber-criminales hizo que los laboratorios de seguridad de la industria asistiéramos a un aumento exponencial del nuevo malware, multiplicándose el número de nuevos ejemplares incluso por 10. En esta situación, y viendo que los usuarios podrían infectarse muy fácilmente, sólo cabían dos soluciones: dimensionar con recursos innumerables el laboratorio para llevar a cabo la labor de desinfección de forma manual, o automatizar los procesos y preparar el laboratorio de forma que las rutinas se hicieran de forma rápida y automática.

PandaLabs eligió la opción más innovadora y difícil, planteando un reto hasta el momento no abordado por otras compañías: el desarrollo de un sistema basado en inteligencia artificial que fuese capaz no sólo de reconocer nuevos ejemplares de malware, sino de aprender y adaptarse a las nuevas creaciones de los ciberdelincuentes.

Así nació Inteligencia Colectiva. La primera vez que se puso a disposición del mercado fue en el año 2007 con un pequeño escáner online y gratuito, llamado NanoScan, capaz de identificar malware activo en memoria en tan sólo unos segundos. Dado que la iniciativa fue positiva en cuanto a recepción del mercado y a efectividad de las tecnologías, la gama de retail 2009 fue dotada de una mayor capacidad de detección gracias a su conexión con la nube.

Tendencias Q2 2009

En abril de 2009, coincidiendo con el segundo aniversario, la comunidad de usuarios de todo el mundo se ha convertido realmente en el laboratorio, gracias al lanzamiento del primer antivirus ultra-ligero del mercado basado en la nube: Panda Cloud Antivirus.

En la actualidad, el sistema de Inteligencia Colectiva de Panda permite la correlación y resolución del nuevo malware en sólo 6 minutos, gracias a los miles de ficheros que la comunidad envía todos los días, y comparte ese conocimiento en forma de mayor capacidad de detección a todos los clientes de Panda.

Inteligencia colectiva recibe diariamente 50.000 nuevos ficheros, de los cuales 35.000 son nuevo malware. De éstos, el 99,4% son procesados de forma automática, quedando un 0,6% para resolución manual. La base de datos de Inteligencia Colectiva cuenta con más de 26 millones de ejemplares de malware y ocupa más de 18.000 GB.

Si todo este conocimiento estuviera en el PC del usuario, tendríamos el antivirus perfecto, pero no se podría hacer nada más con el ordenador. Por eso, Inteligencia Colectiva no sólo es nuestra respuesta al incremento exponencial del malware, sino que nos permite ofrecer la máxima detección con el mínimo impacto en los ordenadores de los usuarios.

Inteligencia Colectiva en cifras

- Se reciben 50.000 ficheros diarios, de los que 35.000 son nuevo malware. El 99,4% se procesan automáticamente por Inteligencia Colectiva con una media de 6 minutos por cada resolución.
- El 52% del nuevo malware procesado por Inteligencia Colectiva sólo vive durante 24 h horas, desapareciendo después.
- Durante el primer trimestre de 2009, Inteligencia Colectiva procesó 4.474.350 ficheros.
- Para hacerlo de forma manual, hubieran sido necesarios 1.898 técnicos y 926.347 horas de trabajo.
- La base de datos de Inteligencia Colectiva ocupa más de 18.000 GB o 148 billones de bits.
- Transformando esta cantidad de información en texto, podríamos escribir 727.373 enciclopedias británicas gracias a los 29 billones de palabras que ocuparía la misma extensión que la base de datos de Inteligencia Colectiva.
- Con esta magnitud, podríamos rellenar casi 33 mil millones de páginas de texto, que si pusiéramos una detrás de la otra impresas físicamente, se podría cubrir una distancia de más de 9 millones de kilómetros o ir y volver a la luna 12 veces.
- Y si tuviéramos que enviar toda esta información mediante una línea estándar de ADSL, tardaríamos 1.045 días.

Más información sobre la Inteligencia colectiva en el blog de PandaLabs.

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/