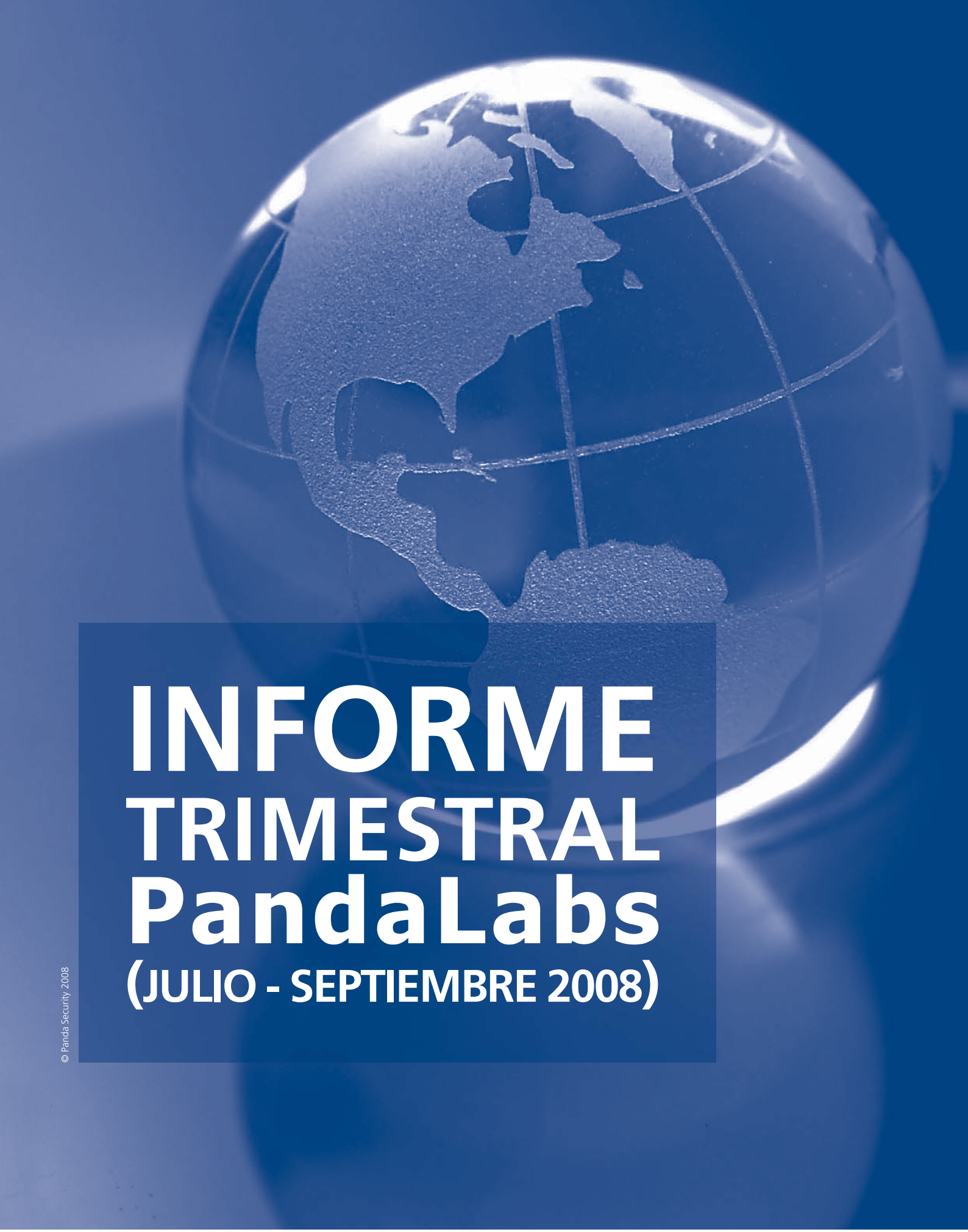


INFORME TRIMESTRAL PandaLabs

(JULIO - SEPTIEMBRE 2008)

PANDA SECURITY | *One step ahead.*

Índice

Introducción

Comienza un nuevo curso y llega el momento de presentar el informe correspondiente al tercer trimestre del año. Tiende a haber una sensación de calma relativa en lo que a malware se refiere durante estos meses, ya que coinciden con el periodo vacacional de la mayoría de países del hemisferio norte. Sin embargo, hemos podido comprobar que los negocios de los ciberdelincuentes no cierran por vacaciones.

Una importante vulnerabilidad descubierta en los servidores DNS provocó una masiva actualización coordinada de servidores DNS. Podréis ampliar la información sobre esta vulnerabilidad en la ya habitual sección de Vulnerabilidades.

La inteligencia colectiva es una tecnología novedosa y de la que oiremos hablar mucho a partir de ahora. Con motivo del lanzamiento de los productos 2009 y con el objetivo de ir familiarizando a los usuarios con este nuevo concepto, hemos preparado un interesante artículo.

El spam sigue dando que hablar y a pesar de todos los medios que se están poniendo para acabar con esta molesta actvidad, los cibercriminales idean nuevas formas de llenar de correos no deseados los buzones de los usuarios.

Las redes sociales están de moda y los ciberdelincuentes lo saben. Analizaremos su enorme popularidad, así como los principales ataques que han tenido lugar contra ellas en los últimos meses.

Asimismo, como en anteriores informes, presentaremos la evolución de malware activo por países en lo que llevamos de año y las cifras del trimestre en lo que a malware se refiere.

Esperamos que os resulte interesante.

Resumen ejecutivo

Según un estudio de investigación realizado por Panda Security, TODOS los antivirus (Panda incluido) tienen clientes infectados. Los ratios de infección varían del 12-13% hasta el 30% aproximadamente.

El Adware ha pasado de un 22,03% durante el anterior trimestre a un 37,49% durante este, debido a la gran actividad de los falsos antivirus durante este trimestre.

España y Estados Unidos son los países con el porcentaje más alto de malware activo durante el tercer trimestre del año superando el 30%.

El Departamento de Justicia de Estados Unidos anunció que iba a presentar cargos contra 11 personas relacionadas con el robo y venta de más de 100 millones de tarjetas de crédito y de débito.

Descubierta vulnerabilidad en DNS que permitía a los usuarios maliciosos redirigir cualquier página web o dominio a un sistema controlado por un usuario atacante.

Las cifras del tercer 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 tercer trimestre de 2008:

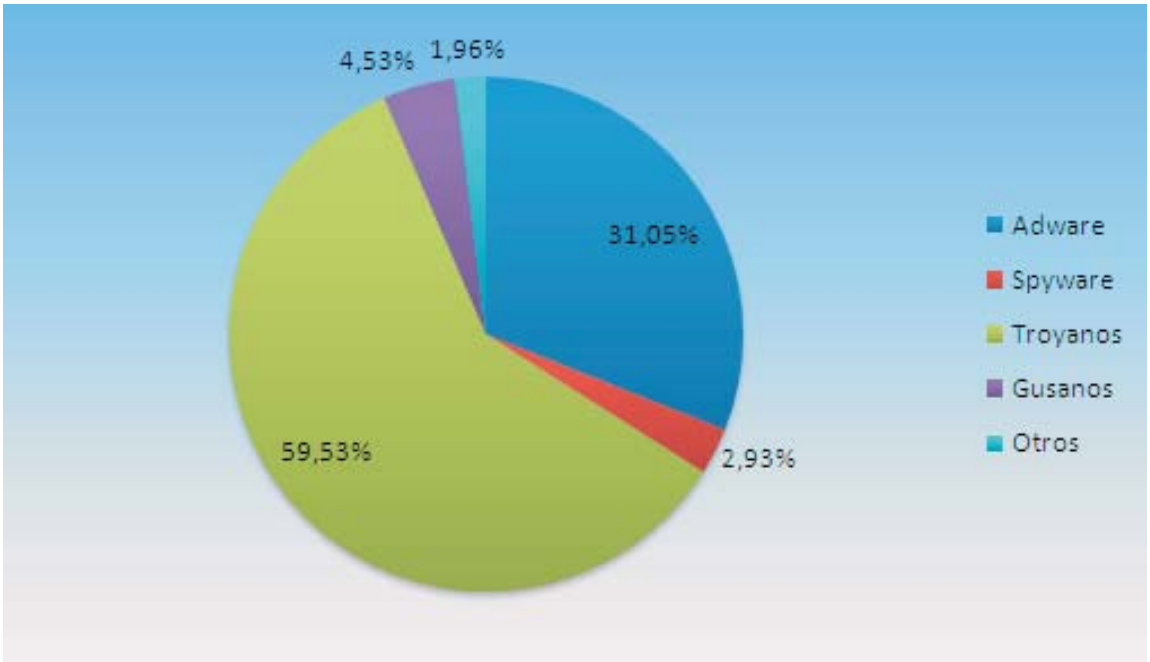


Figura 1. Aparicion de malware trimestral.

Como se puede observar, los troyanos continúan siendo el tipo de malware más detectado en PandaLabs.

Hasta aquí todo normal. Sin embargo, hay que destacar una categoría que ha sufrido un incremento importante; se trata del Adware, que ha pasado de un 22,40% en el segundo trimestre a un 31,05% durante este tercer trimestre del año.

Este aumento se debe en gran medida a la notable cantidad de falsos antivirus que se han detectado durante este trimestre. Los llamados falsos antivirus son un conjunto de aplicaciones que informan de una falsa infección en el equipo ofreciendo la posibilidad de descargarse un software con el fin de erradicar la infección. Una vez descargada dicha aplicación, se solicita al usuario que pague un importe determinado para así poder registrarse y eliminar dicha infección.

Las cifras del tercer trimestre

En la siguiente imagen podemos observar un ejemplo de falso antivirus:

Figura 2. Interfaz de un falso antivirus.

Las cifras del tercer trimestre

Este gran incremento se ha producido debido al aumento de mensajes de spam creados con el objetivo de distribuir este tipo de programas. Además, estos mensajes utilizan técnicas de ingeniería social para engañar al usuario y contienen enlaces maliciosos que supuestamente apuntan a videos relacionados con falsas noticias o videos sobre famosos de contenido sexual.

