HandBrake for Mac server compromise means downloaders have 50-50 chance of Proton RAT malware infection

By Mark Wycislik-Wilson | Published 2 years ago

Follow
2 Comments
Like 6
Share
Tweet

Anyone who downloaded the Mac video transcoder HandBrake in the last few days stands a 50 percent change of being infected with a Trojan. The download for version 1.0.7 of HandBrake was infected after the mirror download server was compromised.

The Trojan allows for an attacker to remotely access an infected computer, and a malware-laced version of the app was made available for download between May 2 and May 6. If you downloaded the app in this window, you're advised to check the SHA1/256 sum, and if you have gone as far as installing the software, there are steps to take to determine if you're infected and remove the malware if you are.

The HandBrake team stresses that it's only the download mirror that was affected; the primary download server was not compromised. It also says that anyone who used the built-in updater to jump to version 1.0.7 will have been protected by DSA signature verification. If you did download the software manually, however, you will need to check for signs of infection.

In a post on the HandBrake support forums, the team behind the app explain how to determine if your system is infected:

> If you see a process called "Activity_agent" in the OSX Activity Monitor application. You are infected.
>
> For reference, if you've installed a HandBrake.dmg with the following checksums, you will also be infected:
>
> SHA1: 0935a43ca90c6c419a49e4f8f1d75e68cd70b274
>
> SHA256: 013623e5e50449bbdf6943549d8224a122aa6c42bd3300a1bd2b743b01ae6793
>
> The Trojan in question is a new variant of OSX.PROTON

Thankfully it is fairly simple to remove the malware if you are infected:

> Open up the "Terminal" application and run the following commands:
>
> - launchctl unload ~/Library/LaunchAgents/fr.handbrake.activity_agent.plist
> - rm -rf ~/Library/RenderFiles/activity_agent.app

Got News? Contact Us

Recent Headlines

Now you can use Siri to launch Google Assistant on your iPhone

Surface Pro 6 beats iPad Pro in bend test

Ubiquiti Networks launches AmpliFi HD Gamer's Edition mesh Wi-Fi system with NVIDIA GeForce NOW QoS

Keep your software up-to-date and one eye on the latest downloads with Update Scanner

BullGuard and NordVPN partner to boost consumer privacy

Stop focusing your information security efforts on the wrong things!

Looking for an open source password manager? Give Bitwarden a spin

Most Commented Stories

deepin 15.8 Linux distribution available for download -- replace Windows 10 now!
93 Comments

Microsoft admits Cortana is an epic failure by shamelessly selling Amazon Echo Dot
78 Comments

Google Store sent me kicking and screaming back to Apple
72 Comments

The re-released Windows 10 1809 is still buggy -- and some fixes won't arrive until next year
63 Comments

Microsoft could be about to hit users of Windows 10's Mail app with ads -- unless they pay up
58 Comments

> - if ~/Library/VideoFrameworks/ contains proton.zip, remove the folder
>
> Then Remove any "HandBrake.app" installs you may have.

Image credit: Ikeskinen / Shutterstock

Wyçislik-Wilson, M. (2017). ‘HandBrake for Mac server compromise means downloaders have 50-50 chance of Proton RAT malware infection’. BetaNews [Online], (

© 1998-2018 BetaNews, Inc. All Rights Reserved. Privacy Policy - Cookie Policy.