El último Informe de Symantec sobre Amenazas en Internet *(Internet Security Threat Report)* desvela que los usuarios domésticos se están convirtiendo en objetivos cada vez más utilizados para que los atacantes realicen sus actividades de suplantación de identidad, así como actos fraudulentos u otros delitos realizados para obtener beneficios económicos.

Aumenta el número de usuarios domésticos que sufre ciberataques con fines económicos

Los atacantes están ahora utilizando una variedad de técnicas para evitar ser detectados y para prolongar su presencia en los sistemas y, de esta manera, contar con más tiempo para apoderarse de información, controlar el ordenador para llevar a cabo tareas de marketing, ofrecer acceso remoto o para poner en peligro la información confidencial del usuario con el objeto de obtener beneficios económicos.

«La capacidad para conocer el entorno actual de las amenazas resulta esencial a la hora de ayudarnos a proteger las interacciones de nuestros ciudadanos en Internet y para garantizar la disponibilidad de nuestros sistemas críticos», afirma David Jordan, director de informática y jefe de privacidad en Arlington County, Va. «La información sobre las amenazas actuales que ofrece el Informe de Symantec sobre Amenazas en Internet, junto con nuestro empleo de tecnologías innovadoras para seguridad, nos ayuda a garantizar el más alto nivel de seguridad para nuestros ciudadanos e instituciones gubernamentales».

El ISTR X ha detectado una media diaria de 57.717 equipos activos de redes bot, contabilizando un total de 4.696.903 equipos durante el primer semestre de 2006

El Informe de Symantec sobre Amenazas en Internet advierte que los usuarios domésticos se están convirtiendo en víctimas cada vez más comunes de los ataques, llegando a representar un 86% de todos los ataques dirigidos a grupos específicos, seguidos de las empresas de servicios financieros. Symantec ha identificado un incremento de los ataques dirigidos a aplicaciones cliente, además de un aumento del empleo de tácticas evasivas para evitar su detección. El empleo generalizado de gusanos en Internet ha dado paso a unos ataques menores y más centrados para realizar actividades fraudulentas, suplantación de identidad y otro tipo de delitos.

«Los atacantes ven a los usuarios finales como el enlace más débil en la cadena de la seguridad, y están centrando sus ataques cada vez más en este grupo para obtener beneficios económicos», asegura Arthur Wong, vicepresidente primero del Symantec Security Response and Managed Services. «Debido a los

TENDENCIAS DE ATAQUE. Los Estados Unidos continúan siendo la principal fuente de ataques con un 37 por 100 del total a nivel mundial. China ha crecido del 7 por 100 al 10 por 100.

efectos que estos hechos están teniendo en nuestra base cada vez mayor de clientes, Symantec ha presentado unas nuevas valoraciones para proteger mejor a los clientes y para ayudarles a hacer frente a las preocupaciones sobre seguridad que tengan en el futuro».

AUMENTAN LOS ATAQUES A LOS EQUIPOS DE SOBREMESA

A medida que los fabricantes de software y las empresas se adaptan con éxito a los entornos cambiantes de las amenazas, gracias a la puesta en marcha de buenas prácticas en seguridad y de estrategias sólidas para implementar defensas, los atacantes han comenzado a adoptar nuevas técnicas como, por ejemplo, el empleo de códigos malintencionados en aplicaciones cliente, incluyendo los navegadores de Internet, los clientes de correo electrónico y otras aplicaciones para equipos de sobremesa. Las vulnerabilidades que afectan a las aplicaciones para la Web representaron un 69% de todas las vulnerabilidades recopiladas por Symantec durante el primer semestre de 2006. Las vulnerabilidades para navegadores Web también han registrado un aumento, con 47 vulnerabilidades registradas en los navegadores Mozilla (comparadas con las 17 en el informe anterior), 38 vulnerabilidades en el Microsoft Internet Explorer (frente a las 25 registradas en el período anterior), y 12 en el Apple Safari (comparadas con las 6 registradas en el informe previo).