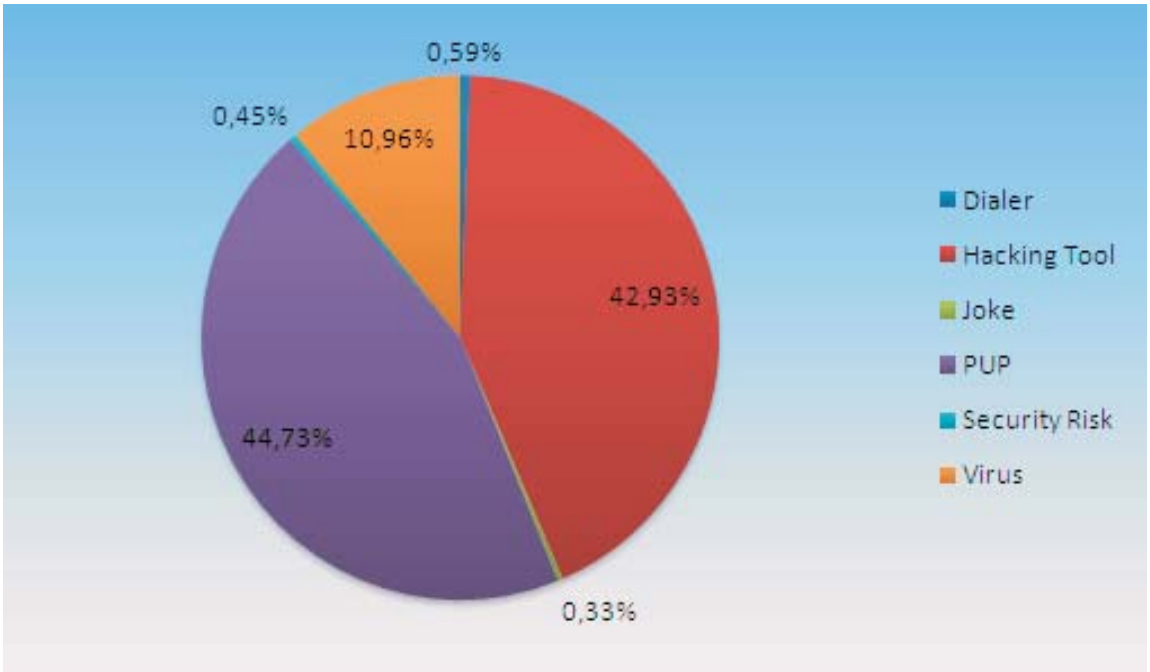


Figura 3. Clasificación de la categoría de Otros.

En esta sección observamos que el tipo de malware predominante son las herramientas de hacking y los PUPs, situándose en un 42,93% y 44,73% respectivamente.

Las cifras del tercer 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. Como puede observarse, la categoría predominante son los troyanos.

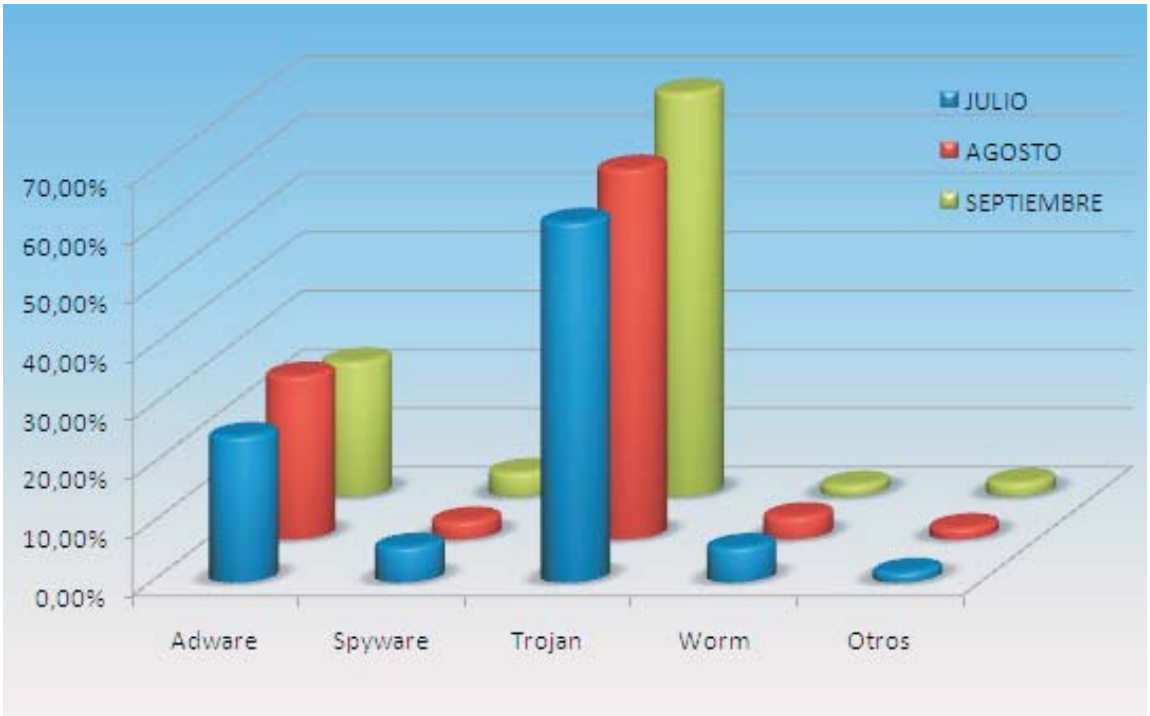


Figura 4. Evolución en la aparición de nuevo malware.

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

Las cifras del tercer trimestre

Amenazas detectadas por los Sensores PandaLabs

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

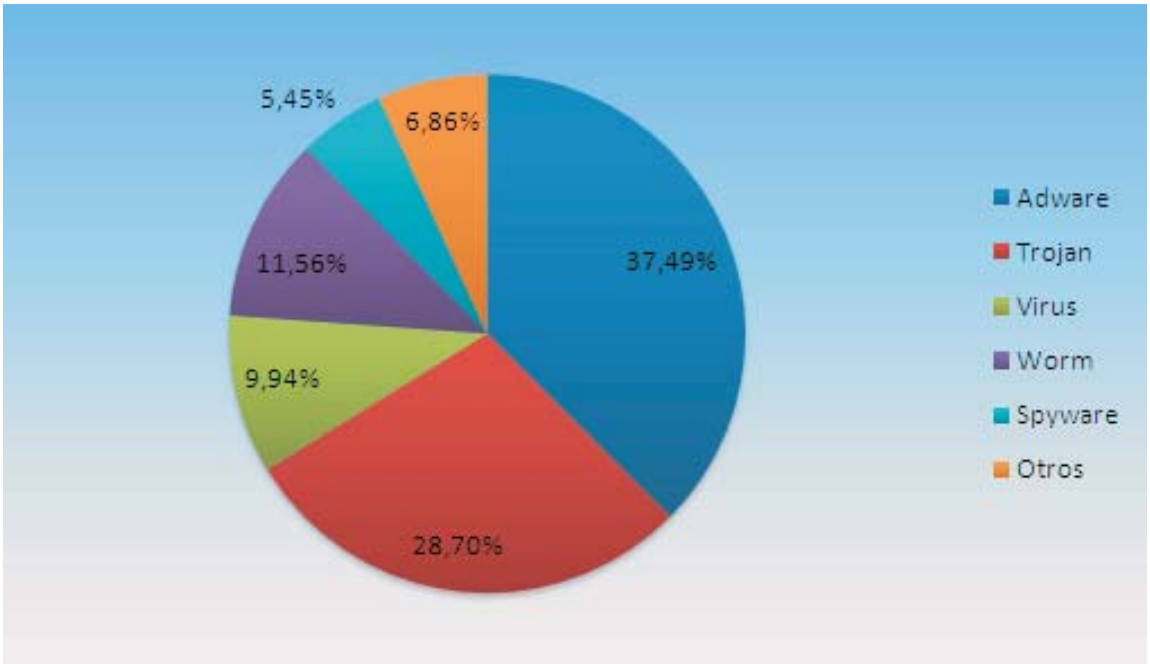


Figura 5. Distribución de malware por categorías.

En este gráfico se observa que también se ha producido un gran incremento del Adware según los datos recogidos por los sensores de seguridad de PandaLabs.

El Adware ha pasado de un 22,03% durante el anterior trimestre a un 37,49% durante este, debido a la gran actividad de los falsos antivirus durante este trimestre.

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.

Figura 6. 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 en lo que llevamos de año:

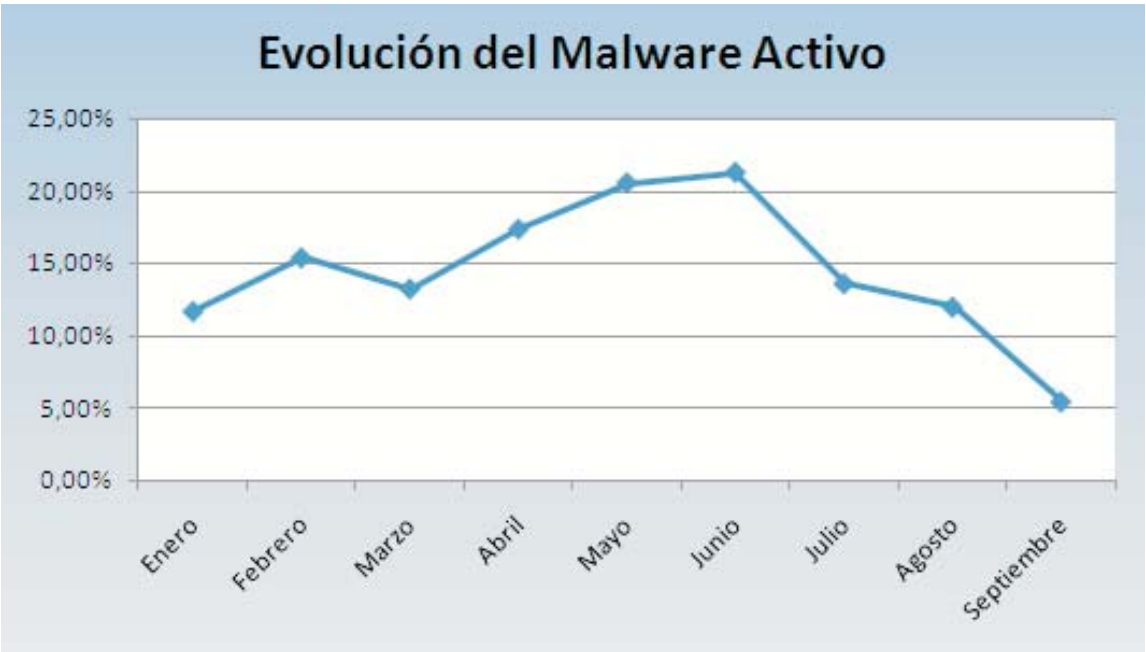


Figura 7. Evolución de malware activo durante 2008.

