70
mil ataques diarios reporta Impsat en sus 1000 clientes en Latinoamérica.

El ciberespionaje encabeza la lista de la criminología en el mundo virtual. Los delincuentes organizados no conocen fronteras en la red. Su procedimiento consiste en catalogar la información que está en los computadores de cualquier usuario para después robarla. ¿Cómo lo hacen? A través de los denominados software espías.

Un usuario inexperto es la mejor víctima. Especialmente si descarga todo tipo de contenidos, programas, aplicaciones de Internet, sin discriminar la procedencia del contenido para instalarlo en el equipo. Frecuentemente el software espía se camufla en propaganda, anuncios, pornografía... O ingresa mediante correos electrónicos.

Estas formas camufladas se conocen como *phishing*, que no son más que pedidos a través de un correo electrónico, llamada telefónica, o un mensaje a un celular para que el usuario entregue sus datos: nombres, direcciones, número de tarjetas... Usualmente son preguntas disfrazadas en promociones, premios u otras formas a las cuales se contesta sin analizar qué está sucediendo desde el otro lado.

El *phishing* aparece también en anuncios, páginas pornográficas u otros programas. Cuando el usuario los abre se activa otra dirección electrónica oculta a la cual ingresa simultáneamente. Es ahí donde opera el software espía porque el usuario deja una huella con todos sus datos, por ejemplo, información sobre cuál es su equipo, la dirección IP de éste, incluso deja los datos de los usuarios que acceden al mismo equipo mediante clave.

Entonces, quien maneja el *software* espía puede con dicha información escanear el equipo víctima y verificar sus vulnerabilidades. Una vez que entra en él saca la información que considera útil. Pero, ¿qué candados tiene el usuario para evitar esto?

Según Arturo de la Torre, especialista en sistemas, es vital la instalación de dos programas. Primero, un antivirus actualizado que tenga la capacidad de determinar patrones de comportamiento de los programas en el computador y diferenciarlos de aquellos que no lo son y entonces neutralizarlos.

En segundo lugar, un programa *antihacker* para detectar y prevenir ataques. Sirve para identificar al computador que trata de ingresar al sistema y lo aísla por un tiempo determinado: 60 minutos o más, eso depende de cómo lo programe el usuario.

Para los entendidos en el tema, la seguridad depende más del factor humano que del tecnológico. Lo básico es capacitar para que el usuario sepa cómo discriminar la información que baja desde la red o la que recibe en su correo electrónico.

Hay herramientas sencillas para neutralizar los ataques, como por ejemplo activar una opción para bloqueo de cuentas de correos electrónicos de determinados emisores. ¿En dónde se activa? En el *Microsoft Outlook*, uno de los más usados por los ecuatorianos.

Los programas espías pueden ser de los siguientes tipos: los *xfiles*, aquellos que descargan o suben información directamente al equipo; el *spyware* o programas dedicados a espiar y entregar reportes al que los instala; el *adware* que es un programa que interactúa desde su máquina hacia otra por actualizaciones o procesos, y los virus (ver recuadros).

El mercado de la seguridad gerenciada en Latinoamérica se estima en 60 millones de dólares en este año, con un crecimiento del 54 por ciento, según el reporte de Impsat Ecuador, que maneja 1000 clientes en Latinoamérica. Según el especialista, Arturo de la Torre, el dinero que produjo el fraude informático en el año 2002 supero los 200 000 millones de dólares mundialmente. ■

software

Detrás de la PC hay un GRAN ESPÍA

Cientos de programas disfrazados monitorean los equipos personales. El robo de información es la consigna de sus creadores. El usuario lo puede prevenir.

Grandes ataques

MSBLAST: Este virus paralizó toda la costa este de EE.UU. en el 2003. Causó un gran apagón en Nueva York, Londres, Estocolmo, Roma...

CÓDIGO ROJO: Afectó a 250 000 sitios *web* en nueve horas, en julio del 2001. Fue creado para atacar la red de la Casa Blanca en EE.UU.

NIMDA: En el 2001, infectó dos millones de PC. Ataca cualquier versión de Windows. El virus desata una búsqueda masiva de direcciones IP a las cuales infectar. Dificulta el tráfico en la red.

Las amenazas de software espía más comunes

ADWARE

Son programas que interactúan de una máquina a otra cuando se conectan a Internet por actualizaciones. Hay que tener cuidado porque *Outlook Office, Word, Excel* o *Power Point* pueden clasificar como tales. Entre los últimos de cuidado están:

Security2k Hijacker
Es una extensión para el navegador de Internet que puede secuestrar la página de inicio para cambiarla a una web falsa de seguridad.

Hotbar
Es una barra de herramientas que tiene publicidad gratuita y muestra anuncios en una secuencia de ventanas nuevas.

ErrorSafe
Es una utilidad de seguridad que se instala sin el consentimiento del usuario, puede ser al arrancar Windows.

Altnet
Puede controlar todos los ficheros subidos con el programa Kazaa Media Desktop.

TROYANOS

Estos programas están destinados a activarse en determinado día y hora, al requerimiento del atacante. Entre los más recientes están los siguientes:

Trojan Downloader -Zlob
Puede descargar otras amenazas en el computador y cambiar las direcciones DNS.

Trojan Agent Winlogonhook
Permite a un *hacker* tener acceso completo al PC mientras el usuario esté navegando en la Internet.

p2pnetwork
Actúa igual que el anterior.

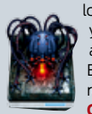
Además, escanea la dirección IP del computador atacado.

Trojan-Downloader-WStart
Es un programa de descargas que, a su vez, puede instalar otras amenazas en la PC.

Trojan Downloader Matcash
Es otro software de descargas que puede promover la entrada de nuevas amenazas.

MONITORES DE SISTEMA

Están dedicados a espiar todo lo que hace el usuario y entregar reportes al que los puso. Entre los últimos reportados están:



Captain Mnemo
Se trata de un monitor de sistema especializado en recolectar contraseñas.

System Spy
Graba todas las actividades realizadas en el ordenador y almacena la información en un único fichero para enviarla posteriormente al *hacker*.

SC-Keylog
Graba todas las actividades de la PC, las pulsaciones del teclado, los programas abiertos y envía la información mediante *e-mail* al *hacker*.

Perfect Keylogger
Graba todas las webs visitadas, las teclas que se pulsan en el teclado y los clics de ratón.

MSN Sniffer
Es una herramienta de monitoreo que graba las conversaciones del *Messenger*.

Fuente: Webroot, firma especializada en software de seguridad.

babaco1. (Del tupí wawa'su). m. Arbusto de la selva ecuatoriana, que produce fruto comestible. 2. Fruto de esta planta.