Tendencias 2009: Internet como plataforma de infección

Autor: El equipo de Laboratorio de ESET Latinoamérica
Fecha: Jueves 11 de Diciembre de 2008

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

Tendencias 2009: Internet como plataforma de infección

ESET, la compañía líder en detección proactiva publica un informe sobre las tendencias que se esperan para el 2009 en materia de códigos maliciosos y seguridad antivirus.

Durante el 2008 se han fortalecido las nuevas estrategias de infección y se marcó el camino para los próximos años en lo relacionado con ataques a través de malware.

Asimismo, la creación y distribución de malware se ha convertido en un gran negocio para muchos, generando elevadas ganancias para los delincuentes que están detrás de esta actividad y llevando la cantidad de códigos dañinos a números impensables años atrás.

Este camino refleja el interés de los creadores de malware por mover íntegramente sus plataformas de infección a Internet, utilizando servidores para descargar una cantidad importante de variantes del mismo malware a los equipos de los usuarios y haciendo uso de las redes sociales como medio de propagación.

El malware ya dejó de ser un fin en si mismo hace tiempo, transformándose en una herramienta para el verdadero objetivo, que es la búsqueda del rédito económico, lo cual derivó en la profesionalización del desarrollo y distribución de códigos maliciosos, al punto de crear un ecosistema industrial en sí.

En lo que cabe esperar para el próximo año se destacan, entre otros, los temas y tendencias que se exponen a continuación.

Automatización de ataques y métodos de engaño

Como siempre, la Ingeniería Social [1] continuará siendo uno de los elementos de mayor importancia en cualquier tipo de infección. Las técnicas utilizadas por los creadores de malware se diversifican y perfeccionan para seguir engañando al usuario para que termine instalando un programa que producirá algún daño en su sistema.

Los creadores de malware se aprovecharán de temas de alto impacto, como la incertidumbre financiera y económica, que serán utilizados como excusa para la divulgación de malware.

A las técnicas ya conocidas que explotan las vulnerabilidades humanas (como el morbo, la ambición, las tragedias, las cuestiones sexuales, etc.) se sumarán herramientas automatizadas que permitirán la rápida creación y propagación de páginas web con scripts dañinos, sometidos a métodos de ofuscación que

potenciarán la velocidad con que una amenaza puede afectar a los usuarios, como ya se está dando en ataques del tipo *Drive-by-Download* [2].

Las vulnerabilidades y las actualizaciones

Durante años se manifestó la necesidad de actualizar los sistemas operativos y aplicaciones utilizados, con los parches de seguridad publicados por los desarrolladores de software.

Esta necesidad se hace cada vez más evidente debido a la gran cantidad de malware que en la actualidad aprovecha las vulnerabilidades de los sistemas operativos, navegadores, reproductores multimedia, paquetes de ofimática y cualquier otra aplicación, para instalar códigos dañinos en la computadora del usuario sin que éste se percate de tal situación.

La utilización de las vulnerabilidades como medio de distribución de malware se verá en mayor medida en el futuro cercano, llegando al punto en el que se expanda un "mercado negro" de *exploits 0-day* (códigos para explotar agujeros de seguridad desconocidos o sin solución) que permitan a los creadores de malware adquirirlos y utilizarlos aún antes de que el desarrollador del software involucrado esté informado y/o esté trabajando en una actualización.

Masificación de falsos programas de seguridad

En el año 2008 se registró un alto porcentaje de aumento de la difusión de aplicaciones diseñadas para romper el esquema de los códigos maliciosos tradicionales, y para infectar a los usuarios con infinidad de malware a través de una misma vía, la falsa afirmación de ser supuestas herramientas de seguridad: los *rogue* [3].

Teniendo en cuenta la masificación y las técnicas de infección empleadas por este tipo de programas dañinos, todo indica que se ampliará peligrosamente su familia con diferentes variantes y métodos de infección cada vez más nocivos, sobre todo si se toma nota de la forma específica en que los creadores de este tipo de malware lo aprovechan para generar un rédito económico.

Internet como plataforma de ataque

El uso masivo de Internet y del acercamiento del usuario a las plataformas móviles ofreciendo servicios a través de la red (*Cloud Computing*), no pasó desapercibido a los creadores de malware.

