

## **El papel que juega Internet en la propagación de programas malignos**

## Introducción

Empresas de todos los tamaños dependen de Internet como parte de sus operaciones diarias. La página Web de la empresa es el principal punto de entrada para sus clientes actuales y futuros, así como para sus accionistas; los empleados dirigen la mayoría de sus operaciones a través de la Web; y el e-mail tiene mucho que ver en la eficiencia y la rapidez con que se realizan las comunicaciones internas y externas. Por lo tanto, el acceso al e-mail y a la Web representan el 90 por ciento de las aplicaciones principales de negocio utilizadas por pequeñas y medianas empresas.

Las herramientas de Internet han cambiado drásticamente la cara del mundo empresarial, añadiendo una eficiencia y productividad extraordinarias. Desafortunadamente estos mismos beneficios se han producido también para los autores de programas malignos. Mientras que antiguamente las amenazas necesitaban meses para infectar unos cientos de ordenadores, Internet ofrece el medio de infectar cientos de miles de ordenadores en cuestión de minutos.

## La Evolución de las Amenazas Informáticas

Las amenazas informáticas han sido parte de la vida diaria desde 1986, cuando se descubrió el virus de autoarranque Brain. Los virus de autoarranque se propagaban autogardándose en floppy disks y se trasferían al usuario del ordenador cuando éste se arrancaba. En 1995 los virus de autorranque daban paso a los virus macro. Éstos se escribían en lenguaje script y tenían como objetivo el mundo Microsoft y los documentos Excel. Ambos tipos de virus tenían unas técnicas de propagación lentas e ineficientes, dependiendo de los usuarios para llevarlos vía floppy disks de un ordenador a otro. Para eliminar estas amenazas bastaba con utilizar programas antivirus en el puesto informático.

Todo empezó a cambiar en 1999 cuando el virus Melissa hizo su entrada. La primera amenaza basada en e-mail, Melissa no necesitaba llevarse de un ordenador a otro. En vez de eso se podía distribuir más rápida y fácilmente utilizando la velocidad y la eficiencia de las comunicaciones de red. Las diferentes variedades de amenazas futuras se construyeron bajo este concepto. Por ello Internet se convirtió en el nuevo medio de transporte con la distribución de virus por e-mail, gusanos de red y amenazas alojadas en páginas Web.

A parte de la facilidad de propagación, Internet ofrecía a los autores de programas malignos la capacidad de publicar y compartir su código con sus colegas. Estas nuevas versiones de amenazas de red se desarrollaron con sólo unas modificaciones en el código existente. Incluso aprendices de programadores podían desarrollar y distribuir, rápida y fácilmente, nuevas amenazas a las masas. De igual forma los dueños de redes bot y de listas de spam empezaron a alquilar o vender su código malicioso, ofreciendo a los programadores una distribución en red de sus creaciones.

Debido a la velocidad y la eficacia de estas amenazas, los programas antivirus usados en el puesto informático ya no eran suficiente protección pues no daban abasto con la cantidad de amenazas recibidas y el índice tan elevado de generación de nuevas amenazas.

## Un Método Eficiente de Propagación

Como ya hemos mencionado anteriormente, Internet ofrecía un entorno apropiado para la creación y propagación de amenazas informáticas. La idea de Internet es que todos los ordenadores estén conectados entre sí y puedan comunicarse unos con otros. Los autores de programas malignos pronto se dieron cuenta de que podrían sacar provecho de esta potente red común para propagar sus amenazas. En vez de infectar un ordenador cada vez, los autores de programas malignos podían llevar sus creaciones a las masas de forma simultánea.

El nacimiento de Internet ofreció el mecanismo de propagación de amenazas mediante el empleo de numerosas técnicas, incluyendo e-mail, spam, bots, gusanos de red y drive-by-downloads.

## Virus

La primera amenaza importante basada en Internet se propagó vía e-mail. Los virus como "Loveletter" se enviaban vía e-mail en el adjunto. El virus se lanzaba cuando se abría el adjunto, infectando el equipo del usuario. Entonces se reenviaba una copia a todos los contactos de la libreta de direcciones de la víctima de forma automática, utilizando el nombre de la víctima como remitente. De esta manera los destinatarios creían que el mensaje era de alguien conocido. "Loveletter" infectó cientos de miles de equipos en un sólo día y causó pérdidas de entre 5.000 millones y 7.000 millones de dólares.

