Si has utilizado el software de edición multimedia VSDC desde febrero a fines de marzo de este año, es probable que tu computadora se haya infectado con un troyano bancario.

El sitio web oficial de VSDC, una de las apps gratuitas más populares de edición y conversión de videos con más de 1.3 millones de visitas al mes, fue hackeado, una vez más.

Según un nuevo informe que Dr. Web publicó hoy, los piratas informáticos secuestraron el sitio de VSDC y reemplazaron sus enlaces de descarga de software que conducen a versiones de malware, engañando a los visitantes para que instalen el peligroso troyano bancario Win32.Bolik.2 y el ladrón de información KPOT.

Lo irónico es que aunque el sitio web de VSDC es tan popular y ofrece descargas de software, sigue ejecutándose en una conexión HTTP insegura.

Aún no está claro cómo los piratas informáticos lograron secuestrar el sitio web, pero los investigadores revelaron que la infracción nunca tuvo la intención de infectar a todos los usuarios, a diferencia del ataque del año pasado.

En su lugar, los investigadores de Dr. Web encontraron un código JavaScript malicioso en el sitio web de VSDC que fue diseñado para verificar la geolocalización de los visitantes y reemplazar los enlaces de descarga solo para visitantes de Reino Unido, Estados Unidos, Canadá y Australia.

El código malicioso inyectado en el sitio web pasó desapercibido por casi un mes, entre el 21 de febrero de 2019 y el 23 de marzo del mismo año, hasta que el investigador lo descubrió y notificó a los desarrolladores de VDSC.

Los usuarios dirigidos recibieron un peligroso troyano bancario diseñado para realizar *«inyecciones web, intercepciones de tráfico, registro de claves y robo de información de diferentes sistemas de banco-cliente».*

Además, los atacantes cambiaron el troyano Win32.Bolik.2 a KPOT Stealer, una variante de

Trojan.PWS.Stealer, el 22 de marzo, que roba información de navegadores web, cuentas de Microsoft, servicios de mensajería y otros programas.

Según los investigadores, por lo menos 565 visitantes descargaron el software VSDC infectado con el troyano bancario, mientras que 83 usuarios han infectado sus sistemas con el ladrón de información.

El sitio de VSDC ha sido hackeado varias veces en los últimos años. El año pasado, los hackers desconocidos lograron obtener acceso administrativo a su sitio web y reemplazaron los enlaces de descargar, y finalmente las computadoras de sus visitantes con AZORult Stealer, X-Key Keylogger y la backdoor DarkVNC.

¿Qué hacer si fuiste víctima?

Se debe tener en cuenta que el solo hecho de instalar la versión limpia de la actualización de software sobre el paquete malicioso no eliminará el código de malware de los dispositivos infectados.

Si descargaste el software en el periodo antes mencionado, debes instalar inmediatamente un software antivirus, con las últimas bases de datos actualizadas y analizar el sistema en busca de malware.

Además, a los usuarios afectados se les recomienda cambiar sus contraseñas para redes sociales y sitios web bancarios, luego de limpiar los sistemas.