Durante el próximo año se verá incrementada la aparición de:

- *Exploits* para mayor cantidad de navegadores, ampliando la "oferta" actual existente para Internet Explorer y Firefox.
- Mayor cantidad de abuso de servidores ajenos y vulnerables a través de herramientas automáticas (*bot*) para encontrar estos servidores e instalar scripts, que permitan vulnerar sistemas no actualizados de usuarios y empresas, infectándolos.
- Mayor movilidad del malware destinado a servidores vulnerables e incremento en la cantidad de variantes de cada malware. Esto tiene como objetivo lograr menores índices de detección por parte de las herramientas antivirus.
- Registro y aparición de dominios creados para propagar malware utilizando técnicas de posicionamiento en buscadores (SEO) [4]. En este sentido el *rogue* actual ha demostrado ser muy efectivo en su propagación.
- Mayor disponibilidad de herramientas públicas y/o comerciales para realizar los ataques mencionados. Estas herramientas son desarrolladas por grupos que proveen servicios ilegales de este estilo.

Con este tipo de movilidad en Internet cada componente dañino posee un rol dinámico y activo, buscando maximizar la posibilidad de infección ya sea a través de scripts, de vulnerabilidades encontradas o a través de las miles de variantes de cada malware en particular que aparecen diariamente.

Nuevos métodos de ocultamiento

Este año tuvimos la experiencia de las acciones provocadas por códigos maliciosos como MebRoot (malware con capacidades de *rootkit* que infecta la MBR de los discos rígidos) y, bajo esta perspectiva, todo parece indicar que surgirán y/o se perfeccionarán nuevas técnicas que permitan al malware ocultar en el sistema sus actividades dañinas.

Así mismo la aparición de scripts dañinos en archivos que típicamente se piensa que son inocuos (*.PDF*, *.MP3*, *.SWF*, .XPI, etc), producirán nuevas olas de posibles infecciones, ya que para el usuario estos archivos suelen pasar desapercibidos.

Servicios a disposición del malware

El *Malware as a Service (MaaS)* se afianzará y se potenciará el desarrollo de economías alternativas que dependen de la aparición de nuevos programas maliciosos. Este tipo de aplicaciones dañinas orientadas a ofrecer servicios son similares al modelo legal de distribución de software como servicio, basado en la lógica del negocio *Software as a Service (SaaS)*.

Los mercados de delincuentes como los que se encuentran en regiones de Europa del Este y en Brasil utilizan el servicio de programadores para el diseño de software dañino, con el ánimo de infectar a la mayor cantidad de usuarios posibles, buscando obtener información privada [5] que pueda ser utilizada para realizar robos, fraudes y estafas.

En este sentido se pueden diferenciar varias categorías:

La primera de ellas se encarga de la creación y propagación de distintas variantes de troyanos bancarios triviales y especialmente orientados tanto a ataques de *phishing* como de *pharming* para obtener información confidencial.

Otra rama está orientada a crear redes de equipos infectados (*botnets*), utilizadas para ser alquiladas y ofrecer servicios como alojamiento de sitios web ilegales, material pornográfico, distribución de spam, warez, cracks, ataques DDoS, entre otros.

Una rama más especializada pero igualmente peligrosa, se dedica a crear nuevos tipos de malware con mayores capacidades técnicas y que podrán ser utilizadas por otros desarrolladores en el futuro.

Y por último, están los delincuentes que comercializan y obtienen ventajas competitivas y económicas del desarrollo de nuevas herramientas dañinas y del robo de información confidencial.

Explotación de fuentes de información populares

La masificación de las redes sociales, con millones de usuarios haciendo uso de estas plataformas, permite a los delincuentes contar con una gran base de datos de usuarios a quienes se podrá engañar, infectar o estafar.

El desarrollo de estos medios de comunicación como recurso económico, y la posibilidad de interconectar millones de usuarios, da un nuevo margen de desarrollo a los creadores de malware, quienes se verán tentados por la gran cantidad de dinero que se mueve en estas plataformas virtuales.

Por otro lado seguirán creciendo las técnicas de engaño, aprovechando el buen nombre de los medios de comunicación más populares (diarios, revistas, sitios web, etc.), lo cual da credibilidad a las noticias falsas que se difunden, que generalmente contienen malware.

En el próximo año se incrementará el uso de diferentes métodos destinados a la obtención de información sobre potenciales víctimas y la difusión de malware a través de las comunidades virtuales, utilizando las mismas técnicas de Ingeniería Social ya conocidas desde hace tiempo.

