forum.handbrake.fr

Mirror Download Server Compromised - HandBrake

SECURITY WARNING

Anyone who has downloaded HandBrake on Mac between [02/May/2017 14:30 UTC] and [06/May/2017 11:00 UTC] needs to verify the SHA1 / 256 sum of the file before running it.

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

Detection

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

Removal

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

Further Actions Required

Based on the information we have, you must also change all the passwords that may reside in your OSX KeyChain or any browser password stores.

Apple

We have been informed that the process to update the definitions for OSX's XProtect feature started this morning, so this should start rolling out to machines automatically soon if not already.

Summary

- HandBrake–1.0.7.dmg was replaced by another unknown malicious file that DOES NOT match the SHA1 / SHA256 hashes on our website or on our Github Wiki which mirrors these: https://github.com/HandBrake/HandBrake/wiki/Checksums
- The Affected Download mirror (download.handbrake.fr) has been shutdown for investigation.
- The Primary Download Mirror and website were unaffected.
- Downloads via the applications built-in updater with 1.0 and later are unaffected. These are verified by a DSA Signature and will not install if they don't pass.
- Downloads via the applications built-in updater with 0.10.5 and earlier did not have verification so you should check your system with these older releases

When relevant information becomes available we will update this post.

Notices

- 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. During this time, old versions of HandBrake will not be available.

Mirror Download Server Compromised. (2017). forum.handbrake.fr [Online] 6 May, 2017. https://forum.handbrake.fr/viewtopic.php?f=33&t=36364 (Accessed 21 June, 2018). Used with permission of Handbrake.