NAVEGUE SEGURO EN INTERNET

Programas maliciosos

Hasta hace unos años, los virus eran considerados la principal amenaza para los equipos informáticos.
En la actualidad existen otras amenazas derivadas de los virus. Están los gusanos informáticos, que son programas que, a diferencia de los virus, se propagan realizando copias de si mismos con consecuencias similares y también los troyanos, que una vez se introducen en el sistema, capturan contraseñas, pulsaciones del teclado o permiten el acceso remoto al computador.

En los últimos años, y debido principalmente al uso cotidiano de computadores y la masificación del acceso a Internet, han aparecido otras amenazas catalogadas bajo el término "malware", que es la forma abreviada para *MAL*icious soft*WARE*, es decir, programas maliciosos.

Malware es cualquier programa, documento o mensaje que pueda resultar perjudicial para un computador, tanto por pérdida de datos como por disminución de su productividad. Bajo esta denominación encontramos los siguientes:

Dialer (marcador): programa que busca establecer conexiones telefónicas con números en otros países o de tarifa especial.

Spyware (Software/ programa espía): programa que monitorea y recolecta información sobre los hábitos del usuario al navegar en Internet y los envía de forma secreta a empresas de publicidad

Hoax: Mensaje de correo electrónico advirtiendo sobre falsos virus

Spam: Envío indiscriminado de mensajes de correo no solicitados, con fines publicitarios o buscando saturar una red específica

¿Qué es un dialer malicioso?

Es un programa que suele ser utilizado para redirigir, de forma maliciosa, las conexiones mientras el usuario navega en Internet.
Su objetivo es finalizar la conexión telefónica que el usuario de internet esté utilizando en ese momento y establecer otra, marcando, bien sea, un número de teléfono con tarifa especial o un número en otro país.

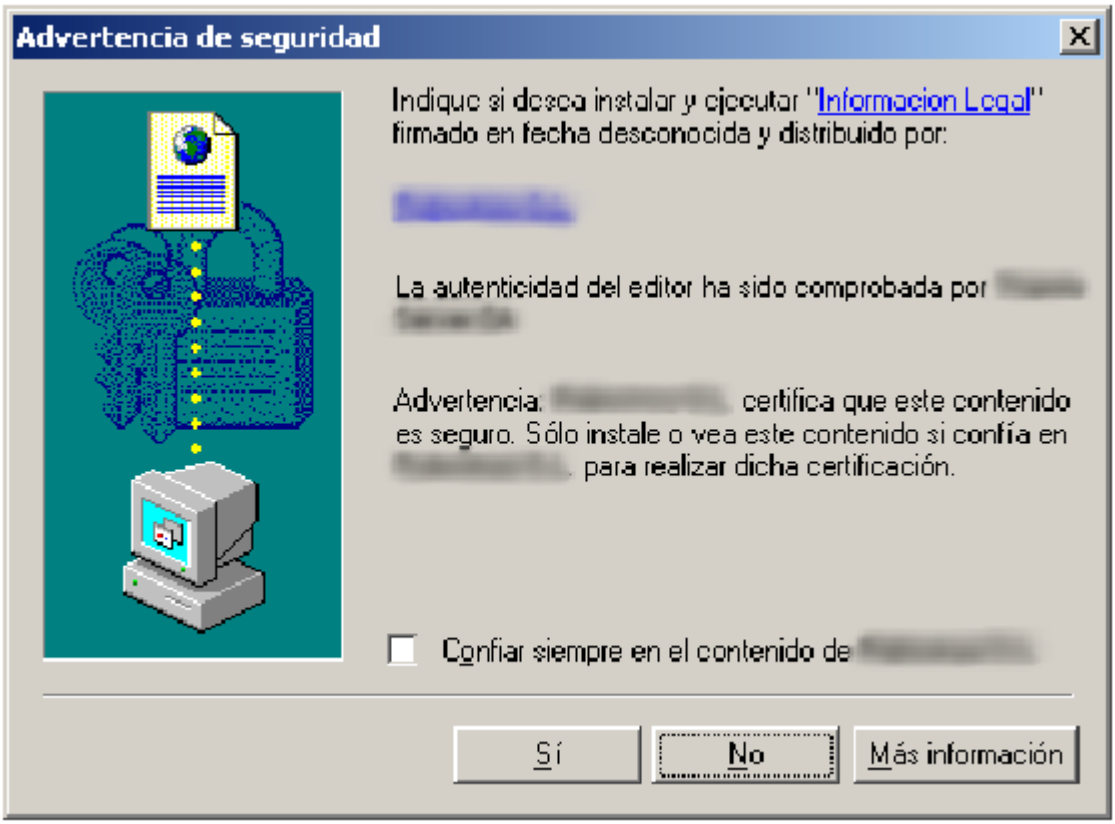
¿Cómo funcionan los dialers?

