¿Qué busca un atacante cuando entra en su computadora?

Hasta hace algunos años, ingresar furtivamente a una computadora era un proceso relativamente complicado, que solo unos pocos escogidos eran capaces de lograr.

Estos primeros piratas ó hackers, eran individuos bastante inteligentes, con amplios conocimientos del funcionamiento interno de los sistemas operativos y posaderas de acero que les permitían pasar cientos de horas sentados frente a un monitor, devanándose los sesos mientras repasaban uno a uno los cientos de huecos en la seguridad de sus objetivos informáticos.

Para esa primera generación, investirse con el título de hacker era casi una cuestión de honor. El epíteto era otorgado cuando un individuo demostraba que había perpetrado uno o varios ataques a sitios con algún valor estratégico dentro del ciberespacio. Además, era necesario hacer gala de preceptos teóricos (que rayaban en lo poético) como por ejemplo la libertad de las ideas, el libre acceso a la información y la anarquía sin reglas del mundo virtual; estas normas hacían vibrar una fibra neo-hippie en todo el asunto, aportándole un matiz tecnológico a ideas nacidas en los años sesenta.

No faltó quien albergara en su corazón la secreta esperanza de descubrir algún complot gubernamental, penetrar la seguridad de un banco para hacerse rico instantáneamente o descubrir los códigos de lanzamiento del arsenal nuclear de alguna superpotencia, para sentirse Lex Luthor por unos minutos. Como no existía un marco jurídico que castigara los delitos cometidos en el mundo virtual, los atacantes llegaron a pensar que no había crimen alguno tras sus acciones.

Superado el tiempo de los protohackers, surgió una segunda generación que conservaba parte de los ideales fundamentales del asunto, pero que extendía sus objetivos a cualquier computador, personal o corporativo, que fuese susceptible a ser intervenido. En realidad eran pocos los PCs que valían el esfuerzo, pero herramientas especializadas aceleraron notablemente el proceso, haciendo menor el tiempo necesario para obtener información, que en muchos casos no tenía ningún valor real para el atacante.

De un tiempo para acá el problema ha tomado matices pandémicos. Ya no es necesario que piratas malintencionados dediquen largas horas a intervenir un computador. Hoy día, cualquiera con medianos conocimientos informáticos tarda poco más que unos segundos enviando una de las miles de forma de spyware que abundan en Internet y que le permiten acceder a la información realmente importante que almacena su computadora. Los programas espía más modernos usan criterios para seleccionar la información que consideran importante, capturando datos personales como passwords de acceso, números de tarjetas de crédito, claves de correo electrónico o cualquier otra cosa que considere relevante; una vez capturada la información es enviada automáticamente al atacante quien puede disponer de ella cuando y como quiera.

Se estima que ocho de cada diez computadoras conectadas a Internet tienen instalado algún tipo de programa espía, que aunque no interfieren con el funcionamiento del computador, está enviando constantemente datos acerca del usuario. Aunque el problema es grave en el hogar, puede llegar a ser inaceptablemente peligroso en ambientes corporativos, donde los expertos en seguridad se preguntan cuánta información puede estarse filtrando en su entorno empresarial. Aunque muchos fabricantes de software ofrecen soluciones al problema de las intrusiones por piratas informáticos y spyware, es necesario que siga recomendaciones básicas de seguridad como crear una clave de acceso suficientemente robusta e instalar un firewall actualizado y sólido.

Por evidente que parezca, un consejo aceptable para evitar instalar programas espía es leer los mensajes que aparecen en la pantalla, he visto cientos de veces como los usuarios no se dan un tiempo para leer los avisos que el sistema genera, aceptando o rechazando las advertencias sobre instalaciones sin siquiera tomarse un tiempo para ver de qué se trata. Hasta el firewall más elaborado será totalmente inútil si son usuarios certificados quienes autorizan la instalación de software que puede ser malicioso; tómese un tiempo y lea las advertencias, ante la duda es mejor tomar el camino seguro y rechazar servicios fantasma no solicitados, recuerde que en el océano de Internet, navegan piratas dispuestos a apoderase de su bien más preciado, la información.

Freddy E. Molina
http://www.pc-news.com/detalle.asp?sid=&id=11&Ida=1870