Para hacer que el usuario abriese el adjunto, el autor incluía texto en el cuerpo del mensaje diciendo que el adjunto era una carta de amor para el destinatario. Esta técnica era una versión rudimentaria de lo que ahora se denomina "ingeniería social". Su definición sería un método empleado por los autores de programas malignos que engaña a los usuarios para infectar sus sistemas. La "ingeniería social" saca provecho de algo contra lo que el software de seguridad nunca podrá luchar, los usuarios.

## Spam

La derivación lógica en cuanto a amenazas basadas en e-mail es el spam. Mientras que el comportamiento de las primeras amenazas vía e-mail era en cadenas de cartas, dependiendo de un error del usuario para continuar su propagación, el spam se envía a sus destinatarios de forma directa.

La mayoría del spam llega en forma de publicidad de productos o servicios. El spam se utiliza normalmente para anunciar una página Web para adultos, fármacos ilegales y otras ofertas promocionales. Así que la mayoría del spam es un incordio. Sin embargo alguna vez se emplea como vehículo de distribución de amenazas como virus, software espía, trojanos y rootkits.

La empresa Gartner, líder en estudios tecnológicos estima que entre el 2 y el 6 por ciento del spam incorpora una de esas amenazas. Aunque este número parece pequeño cuando lo unimos a que entre el 80 y el 95 por ciento del mail que recibe una empresa es spam, esta cifra se convierte en significativa. En cuanto a si estos mensajes llevan o no una amenaza, lo que importa a las empresas, de momento, es la cantidad desorbitada de spam que se recibe es ya que puede causar un impacto importante en el rendimiento de la red.

### **Gusanos de Red**

Un gusano de red tiene la capacidad de moverse a través de la red de la empresa sin depender de nadie y sin darnos cuenta, ya que no necesita intervención del usuario para propagarse. Por ejemplo, en Julio del 2001, el gusano Código Rojo infectó 359.000 sistemas en 14 horas, causando daños por más de 2.600 millones de dólares. De igual manera, en Septiembre de 2001 el gusano Nimda infectó más de 160.000 sistemas en siete horas y llegó a los 450.000 en 24 horas.

Los gusanos normalmente se propagan a través de las vulnerabilidades del sistema operativo pero también se pueden enviar en los adjuntos de los e-mails. Una vez que un gusano está en el sistema del usuario, su motor SMTP incorporado le permite eludir completamente los programas de e-mail y moverse libremente a través de toda la red de la empresa sin la interacción de ningún usuario. Además el gusano se puede autoenviar a cualquier dirección de e-mail. Como el gusano no utiliza la aplicación de e-mail existente el operador del equipo infectado ni se entera de que el gusano se ha propagado a sí mismo.

Los gusanos consumen gran cantidad de banda ancha de la red ya que se replican y propagan libremente. Como resultado, el rendimiento de la red puede sufrir o puede colapsarse. Los gusanos pueden incluso llevar otras amenazas, como pueden ser software espía, virus y troyanos que pueden causar problemas adicionales.

### **Bots**

Cuando los autores de programas malignos quieren enviar una alta concentración de spam, virus o software espía, suelen emplear una red bot para hacer el trabajo. Un "bot" que es la forma corta de "Web Robot", es un programa de software que actúa de manera automática para realizar trabajos repetitivos a través de Internet. Una red bot puede consistir en unos 20.000 ordenadores infectados, también conocidos como "zombis" que se utilizan juntos para coordinar el lanzamiento de amenazas a gran escala. Las grandes redes bot, también conocidas como "botnet" pueden llegar a tener millones de zombis.

Como los bots tienen la capacidad de comunicarse con otros servicios basados en red, se suelen utilizar para comunicarse con otros ordenadores a través de diferentes protocolos de red. Los bots unidos a software espía se utilizan para robar información personal sensible. Esta información normalmente es el número de tarjeta de crédito, información del banco y otro tipo de información del consumidor, pero también puede ser logins de VPN y otro tipo de información de la empresa. También se pueden utilizar para lanzar ataques DDos (Distributes Denial of Service), en donde grandes cantidades de zombis colapsan la red de la víctima simultáneamente con millones de peticiones de conexión haciendo que ésta se pare. Los ataques DDos suelen tener como objetivo páginas como EBay, America Online, Amazon, CNN, E-Trade y Yahoo.