Como podemos observar, el año 2008 comenzó con uno de los porcentajes más bajos de infección (12%) de malware activo únicamente superado por el 8,53% de febrero del 2007. Después se ha producido un incremento constante, alcanzando la cota máxima en junio con un 21,27%. A partir de entonces se ha producido un descenso progresivo del malware activo alcanzado el porcentaje más bajo del año en septiembre con un 5,38%* (*datos recogidos hasta el 17/09/2008).

Malware activo

A día de hoy la media de malware activo asciende al 14,48%. Casi un 3% 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 8. Países con mayor porcentaje de malware (Junio-Septiembre)[1].

En está gráfica podemos observar que España y Estados Unidos son los países con el porcentaje más alto de malware activo durante el tercer trimestre del año superando el 30%.

Sin embargo, en líneas generales se ha notado una disminución importante del volumen de PCs infectados con malware activo durante este trimestre.

[1] Países ordenados por número de análisis realizados.

Malware activo

Este cambio se puede apreciar si comparamos los datos de este trimestre respecto a los del primer semestre del año, en el que todos los países superaban el 30% de infección llegando incluso a sobrepasar el 40% como Rusia, España y Mexico:

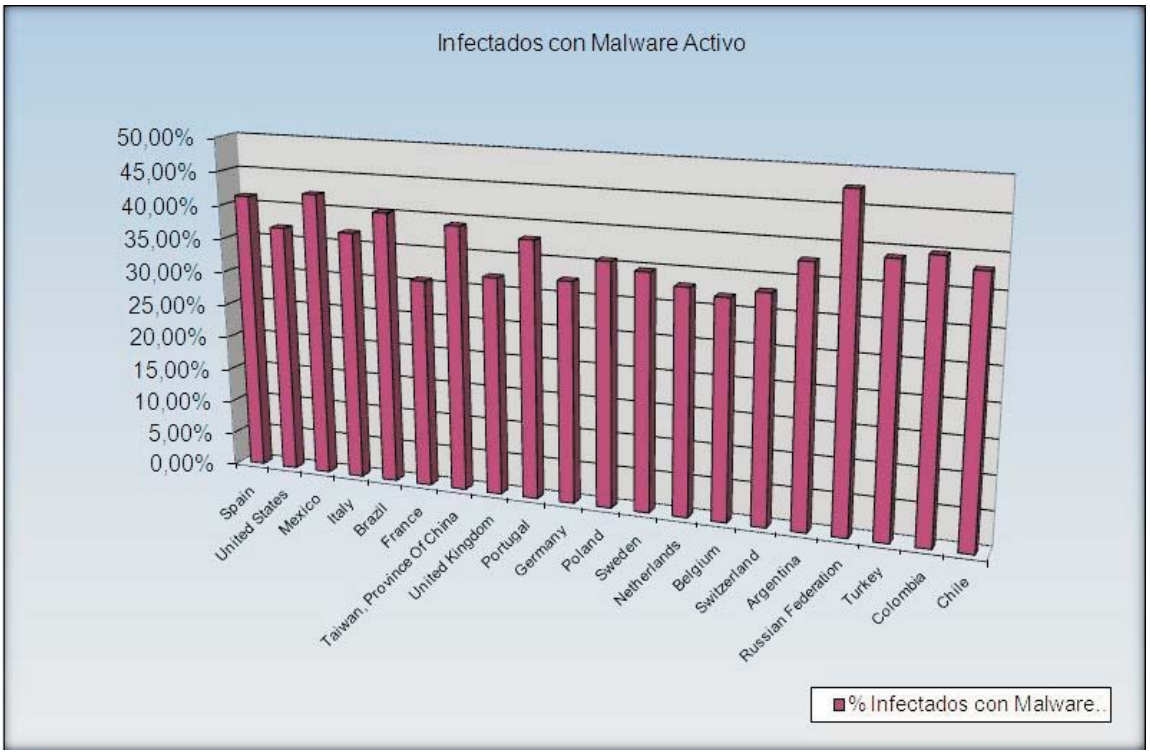


Figura 9. Países con mayor porcentaje de malware (primer semestre).

Estos datos son positivos, porque reflejan que la situación en cuanto a malware activo está mejorando. Esperemos que esta tendencia a la baja continúe durante el último trimestre del año y que no esté relacionada con la relativa calma del período vacacional.

Tendencias del trimestre

Hay quien pudiera pensar que el tercer trimestre puede ser el más tranquilo del año, ya que coincide con el periodo vacacional de la mayoría de países del hemisferio norte. Pero año tras año se ha demostrado que esto no es así, podemos acordarnos de apariciones de gusanos como el Blaster para abrirnos los ojos. Y este año no ha sido diferente.

Comenzamos el trimestre alertados por una masiva actualización coordinada de servidores DNS. Nunca en la historia se había dado un caso similar, con tantos fabricantes distintos actuando de forma coordinada para solucionar un problema de seguridad. Un mes después, Dan Kaminsky, investigador de seguridad que dio a conocer la vulnerabilidad, expuso todos los detalles en lo conferencia Black Hat USA que tiene lugar todos los años en Las Vegas. Sus declaraciones no dejaban lugar a dudas: "Every network is at risk. That's what this flaw has shown." En la sección de vulnerabilidades podéis leer los detalles y explicación del funcionamiento de esta vulnerabilidad.

Verano tormentoso. El Storm worm lleva ya mucho tiempo dando que hablar, y estos meses ha seguido así. En julio se comenzó a ver un mensaje generado por el Storm worm utilizando de nuevo técnicas de ingeniería social; esta vez el mensaje informaba de la creación de una nueva moneda, llamada Amero, que iba a sustituir al dólar en Norteamérica:

The U.S. Government began to realize the plan to replace the Dollar with the "Amero", the new currency of the North American Currency Union. Canada, the United States of America and Mexico have resolved to unit in order to resist the Worldwide Financial Crysis. You can become acquainted with the plan of the implementation of Amero, just click on the icon under this text.

Figura 10. Mensaje generado por el Storm Worm.

Tendencias del trimestre

Y ya metidos en el campo de la ciberdelincuencia, este verano hemos podido dar un respiro y recibir buenas noticias. El Departamento de Justicia de Estados Unidos anunció que iba a presentar cargos contra 11 personas relacionadas con el robo y venta de más de 100 millones de tarjetas de crédito y de débito. Los cargos presentados incluyen conspiración, intrusión en ordenadores, fraude y robo de identidad.

Básicamente, los acusados se dedicaban a introducirse en las redes de minoristas (el listado es extenso: TJX Cos, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 y DSW) a través de redes inalámbricas. Una vez dentro de la red, los hackers instalaron troyanos que les permitían la captura de todo tipo de datos: números de tarjetas de crédito, contraseñas, etc. Todos esos datos robados eran enviados a servidores controlados por los hackers en Estados Unidos y Europa del Este.

Estamos hablando de una banda de delincuentes internacional, con 3 estadounidenses, un estonio, 3 ucranianos, 2 chinos, y un último acusado del que aún se desconoce su origen.

Vulnerabilidad en DNS

Este trimestre hay que destacar la vulnerabilidad descubierta en los servidores DNS, que permitía a los usuarios maliciosos redirigir cualquier página web o dominio a un sistema controlado por un usuario atacante.

El protocolo DNS es un sistema que traduce los nombres de las páginas web a direcciones IP que Internet puede interpretar. Por ejemplo, la página web de www.pandasecurity.com se traduce en números a 88.221.26.28. Así, cuando un usuario accede a esta página web, lo que Internet realmente interpreta son los números asociados a esa página.

Fue el investigador Dan Kaminsky quien, tras varios de meses de investigación, descubrió esta vulnerabilidad. Este investigador iba a exponer la descripción completa de la vulnerabilidad en el BlackHat de Las Vegas, que se celebró a principios agosto. Sin embargo, esta información se publicó por error en un blog muy conocido, y a pesar de que se eliminó, esta información pudo ser accesible.

La vulnerabilidad utiliza dos características muy conocidas del protocolo DNS:

Predicción del puerto origen y del ID de transacción

DNS utiliza paquetes UDP para enviar y recibir peticiones. La mayoría de los servidores DNS utilizan el mismo puerto origen para conectarse a otro servidor DNS en un período corto de tiempo. Sin embargo, los IDs de transacción son aleatorios. A pesar de ello, esta medida de seguridad no es suficiente y los usuarios maliciosos podrían falsificar paquetes para enviar paquetes respuesta al servidor DNS atacado antes de que el servidor DNS auténtico envíe su respuesta.

Para comprender mejor este proceso, hemos preparado una serie de gráficas que ilustran diferentes situaciones en relación a los servidores DNS.

