

Arnaldo Coro Antich

La conexión a la Internet que se realice desde cualquier país del mundo utilizando una computadora que tenga instalado el sistema operativo WINDOWS, atrae de inmediato la atención de los "perros de presa" de la Microsoft Corporation.

Estos "watchdogs" digitales, están siempre a la espera de que algún "usuario" se conecte a la red de redes para de inmediato comenzar a fisgonear en la computadora con la que se ha realizado la conexión.

Aunque muchos incautos niegan que esto sea así, lo cierto es que, por citar solo un ejemplo, bien escondido en el complejo de configuración de WINDOWS XP, hay una opción mediante la cual, cada vez que la computadora "salga a la Internet", esta envía automática y silenciosamente un mensaje a las "fincas de servidores" de MICROSOFT, alertando que dicha máquina esta en línea, para supuestamente realizar una inocente revisión, cuyo objetivo es saber si el sistema operativo esta o no actualizado con respecto a los múltiples "parches" para corregir fallas de seguridad, que continuamente MICROSOFT tiene que emitir.

Todo este proceso silencioso y encubierto transcurre simultáneamente, mientras el inocente usuario navega por la Internet, en busca de información o envía y recibe correos electrónicos, se conecta al sitio WEB de una emisora de radio, o descarga ficheros de música.

El procedimiento espía esta concebido para que no endentezca mucho la transferencia de datos hacia y desde la Internet, con el fin de que no llame mucho la atención al cibernavegante.

PERO NO SOLO SE TRATA DE "ACTUALIZACIONES"

Las cada vez mas frecuentes "fugas de información" que han dado lugar incluso a la quiebra de empresas, y la ruina de no pocas personas victimas de los delitos informáticos, especialmente el llamado "robo de identidad" ocurren simple y sencillamente por no tomar las medidas, incluso mínimas, de seguridad informática.

En el caso de los productos informáticos de la Microsoft Corporation, este es un mal histórico, que se remonta a las primeras versiones del sistema operativo MS-DOS (Microsoft Disk Operating System), pero que se ha ido agudizando a medida que se hacen cada vez mas complejos los sistemas operativos de interfase grafica de usuario y los programas que funcionan en los mismos.

Es así que el mas reciente sistema operativo WINDOWS VISTA, tuvo que recibir su "primer parche de seguridad" incluso un día antes de que saliera oficialmente al mercado y este proceso ha continuado hasta el punto que la Microsoft no tuvo otra opción que admitir o mas bien se podría decir, recomendar, a los fabricantes de máquinas computadoras que podían incluir en los nuevos modelos la instalación predeterminada de fábrica del WINDOWS XP en lugar del WINDOWS VISTA, dado el rechazo desatado entre los compradores al ultimo engendro salido de la esquina noroeste de los Estados Unidos de

América.

MICROSOFT EN PLENA COLUSIÓN CON LA NATIONAL SECURITY AGENCY , EL FEDERAL BUREAU OF INVESTIGATION, LA CENTRAL INTELLIGENCE AGENCY

Secreto a voces, más bien a gritos, es el hecho de que al dotar a sus programas y sistemas operativos de toda una serie de "puertas traseras" y "agujeros de seguridad introducidos intencionalmente" la Microsoft Corporation, al igual que otras de los mas importantes consorcios productores de software en los EE.UU.

incluso re-enrutan las conexiones

automáticas de ciertos usuarios hacia los servidores de ficheros de esas agencias de inteligencia.

Esta "practica' surgida desde los inicios de la llamada conectividad global, se exagera a partir de los sucesos del 11 de Septiembre de 2001 en Nueva York, Washington y Pennsylvania, bajo el manto protector de la llamada "Ley Patriota".

Ante la pregunta ¿Que hacer si se están utilizando sistemas operativos y paquetes de programas (Como Microsoft Windows y Microsoft Office) en máquinas computadoras que se conectan a la Internet?

La respuesta inicial tiene dos variantes:

A corto plazo: Asesorarse muy bien con un especialista de primer nivel en Seguridad informática para cancelar todas las opciones que impliquen la conexión automática, sin conocimiento del usuario, a cualquier sitio en la red de redes

Y...

A mas largo plazo, pero no muy largo: Iniciar de inmediato el estudio de los sistemas operativos y programas de software libre y no propietario, con el fin de realizar en forma ordenada y coherente la "migración", que asegure y garantice que ningún "producto de la Microsoft Corporation" cuyos códigos fuentes son totalmente secretos, quede trabajando en los equipos de computación que necesitamos proteger de esas nefastas intrusiones.

WINDOWS XP tiene 40 millones de líneas de código fuente... de las cuales ni una sola es de dominio publico, por lo tanto es posible asegurar que dentro de las mismas existan muchísimas otras operaciones encubiertas

capaces de vaciar los contenidos de los discos duros de las computaras, determinar los hábitos de navegación

por Internet como por ejemplo los sitios WEB mas visitados, y por supuesto husmear en todo el tráfico de correo electrónico que se lleve a cabo.

Al cargar en una computadora un sistema operativo de software libre y no propietario debidamente validado, se sabe siempre que hace cada programa y como lo hace, así como se cuenta con la gama completa de los códigos fuente al ser estos de carácter publico, lo que

permite a su vez implementar sistemas de protección contra los delitos informáticos cuya puesta en acción resulta imposible con los sistemas operativos y programas de software propietario, como son las diferentes versiones de WINDOWS y la suite Ofimática "OFFICE".

Fuente: www.rebellion.org