

¡Atención, peligro! Cinco sugerencias para utilizar PC de uso público

Por Kim Komando

Hay un chico en Nueva York que podría haber hurgado en sus asuntos. En caso de que lo haya hecho, es probable que asaltara su cuenta bancaria en línea.

Juju Jiang se declaró culpable y ahora cumple condena, pero durante un par de años espío equipos públicos mediante un software que registra las teclas presionadas. Eso le servía para hacerse con nombres de usuario y contraseñas. Algunas de estas informaciones las utilizó para robar dinero, otras las vendió en el Web.

Lo sorprendieron mientras manipulaba el equipo personal de una víctima estando ella presente. La víctima contemplaba atónita cómo el agresor hurgaba en su máquina. El delincuente utilizaba GoToMyPC, un programa que permite a los viajeros obtener acceso a sus equipos a distancia. Como la víctima había utilizado GoToMyPC con anterioridad en un equipo público, Jiang pudo hacerse con el nombre y la contraseña.

Todo esto ilustra un problema que hasta ahora no se había considerado, y es que resulta muy fácil instalar software espía en equipos de acceso público como los de cibercafés, aeropuertos, bibliotecas y otros espacios públicos.

Mediante software espía, un delincuente puede robarle sus nombres de usuario y contraseñas, lo que en último término podría traducirse en un robo de su dinero o en una suplantación de su identidad. Lo suficiente como para tener cuidado con los equipos de acceso público.

El software pasa inadvertido

Se usa software para espiar porque pasa inadvertido para el ojo inexperto. También se puede emplear hardware para conseguir casi el mismo resultado instalándolo entre el teclado y el equipo. Pero claro, esto es demasiado evidente en un sitio público.

El programa, muy al contrario, registra con total discreción las teclas que la víctima presiona en el teclado. A continuación, envía el registro por correo electrónico según un plan establecido, aunque también puede descargarse. Otros programas toman imágenes de los sitios visitados en el Web, que también se envían por correo electrónico.

Como ya he dicho, el software espía no despierta sospechas, y no advertirá su presencia a menos que sepa cómo buscarlo. Recomiendo buscar este tipo de software en un equipo antes de usarlo; a continuación explico cómo hacerlo.

No debe olvidar, por otra parte, que existen otras amenazas aparte del software espía. Créanme, esto es peor que usar un lavabo público.

Cinco consejos para cuando utilice un equipo ajeno:

Compruebe si hay software espía

Descargue X-Cleaner Spyware Remover del sitio spywareinfo.com y guárdelo en un disquete. Si el equipo público dispone de disquetera, inserte el disco y ejecute X-Cleaner desde ahí para rastrear el disco duro. No es necesario instalarlo.

Borre las huellas

Siempre que se usa un explorador de Internet, éste guarda un registro de los sitios visitados. Cuando termine de explorar con Microsoft Internet Explorer, haga clic en Herramientas y, después, elija Opciones de Internet. En la ficha General, haga clic en Eliminar archivos y también en Eliminar cookies. Por último, haga clic en Borrar Historial.

Si utiliza Netscape Navigator, es algo más complicado. Siga estas instrucciones.

- Antes de conectarse, compruebe la configuración. Haga clic en Editar y elija Preferencias. Haga clic en la flecha que aparece junto a Navigator y seleccione Historial. A la derecha aparece la sección Navegación por el historial. En la opción Recordar páginas visitadas los últimos X días, escriba un cero (0).
- Haga clic en la flecha que aparece junto a Privacidad & seguridad y elija Cookies. Seleccione la opción Desactivar cookies y la opción para desactivar cookies en correos electrónicos y grupos de noticias.
- Cuando acabe de explorar, haga clic en Editar y elija Preferencias. Haga clic en la flecha que aparece junto a Navigator y elija Historial. Haga clic en los botones Borrar historial y Borrar barra Dirección. Haga clic en la flecha junto a Privacidad & seguridad en la parte izquierda y elija Cookies. A continuación, haga clic en el botón Gestionar cookies almacenados. En la ficha Cookies almacenados, haga clic en Eliminar todos los cookies.
- Luego, de nuevo en Preferencias, haga clic en la flecha junto a Avanzadas, en la parte izquierda, y elija Caché. Haga clic en el botón Vaciar caché de memoria y, después, en el botón Vaciar caché de disco.

Proteja sus contraseñas

Los exploradores también registran las contraseñas. Antes de explorar con Internet Explorer, haga clic en Herramientas y seleccione Opciones de Internet. En la ficha Contenido, haga clic en el botón Autocompletar y después elimine la marca de las cuatro casillas de verificación que aparecen en el siguiente cuadro de diálogo.

Cuando acabe, vuelva a hacer clic en Herramientas y seleccione Opciones de Internet. De nuevo en la ficha Contenido, haga clic en el botón Autocompletar y, a continuación, haga clic en los botones Borrar formularios y Borrar contraseñas.

En el caso de que utilice Netscape, haga clic en Editar y elija Preferencias. Haga clic en la flecha junto a Privacidad & seguridad y elija Contraseñas. Borre la marca de la casilla de verificación Recordar contraseñas. Cuando termine, vuelva a esta pantalla y haga clic

en el botón Gestionar contraseñas almacenadas. En la ficha Contraseñas guardadas, haga clic en el botón Eliminar todo.

Netscape dispone de una función similar a Autocompletar, que guarda los datos introducidos en formularios. Para desactivarla, en Privacidad & seguridad, seleccione Formularios y, a continuación, elimine la marca de la casilla Guardar los datos de formularios de las páginas web al terminar de rellenar los formularios. Cuando acabe de explorar, vuelva a esta pantalla y haga clic en el botón Gestionar datos del formulario almacenados. Por último, haga clic en Eliminar todos los datos guardados.

Esta limpieza del explorador nos permite asegurarnos de que nadie podrá rastrear nuestra exploración ni hacerse con nuestra contraseña mirando los datos guardados. Ahora bien, un programa que registre las teclas presionadas sí capta las contraseñas.

A algunos de estos programas, no a todos, podemos burlarlos si copiamos y pegamos los números y letras de una contraseña. Por ejemplo, digamos que la página que tiene abierta contiene texto, y que su contraseña es «jim» (¡espero que no sea tan fácil!). Pues bien, busque en el texto de la página una «j», una «i» y una «m», cópielas y péguelas después una a una en el cuadro para la contraseña.

Podríamos decir que la mejor contraseña es la temporal. Úsela fuera de casa y luego cámbiela.

No confíe en el cifrado

En el mercado hay a nuestro alcance una serie de programas que se usan para cifrar el correo electrónico. Sin embargo, el correo se cifra cuando hacemos clic en el botón de envío: demasiado tarde si hay un programa que registre las teclas presionadas, ya que guarda el mensaje y la contraseña en el mismo momento de escribirlos.

Use su sentido común

Los equipos de acceso al público pueden ser seguros, pero no hay forma de estar tranquilos por completo. Uno puede tomar medidas de seguridad en su equipo de casa o del trabajo, pero nunca se sabe qué ocurre con una máquina expuesta al público.

Tenga cuidado con estos equipos. No realice operaciones bancarias ni bursátiles con ellos si es posible, ni tampoco operaciones con tarjetas de crédito. Si tiene que ver su correo, utilice una contraseña temporal. Pregunte al administrador cómo borrar todo rastro de su actividad.

Si sólo va a explorar, no debería haber inconveniente, pero evite las operaciones delicadas. Podría haber cualquier Juju Jiang al acecho.