Vulnerabilidad en DNS

La siguiente imagen muestra el proceso que se lleva a cabo en unas condiciones normales, en las que un usuario solicita acceder a una determinada página web, en este caso www.pandasecurity.com:

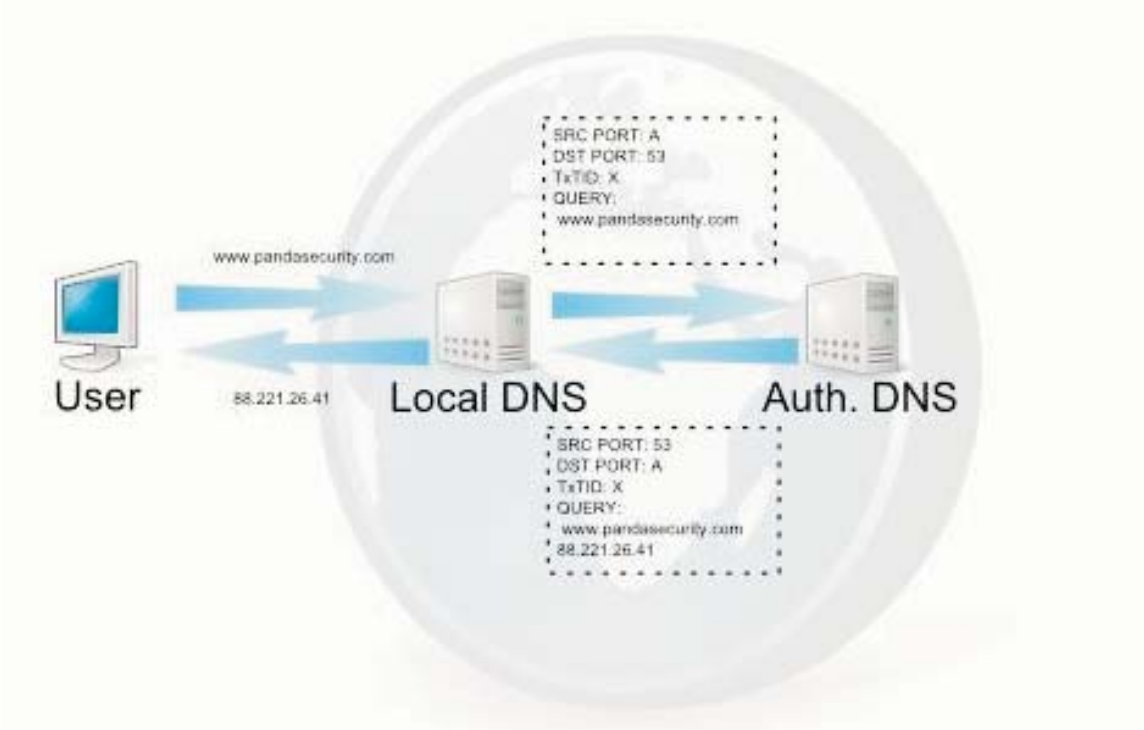


Figura 10. Proceso habitual del servidor DNS.

Como se puede observar, entre la información que se intercambia hay un puerto origen, en este caso A, un puerto destino, en este caso 53, y un ID de transacción que es aleatorio en cada petición.

Vulnerabilidad en DNS

La siguiente imagen refleja un caso en el que un usuario malicioso crea un servidor DNS "trampa" (en la figura DNS Spoofer) con el objetivo de saber cuál es el puerto origen y así poder utilizarlo con fines maliciosos:

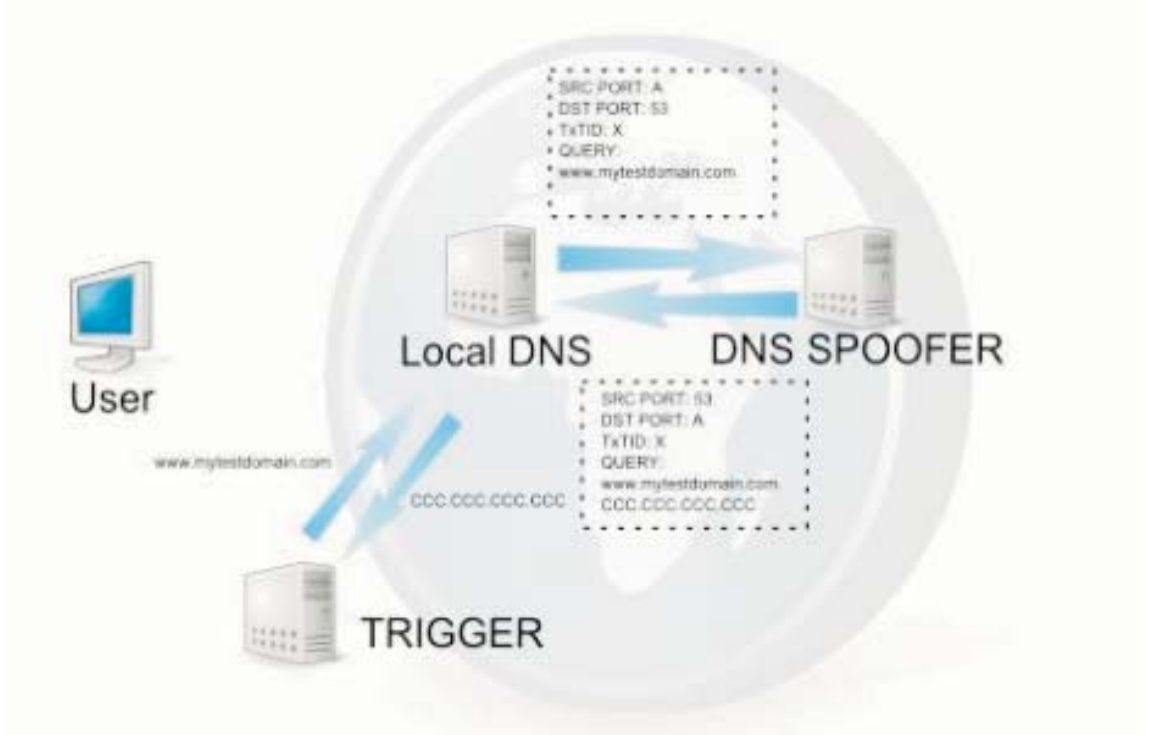


Figura 11. Proceso con servidor DNS "trampa".

Vulnerabilidad en DNS

Para conocer el puerto origen utilizado por el DNS intermedio (Local DNS), se utiliza un trigger, cuya función es forzar al DNS local a que haga peticiones al DNS falsificador.

Por último, el siguiente gráfico muestra cómo se realiza el ataque al servidor DNS:

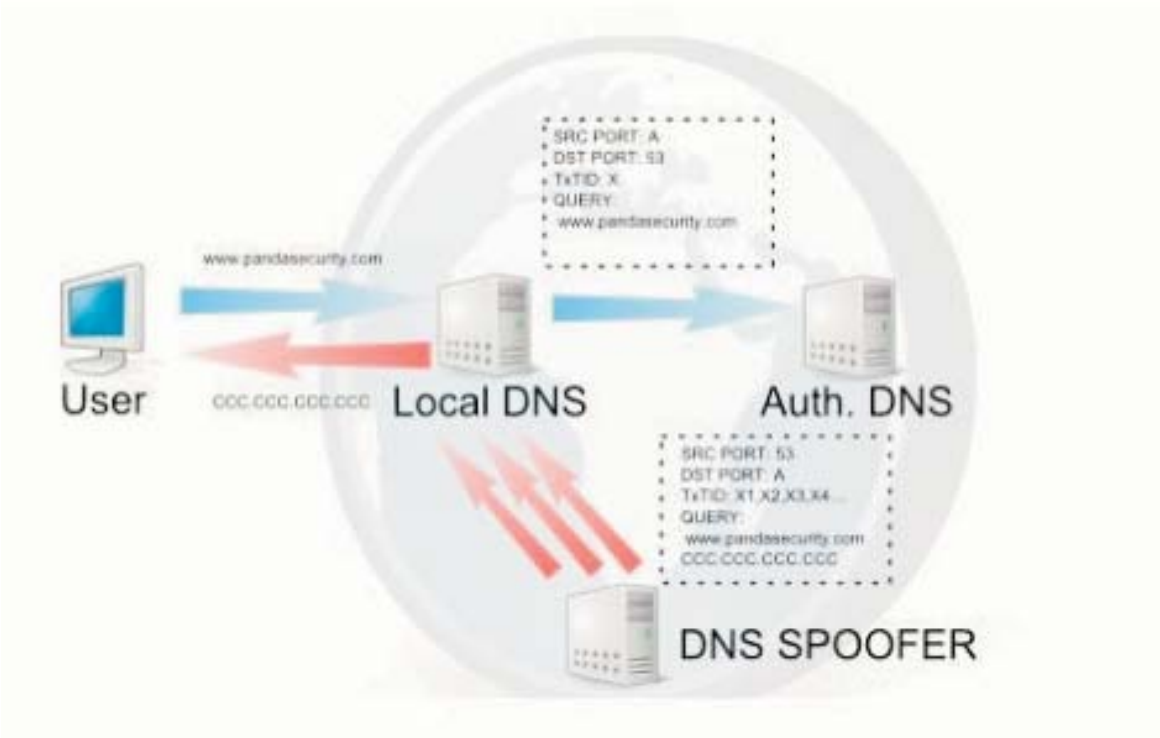


Figura 12. Ataque a servidor DNS.

Gracias al servidor "trampa" el usuario atacante puede predecir el puerto origen y el puerto destino. Sin embargo, como el id de transacción es aleatorio, el servidor DNS falsificador lanza constantemente paquetes con diferentes ids de transacción hasta encontrar uno correcto. Si los paquetes lanzados desde el DNS falsificador llegan antes que los del DNS autorizado, el usuario afectado será redirigido a la página web seleccionada por el usuario atacante.

Vulnerabilidad en DNS

Registros adicionales de recursos

Los servidores DNS pueden incluir información adicional en su respuesta para evitar futuras preguntas y mejorar la eficiencia del proceso, como por ejemplo, la dirección IP de los nombres de servidores del dominio atacado.

Una combinación de estas dos características (predicción del puerto origen y del ID de transacción, y registros adicionales de recursos) permitiría a un usuario atacante controlar todo el tráfico dirigido al dominio.

Esta es la primera vez en la que tantos fabricantes (Cisco, Microsoft, etc.) se han coordinado para garantizar la seguridad de los usuarios en el menor tiempo posible. Gracias a esto, a pesar de que la información se filtró antes de tiempo, se han evitado males mayores. En cualquier caso no debemos bajar la guardia ya que quedan muchos sistemas aún sin parchear.

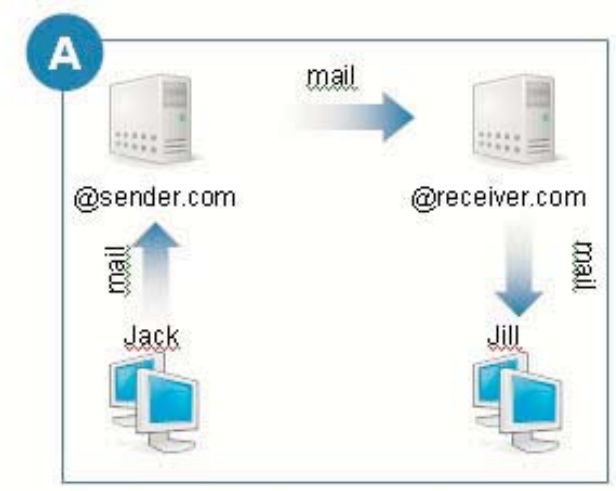
NDRs: evolución en el envío de spam

En el último año ha podido apreciarse el auge de un nuevo tipo de amenaza denominada NDR.