Los dialers son descargados inadvertidamente al navegar en ciertas páginas de internet. Estas páginas son por lo general las que ofrecen acceso a contenido gratuito de entretenimiento (juegos, canciones, imágenes, videos, etc.) así como programas sin licencia y contenido para adultos.

Estas páginas, en la mayoría de casos, carecen de criterios éticos, aprovechando la desinformación y confusión de los usuarios con poco conocimiento para lograr instalar programas en su computador.

Los marcadores telefónicos normalmente se descargan mediante un archivo ejecutable (extension.exe), o mediante un control ActiveX, que es un estándar definido por Microsoft para subprogramas que se encuentran en una pagina Web y solo funcionan con el navegador Internet Explorer.

Esta es la ventana de advertencia de seguridad que se despliega para solicitar la instalación y ejecución de un control ActiveX.



Para el caso de los dialers, la función del control ActiveX es descargar, instalar y ejecutar el programa malicioso de forma inadvertida.

Una vez instalado en el computador, el programa dialer buscará establecer llamadas telefónicas a un número de tarifa especial o a números internacionales predefinidos. Estas llamadas pueden ser realizadas periódicamente por el programa o cada vez que el usuario acceda a una página específica.

Los dialers afectan únicamente a los usuarios que acceden a Internet haciendo uso de líneas y modem convencionales a través de la RTPBC (Red Telefónica Pública Básica Conmutada) o líneas RDSI (Red Digital de Servicios Integrados) que cuenten con los permisos necesarios de marcación a numeración especial o de larga distancia internacional.
Los usuarios que se conectan a internet por modem ADSL o cable modem no son susceptibles a los programas maliciosos de marcación, siempre y cuando el computador no tenga otra línea o derivación conectada a un modem convencional.

Características generales

En materia de dialers es común encontrar muchas irregularidades que a apelan a la desinformación y falta de conocimiento de los usuarios.

Las paginas de donde son descargados:

- No ofrecen términos y condiciones de uso claros o los ubican en lugares poco visibles, empleando otros idiomas, letra de tamaño muy reducido o colores que no facilitan su lectura.

- Saturan al usuario, indicándole reiteradamente que es preciso hacer clic en "SI" o "ACEPTAR" en determinada ventana emergente (pop up), esto como requisito para tener acceso a cierto contenido o para cargar el "*visor de contenidos*", que, dicho en otras palabras, es el mismo programa dialer.

- No informan al usuario que se van a instalar programas en el disco duro y que estos van a hacer modificaciones en el sistema, generalmente la creación de nuevos accesos a Internet, omitiendo los que el usuario emplea usualmente.

- No suelen informar de los costos de conexión asociados, previa ni posteriormente a su instalación.

Los programas dialers:

- Aprovechan las vulnerabilidades del navegador para instalarse en el sistema, a veces sin intervención del usuario.

- Intentan cambiar la conexión a Internet sin previo aviso, realizando marcaciones de manera inadvertida para el usuario, sin brindar avisos visuales o sonoros.

- Suelen crear un acceso directo (generalmente en el escritorio) para acceder al servicio, lo que se traduce en nuevos intentos de marcación.

- No permiten ser desinstalados fácilmente o requieren de programas específicos para hacerlo.

Consejos prácticos

A continuación se presentan algunos consejos prácticos para evitar y/o prevenir las amenazas de los dialers maliciosos:

- Procure conocer el número de acceso de su proveedor de internet y verifique que este sea el mismo que vaya a marcar su modem cuando aparece la ventana de conexión de acceso a Internet.

- Lea con atención las advertencias de las páginas web visitadas así como las de cualquier programa que instale en su computadora.

