HandBrake for Mac Compromised with Proton Spyware

By Michael Mimoso

Published: 2017-05-08 · Archived: 2026-04-10 03:07:37 UTC

The open source HandBrake project is warning anyone who recently downloaded the Mac version of the software that they're likely infected with malware.

The handlers of the open source HandBrake video transcoder are warning anyone who recently downloaded the Mac version of the software that they're likely infected with malware.

HandBrake warned users on Saturday of a compromise of one of its mirror download servers, and said anyone who grabbed the software between May 2 and May 6 could have also downloaded a variant of the OSX.PROTON Trojan onto their Mac system.

"Anyone who has installed HandBrake for Mac needs to verify their system is not infected with a Trojan," said an advisory. "You have 50/50 chance if you've downloaded HandBrake during this period."

Apple, however, has since pushed out a XProtect signature preventing any new infections. HandBrake, meanwhile, advises its users to also change all passwords in their OSX KeyChain or passwords stored in their browsers.

HandBrake is free software that is used to convert video from a variety of formats to a supported codec. There are Windows, Mac and Linux versions. The warning was for the Mac version. The handlers advise verifying the SHA1 or SHA256 sum of the file before running it.

The bad SHA checksums are:

> SHA1: 0935a43ca90c6c419a49e4f8f1d75e68cd70b274
> SHA256: 013623e5e50449bbdf6943549d8224a122aa6c42bd3300a1bd2b743b01ae6793

"If you see a process called 'activity_agent' in the OSX Activity Monitor application, you are infected," the advisory said.

Proton is a remote access Trojan, or RAT, sold in Russian underground forums. Researchers at Sixgill published an analysis of the Mac malware, which is used to spy on the victim's activities; it can monitor keystrokes, upload files to remote machines, download files from the web, steal screenshots and connected directly via SSH or a remote admin tool such as VNC.

"The malware is shipped with genuine Apple code-signing signatures," the Sixgill report said. "This means the author of Proton RAT somehow got through the rigorous filtration process Apple places on MAC OS developers of third-party software, and obtained genuine certifications for his program."

The price, according to the researchers, is steep at around 100 Bitcoin ($163,600 today).

Patrick Wardle, a Mac security expert, said on the Objective-See blog on Saturday that the Proton variant has zero coverage on VirusTotal by antimalware engines. Wardle said that when the infected HandBrake app runs, it asks via a phony authentication popup for the user's credentials.

"If the user is tricked into providing a user name and password, the malware will install itself," Wardle said, adding that the credentials allow the malware to elevate privileges.

By compromising the HandBrake mirror, the attackers were able to follow the road map provided by the other Mac malware such as KeRanger, which infected the legitimate BitTorrent client Transmission, which was developed by the same author. The HandBrake team said it does not share infrastructure with Transmission.

"The HandBrake Team is independent of the Transmission Developers," HandBrake said in its advisory. "The projects share history in the sense that the same author created these apps but he is not part of the current HandBrake team of developers. We do not share our virtual machines with the Transmission project."

HandBrake also provided instructions for removing the Trojan from the Terminal application.

"The Download Mirror Server is going to be completely rebuilt from scratch so downloads may be a bit slower than usual while the primary picks up the load," HandBrake said. "During this time, old versions of HandBrake will not be available."