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

Por tanto no se trata de spam sino de correos legítimos enviados normalmente por servidores de correo mal configurados. Actualmente, las principales empresas antispam no consideran que el spam sea una cuestión de contenido sino que se trata de un correo "no solicitado y enviado de forma masiva". Los NDRs son considerados correos solicitados, ya que teóricamente responden a un envío realizado por la víctima. Por tanto las técnicas antispam utilizadas hasta ahora no son válidas en este tipo de mensajes.

Para comprender el funcionamiento, en el siguiente gráfico veremos el flujo de mensajes habitual en los envíos de correo. En estos ejemplos tenemos a jack@sender.com que quiere enviar un correo electrónico a Jill@receiver.com.



En el caso A, Jack envía un mensaje a través de su servidor @sender.com. El servidor de Jack se comunica con el servidor @receiver.com y le envía el mensaje. Finalmente el servidor de Jill deposita el correo en su buzón.

El caso A se trata de un caso normal de envío satisfactorio.

NDRs: evolución en el envío de spam

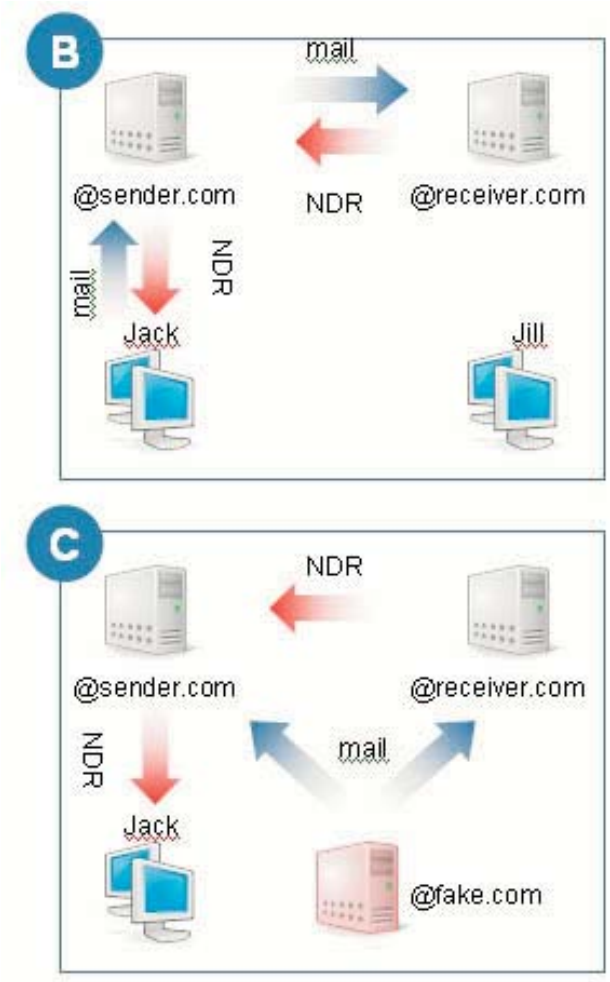


Figura 14. NDRs: evolución del envío de spam.

En el caso B, suponemos que Jack se confunde al escribir la cuenta de correo de Jill, por tanto cuando el servidor de Jack envía el correo al servidor de Jill (@receiver.com), este último le indica mediante un mensaje (NDR) que la cuenta a la que ha enviado el mensaje no existe. Ese mensaje es enviado al servidor de Jack que finalmente lo deposita en su buzón.

Por tanto Jack, al recibir el NDR, se da cuenta de que Jill no ha recibido su correo ya que se confundió escribiendo la dirección de correo.

Este servicio que ofrecen los sistemas de correo, por un lado ha sido aprovechado por las mafias de spam para engañar a los servidores de correo y hacer llegar spam a sus usuarios (caso C) y por otro lado son resultados colaterales de los envíos masivos por parte de los spammers a direcciones generadas automáticamente.

Por tanto el NDR ilegítimo se genera al enviar correos a cuentas inexistentes tanto del propio servidor de Jack (@sender.com) como al de Jill (@receiver.com) haciéndose pasar por Jack. De tal forma que cuando los servidores verifiquen que las cuentas a las que se envían los mensajes no existen, estos enviarán un NDR a la cuenta de Jack indicándole que las direcciones a las que ha intentado enviar el mensaje no existen.

Por tanto Jack recibirá unos NDRs de mensajes que él no ha enviado, es decir, recibirá un NDR ilegítimo y en ocasiones recibirá adjunto el mensaje (spam) que ocasionó el NDR.

NDRs: evolución en el envío de spam

¿Cómo es posible que un servidor de correo acepte un correo de alguien haciéndose pasar por mí?

El protocolo SMTP (detallado en el ejemplo anterior), no permite la autenticación acordada entre todos los servidores de correo. Este inconveniente permite que cualquier servidor remitente pueda identificarse como el transportista en origen de un nombre de dominio. Esto lo aprovechan los suplantadores de identidad de direcciones de correo electrónico para llevar a cabo su fin.

¿Existe alguna forma de verificar el origen del mensaje?

A nivel de servidores, existen tecnologías o configuraciones que evitan en gran medida la recepción de correos con identidades falseadas:

- Verificación SPF (Sender Policy Framework): extiende el protocolo SMTP para permitir comprobar las máquinas autorizadas a enviar correos para un dominio determinado. La idea es identificar las máquinas autorizadas por su dirección IP, y que esta identificación la haga el responsable del dominio que recibirá el correo.

- Rechazar correos que vengan de servidores que no tengan registro de DNS inverso: para comprobar si el origen es una conexión dinámica o dialup (RTB/56kb por ejemplo) los cuales no disponen de un DNS inverso autorizado.

A nivel de clientes de correo, se utilizan sistemas de firmas o claves públicas. Es decir, cada usuario firma su correo mediante un sistema de claves públicas y privadas que le identifican de forma unívoca.

Este sistema de identificación es útil de cara a verificar la identidad del emisor o de cara a codificar información que solo debe ser leída por el receptor. Estas tecnologías funcionan a nivel de cliente de correo y en ningún caso evitan la problemática del NDR.

NDRs: evolución en el envío de spam

¿Es posible diferenciar los NDRs legítimos de los NDRs ilegítimos?

Una problemática añadida para la detección de los NDRs ilegítimos es que a pesar de existir un RFC que define la estructura de estos mensajes, la realidad en calle es que la variabilidad de estos según la configuración y tipo de servidor es muy grande, haciendo difícil definir unas políticas únicas de detección de este tipo de mensajes.

Los NDRs podemos agruparlos en los siguientes tres casos:

1. Mensajes NDRs solo con texto de aviso de error.

2. Mensajes NDRs con texto de aviso de error más cabeceras del mensaje que ocasionó el NDR

3. Mensajes NDRs con texto de aviso de error más cabeceras y cuerpo del mensaje que ocasiono el NDR

En el caso 3, al disponer el contenido del mensaje de spam que ocasionó el NDR, es posible detectarlo como NDR ilegítimo utilizando las técnicas de detección antispam habituales.

Son los mensajes del caso 2 y 1 los mas difíciles de detectar ya que el contenido de mensaje que originó el NDR es escaso o nulo, por lo cual dificulta o incluso imposibilita distinguirlo de un NDR legítimo.

Conclusión

Algunas soluciones antispam han optado por introducir tecnologías de filtrado de NDRs (tanto legítimos como ilegítimos) o sistemas de etiquetado de correo de cara a identificar NDRs legítimos. Esto repercute en una alta tasa de Falsos Positivos por lo que no puede asumirse como una solución global. Además, como hemos comentado previamente, la falta de homogeneidad en la generación de los NDRs por parte de los servidores de correo hace que muchas de estas técnicas sean inútiles.

A pesar de todos los esfuerzos por acabar con este tipo de amenaza, todas las empresas y expertos reconocen que el fin de este tipo de mensajes pasa por la voluntad por parte de los proveedores, empresas e instituciones estandarizadoras de definir configuraciones básicas para los sistemas de correo que eviten este tipo de abusos.

Redes sociales en el punto de mira

Una red social se define como un servicio basado en Internet que permite a los individuos construir un perfil público o semi-público dentro de un sistema delimitado, articular una lista de otros usuarios con los que comparten una conexión, y ver y recorrer su lista de las conexiones y de las hechas por otros dentro del sistema.

Vivimos en un mundo cada vez más globalizado y en el que contamos con diversos mecanismos que permiten salvar las barreras geográficas. El concepto de comunicación tal y como lo conocíamos ha cambiado y las redes sociales se han convertido en una herramienta de gran utilidad en ese nuevo concepto de relación entre las personas: una comunicación global.

Se han creado auténticos mundos virtuales gracias a las redes sociales, en los que millones de personas se comunican y comparten sus conocimientos, aficiones, inquietudes, emociones…

El número de usuarios de este tipo de redes sociales ha aumentado considerablemente en los últimos años. Existe una amplia variedad de redes sociales que se diferencian por su temática, funcionalidades, estética, etc., pero el concepto es el mismo: poner a disposición del usuario una herramienta que le permita comunicarse con otros usuarios.

Sin embargo, desde hace unos años, la popularidad y la confianza que ofrecen las redes sociales están siendo aprovechadas por los ciberdelincuentes, que han encontrado una nueva vía de explotación de sus actividades fraudulentas.

En este artículo analizaremos las razones de la enorme popularidad de la que gozan las redes sociales, y lo acompañaremos de cifras y datos que así lo corroboran. Además, nos centraremos en algunos ejemplos de los ataques que han sufrido estas redes sociales y sus consecuencias.

Popularidad de las Redes Sociales

Desde la aparición de las primeras redes sociales, el número de usuarios de las mismas ha ido creciendo exponencialmente. Actualmente, las redes sociales gozan de una gran popularidad en Internet. Cabe destacar que, según los datos proporcionados por Alexa de los 500 sitios web más visitados a nivel mundial[2] , entre los 50 primeros puestos hay 7 redes sociales.

[2] Datos correspondientes al 05/09/2008 y extraídos de la página web:
http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none

Redes sociales en el punto de mira

La primera es Facebook, que ocupa el quinto lugar, en séptimo puesto está Myspace, le sigue en el puesto 16 Hi5 y en el 19 Orkut. Posteriormente, en los puestos 32, 38 y 47 están Flickr, Friendster y Skyrock respectivamente.

