Tendencias 2010: la madurez del crimeware

Autor: Equipo de Laboratorio de ESET Latinoamérica
Fecha: Viernes 20 de Noviembre de 2009

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

Índice

Tendencias 2010: la madurez del crimeware

Ante la proximidad del inicio de un nuevo año, el equipo de ESET, la compañía líder en detección proactiva de amenazas, desarrolló el presente informe sobre las tendencias para el 2010 en materia de códigos maliciosos y seguridad antivirus.

En la edición del año pasado, los especialistas en seguridad informática de ESET Latinoamérica pronosticaron el traslado de los principales ataques de malware hacia Internet, utilizando esta última como plataforma de ataque. Esta tendencia se vio confirmada durante 2009 y se espera que continúe durante 2010.

En materia de códigos maliciosos, durante el 2010 el crimeware [1] será el vector de ataque sobresaliente. La tendencia de los ciberatacantes a monetizar su tarea ha encontrado en el cibercrimen un aliado, motivo por el cual se verá un claro aumento en los códigos maliciosos creados con fines económicos y financieros.

A continuación se describirán detalladamente estas y otras tendencias en materia de malware para el año 2010.

Internet como plataforma de infección

Se espera que la orientación pronosticada por el equipo de ESET en el informe “Tendencias 2009: Internet como plataforma de infección” [2] continúe y se acentúe durante el 2010.

El crecimiento en las tasas de conectividad será la principal variable para que los atacantes persistan en la utilización de Internet como medio preferido para propagar malware e infectar a los usuarios. Asimismo, Internet también será aprovechada por los cibercriminales para controlar y administrar sus organizaciones. Como se expondrá en el presente artículo, la conformación de grupos de atacantes trabajando en forma conjunta se verá potenciada por la posibilidad de comunicarse en forma dinámica, anónima y segura a través de Internet.

La utilización de sitios benignos como medio para la propagación continuará siendo una vía de ataque efectiva para los creadores de malware. La escasa seguridad que presentan la mayoría de los sitios web (incluso algunos muy populares en cantidad de visitas), facilitará que sean utilizados por los atacantes para inyectar contenidos maliciosos que infecten a los usuarios durante la navegación por las páginas web allí alojadas.

Redes sociales

Las redes sociales también constituirán un medio preferido para la propagación de malware por parte de los ciberatacantes. El tiempo promedio de visita de los usuarios en este tipo de plataformas está en aumento constante y los atacantes aprovecharán este factor para continuar explotando las diversas oportunidades que estas redes ofrecen para enlazar a contenidos maliciosos.

Así como a comienzos de 2009 Facebook fue la primera red afectada por la propagación del gusano Koobface [3], a lo largo del año otras plataformas como Linkedin o Twitter también fueron atacadas. En consecuencia es de esperar que las redes sociales más populares se conviertan en potenciales blancos de ataque durante el próximo año.

Además, las mismas serán utilizadas por los creadores de malware con fines organizativos, tales como comercializar sus creaciones o administrar redes botnets, entre otras tareas.

Malvertising

La publicidad *on-line* permite a los atacantes posicionar sus sitios en diversas páginas de Internet para, de este modo, direccionar a los usuarios hacia contenidos maliciosos.

La alta tasa de utilización de esta técnica permite que muchos sitios con contenido malicioso se encuentren publicitados en páginas web legítimas o en populares buscadores, siendo ésta una herramienta de alto valor para los atacantes que continuará en crecimiento.

También conocido como *malvertising*, el abuso de publicidad con contenidos maliciosos será tendencia durante el próximo año. En sus escasas apariciones durante el 2009, la utilización más frecuente de esta técnica consistió en la compra de espacios publicitarios realizados con Flash, colocando allí anuncios con script maliciosos para explotar vulnerabilidades en determinadas versiones del reproductor.

En forma genérica, el *malvertising* consiste en ubicar espacios publicitarios en sitios web o redes sociales que enlacen directa o indirectamente a la instalación de software malicioso. Esta técnica permite a los atacantes tener como potencial víctima a cada persona que visite el sitio web donde se alojó la publicidad en línea.

Crimeware

Crimeware [1] es cualquier tipo de malware que ha sido diseñado y desarrollado para perpetrar un crimen del tipo financiero o económico.

Llamamos cibercrimen a cualquier delito que se realice con una computadora, a través del uso de tecnologías informáticas o siendo una computadora o recurso informático el destinatario del mismo. En este sentido, muchos delitos conocidos desde la Antigüedad, hoy se realizan por medio de recursos informáticos.

