Revista Digital Universitaria
10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

ARTICULO

MALWARE, UNA AMENAZA DE INTERNET

Luis Fernando Fuentes
UNAM-CERT
Universidad Nacional Autónoma de México
lfuentes@seguridad.unam.mx

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Resumen

La cantidad de malware y la evolución de sus técnicas de infección y propagación se han incrementado de manera considerable a través de los últimos años, lo cual se convierte en un problema que debemos enfrentar y al que están expuestos todos los usuarios de Internet.

INICIO

El malware es un término general, proveniente de la contracción malicious software, que se le ha adjudicado a todo aquel software que perjudica a la computadora. Actualmente, es una de las principales amenazas que afectan a los sistemas de cómputo. Puede tratarse de un virus, un caballo de Troya, una puerta trasera (backdoor), un programa espía (spyware), hasta un devastador gusano que puede echar abajo toda una infraestructura de red, aun redes nacionales y corporativas.

A causa del malware, derivan otros ataques como: DDoS (Distributed Denial Of Service), distribución de correo spam, propagación de virus y gusanos hacia otras redes, sitios phishing, expansión de botnets (redes de equipos comprometidos), fraudes de banca electrónica, pharming y su variante de pharming by driving, entre otros.

El malware es cada vez más sofisticado, muchas soluciones de prevención, como el software antivirus y antispyware, se están viendo superadas, en el tiempo de respuesta, por estas amenazas, lo cual se debe a que el virus aprovecha las ventajas de la tecnología para ser nocivo, rápido y sutil en la forma de engañar a sus víctimas.

La propagación de este conflicto tiene su origen en aspectos como: la escasa atención a las actualizaciones del sistema operativo; el no adoptar esquemas de actualización centralizadas; la falta de mecanismos de prevención en los equipos, como implementar buenas prácticas de seguridad: firewalls personales, actualizaciones en el software antivirus, etc.

El análisis de malware

Para investigar acerca de los códigos maliciosos es necesario contar con mecanismos que permitan estudiar la manera en que opera el malware, uno de éstos consiste en la realización de un análisis bajo ambiente controlado que permita generar información para mitigar el impacto, alertando a los involucrados.

El análisis de malware se compone principalmente de dos técnicas. La primera consiste en el examen de comportamiento (análisis dinámico), y el estudio de su código (análisis estático). La segunda técnica es más compleja que la primera, puesto que se requiere de aplicar técnicas como la ingeniería inversa y depuradores para desensamblar el código, debido a que la mayoría de las ocasiones se parte de un archivo binario y no se cuenta con el código fuente. Es necesario tener un conocimiento técnico avanzado para interpretar el código desensamblado o código máquina. Además, en algunas ocasiones esta técnica es muy laboriosa y exige una fuerte inversión de tiempo sin arrojar resultados concretos o datos que trasciendan en el análisis. La otra parte con la que se complementa el análisis de malware, el análisis de comportamiento, no resulta tedioso y monótono y es un proceso mucho más atractivo para los investigadores y por el cual prefieren comenzar.

El objetivo del análisis de comportamiento (behaviour analysis), es investigar la actividad del malware en el sistema comprometido. El comportamiento se puede observar a través de un ambiente controlado, ya sea virtual o bien, por medio de una red donde esté limitado el tráfico con el propósito de evitar la propagación e infección hacia otros equipos de la organización. En este punto, se monitorea la actividad de los procesos maliciosos que ejecuta el malware, los puertos que abre, su actividad en la red (es decir, si se comunica a un servidor remoto o a algún dominio), el tipo de protocolo que utiliza para comunicarse con él (HTTP, IRC, etc.) y la manera en que se activa en el sistema comprometido (que puede ser mediante la activación de un servicio o iniciándolo directamente desde los archivos de inicio). Para este proceso, resulta más sencillo utilizar equipos virtuales, pues permiten regresar al escenario original de manera más sencilla, aunque algunos binarios maliciosos ya son capaces de detectar este tipo de ambientes para evitar su ejecución y de esta forma dificultar su análisis.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

La importancia del análisis de Malware surge por la clara evolución y tendencia de esta amenaza, así como de la necesidad de alertar a la comunidad acerca de los nuevos códigos maliciosos que se alojan dentro de sus redes, y pueden presentar nuevas técnicas y métodos de propagación, lo cual los hace más difíciles de identificar y de erradicar por parte de las firmas antivirus.

Técnicas de propagación

La ventaja que tiene el malware, en comparación con otras sofisticadas técnicas de intrusión, es que aprovecha, la mayoría de las ocasiones, la inocencia de los usuarios; es decir, los desarrolladores de malware utilizan técnicas como ingeniería social para engañar y abusar de sus víctimas, aunque no debemos dejar de lado el hecho de que las técnicas evolucionan de manera permanente.