Red Social	Puesto	URL
Facebook	5	www.facebook.com
Myspace	7	www.myspace.com
Hi5	16	www.hi5.com
Orkut	19	www.orkut.com
Flickr	32	www.flickr.com
Friendster	38	www.friendster.com
Skyrock	47	www.skyrock.com

Figura 13. NDRs: evolución del envío de spam.

Por otra parte, la siguiente gráfica de Google Trends representa el volumen de búsquedas realizadas por los internautas de una palabra o frase concreta correspondiente a algunas de las redes sociales más extendidas:

Figura 14. Volumen de búsquedas de las principales redes sociales.

Redes sociales en el punto de mira

El éxito de las redes sociales se puede resumir en los siguientes puntos:

- El ser humano es una criatura social. Necesita comunicarse con otras personas y ampliar estas relaciones.
- No existen barreras. Las redes sociales permiten salvar las limitaciones que presenta la comunicación tradicional, como las barreras geográficas e incluso económicas.
- Fuente de información y conocimientos. Los usuarios que conforman las redes sociales comparten información y conocimientos entre ellos.
- Identidad online. No todo el mundo puede disponer de su propia página web, sin embargo, las redes sociales ofrecen a los usuarios la posibilidad de tener un espacio web propia y personalizarla a su gusto.
- Naturaleza viral. La necesidad de expandir la red de contactos hace que los usuarios inviten a sus amigos y esos amigos a su vez inviten a sus amigos, y así sucesivamente.

Ataques a Redes Sociales

La popularidad y el gran número de usuarios de este tipo de sitios web no ha pasado desapercibido para los ciberdelincuentes, que desde hace algunos años utilizan las redes sociales como un vector de ataque para llevar a cabo sus actividades fraudulentas. Y es que las redes sociales reúnen unos requisitos muy apetecibles para los ciberdelincuentes:

- Cuentan con un gran número de usuarios, lo que permite una distribución rápida del malware. Si se infecta un usuario, cualquier usuario que acceda a dicho perfil, quedaría automáticamente infectado.
- Almacenan muchos datos personales sobre los usuarios, ya que es necesario crear un perfil personal para acceder a ellas. La información va desde el nombre o dirección de correo electrónico hasta aficiones, edad, etc.

  Toda esta información puede ser fácilmente accesible para los ciberdelincuentes y se puede utilizar para realizar, por ejemplo, suplantaciones de identidad, ataques dirigidos, o incluso vender los datos obtenidos.
- Los usuarios de las redes sociales confían en sus contactos. Los ciberdelincuentes pueden suplantar la identidad de un miembro de esa red con relativa facilidad y hacerse pasar por él para no levantar ninguna sospecha.

Redes sociales en el punto de mira

Los ataques a redes sociales no son algo novedoso, ya que el primer ataque se produjo en 2005. Sin embargo, sí se puede apreciar un aumento y una diversificación de estos ataques a medida que el número de usuarios de las redes sociales ha aumentado. A través de ellas no solo se distribuye malware, sino que también se realizan ataques de phishing y suplantación de identidad o incluso se distribuye spam.

Casos más destacados

La mayoría de los ataques se han producido contra las redes sociales más populares, como MySpace, Orkut o Facebook. Esto no quiere decir que sean menos seguras que otras, sino que cuentan con un mayor número de usuarios, lo que aumenta las probabilidades de beneficio de un ataque.

Vamos a hacer un repaso de los ataques más significativos que han sufrido estas redes sociales:

MySpace, la más atacada

MySpace, una de las redes sociales más populares, ha sufrido numerosos ataques y de hecho fue víctima del primero. Se trataba del gusano detectado como MySpace.A creado por un usuario de MySpace y que le permitió añadir un millón de usuarios a su lista de contactos.

A finales de 2006, se distribuyó por esta red social un gusano que aprovechaba los perfiles de los usuarios de esa red para propagarse, infectando a todos los usuarios que visitaran un perfil infectado.

Por esas mismas fechas, un banner publicitario en la misma red aprovechó una vulnerabilidad en Windows Metafile para infectar a más de un millón de usuarios con spyware. Apenas unos días después se descubría, también en esa red, un gusano que incrustaba un código Java script en los perfiles de usuario. Cuando alguien intentaba visitar uno de esos perfiles, era redirigido a una web que culpaba al gobierno de Estados Unidos de los ataques del 11-S.

Pero el caso más grave tuvo lugar a principios del 2007. Esta vez se aprovechó de una característica del reproductor QuickTime de Apple para propagar un gusano. Los ciberdelincuentes asociaron varias películas subidas con este reproductor a distintos perfiles. Dicha película tenía un código malicioso, permitiendo a los hackers modificar el perfil de cualquier usuario que visitase el perfil infectado que ellos habían creado.

Redes sociales en el punto de mira

Además, este gusano presentaba la funcionalidad de enviar spam a todos los contactos de los usuarios infectados. Estos mensajes contenían un supuesta película. Cuando el usuario intentaba verla, era conducido a una página web pornográfica desde la que se descargaba un adware de la familia Zango, diseñado para mostrar publicidad personalizada.

Facebook y sus problemas de seguridad

Desde su creación, Facebook se ha convertido en una de las redes sociales con más éxito de Internet, lo que la convierte en un objetivo para los ciberdelincuentes.

A principios del año 2007 un hombre de Illinois, Estados Unidos, se hizo pasar por un adolescente para atraer a menores e intercambiar fotos con ellos. El hombre fue detenido y varios medios y asociaciones comenzaron a criticar la forma en que Facebook protegía a los menores.

A mediados del mes de julio, Facebook tuvo que enfrentarse a un nuevo problema de seguridad. En este caso se trató de un problema de programación que provocó que cuando un usuario introducía su clave, en vez de a su cuenta, era dirigido a la bandeja de correo de otro usuario, de modo que la información confidencial de unos usuarios quedó a la vista de otros.

Aunque, sin duda, el caso más grave ocurrió a mediados del mes de diciembre, cuando una compañía canadiense de pornografía fue denunciada por Facebook como responsable de haber "hackeado" la cuenta de 200.000 usuarios, logrando acceso a datos como su nombre de usuario, su contraseña o su dirección de correo.

También, a comienzos de este año, más de 50.000 usuarios de Facebook se vieron afectados por la instalación de un adware, que estaba camuflado como si de una aplicación adicional de la red social se tratara.

Las víctimas recibían una invitación indicando que tenían una invitación "Secret Crush". Sin embargo, para saber de quién se trataba, debían invitar a 5 personas más a instalar dicha aplicación.

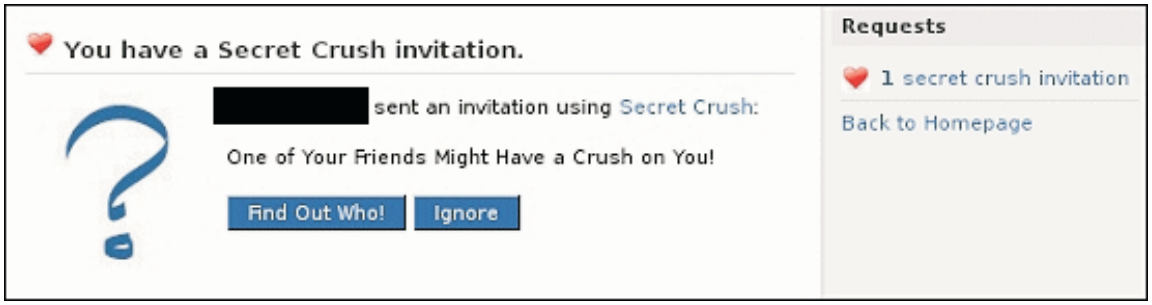


Figura 15. Imagen de la invitación "Secret Crush".

Redes sociales en el punto de mira

Una vez realizadas estas 5 invitaciones, en lugar de saber quién era el admirador secreto, se les indicaba que debían instalar otra aplicación adicional llamada Crush Calculator, que contenía finalmente el adware.

Por otra parte, en febrero de este año, salió a la luz un caso de suplantación de identidad en Facebook un tanto curioso. Un informático de 26 años fue condenado a tres años de cárcel por suplantar la identidad de Moulay Rachid, hermano menor del rey de Marruecos.

También en este año, pero en marzo, fue cuando un grupo de hackers lanzó un ataque contra MySpace y Facebook. Este ataque aprovechaba un exploit en el control activex que permite a los usuarios subir imágenes a sus perfiles. La vulnerabilidad les permitía saturar el búfer de dicho control para que interpretara las instrucciones que los ciberdelincuentes desearan darle, en lugar de aquellas para las que originalmente estaba diseñado.

Troyano en *Orkut*

A finales de febrero de este año, un troyano detectado como Orkut.AT utilizaba la red social *Orkut* para distribuirse. El procedimiento seguido era el siguiente:

En primer lugar aparecía un perfil en el "scrapbook" (libro de notas) del usuario que contenía una imagen de un vídeo de YouTube de Giselle, una participante del "reality show" Gran Hermano en Brasil. Esto pone de manifiesto que la ingeniería social sigue siendo una de las técnicas más utilizadas por los ciberdelincuentes para atraer la atención de los usuarios y así poder distribuir sus creaciones.

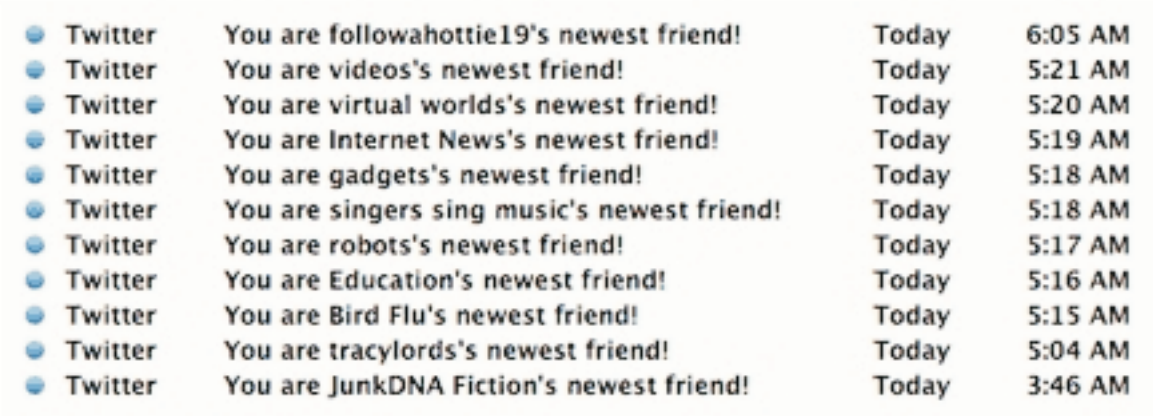
En segundo lugar, cuando el usuario pinchaba sobre el enlace, se le mostraba un mensaje diciendo que no puede ver el vídeo porque no tiene el códec correspondiente y se le ofrecía la posibilidad de descargarlo. Sin embargo, lo que se descargaba era una copia del troyano. Para evitar sospechas, mientras el troyano era descargado, el usuario era redirigido a una página en la que se le mostraba el vídeo prometido.

