

¡Bu! Aumentan los ataques de los falsos programas antivirus (Scareware); BBB aconseja sobre cómo proteger su computadora

Los expertos computacionales han informado sobre el aumento de los falsos programas antivirus (scareware), otra técnica engañosa usada por los piratas informáticos para robar información personal y propagar virus en línea. Últimamente, empresas como Google, Twitter y New York Times están siendo explotadas por estos piratas informáticos como parte de ataques masivos de falsos programas antivirus a los consumidores. Better Business Bureau ofrece consejos a los consumidores sobre cómo proteger sus computadoras y la información personal contra la amenaza de los falsos programas antivirus.

“Los recientes ataques de falsos programas antivirus aparecen en todas partes y se pueden encontrar incluso en los sitios Web más confiables de la Internet,” dijo Alison Southwick, vocera de BBB. “La amenaza de los falsos programas antivirus socava la confianza del consumidor en sitios Web comprometidos, y en la Internet en general, pero hay medidas que los usuarios de computadoras pueden tomar para protegerse”.

A mediados de septiembre, los visitantes del sitio Web de New York Times repentinamente recibieron una ventana emergente, la que se veía como un mensaje de la propia computadora, advirtiendo que ésta había sido infectada con un virus. Entonces, se le decía al usuario que visitara el sitio Web para comprar y descargar el software antivirus que podía solucionar el problema. El supuesto software antivirus en realidad instalaba aún más virus y programas maliciosos en la computadora, y el número de la tarjeta de crédito del usuario ahora estaba en manos de los piratas informáticos.

De acuerdo con New York Times, la ventana emergente era generada por un anuncio no autorizado. New York Times supo más tarde que había vendido espacio para anuncios a piratas informáticos que se hacían pasar por Vonage. Click Forensics ha informado que es el trabajo de delincuentes cibernéticos ucranianos.

La misma situación de la página Web de New York Times se está produciendo en toda la Internet. De acuerdo con la revista Computer World Magazine, los piratas informáticos no sólo están usando anuncios en ventanas emergentes, sino que también están “contaminando los resultados de búsquedas en Google”. Los piratas informáticos controlan las noticias y los temas importantes en línea, tales como la muerte de Patrick Swayze y el Abierto de los Estados Unidos (US Open). Asimismo, a través de técnicas de optimización de motores de búsqueda pueden garantizar que sus sitios Web aparezcan entre los primeros resultados. Las víctimas que hacen clic en los resultados de búsqueda falsos reciben una ventana emergente de un falso programa antivirus.

Microsoft ha estado advirtiendo al público que los ataques con los falsos programas antivirus están aumentando seriamente y que en la actualidad los

está combatiendo. La empresa presentó demandas contra cinco compañías acusándolas de ser la fuente de los ataques de falsos programas antivirus.

A continuación están las medidas que los usuarios de computadoras pueden tomar para proteger sus computadoras de dichos ataques:

Nunca baje la guardia. Un ataque de falsos programas antivirus se puede producir en sitios de noticias confiables como New York Times, en resultados de búsquedas de Google e incluso en Twitter.

Proteja su computadora. Instale actualizaciones para su sistema operativo, compre software antivirus de un nombre en el que confíe y mantenga ese software actualizado. También instale todos los parches de seguridad y las actualizaciones para su navegador Web y programas como Adobe Flash Player.

Actúe inmediatamente durante un ataque. Si recibe una ventana emergente de un falso programa antivirus, los expertos recomiendan forzar la ventana para cerrarla a través de su administrador de tareas. Para hacerlo, presione las teclas ctrl, alt y delete (suprimir) al mismo tiempo, abra su administrador de tareas, busque el navegador en la lista de programas ejecutables y haga clic en "end task" (finalizar tarea). Finalmente, ejecute un escáner antivirus con un software confiable y legítimo.

Si hizo clic en la ventana emergente y efectivamente compró el software, el pronóstico no es bueno. The [Washington Post ofrece consejos](#) en su blog Security Fix (soluciones de seguridad), pero para la persona con pocos conocimientos computacionales, podría ser necesario llamar a un profesional.

Para obtener más consejos sobre cómo combatir a los piratas informáticos y mantener la seguridad en línea, visite www.bbb.org