



SPYWARE

Ing. José Guillermo Rodríguez Ávila
Operador de Sistemas
Edición 05-04

El spyware es quizás la más inquietante de todas las amenazas informáticas, ya que se entromete de lleno en tu vida privada, sin que te des cuenta.

¿QUÉ ES?

El spyware es un tipo de malware difícil de detectar. Recopila información sobre sus hábitos y su historial de navegación o información personal (como números de tarjetas de crédito) y a menudo utiliza Internet para enviar esta información a terceros sin su conocimiento.

¿DE DÓNDE PROVIENE EL SPYWARE?

A menudo, el spyware está incluido dentro de otro software o en descargas de sitios de intercambio de archivos (por ejemplo, sitios donde descarga música o películas gratis) o se instala cuando abre un adjunto de un correo electrónico. Debido a la naturaleza secreta del spyware, la mayoría de la gente ni siquiera sabe cuándo tiene spyware en su equipo.

¿CÓMO RECONOCER EL SPYWARE?

Pueden aparecer iconos nuevos o no identificados en la barra de tareas en la parte inferior de su pantalla, y las búsquedas pueden provocar que se le redirija a un motor de búsqueda diferente. Aparecen mensajes de error aleatorios cuando realiza operaciones que antes funcionaban correctamente.

TIPOS DE SPYWARE

El spyware se puede dividir en dos categorías: INTERNO, el mismo programa posee líneas de código para recolectar datos y EXTERNO, son programas independientes los que se encargan de recoger la información.

Dentro de éstas, los programas espía se clasifican en:

- **Keyloggers:** El hacker monitoriza el ordenador de tal forma que es capaz de registrar las pulsaciones que el usuario realiza sobre el teclado.
- **Adware:** Es el programa espía más común y actúa mostrando anuncios, generalmente en forma de ventanas emergentes, que no han sido solicitados por el navegante. Si este último hace clic sobre los pop-ups e introduce sus datos para "comprar" lo que se anuncia o saber más sobre el producto, el spyware se encarga de enviar esa información al hacker.
- **Browser hijacking:** Su función no es otra que la de secuestrar la página inicial del navegador para llenarla de anuncios, por lo que es más molesto que peligroso.

¿CÓMO EVITAR EL SPYWARE?

- Asegúrese de que su navegador, su sistema operativo y su software tienen las actualizaciones y los parches de seguridad más recientes.
- Establezca niveles más altos de seguridad y privacidad en su navegador.
- Extreme las precauciones si frecuenta sitios de intercambio de archivos.
- Evite descargarse contenidos de páginas desconocidas o de dudosa reputación.
- No haga clic en las ventanas emergentes de publicidad.

¿CÓMO ELIMINAR EL SPYWARE?

Un buen software antivirus puede encontrar y eliminar cualquier spyware en su equipo, ya que normalmente incluye protección antispyware. También puede comprobar Programas y características en busca de algo que no pertenezca a su equipo.

EJEMPLOS DE PROGRAMAS SPYWARE

CoolWebSearch: Controla el navegador y, por tanto, las páginas y las búsquedas se dirigen a lo que el hacker quiere, y no a lo que el usuario solicita.

Gator, KeenValue o n-CASE: Programas que abren ventanas emergentes de publicidad en Internet.

Perfect Keylogger: Graba los sitios web que se visitan y las contraseñas que se escriben en el teclado.

GLOSARIO:

Keyloggers: Es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado.

Adware: Software que, de modo automático, exhibe al usuario anuncios publicitarios.

Browser Hijacking: Software no deseado que modifica la configuración de un navegador web sin permiso del usuario, para inyectar publicidad no deseada en el navegador del usuario.

Pop-Ups: Ventanas Emergentes

FUENTES:

<https://www.pandasecurity.com/mexico/homeusers/security-info/cybercrime/spyware/>

<https://www.avast.com/es-es/c-spyware>

<http://www.valor-top.com/blog/que-es-un-spyware>