Una vez infectado el equipo, el troyano publicaba su mensaje malicioso en los "scrapbooks" de todos los contactos de Orkut de su nueva víctima.

Redes sociales en el punto de mira

Spam en *Twitter*

Como hemos mencionado anteriormente, el spam también ha llegado a las redes sociales y a finales de mayo se detectaron mensajes de spam en *Twitter*.



Twitter	You are followahottie19's newest friend!	Today	6:05 AM
Twitter	You are videos's newest friend!	Today	5:21 AM
Twitter	You are virtual worlds's newest friend!	Today	5:20 AM
Twitter	You are Internet News's newest friend!	Today	5:19 AM
Twitter	You are gadgets's newest friend!	Today	5:18 AM
Twitter	You are singers sing music's newest friend!	Today	5:18 AM
Twitter	You are robots's newest friend!	Today	5:17 AM
Twitter	You are Education's newest friend!	Today	5:16 AM
Twitter	You are Bird Flu's newest friend!	Today	5:15 AM
Twitter	You are tracylords's newest friend!	Today	5:04 AM
Twitter	You are JunkDNA Fiction's newest friend!	Today	3:46 AM

Figura 16. Mensajes de *spam* en *Twitter*.

Los usuarios de *Twitter* recibieron oleadas de correos electrónicos del sistema interno de *Twitter*, avisando de la existencia de nuevos followers (usuarios registrados). El problema está en que los perfiles de estos nuevos followers contienen anuncios publicitarios de tipo spam. De esta manera, cuando un usuario intentara saber quién es el follower, visualizaría el spam.

Consejos para navegar por las Redes Sociales

En la actualidad, las redes sociales se han convertido en un importante objetivo para los ciber-delincuentes. Por ello, conviene permanecer alerta ante posibles ataques y seguir una serie de pautas para navegar de forma segura por las redes sociales.

Además de las medidas de seguridad básicas como tener instalada y correctamente actualizada una solución de seguridad en el equipo, hay otra serie de medidas que pueden ayudar a prevenir estos ataques.

Es conveniente no compartir datos confidenciales, como direcciones de correo o claves, a través de foros o chats para intercambiar información, conversar, etc. Por otra parte, es aconsejable no proporcionar más información de la necesaria en los perfiles. En caso de que sea obligatorio proporcionar datos privados como la dirección de correo, se debe seleccionar la opción de "no visible para el resto de usuarios" o similar, de tal modo que nadie salvo el propio usuario y los administradores puedan tener acceso a esos datos.

Inteligencia Colectiva

La principal novedad de la gama de productos 2009 de Panda Security respecto a versiones anteriores es la "Inteligencia Colectiva". A continuación vamos a explicar los motivos que nos han llevado a realizar esta evolución tecnológica.

Situación actual

En primer lugar comencemos con los hechos. Existen dos críticas constantes que son aplicables a todos los antivirus en mayor o menor medida:

- El hecho de ser reactivos de cara a la aparición de nuevas amenazas.
- El alto consumo de recursos en el que incurren.

El hecho de ser reactivos es algo inherente a la principal tecnología que incorporan todos los productos antivirus: la detección por firmas. Básicamente esta tecnología se basa en incorporar firmas que permitan al producto reconocer código malicioso en los ficheros. Si bien es una tecnología muy antigua, que ya incorporaban los primeros antivirus de la historia, ha demostrado ser tremendamente válida y eficaz. Pero tiene una gran desventaja: es necesario conocer previamente el código malicioso para poder añadir la firma, probarla, y hacérsela llegar al usuario del producto.

Con la multiplicación del nuevo malware existente en circulación, todas las compañías antivirus tienen una idea, aunque muy pocas son capaces de confesarla públicamente: si sólo vemos el malware que conocemos, las probabilidades de que nuestros clientes estén infectados por malware nuevo del que aún no tenemos constancia son muy altas. Si a esto le añadimos que la aparición de nuevo malware ha crecido de forma exponencial durante los últimos años, las perspectivas no son precisamente halagüeñas. Además, aunque se tiene la certeza de que esto es así, hay que demostrarlo científicamente para poder afirmar con rotundidad que es un problema real que debemos atajar.

Éste es un problema conocido desde hace muchos años, y de hecho la mayoría de compañías antimalware han ido desarrollando nuevas tecnologías que permiten detectar parte de los nuevos códigos maliciosos que aparecen y así no tener que depender de las firmas. Hablamos de tecnologías con muchos años, como la tecnología heurística, y otras más recientes como la de análisis de comportamiento.

Inteligencia Colectiva

Esto nos lleva a la segunda crítica mencionada previamente: el alto consumo de recursos. Las amenazas van evolucionando con el tiempo, y las compañías antivirus nos vamos adaptando. Es ley de vida, pero puede tener unos efectos colaterales desastrosos. Aparecieron los virus y surgieron los programas antivirus. Empezaron a surgir otro tipo de amenazas y las compañías antivirus empezamos a integrar en los antivirus todo tipo de nuevas tecnologías para combatir estas amenazas: firewall, antispam, antispyware, heurísticos, analizadores de comportamiento, filtrado de contenidos, etc. A todo esto, la aparición de millones de ejemplares nuevos de malware ha llevado a multiplicar el tamaño del fichero de firmas, que se carga en la memoria del PC. Recientemente la mayoría de compañías hemos empezado a añadir otro tipo de características a nuestros productos, como backup o "tune-up". Si bien todos lo hacemos con la mejor de las intenciones: tratar de proteger más y mejor a los usuarios, estamos cargando los ordenadores con tareas que en ocasiones podríamos calificar de mastodónticas.

El nacimiento de la Inteligencia Colectiva

En los laboratorios de las compañías antivirus, además de analizar los nuevos ficheros y crear firmas para detectarlos y desinfectarlos, tenemos un equipo de personas encargadas de desarrollar tecnologías para poder detectar nuevos especímenes de malware de manera automática. En la actualidad, Pandalabs cuenta con un sistema que es capaz de clasificar la mayoría de ficheros que conseguimos: en 2007, el 94.4% de todas las nuevas detecciones se pudieron añadir gracias a este sistema.

La pregunta es obvia: ¿Por qué no integrar esto en los antivirus que vendemos? ¿No protegeríamos mejor? Sí, pero la capacidad de proceso que se requiere es tal, que es completamente inviable integrar esto para su ejecución en PCs de sobremesa. Además habría que sumarlo a todo lo que ya está y que en ocasiones parece asfixiar a nuestro PC.

Partiendo de esta base, comenzamos a pergeñar la idea de la "Inteligencia Colectiva": ¿Y si en vez de mandar al PC local que haga todo el trabajo duro de cálculo y decisión, dejamos gran parte de ese esfuerzo para nuestros servidores y así aligeramos de trabajo a los PCs de nuestros clientes? La idea era tentadora, y además podría dar mucha más capacidad de detección: actualmente, cuando se estudia el comportamiento de un fichero en ejecución, se mira en el PC que se está ejecutando, y esa es la información en la que se basará este programa para dar un veredicto sobre el fichero. En ocasiones no hay información suficiente y no se puede tomar una decisión final sobre si es bueno o malo. En cambio, si tenemos un repositorio central donde podemos correlacionar todas las evidencias de un mismo fichero, o incluso de ficheros similares, contaremos con mucha más información para poder dar un dictamen.

Inteligencia Colectiva

Aterrizando las ideas

En cualquier caso, de la teoría a la práctica hay un largo recorrido: ¿Qué infraestructura es necesaria? ¿Qué información se puede obtener respetando la legalidad vigente en los diferentes países? Pero estos factores no podían hacer nada contra nuestra determinación, la idea era demasiado buena para poder tirarla abajo a las primeras de cambio.

Sobre la información a obtener, resultó relativamente sencillo. Cuando explicamos internamente la idea, hubo quien pensó que necesitábamos subir todos los ficheros a nuestros servidores para poder analizarlos aquí. Por supuesto nada más lejos de la realidad. Para poder clasificar un fichero nos hace falta un identificador del mismo y algo de información del fichero. Si analizas un fichero de 2 kb, vamos a necesitar unos pocos bytes de información, y lo mismo es si el fichero ocupa 10, 20 ó 100 Mb. Pero lo mejor es que ni siquiera necesitamos una parte del fichero, sino unos checksums, por lo que minimizamos la información a enviar y además nos aseguramos de no llevarnos ningún dato personal.

Primeras pruebas de concepto y demostración empírica de la existencia del problema

El año pasado lanzamos una prueba de concepto de esta tecnología; era un antivirus basado en web que no tenía fichero de firmas y ocupaba menos de 400kb. Sólo hacía análisis bajo demanda de los ficheros que estaban en ejecución en memoria, y aún así tuvo una gran aceptación. Tras un tiempo de uso, decidimos estudiar los datos obtenidos y a su vez comprobar realmente si la potencia del nuevo concepto era la misma que imaginábamos. Los datos fueron muy buenos y muy preocupantes al mismo tiempo.

De cada ordenador que lanzaba un análisis se hacía una consulta en el centro de seguridad de Windows para ver si tenía o no antivirus, si estaba activo, actualizado, etc. A la hora de trabajar con los datos, separamos todos aquellos PCs que no tenían un antivirus instalado, activo y actualizado. Y comenzamos a sacar los datos por fabricante antivirus. ¿Cuál fue el resultado? TODOS los antivirus (Panda incluido) tenían clientes infectados. Publicamos un paper con todos los datos, pero resumo lo más interesante:

- Sólo el 37,45% de los PCs tenían un antivirus activo y actualizado.
- Más del 23% de los ordenadores analizados que tenían un antivirus activo y actualizado tenían malware en memoria. Al hablar de malware nos referimos a todo tipo de amenazas, como virus, troyanos, gusanos, spyware, etc.