Anteriormente, los intrusos desarrollaban códigos maliciosos para poner a prueba sus conocimientos en cómputo y era común propagarlos a través de dispositivos de almacenamiento como diskettes y CD-ROM. Generalmente estos códigos informáticos infectaban los sectores de arranque o renombraban algún archivo válido del sistema para evitar su adecuado funcionamiento. El malware de aquella época requería de la intervención del usuario para infectar el equipo. Hoy en día, estas técnicas de infección y de propagación son obsoletas. El malware de esta generación es capaz de autoreplicarse aprovechando alguna vulnerabilidad o simplemente con incrustar código a través de alguna aplicación, aunado a que los intereses de los atacantes también han cambiado: ahora enfocan el desarrollo de sus códigos para robar información sensible, modificar registros DNS (Domain Name Services), explotar vulnerabilidades, usurpar sitios Web, etc., buscando con ello algún beneficio económico.

Un ejemplo palpable de esta evolución es que a partir de Julio del 2007, se comenzó a identificar malware dirigido a las redes mexicanas, dicho malware es indiscutiblemente desarrollado por bandas mexicanas dedicadas al ciber crimen. Los primeros indicios de estos códigos empleaban técnicas de pharming (modalidad utilizada por los intrusos que consiste en suplantar el Sistema de Resolución de Nombres de Dominio DNS, Domain Name System, con el propósito de conducir al usuario a una página Web falsa), esto lo realizaban modificando la información del archivo hosts del sistema comprometido, principalmente dirigiendo a los usuarios hacia sitios bancarios falsos. Después, comenzaron a explotar vulnerabilidades utilizando estas técnicas de modificación de tablas DNS con dispositivos routers, con ello no solamente pueden redireccionar un equipo al destino falso sino todos aquellos que tengan acceso a red mediante este dispositivo. Seguido de esta evolución, los atacantes comenzaron a combinar la modificación del archivo hosts con la usurpación del sitio bancario en el propio equipo infectado con la intención de que su víctima realice sus transacciones bancarias ahí mismo y los datos confidenciales sean enviados hacia otro servidor remoto.

Desde el nacimiento del proyecto Malware de la UNAM, se ha identificado claramente la evolución de los códigos maliciosos, algunos otros ejemplos que demuestran esto son: el impacto que han tenido las botnets, los códigos maliciosos empaquetados para evitar ser analizados; el surgimiento de códigos híbridos que combinan características de gusanos con bots y troyanos y la manera en que el malware de esta época utiliza técnicas de polimorfismo y metamorfismo para evitar ser detectado por las firmas Antivirus. Sin embargo, esta evolución se puede resumir con mencionar que estamos ante una nueva generación de malware que está incrementando de manera vertiginosa sus habilidades para propagarse y causar daño. Estamos ante códigos maliciosos con características destructivas más variadas, incluyendo multiplataforma, multiexploit, que aprovechan vulnerabilidades de día cero, con una rápida capacidad de propagación, y el empleo de nuevas estrategias de ofuscamiento para cambiar su apariencia y su comportamiento (polimorfismo y metamorfismo respectivamente).

Conclusiones

No cabe duda, las nuevas vulnerabilidades de Internet se hacen tangibles con la presencia de códigos maliciosos que ponen en riesgo la seguridad de los datos de los usuarios, provocando un número considerable de delitos que derivan en pérdidas económicas personales o para toda una organización, a tal grado, que no hace falta contar con algún tipo de armamento para realizar históricos asaltos bancarios o dejar sin funcionamiento una corporación, sino basta con propagar un malware a través de Internet y esperar a que la actividad maliciosa surja efecto.

Los intrusos van perfeccionando sus técnicas. Se trata de individuos que trabajan en conjuntos bien organizados por lo que resulta de mucha utilidad seguir sus pasos, analizar sus herramientas y códigos para tener la capacidad de contrarrestar su impacto, además de conocer sus tendencias. Si no se conoce como actúa un intruso, no se tendrá la habilidad para enfrentarlo. Paralelo a esto, se debe inculcar una cultura de seguridad en las organizaciones y utilizar métodos preventivos que difundan el uso de herramientas para la protección de los sistemas de cómputo, así como el empleo de buenas prácticas de seguridad en las dependencias.

10 de abril 2008 • Volumen 9 Número 4 • ISSN: 1067-6079

Bibliografía

Roger A. Grimes "Malicious Mobile Code: Virus Protection for Windows" O'Reilly Computer Security.

Ed Skoudis "Malware: Fighting Malicious Code".

Luis Fernando Fuentes "Códigos Maliciosos", Propiedad intelectual UNAM-CERT.

Mesografía

Usuario Casero - http://www.seguridad.unam.mx/doc/?ap=prf&id=194

Malware UNAM - http://www.malware.unam.mx/

Blog Malware - http://www.malware.unam.mx/blog.dsc?semana=10&anio=2008

Casos Pharming - http://www.seguridad.unam.mx/pharming.dsc#julio