INCREMENTO DE LAS TÉCNICAS EVASIVAS

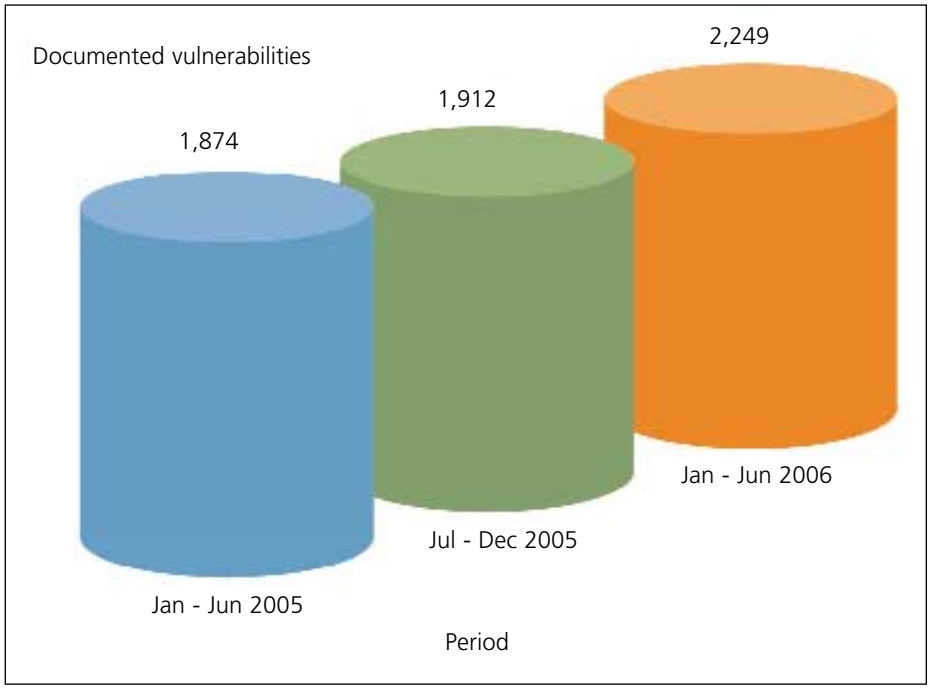
Durante el período correspondiente a este informe, un 18% de todas las muestras de códigos malintencionados detectadas por Symantec no se han visto hasta la fecha, lo que indica que los atacantes están intentando evitar ser detectados por los antivirus basados en firmas y por los sistemas para detección/prevención de intrusiones.

Los atacantes que utilizan técnicas de *phishing*, también están evitando ser detectados por las tecnologías para filtrado de mensajes, mediante la creación de mensajes múltiples y aleatorios, y la distribución de dichos mensajes de modo incontrolado y masivo. Durante el primer semestre de 2006, se detectaron 157.477 mensajes únicos de *phishing*, lo que significa un incremento del 81% frente al período anterior. Al mismo tiempo, los mensajes no deseados *(spam)* representaron un 54% de todo el tráfico monitorizado del correo electrónico, lo que supone un ligero aumento desde el 50 % registrado en el período anterior. La mayoría de los implicados en el envío de *spam* están optando por eliminar el código malintencionado de sus mensajes para, de esa manera, evitar la posibilidad de ser bloqueados, incluyendo en vez de dichos códigos unos enlaces a sitios Web que son los que contienen códigos malintencionados.

El sector objetivo más atacado durante los primeros 6 meses de 2006 ha sido el de los usuarios domésticos

LAS GANANCIAS ECONÓMICAS IMPULSAN LAS ACTIVIDADES MALINTENCIONADAS

Las ganancias económicas siguen siendo la principal motivación detrás de muchas de las amenazas registradas durante el período correspondiente a este informe. De esta manera, los ataques con redes de *bots* se pueden utilizar no sólo para distribuir códigos malintencionados, sino también para enviar mensajes de tipo *spam* o *phishing*, para descargar



TENDENCIAS EN VULNERABILIDADES. Entre el 1 de enero y el 20 de junio de 2006, el número total de vulnerabilidades creció un 18 por 100 sobre el periodo anterior. El incremento se debe fundamentalmente a gran número de vulnerabilidades asociadas a aplicaciones Web.

adware y *spyware*, para atacar a una organización, o para capturar información confidencial. Symantec identificó más de 4,6 millones de ordenadores activos y diferentes pertenecientes a redes de *bots*, y registró una media de 57.717 ordenadores activos pertenecientes a redes de *bots* al día durante este período. Las redes de bots se están utilizando cada vez más para realizar ataques para denegación de servicios (*denial-of-service*, DoS), una de las principales amenazas para las organizaciones, ya que estos ataques pueden producir un corte en las comunicaciones, además de pérdidas de ingresos, daños a la marca y a la reputación de la compañía y una posibilidad para ser víctimas de planes criminales para extorsión. Durante el primer semestre de 2006, Symantec registró una media de 6.110 ataques para DoS al día.