Desde este punto de vista los códigos maliciosos se encuentran entre los más valiosos recursos para llevar adelante el cibercrimen. Las altas tasas de propagación, la posibilidad de controlar computadoras remotamente y robar información a través de botnets, junto con la capacidad de modificar las configuraciones de los sistemas (entre muchas otras acciones que realiza un malware), facilitan la concreción de otros delitos de mayor gravedad, específicamente orientados al robo de información en línea o robo de dinero.

Por lo tanto es de esperarse que aumente la cantidad de códigos maliciosos de este tipo, tanto en cantidad como en proporción respecto al total de malware existente.

Botnets

Las redes botnets [4] son uno de los recursos principales del cibercrimen en la actualidad, ya que permiten el control remoto de sistemas infectados y, por medio de estos, la realización de diversas acciones maliciosas en forma masiva y anónima.

De acuerdo con lo expuesto, es de esperar que el número de redes botnets continúe en aumento como así también la actividad de éstas y la cantidad de acciones maliciosas ejecutadas desde los equipos infectados, dado que los desarrolladores de malware encuentran mayor rédito económico en los códigos maliciosos del tipo bot [5].

Estas botnets comenzarán a utilizar en forma constante nuevas tecnologías como redes *Fast-Flux* y nuevos protocolos de comunicación (como redes sociales, comunicaciones cifradas o redes *peer-to-peer)*, indicando la paulatina desaparición de las comunicaciones anteriores por canales de chat IRC y, en menor medida, de las comunicaciones HTTP en texto plano.

Partners de negocio

Se denomina Partnerka [6] a las redes de negocios que trabajan de forma conjunta en la propagación y distribución de amenazas y delitos informáticos. El malware, como parte del escenario de cibercrimen, se verá también involucrado en estas redes.

Básicamente, consiste en una serie de atacantes que trabajan en forma conjunta para la realización de alguna acción maliciosa, como el envío de spam o la propagación de un malware, entre otros. Una vez definido el objetivo, los atacantes comparten recursos a través de Internet y comienzan a realizar las tareas tendientes a lograrlo.

De esta forma, al ser muchos individuos que trabajan en equipo, los cibercriminales logran ataques más complejos, en mayor escala y con mayores dificultades para rastrear sus orígenes.

Además, aumentará la aparición de códigos maliciosos administrados y propagados por grupos de profesionales, los cuales ya no serán más producto y creación de individuos trabajando de manera solitaria.

Malware desarrollado en Latinoamérica

Como consecuencia del crimeware y los réditos económicos que obtienen los creadores de malware, se verá con mayor frecuencia durante el 2010 la aparición de códigos maliciosos desarrollados en América Latina y apuntados directamente a víctimas hispanoparlantes y de los países de la región.

Los troyanos bancarios, desarrollados en primer lugar en Brasil y luego en México y Argentina, serán los de mayor notoriedad, aunque también se detectarán tanto malware como ataques de Phishing provenientes de distintos países de la región. Además será más frecuente el funcionamiento de redes botnets diseñadas y administradas desde Latinoamérica, principalmente con objetivos de acciones maliciosas focalizadas en la región.

Ataques dirigidos

Las amenazas orientadas a CIOs, CSOs, gerentes, directores, dueños o cualquier otro alto cargo en empresas, tienen como claro objetivo la obtención de dinero. También conocido como *Whaling*, el envío de mensajes de correo específicos a ciertos integrantes de compañías (con solicitudes de información o archivos adjuntos potencialmente maliciosos) es una amenaza a la que deberán estar atentas las empresas.

Dado que no son masivos, este tipo de ataques no suelen mencionarse con frecuencia en campañas de concientización en seguridad, pero su impacto puede ser más alto que un ataque con mayor índice de popularidad.

También se percibirá el aumento de ataques persistentes, conocidos por sus siglas en inglés como APT (*Advanced Persistent Threat,* en español Amenazas Avanzadas y Persistentes). Se trata de ataques usualmente específicos, que no utilizan ninguna tecnología novedosa y que, entre otras herramientas, suelen llevarse a cabo por medio de códigos maliciosos especialmente diseñados para perdurar en el tiempo, en los sistemas afectados, sin ser detectados. Por lo general, están orientados a grandes empresas y buscan robar información confidencial y valiosa.

El eslabón humano

Muchas de las amenazas informáticas existentes poseen componentes técnicos complejos que les permiten perpetrar los ataques. Sin embargo, la Ingeniería Social [7] ha sido y seguirá siendo, una estrategia de uso masivo para los desarrolladores de códigos maliciosos.