Juegos en línea y sus métodos de propagación

El crecimiento de las plataformas virtuales dio como resultado que gran cantidad de jugadores se muevan hacia ellas y durante este año también se notó en Latinoamérica un incremento importante en cuanto al uso de estos juegos, a punto tal que la familia de troyanos denominados OnLineGames [6], una de las principales amenazas propagadas, fue diseñada para explotar este tipo de actividad.

Todo indica que América Latina esta viendo potenciadas estas capacidades luego de que estos juegos hicieran furor en Asia; por lo tanto, los creadores de malware seguirán aprovechando estas ventajas.

Con respecto al medio de propagación elegido por este tipo de troyanos prevalece el uso de medios removibles como memorias y llaves USB [7], que permiten una amplia difusión en ambientes de jóvenes en donde los juegos son muy populares. Luego esta difusión alcanza a cualquier otro entorno doméstico, académico y empresarial debido al uso masivo de estos dispositivos.

Evolución de las capacidades de infección

El año pasado anunciábamos esto como una tendencia que se vio reflejada en el último cuatrimestre: la posibilidad de modificar múltiples tipos de archivos como *.MP3*, *.PDF*, *.SWF*, extensiones de navegadores como *.XPI*, etc., y no nos hemos equivocado [8].

Los creadores de malware han logrado potenciar la posibilidad de que un usuario que descargue cualquiera de estos archivos pueda infectarse, demostrando que cualquier aplicación y cualquier tipo de archivo puede ser vulnerable y/o utilizado como vía de infección.

Las tecnologías ampliamente adoptadas y utilizadas por la mayoría de los usuarios abren nuevas vías de infección para los desarrolladores de malware, y es por eso que las capacidades y medios de propagación siguen creciendo. Hay que recordar que el malware es tanto una herramienta como un negocio y, como tales, se adaptan a los medios utilizados por el usuario. Esta lección debería quedar clara para el futuro.

Nuevas tecnologías

Lo mencionado el año pasado [8] sobre infecciones por intermedio de dispositivos de almacenamiento extraíbles (USB, memorias flash, etc) ha sido superado por los delincuentes, que ya utilizan estos medios masivamente para propagar sus amenazas.

Es válido hacer una mención aparte con respecto a los dispositivos móviles como *smartphones* y *Pocket PCs*, cada vez más utilizados, que lentamente se van volviendo un objetivo para los delincuentes dada la mayor masificación de los mismos.

A medida que se produzca una estandarización de los sistemas operativos para estos aparatos, se irá notando una tendencia mayor a crear y desarrollar métodos que los vuelvan un objetivo para todo tipo de ataques y amenazas informáticas.

Sin embargo aunque es esperable encontrar nuevos vectores de ataque para estos dispositivos durante el 2009, no se espera una gran cantidad de ellos en comparación con los existentes para plataformas de PC y servidores.

Los métodos de siempre

Estas tendencias marcarán el rumbo para años futuros, pero es importante recordar que los medios de propagación e infección por canales ya conocidos no disminuirán, e incluso cabe la posibilidad de que los mismos se vean potenciados por algunos de los nuevos vectores mencionados.

El spam seguirá siendo difícil de controlar y si a ello le sumamos la posibilidad de propagación de casos de *phishing* y malware a través del correo, esto lo convierte en una de las amenazas más riesgosas para cualquier organización, por lo que contar con filtros antispam adecuados en los equipos o en el perímetro es una prioridad.

Las *botnets* representan una nueva economía en sí misma, ya que por medio de ellas los delincuentes pueden ofrecer servicios ilegales a cualquier costo, y el dinero obtenido es casi imposible de rastrear. Técnicamente las redes de usuarios infectados pueden ser utilizadas para cualquier fin como los ya mencionados en *MaaS*.

Protección

La gran cantidad de malware existente, en el rango de las miles de variantes, hace necesario por parte de los delincuentes una amplia capacidad para propagar las amenazas y que las mismas lleguen al usuario en el menor tiempo posible, siendo para ello necesario contar con **herramientas de protección proactiva de última generación**, capaz de detectar cualquier variante en cualquier momento sin la necesidad de una actualización del software.