Inteligencia Colectiva

- Estos son los porcentajes de infección que encontramos en las principales compañías antivirus:

CA:	23,32%
McAfee:	24,18%
Panda:	15,54%
Symantec:	22,20%
Trend Micro:	17,08%

Aparecen en orden alfabético porque no es un ranking. En el estudio aparecían en total más de 30 compañías diferentes, todas con unos ratios de infección que iban del 12-13% hasta el 30% aproximadamente.

Integración de la Inteligencia Colectiva en los productos

Visto lo visto estaba claro hacia dónde debíamos ir, por lo que comenzamos a aplicar estas tecnologías a nuestra gama de productos 2009 que estábamos desarrollando. ¿En qué se diferencian de los anteriores productos? El cambio más radical es la integración de la Inteligencia Colectiva, ¿pero qué beneficios aporta esto?:

- Fichero de firmas optimizado (el fichero de firmas es el que se carga en memoria para detectar malware conocido).
- Conexión con la Inteligencia Colectiva cuando se realiza un análisis para maximizar la detección de malware.

Inteligencia Colectiva

Este es un gráfico que refleja el funcionamiento básico del sistema:

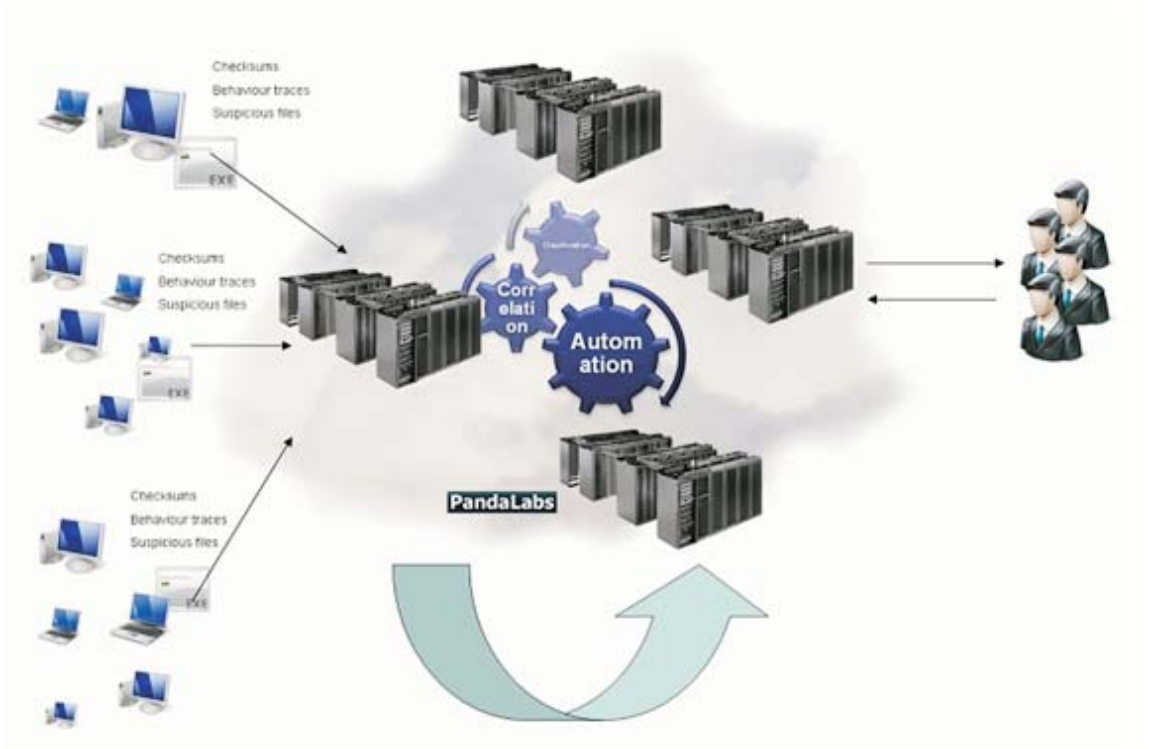


Figura 17. Gráfico que representa el funcionamiento del nuevo sistema.

A todo esto, hay que añadirle TruPrevent 2.0: la fusión de TruPrevent 1.0 con la *Inteligencia Colectiva*. La primera versión de las tecnologías TruPrevent estaba diseñada para complementar la tarea de los antivirus, ayudándoles a frenar el malware desconocido. Para ello, estas tecnologías analizaban el comportamiento de todos los programas que ha dejado pasar el antivirus y bloqueando aquellos que realizan acciones nocivas y resultan ser virus desconocidos.

El método de detección de TruPrevent 1.0 consiste en analizar todos los elementos o amenazas potenciales mediante distintas técnicas, llevando a cabo inspecciones complementarias en profundidad en diferentes capas de la infraestructura. Tecnológicamente, TruPrevent consta de dos tecnologías principales: el análisis de comportamiento y el bloqueo por comportamiento.

Inteligencia Colectiva

Panda lanzó al mercado esta tecnología en 2004. Desde entonces, han sido cuatro años de innovación y mejora que han concluido con esta nueva versión. En ella, por un lado los diferentes motores (heurístico, análisis de comportamiento, etc.) se han adaptado al malware actual, utilizando nuevos sensores, etc. Además cada vez que detectan algo, consultan a la nube para obtener información del fichero, por lo que podemos poner TruPrevent en un modo más agresivo a la hora de detectar malware siguiendo con unos ratios de falsos positivos prácticamente inexistentes.

En definitiva, se ha adaptado TruPrevent a la realidad actual del malware, caracterizada por una auténtica avalancha de códigos maliciosos nuevos cada día. Con esta nueva tecnología se consigue detectar y bloquear un mayor número de ejemplares, con un menor consumo de los recursos del PC, al estar gran parte de la información alojada en los servidores de Panda y no en el PC del usuario.

Preguntas y respuestas

Cuando nos encontramos con tecnologías novedosas siempre surgen preguntas a la que es necesario dar respuesta. Recojo a continuación las preguntas más frecuentes que me han realizado al respecto:

P: ¿Qué quiere decir tener un fichero de firmas optimizado?

R: Desde PandaLabs utilizamos nuestra red de más de 4.000.000 de sensores para poder saber qué malware está actualmente en circulación y así seleccionar las firmas necesarias para proteger los PCs ante el malware que realmente está activo.

Por ejemplo, una prueba de concepto de un malware que nunca se ha visto en calle por ninguno de nuestros sensores y se creó en el año 2000, no es necesario que vaya incluido. Si hablamos de un virus que apareció en 1995 pero que se ha visto activo estará incluido.

En cualquier caso, a través de la Inteligencia Colectiva contamos con millones de firmas, no sólo de todo el malware, sino también de millones de ficheros buenos conocidos, lo que nos hace contar con la mayor capacidad de detección disponible actualmente.

Además, contamos aún con una baza muy importante: las tecnologías proactivas TruPrevent, aunque se benefician de la comunicación con la Inteligencia Colectiva no requieren estar conectadas a Internet para detectar y parar malware desconocido.

Inteligencia Colectiva

Conclusión: protección al cubo → Firmas + TruPrevent + Inteligencia Colectiva, consumiendo menos recursos.

P: ¿Por qué se sigue utilizando el fichero de firmas, teniendo la Inteligencia Colectiva todas las firmas? ¿No se puede prescindir de él?

R: El uso de la Inteligencia Colectiva requiere de conexión a Internet. Si bien es cierto que más del 99% de las infecciones que se producen hoy en día vienen a través de Internet, queda una pequeña ventana de riesgo si estamos sin conexión e introducimos ficheros mediante algún método de almacenamiento desde un CD hasta un dispositivo USB. Por este motivo se mantiene el fichero de firmas con todo el malware activo, para proteger ante estos ataques.

P: Al tener que estar en contacto con la inteligencia colectiva, ¿no se resentirá mi conexión a Internet debido al ancho de banda necesario para realizar las consultas?

R: No. Como he explicado anteriormente, sólo se necesitan unos pocos bytes por cada fichero. Asimismo, la respuesta que obtendremos es también de unos pocos bytes. Además, el sistema es inteligente y crea una caché local para no estar continuamente preguntando por los mismos ficheros.

P: Entiendo que gracias a la Inteligencia Colectiva el producto consumirá menos recursos, ¿pero no notaré ralentización en mi sistema debido a la comunicación entre mi ordenador y la inteligencia colectiva, quedando a la espera de respuesta cada vez que me llegue un nuevo fichero?

R: No, el sistema ha sido concebido desde el principio no sólo para aumentar la capacidad de detección, sino para disminuir el consumo de recursos y la percepción de pesadez que tienen los productos antivirus que no incorporan esta tecnología.

P: ¿Entonces ahora estoy completamente protegido?

R: No. Y no quiero dejar lugar a dudas, malentendidos o ambigüedades: NO. No existe tecnología que hoy en día pueda garantizarnos una completa protección. Eso sí, desde mi experiencia personal puedo calificar esta tecnología como la que nos ofrece una mejor protección de todas las existentes en el mercado.

Inteligencia Colectiva

Futuro próximo

¿Y ahora qué? La verdad es que el ideal que teníamos no se ve completamente reflejado en los productos 2009, ya que somos muy ambiciosos. No puedo hablar de ello aún, pero digamos que nuestra idea es algo más parecido a Nanoscan, un antivirus muy muy pequeño y ligero. Estamos convencidos de que es la vía correcta; recientemente Trend Micro anunció que van a sacar productos con conexión a "la nube", y con el tiempo el resto de nuestros competidores nos irán siguiendo.

Además la *Inteligencia Colectiva* tiene otro beneficio que no he mencionado en todo el artículo, aunque seguramente muchos de vosotros lo habréis deducido ya: si creo nuevos sistemas de clasificación y detección de malware, puedo llegar a aplicar esta tecnología a todos los productos de forma transparente, ya que las nuevas tecnologías se aplicarán a nuestros sistemas de *Inteligencia Colectiva* en vez de a los productos instalados en los PCs de nuestros clientes.

Sobre PandaLabs

PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- Desde ***PandaLabs*** se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.

- ***PandaLabs*** se encarga asimismo de llevar a cabo el análisis detallado de todos los tipos de malware, con la finalidad de mejorar la protección ofrecida a los clientes de Panda Security, así como para informar al público en general.

- Del mismo modo, ***PandaLabs*** mantiene un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad. Su objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.

- Se puede obtener información sobre las últimas amenazas descubiertas en el blog de ***PandaLabs*** en: http://pandalabs.pandasecurity.com/.