Adware

Curiosamente, el universo de la informática se ha tornado más simple en el uso y a la vez más complejo al intentar elegir el hardware o software idóneo que satisfaga nuestras necesidades de información. Cada día se incrementan las aplicaciones desarrolladas para facilitar y enriquecer las actividades diarias empleando una computadora de escritorio, tableta o teléfono inteligente; al mismo tiempo, son más los proveedores que buscan ser parte de este gran negocio global. En efecto, de acuerdo a Statista, empresa dedicada a la generación de estadísticas y estudios de mercado, la tienda en línea Apple Store, durante junio de 2015 registró 1.5 millones de aplicaciones disponibles para sus usuarios, nada mal para una sola marca de computadoras. Esto significa que estamos inmersos en un mercado cada vez más competitivo, agresivo y voraz buscando en todo momento, llegar a los ojos del consumidor para ofrecer sus productos o servicios; es por ello que existe el *adware*.

La palabra *adware* significa ***ad****vertisement-soft****ware*** o programas que despliegan en pantalla anuncios publicitarios. Aunque no necesariamente son dañinos pues muchos de ellos no contienen malware (o código maligno que dañe, robe o modifique indebidamente datos o software), llegan a ser molestos para el usuario por la frecuencia en que son desplegados en pantalla. Es común que el *adware* aparezca en todos los dispositivos, especialmente en teléfonos inteligentes y tabletas, sobre todo cuando se instala software gratuito (*freeware*) o de evaluación (*shareware*); no obstante, si el usuario paga por la versión completa o con mayores recursos, seguramente el *adware* desaparecerá; pero esto no siempre sucede así. Tres de los grandes problemas al instalar software sin costo son: saturación de anuncios publicitarios; la posible presencia de *malware* (generalmente troyanos); o bien el usuario, que al no leer las condiciones de uso, autoriza sin saberlo la adición de barras de herramientas publicitarias en su navegador, modificación de la página de inicio o la alteración de los resultados de búsquedas consumiendo además, recursos de su computadora haciéndola cada vez más lenta.

De los tres problemas anteriores, el segundo es uno de los más peligrosos. Efectivamente, los hackers de sombrero negro o mal intencionados, han desarrollado cierto tipo de *adware* engañoso y maligno cargado con software cuyas funcionalidades invaden la privacidad del usuario robando información, instalando *malware*, monitoreando la actividad realizada al navegar por la web (*spyware*), rastreando contraseñas y operaciones bancarias, efectuando capturas de pantallas o haciendo uso del procesador y memoria sin nuestro consentimiento (*bot*) secuestrando literalmente nuestro equipo de cómputo.

Por lo anterior, es indispensable seguir las siguientes recomendaciones:

Mantener actualizado el sistema operativo. Es importante recordar que los sistemas operativos (Windows, Android, iOS, Linux, etc.) son muy complejos y por tanto, no son infalibles; para corregir las vulnerabilidades existentes, es necesario actualizarlos constantemente. Esto, aunque no evita las amenazas, al menos disminuye el riesgo de ser "hackeado".

Evitar instalar software de sitios inseguros. Acceder a páginas de organizaciones conocidas brindan cierto grado de confianza haciendo que por reputación, imagen o ética, no resulte conveniente instalar malware en los equipo de cómputo. Es conveniente realizar una pequeña investigación sobre la autencidad del software ofrecido.

Si se instala un programa *shareware* o *freeware*, leer en su totalidad las condiciones de uso. Aunque se instale software de empresas conocidas o en tiendas oficiales, no garantiza la ausencia de *adware*. Si bien, es poco probable la presencia de *malware*, seguramente no evitaremos los anuncios continuos durante la ejecución de estos programas, por ello es fundamental revisar que nos ofrece el proveedor y a qué estamos condicionados.

Instalar un programa antivirus y actualizarlo constantemente. Aunque el término antivirus suene obsoleto, lo cierto es que la mayoría de estos paquetes contienen funciones *antiadware*, *antispyware* y *antispam*. Su actualización constante, disminuirá la probabilidad de efectivizar ataques a nuestro sistema.

Jamás presionar clic sobre ventanas emergentes (pop-up) o banners con publicidad que ofrece grandes beneficios a cambio de datos personales o pagos irrisorios, seguramente redirigirán el acceso a páginas web falsas o instalarán malware en nuestro equipo.

Siguiendo las medidas anteriores, no evitaremos la presencia de *adware,* pero sí disminuirá la probabilidad de que nuestro sistema se torne más lento o en el peor de los casos se vea afectado por algún *malware*.

REFERENCIAS

- Kaspersky (2016). What is adware? Definition. Kaspersky Labs. Tomado de https://usa.kaspersky.com/internet-security-center/threats/adware#.VvxHbhZ3EdV
- Raja. S. (2011). Accurate Adware Detection using Opcode Sequence Extraction. IEEE Computer Society. Tomado de http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6045962&tag=1
- Statista (2016). Facts and statistics on Apple. Tomado de http://www.statista.com/topics/847/apple/