The official website of a popular video editing software was infected with a banking trojan

news.drweb.com/show/

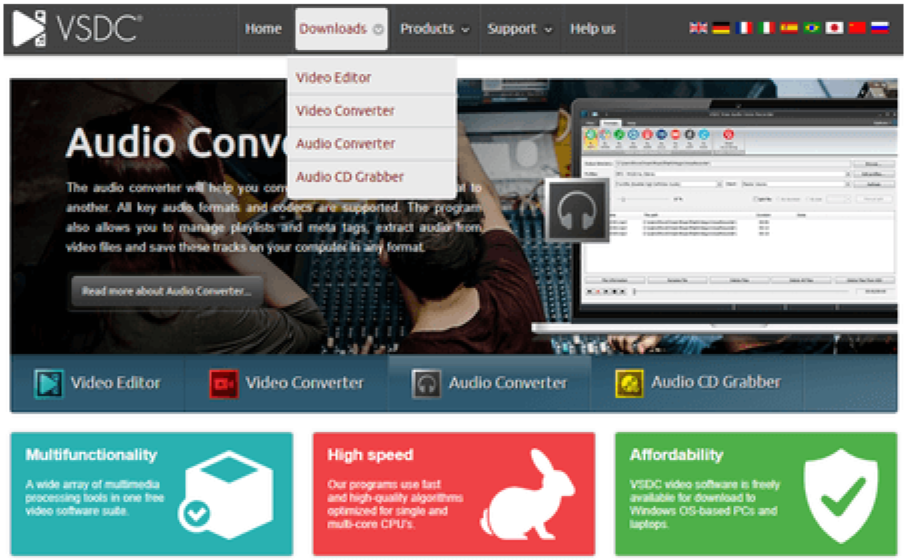
Doctor Web

Back to news

April 11, 2019

Doctor Web researchers discovered that the official website of a well-known video editing software, VSDC, was compromised. The hackers hijacked download links on the website causing visitors to download a dangerous banking trojan, Win32.Bolik.2, and the Trojan.PWS.Stealer (KPOT stealer) along with the editing software.

VSDC is a popular, free software for editing video and sound. According to SimilarWeb statistics, monthly visits of the VSDC website come close to 1.3 million users. However, the security measures taken by the website's developers often turn out to be insufficient for such traffic volume, which endangers a large number of people.


VSDC
Home
Downloads
Products
Support
Help us
Video Editor
Video Converter
Audio Converter
Audio CD Grabber
Audio Conv
The audio converter will help you con... to another. All key audio formats and codecs are supported. The program also allows you to manage playlists and meta tags, extract audio from video files and save these tracks on your computer in any format.
Read more about Audio Converter...
Video Editor
Video Converter
Audio Converter
Audio CD Grabber
Multifunctionality
A wide array of multimedia processing tools in one free video software suite.
High speed
Our programs use fast and high-quality algorithms optimized for single and multi-core CPU's.
Affordability
VSDC video software is freely available for download to Windows OS-based PCs and laptops.

Last year unknown hackers gained access to the administrative side of the VSDC website and replaced the download links. Instead of the editing software, users received a JavaScript file, which then downloaded the AZORult Stealer, X-Key Keylogger and the DarkVNC backdoor. The VSDC team stated that they closed the vulnerability, but recently we received information about additional cases of infection through their website.

According to our researchers, the VSDC developer’s computer has been compromised several times since the previous incident. One such hack led to the website being compromised again between 2019-02-21 and 2019-03-23. This time hackers took a different approach to spreading the malware: they embedded a malicious JavaScript code inside the VSDC website. Its task was to determine the visitor’s geolocation and replace download links for users from the UK, USA, Canada and Australia. Native website links were substituted by links to another compromised website:

- https://thedoctorwithin[.]com/video_editor_x64.exe
- https://thedoctorwithin[.]com/video_editor_x32.exe
- https://thedoctorwithin[.]com/video_converter.exe

Users that downloaded software from that website also received a dangerous banking trojan, Win32.Bolik.2. Same as its predecessor, **Win32.Bolik.1**, this malware has qualities of a multicomponent polymorphic file virus. Trojans of this family are designed to perform web injections, traffic intercepts, key-logging and stealing information from different bank-client systems. At the moment we have information on at least 565 cases of infection with this trojan via videosoftdev.com site. It’s worth mentioning that so far only Dr.Web products successfully detect all the trojan’s components.

Additionally, on 22.03.2019 the attackers changed the Win32.Bolik.2 trojan to another malware, a variation of the Trojan.PWS.Stealer, KPOT Stealer. This trojan steals information from browsers, Microsoft accounts, several messengers and some other programs. In just one day it was downloaded by 83 users.

The VSDC developers were notified about the threat; and at the present moment, download links were restored to the originals. However, Doctor Web experts recommend that all VSDC users check their devices with our antivirus.

Indicators of compromise

#banker #banking_trojan #virus

What is the benefit of having an account?

Tell us what you think

To ask Doctor Web’s site administration about a news item, enter @admin at the beginning of your comment. If your question is for the author of one of the comments, put @ before their names.

Other comments