El eslabón humano es un factor más en la cadena de seguridad de cualquier sistema y los agresores intentan engañar a sus víctimas para utilizarlas en la realización de los ataques e infecciones.

Los temas calientes

En el empleo de técnicas de Ingeniería Social [7], uno de los aspectos primordiales es captar la atención de quien está frente a la computadora. Para ello no hay nada más efectivo que utilizar las temáticas que están presentes en los medios de comunicación o la vida privada de los usuarios.

En línea con esto, se espera que durante el 2010 se mantenga la propagación de amenazas en fechas especiales (día de San Valentín, Halloween) y fechas patrias (como el Día de la Independencia). Asimismo, el malware aprovechará temáticas en auge para encubrir sus verdaderos objetivos, como ocurrió durante 2009 con las actualizaciones de software, la asunción del presidente Obama en Estados Unidos o el estado de salud de Fidel Castro. También es muy probable que otros tópicos sean utilizados en la propagación de malware durante 2010, continuando el aprovechamiento de los “temas calientes”.

Recesión mundial

La crisis mundial ocurrida durante 2009 ha tenido una gran presencia en los medios. Por lo tanto, durante el próximo año serán muy aprovechados por los diseñadores de códigos maliciosos los titulares relacionados con la economía, el dinero, los países en crisis, las oportunidades laborales y temas afines , para llevar a cabo infecciones por medio de técnicas de Ingeniería Social.

Igualmente, el contexto de las crisis económica seguirá siendo utilizado para ataques de Scam [8] y Phishing [9], al estar directamente relacionados con el robo de dinero a las víctimas.

Mundial 2010

En junio de 2010 se llevará a cabo una de las competiciones deportivas más populares: el Mundial de Fútbol Sudáfrica 2010. Es de esperarse que, en el primer semestre del año, esta sea una temática muy explotada por la Ingeniería Social por el gran interés que despertará en la mayoría de los usuarios.

Falsas noticias, promociones de viajes, regalos temáticos o videos relacionados con el tema son algunos de los probables contenidos que serán utilizados.

Spam

El correo no deseado seguirá en aumento durante 2010 y también continuará la propagación de mensajes publicitarios no solicitados en otros medios distintos del correo electrónico, como las redes sociales, los sistemas de mensajería instantánea o los blogs en la web.

Plataformas de ataque

Así como Internet continuará siendo una de las principales vías de ataque, las vulnerabilidades en los sistemas operativos [10] y sus aplicaciones también seguirán siendo explotadas por los códigos maliciosos. Una de las principales tendencias para el año 2010 estará constituida por la creación de códigos maliciosos para plataformas que, a pesar de contar con algunos ejemplares de malware hace años, comenzarán a ser utilizadas con mayor frecuencia en búsqueda de víctimas.

Malware multi-plataformas

Las plataformas distintas a Microsoft Windows, particularmente Mac OS X y Linux, se verán afectadas por nuevas variantes de códigos maliciosos. Particularmente el sistema operativo de Apple ha incrementado el número de usuarios durante 2009 y esta tendencia continuará, por lo que la producción de códigos maliciosos para esta plataforma se destacará durante el año 2010.

El rogue [11] ha sido y continuará siendo durante el 2010 el malware más efectivo y utilizado por los atacantes como herramienta para realizar infecciones multi-plataforma.

Windows 7

A finales del año 2009 Microsoft lanzó la última versión de su sistema operativo Windows 7. El mismo incorpora mejoras de seguridad para contrarrestar el malware existente en la actualidad. Sin embargo, es probable que durante 2010 aparezcan nuevos códigos maliciosos desarrollados para infectarlo.

Se estima que la aparición de este tipo de malware será lenta pero irá en aumento, a medida que el número de usuarios se incremente y las potenciales víctimas abandonen Windows XP, la versión más utilizada en estos momentos y la preferida por los atacantes durante los últimos años.

Además, es de esperarse que aparezca malware multi-versión capaz de afectar a usuarios en Windows XP como también en Windows 7, como el caso de los bootkits [12], una amenaza que permite infectar diversas versiones de los sistemas operativos de Microsoft.

Dispositivos móviles

La utilización de dispositivos móviles de alta gama o Smartphones se encuentra en incremento, particularmente en el sector empresarial. Estos dispositivos suelen poseer acceso a sistemas e información corporativa confidencial que, en la mayoría de los casos, se encuentra desprotegida.

Por tal motivo, a lo largo de 2010 se observarán nuevas variantes de ataque para estos dispositivos y un significativo aumento en la cantidad de amenazas.

