Qué tan peligroso es navegar por páginas web piratas

22/07/2021

Hoy en día, la seguridad y privacidad en la red son dos de los factores que más preocupan a la mayoría de las personas. A diario, son muchas las amenazas a las que puede estar expuesto un internauta mientras navega por la web: **malware, hackeo, enlaces maliciosos y hasta doxing** (chantaje en la red), son algunas de las estrategias que usan los ciberdelincuentes para intentar acceder a la información relevante de las personas.

Sin embargo, muchas veces el trabajo de estos delincuentes no es tan difícil, pues son los mismos usuarios los que dejan el camino libre para que estas personas puedan atacarlos. Así, **uno de los fallos más comunes que se puede observar en la actualidad es acceder a páginas web piratas.**

¿Qué es una página pirata?

Aunque el término parezca sencillo, es claro que, aunque muchas personas acceden a este tipo de sitios a diario, son pocas las que realmente sabrían reconocerlos. En pocas palabras, **una página pirata es un sitio web en el que se puede hallar algún contenido ilegal.** Son páginas en las que se alojan desde series y películas que se pueden ver o descargar de forma gratuita, hasta programas y juegos crackeados, es decir, que no necesitan de una licencia para poder ser instalados en cualquier computador.

Claro, es lógico que muchas personas accedan a estas páginas por ignorancia, en busca de contenido útil que pueda suministrar una solución a un problema o necesidad. No obstante, el hecho de que su búsqueda sea con buenas intenciones no las exime de poderse convertir en víctimas de

hackers que siempre andan colocando una que otra trampa en sitios web piratas.

Ante esta realidad, Infobae trae algunos puntos que reflejan las formas en que una persona puede ser engañada para abrir un espacio en su seguridad y así **dar vía libre para que los delincuentes accedan a sus máquinas de forma casi que imperceptible.**

Descarga de malware

En el lenguaje informático existe una palabra denominada como **Backdoor**, que define la forma en que los virus pueden afectar una computadora u otro dispositivo tras la fachada de un programa o aplicación útil y sana.

No es sorpresa que muchos de los softwares que se encuentran alojados en páginas piratas puedan contener tras de sí un malware que puede tomar control de la máquina y robar datos importantes que se encuentran en esta. Aunque en la mayoría de los casos, **los programas funcionan con normalidad, al momento de ser instalados también se depositan aplicaciones alternas que van haciendo daño al sistema interno del computador.**

Una persona utiliza un ordenador portátil. EFE/SASCHA STEINBACH/Archivo

Enlaces maliciosos

Es una de las trampas más comunes: al ingresar a una página pirata, puede ser que el sitio en sí ni siquiera sea peligroso, pero **cuenta con algunos enlaces a los que son obligatorios acceder** para poder descargar o gozar de la información que se encuentra alojada en ellos. Es en ese momento cuando un internauta podría estar dando vía libre a la descarga de un malware o cayendo en una estrategia de phishing en la que podría perder contraseñas u otro tipo de datos

personales relevantes.

Robo de información personal

Por supuesto, el robo de información personal es una amenaza latente en cualquier página pirata que se visite, especialmente aquellas que **solicitan llenar un formulario o registro para poder acceder o descargar sus contenidos.** En muchas ocasiones solo es necesario que los hackers cuenten con datos como el correo electrónico, el nombre, número telefónico o cuentas de redes sociales para poder crear una estrategia mucho más personalizada para cada una de sus víctimas.

Es en este punto, más que en cualquiera de los anteriores, donde el sentido común debería estar más presente. En caso de que una página de dudosa reputación le solicite este tipo de información para acceder a ella, lo mejor es **dar clic en el botón de Atrás** y retirarse de ella. Es casi seguro que su información no llegaría a un sitio seguro y estaría dando vía libre para que los ciberdelincuentes conozcan información personal de primera mano.

Teniendo en cuenta todos estos peligros, ahora lo importante es ser más precavidos en el futuro: mantener actualizados los sistemas que se usan para la protección del dispositivo, **como el antivirus o el firewall**, además del navegador web. También evitar al máximo el ingreso a plataformas o páginas dudosas y no dar clic en cuanto enlace o anuncio aparezca. De esta forma, los protocolos de seguridad y privacidad se pueden mantener estables.

Fuente: Infobae