Otros ataques con fines económicos utilizan códigos malintencionados modulares, un tipo de *malware* que se autoactualiza o que descarga una amenaza más agresiva cuando logra instalarse en el equipo de la víctima, para poner al descubierto información confidencial del usuario. Durante el primer semestre de 2006, los códigos malintencionados modulares representaron un 79% de las principales 50 muestras de este tipo de código recogidas por Symantec. Asimismo, las amenazas con códigos malintencionados que ponen al descubierto datos confidenciales representaron 30 de las principales 50 muestras entregadas a los responsables de este informe.

Por vez primera, los impulsores del estudio han realizado un seguimiento de los sectores que están siendo objetivo de los ataques mediante técnicas de *phishing* —otros medios para obtener beneficios económicos. No resulta sorprendente saber que el sector de los servicios financieros es el que más ataques de este tipo está sufriendo, recibiendo un 84% de los sitios con *phishing* analizados por la Red de Informes sobre Phishing de Symantec y por el Symantec Brightmail AntiSpam durante este período.

OTROS ASPECTOS QUE DESTACA EL ESTUDIO

• **Vulnerabilidades:** El estudio ha recopilado 2.249 nuevas vulnerabilidades durante el primer semestre de 2006, lo que supone un incremento del 18% frente al período anterior, y la mayor cantidad de vulnerabilidades registradas durante cualquier período correspondiente a un informe.

• **Ventana de exposición y tiempo hasta el lanzamiento de un parche:** La ventana de exposición para las empresas y lasa los navegadores Web fue de 28 días, lo que supone una reducción desde los 50 días del período anterior. El Microsoft Internet Explorer tuvo una ventana de exposición media de nueve días (una reducción desde las 25 registradas anteriormente), el Apple Safari tuvo cinco días (un aumento desde las cero anteriores), el Opera registró dos días (un descenso desde las 18 previas), y el Mozilla un día (un aumento desde los dos negativos previos). Por vez primera, Symantec realizó un seguimiento del tiempo medio que precisan los fabricantes de sistemas operativos para lanzar un parche para una vulnerabilidad. Sun fue la empresa que más tiempo tardó en lanzar un parche, con 89 días, seguido de HP con 53 días. Apple precisó una media de 37 días, mientras que Microsoft y Red Hat registró la media menor para el lanzamiento de parches, con 13 días.

• **Aplicaciones engañosas:** Tres de los 10 nuevos y principales riesgos a la seguridad fueron las aplicaciones engañosas que ofrecen unos informes falsos o exagerados sobre las amenazas a la segu-

El principal ataque detectado durante el primer semestre de 2006 fue a Microsoft SQL Server 2000 Resolution Service Overflow Attack

ridad en el sistema de un usuario, para persuadirle para que pague dinero y se actualice a otra versión del *software* que promete «eliminar las amenazas» detectadas.

• **Ataques para denegación de servicios:** Los EE.UU., fue la región a donde se dirigieron la mayor parte de los ataques para denegación de servicios (*denial of service*, DoS), representando un 54% del total mundial, y el sector de los proveedores de servicios de Internet (ISPs) fue el segundo objetivo principal para los ataques para DoS. En los EE.UU. se registró el mayor porcentaje de servidores *bot* para «comando y control», con un 42% del total, mientras que China registró el mayor número de ordenadores infectados con *bots*, con un 20% del total en el mundo.

• **Amenazas futuras:** Entre las tendencias futuras, los responsables del estudio esperan ver un resurgir de las técnicas polimórficas y las de otro tipo para evasión en códigos malintencionados Win32, además de un incremento de amenazas que explotan conceptos del «Web 2.0» como la publicación basada en el usuario y tecnologías como el AJAX, las preocupaciones sobre seguridad asociadas con la aparición del Windows Vista, y un aumento en la cantidad de vulnerabilidades debido al uso de «fuzzers» —unos programas o *scripts* diseñados para encontrar vulnerabilidades en el código del software—.

El décimo Informe de Symantec sobre Amenazas en Internet abarca el período de seis meses comprendidos entre el 1 de enero y el 30 de junio de 2006. Este informe se basa en los 40.000 sensores que monitorizan la actividad de Internet en más de 180 países, además de una base de datos con más de 18.000 vulnerabilidades que afectan a más de 30.000 tecnologías de más de 4.000 fabricantes. Symantec también analiza un sistema de más de dos millones de cuentas «anzuelo» para atraer mensajes de correo electrónico de 20 países diferentes en todo el mundo, lo que permite a Symantec medir la actividad de los ataques realizados mediante técnicas de *phishing* y *spam* a escala mundial. Para mejorar el conocimiento del entorno de las amenazas en constante evolución, este informe incluye nuevas valoraciones, como la ventana de exposición para navegadores Web y la proporción de códigos malintencionados nunca vistos hasta la fecha.