Tendencias en Seguridad

Las nuevas amenazas tendrán un alto impacto en la seguridad y será muy importante contar con las herramientas necesarias para enfrentarlas. En este aspecto, se destacan algunas ideas relevantes en materia de soluciones de seguridad para el año entrante.

En primer lugar, cabe destacar el inicio de las discusiones sobre la efectividad de soluciones de seguridad Cloud Computing. Aunque se ha demostrado que una solución de seguridad en formato Cloud Computing presenta más dudas que certezas para la protección del usuario [13], se espera que el debate sobre cuál es el modelo preferido para brindar soluciones ante el malware continúe a lo largo del 2010.

En segundo lugar, la alta tasa de aparición que se espera para malware del tipo adware y rogue llevará el enfrentamiento entre laboratorios y cibercriminales al ámbito judicial, tal como indicara Jurach Malcho [14], líder del Laboratorio de ESET. Los atacantes ya no son individuos sino redes organizadas de profesionales que han incluido abogados en sus filas para enfrentar a las compañías de seguridad.

Finalmente, el *listing* (en castellano, la creación de listas de referencia) será utilizado con mayor frecuencia en soluciones de seguridad. Tanto el *blacklisting* (listado de sitios/archivos maliciosos no permitidos) como el *whitelisting* (listado de sitios/archivos benignos a aceptar) y el *greylisting* (armado de blacklisting en forma dinámica a través de heurísticas) serán muy utilizados para detecciones de amenazas como spam o sitios web maliciosos en tráfico HTTP.

Conclusiones

En la actualidad el cibercrimen es una actividad en crecimiento, tanto en su cantidad de delitos y autores como en las técnicas utilizadas para llevar a cabo dichos crímenes.

En este contexto los códigos maliciosos ofrecen un recurso de alto valor para la realización de ataques a través de Internet y tecnologías informáticas.

El crimeware involucra también a organizaciones, delincuentes, redes botnets, cuentas bancarias y un ecosistema complejo en donde día a día se observan más ataques que atentan contra usuarios y empresas.

Sea a través del lucro directo (utilizando el scam o los troyanos bancarios), indirecto (spyware, redes botnets, entre otros) o a través del robo de información confidencial, cualquiera de estos

objetivos es motivación suficiente para crear un código malicioso y poner en riesgo al usuario, su dinero e información.

Se estima que durante 2010 la mayor amenaza en lo que respecta a los códigos maliciosos será el crimeware, aquel malware que está desarrollado con fines económicos, y que puede atentar contra la economía del usuario o su información de alto valor.

Más información

[1] Crimeware, el crimen del Siglo XXI

http://www.eset-la.com/centro-amenazas/2219-crimeware-crimen-siglo-xxi

[2] Tendencias 2009: Internet como plataforma de infección

http://www.eset-la.com/centro-amenazas/2001-tendencias-eset-malware-2009

[3] Utilizando redes sociales para propagar malware

http://www.eset-la.com/centro-amenazas/2034-utilizando-redes-sociales-propagar-malware

[4] Botnets, redes organizadas para el crimen

http://www.eset-la.com/centro-amenazas/1573-botnets-redes-organizadas-crimen

[5] Botnets, en Centro de Amenazas de ESET Latinoamérica

http://www.eset-la.com/centro-amenazas/amenazas/2235-Botnets

[6] Partnerka: redes organizadas de negocios

http://blogs.eset-la.com/laboratorio/2009/10/09/partnerka-redes-organizadas-de-negocios/

[7] El arma infalible: la Ingeniería Social

http://www.eset-la.com/centro-amenazas/1515-arma-infalible-ingenieria-social

[8] Scam

http://www.eset-la.com/centro-amenazas/amenazas/2178-Spam

[9] Phishing

http://www.eset-la.com/centro-amenazas/amenazas/2144-Phishing

[10] La importancia de las actualizaciones

http://www.eset-la.com/centro-amenazas/1996-importancia-actualizaciones

[11] Rogue

http://www.eset-la.com/centro-amenazas/amenazas/2149-Rogue

[12] Nueva generación de rootkits

http://blogs.eset-la.com/laboratorio/2009/09/25/nueva-generacion-rootkits/

[13] ¿Nube o humo?

http://blogs.eset-la.com/laboratorio/2009/09/29/computacion-nube-o-niebla/

[14] Is there a lawyer in the lab?

http://www.eset.com/download/whitepapers/is-there-a-lawyer-in-the-lab.pdf

http://www.eset.com/download/whitepapers/Lawyer_in_the_lab.pdf