- Evite ingresar a páginas extrañas o poco confiables, que puedan solicitar descargar o instalar archivos sin un motivo claramente justificado. Si se detectan descargas automáticas deben ser canceladas tan pronto sean descubiertas.

- Tenga especial cuidado al navegar en páginas que ofrezcan acceso a contenido gratuito, bien sea software sin la debida licencia, juegos, tonos de timbres, contenido erótico, consulta de horóscopos, suerte, búsqueda de pareja, etc. y mucho más si exigen la instalación de alguna aplicación como requisito previo.

- No silencie el altavoz del módem, de esta forma puede monitorear la actividad del mismo y oír si se produce el marcado de un número nuevo mientras esta conectado a Internet.

- Haga uso de un programa para bloquear marcadores telefónicos (anti dialers) o emplee uno que detecte y remueva posibles programas maliciosos que hayan podido instalarse sin su conocimiento. Para esto solicite la ayuda de un experto u obtenga mayor información sobre estos programas realizando una consulta en internet con la palabra clave "dialers" o "malware", acompañado de las palabras "detectar", "eliminar" o "remover".

- Haga uso de la facilidad de código secreto proveída por su operador de telefonía local. Esto le permitirá activar y desactivar la restricción de llamadas de larga distancia desde su línea, así como llamadas hacia teléfonos móviles o números de tarifa especial. Póngase en contacto con el operador de su línea telefónica para obtener mayor información sobre esta función.

Para usuarios avanzados:

- Configure su navegador en el nivel más alto de seguridad que le sea permitido.

- Si utiliza un sistema operativo multiusuario, es recomendable utilizar un usuario con privilegios de administrador solo para las tareas que lo precisen, y nunca para navegar por Internet, pues dichos privilegios a su vez habilitan ciertas funciones que representan un riesgo potencial.

Glosario

ADSL: Asynchronous Digital Subscriber Line. "Línea de suscripción asimétrica digital". Se trata de un tipo de conexión a Internet y de una clase de modem que se caracterizan por su elevada velocidad.

ActiveX: Tecnología utilizada, entre otras cosas, para dotar a las paginas Web de mayores funcionalidades, como animaciones, video, navegación tridimensional, etc. Los controles ActiveX son pequeños programas que se incluyen dentro de estas páginas. Lamentablemente, por ser programas, pueden ser el objetivo de algún virus.

Anti-dialers: Programas que interceptan los intentos de conexión no autorizados y los bloquean, para que no causen daños al usuario.

Dialers: Programas que marcan un numero de tarificación adicional para acceder a contenidos del tipo adultos, entretenimiento, etc. En ocasiones estas aplicaciones están hechas maliciosamente (de ahi que se conozcan como dialers maliciosos) y, sin el consentimiento del usuario, interrumpen su conexión e inician otra diferente.

Gusano (worm): Es un programa similar a un virus que, a diferencia de este, solamente realiza copias de si mismo, o de partes de el.

Malware: *MAL*icious soft*WARE.* Cualquier programa, documento o mensaje, susceptible de causar perjuicios a los usuarios de sistemas informáticos.

Modem. La palabra MODEM es un acrónimo del término MOduladorDEModulador. Se trata de un dispositivo interno o externo de la computadora que permite transformar ciertas señales de la computadora, transmitir y recibir información por medio de la línea telefónica.

Pop up: Ventana o recuadro de mensaje que aparece de pronto al navegar por ciertas paginas de Internet. Pueden abrirse por alguna acción del mouse, por tiempo o simplemente al entrar a alguna pagina.

RDSI Red Digital de Servicios Integrados): Se trata de una red, en general como evolución de una red telefónica, que proporciona conectividad digital extremo a extremo para el soporte de un amplio rango de servicios, incluyendo servicios de voz y no-voz.

RTPBC (Red Telefónica Pública Básica Conmutada): Es aquella que permite realizar comunicaciones de voz a distancia por medio de alambres de cobre que conforman la red telefónica.

Spam: Es correo electrónico no solicitado, normalmente con contenido publicitario, que se envía de forma masiva.

Spyware: Es un termino general para un programa que monitorea las acciones del usuario en un computador y es utilizado por un hacker o por alguna compañía para recolectar información

Troyano: Programa que llega a la computadora de manera encubierta, aparentando ser inofensivo y, una vez instalado, realiza determinadas acciones que afectan a la confidencialidad del usuario afectado.