### **Drive-By-Downloads**

Un drive-by-download es una amenaza alojada en Web. Es diferente de las amenazas mencionadas anteriormente ya que depende de la víctima para que llegue a ella, en vez de ser enviada al sistema de la víctima. En un drive-by-download, las amenazas como bots, software espía, adware o troyanos se instalan sin el conocimiento o la interacción del usuario. Cuando el usuario visita una página Web infectada, la amenaza se descarga por detrás de forma automática. La página infectada puede ser una página maliciosa desarrollada para parecer legítima o puede ser una página legítima que ha sido pirateada por un autor malicioso y consecuentemente infectada con alguna amenaza. En cualquier caso el usuario normalmente ni se da cuenta de que la página está infectada.

### **Protección Contra las Amenazas Basadas en Internet**

Para asegurar que una empresa está adecuadamente protegida contra las amenazas basadas en Internet, se requiere una detallada descripción del problema y la utilización de múltiples capas de seguridad. Utilizar un software de seguridad en el puesto informático es un primer paso importante pero no es suficiente contra el volumen, la velocidad y la eficiencia de las amenazas basadas en Internet. Este software por sí solo no ofrece la suficiente protección para mantener la red de la empresa segura. Para una completa protección este software de seguridad debe complementarse con una solución de Gateway de Seguridad que escanee el tráfico entrante y saliente con el fin de detectar y eliminar las amenazas antes de que lleguen a cada puesto informático.

La mayoría de los ataques basados en red se propagan a través del e-mail, la Web o la red interna de la empresa, antes de llegar al sistema del usuario. Algunas amenazas, como gusanos de red, llegan directamente a la red de la empresa sin necesidad de utilizar el sistema del usuario. Una solución de Gateway de Seguridad es esencial para mantener las amenazas fuera de la red.

### **Conclusión**

Desde 1999, Internet ha jugado un papel cada vez más importante en la propagación de amenazas. Esto se debe a que ofrece una gran facilidad de propagación y a la comunidad clandestina que inevitablemente soporta. Entre el gran número y variedad de amenazas disponibles, junto con la velocidad y la eficacia de Internet, la seguridad basada en el puesto informático ya no es efectiva. El resultado es que ha surgido la necesidad de disponer de una capa de seguridad adicional en el Gateway de red para apoyar los esfuerzos realizados a nivel cliente.

## Solución de Gestión ProSecure™ STM para Amenazas Web y E-mail de NETGEAR®

El dispositivo ProSecure STM utiliza una tecnología única que detecta y bloquea las intrusiones basadas en un comportamiento de distribución rápido y a gran escala. De este modo se puede detectar intrusiones de spam y programas malignos tan pronto como se produzcan y bloquear todos los mensajes asociados en tiempo real.

El dispositivo ProSecure STM con tecnología Stream Scanning, pendiente de patente, está diseñado para escanear flujos de información a medida que van entrando en la red. NETGEAR STM con la tecnología Stream Scanning es capaz de procesar grandes volúmenes de información en tiempo real, utilizando un simple escáner para identificar spam, programas malignos, brechas de seguridad o aplicaciones innecesarias. Asegurando que los usuarios de la red reciban su e-mail y los contenidos Web limpios y sin retrasos.

El dispositivo ProSecure STM utiliza un sistema de comportamiento de defensa proactivo que soluciona las vulnerabilidades. La solución NETGEAR utiliza un análisis forense para identificar características sospechosas tanto en el tráfico de de entrada como de salida de la red y neutralizarlas hasta que puedan ser examinadas más detenidamente.

© 2009 NETGEAR Internacional, NETGEAR, el logotipo de NETGEAR, Connect with Innovation, and ProSecure son marcas comerciales o marcas registradas de NETGEAR, Inc. en los Estados Unidos y/o otros países. Otros nombres de marcas y nombres de productos son marcas comerciales o marcas registradas de sus respectivos dueños. La información puede cambiar sin previo aviso. Todos los derechos reservados.