A ello debe sumarse la educación del usuario en cuanto al uso seguro y responsable de los recursos tecnológicos, para que no se deje engañar por las técnicas utilizadas por los creadores de malware. Con respecto a este punto, ESET ha desarrollado una Plataforma de Educación en Línea [9] donde el usuario puede conocer las más recientes amenazas y capacitarse para prevenirlas.

La conjunción de soluciones unificadas de protección proactiva y heurística, junto con el trabajo en la prevención mediante la educación, información y capacitación, representan factores claves a la hora de elevar el nivel de protección de cualquier recurso informático, sin importar que sea una computadora hogareña o una red corporativa.

Conclusiones

Durante el 2008 se observó cómo comenzó la tendencia de mudar los ataques de códigos maliciosos a plataformas en Internet, teniendo como foco lograr la infección en distintos sitios y servidores web, con el fin de atacar directamente a sus visitantes. De esta forma se logró disminuir las posibilidades de que el usuario advierta una posible infección, y también se aumentaron los obstáculos que enfrentan las empresas antivirus y sus investigadores para localizar fácilmente estos distintos pequeños focos de infección.

Esta tendencia de los diseñadores de malware continuará desarrollándose en el año entrante, y principalmente estará enfocada en la masificación de los equipos zombies controlados por las *botnets* y en la facilidad de controlar servidores infectados difíciles de rastrear.

Teniendo en cuenta esta tendencia, cada vez se torna más importante la capacitación y educación de los usuarios en seguridad antivirus, ya que aunque los tradicionales consejos de no abrir archivos adjuntos a los correos electrónicos, no aceptar archivos llegados por mensajería instantánea, etc. mantienen su vigencia, actualmente otros consejos adquieren mayor relevancia.

Muchos usuarios entrarán a sitios web sin tomar precauciones y podrán ser infectados debido a que la página fue vulnerada por un atacante y éste aprovecha una vulnerabilidad en el sistema del usuario para

infectarlo. En este tipo de casos, sólo un usuario con conocimientos sobre seguridad y las mejores prácticas podrá advertir un comportamiento extraño del sitio web visitado.

La importancia de actualizar [10] tanto el sistema operativo como las aplicaciones también será muy alta, ya que aparecerán grandes cantidades de códigos maliciosos que se aprovechen de *exploits* para realizar ataques e infecciones.

Además, durante este año también se pudo ver que ningún tipo de archivo es seguro, ya que existieron ataques a diversos tipos de ellos. Nuevamente, la educación del usuario y la actualización del sistema operativo y las aplicaciones vuelven a ser vitales para prevenirse de estos ataques.

Sin importar qué solución de seguridad se tenga instalada, ni qué aplicaciones se utilicen en el sistema, la mejor herramienta para combatir las amenazas del próximo año será capacitarse y estar al tanto de las últimas tendencias, así como contar con software de seguridad con capacidades de protección proactiva, como las soluciones de ESET, para detectar malware conocido y desconocido.

Los creadores de malware continúan profesionalizándose para mejorar sus códigos maliciosos y así obtener un mayor rédito económico; por eso también es importante que cada usuario conozca las mejores prácticas de seguridad, ya que será la mejor manera de proteger su equipo, su información y también sus activos.

Más Información:

[1] Ingeniería Social
http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social

[2] Drive-by-Download: infección a través de sitios web
http://www.eset-la.com/threat-center/1792-drive-by-download-infeccion-web

[3] Rogue: Falsos antivirus gratis
http://www.eset-la.com/threat-center/1793-rogue-falsos-antivirus-gratis

[4] Posicionamiento en buscadores, SEO
http://es.wikipedia.org/wiki/Posicionamiento_en_buscadores

[5] Robo de información personal online
http://www.eset-la.com/threat-center/1774-robo-informacion-personal-online

[6] Jugando sucio, un análisis del malware en juegos en línea
http://www.eset-la.com/threat-center/1788-jugando-sucio

[7] Propagación de malware a través de dispositivos removibles
http://www.eset-la.com/threat-center/1796-malware-dispositivos-removibles

[8] Tendencias 2008: Qué nos depara el malware en el futuro
http://www.eset-la.com/threat-center/1709-tendencias-2008

[9] Plataforma de Educación en Línea de ESET Latinoamérica
http://edu.eset-la.com/

[10] La importancia de las actualizaciones
http://www.eset-la.com/threat-center/1996-importancia-actualizaciones