Windows App Runs on Mac, Downloads Infostealer, Adware

By Don Ovid Ladores, Luis Magisa (words)

Published: 2019-02-11 · Archived: 2026-04-05 22:43:14 UTC

Update as of 6:00 P.M. PST, May 3, 2019: Our continued observation of the malware sample showed that it spoofs popular Mac apps, instead of being included in the app installers themselves as previously reported. We made the corrections in the technical analysis in this post. We would also like to thank Objective Development for clarifying this issue.

Update as of 5:00 P.M. PST, February 18, 2019: Further analysis on the sample indicated that it does not bypass the Gatekeeper mechanism as previously reported. We made the necessary changes in the technical analysis in this post. We would also like to thank Apple Product Security team for reaching out to us to clarify this issue.

EXE is the official executable file format used for Windows to signify that they only run on Windows platforms, and to serve as a security feature. By default, attempting to run an EXE file on a Mac or Linux OS will only show an error notification.

However, we found EXE files in the wild delivering malicious payload on macOS recently. While no specific attack pattern is seen, our telemetry showed the highest numbers for infections to be in the United Kingdom, Australia, Armenia, Luxembourg, South Africa, and the United States.

Behavior

The samples pose as installers of popular apps and are often available for download from various torrent websites. Examples of the applications they pose as are as follows:

- Paragon_NTFS_for_Mac_OS_Sierra_Fully_Activated.zip
- Wondershare_Filmora_924_Patched_Mac_OSX_X.zip
- LennarDigital_Sylenth1_VSTi_AU_v3_203_MAC_OSX.zip
- Sylenth1_v331_Purple_Skin__Sound_Radix_32Lives_v109.zip
- TORRENTINSTANT.COM+-+Traktor_Pro_2_for_MAC_v321.zip
- Little_Snitch_583_MAC_OS_X.zip

When the downloaded .ZIP file is extracted, it contains a .DMG file hosting the supposed installer of the spoofed app.

Figure 1. Sample of the malicious file

Figure 2. Installer contained in the .DMG sample we analyzed posing as a legitimate application

Inspecting the installer contents, we found the unusual presence of the .EXE file bundled inside the app, verified to be a Windows executable responsible for the malicious payload.

Figure 3. Suspicious .EXE bundled for Mac app installer

When the installer is executed, the main file also launched the executable as it is enabled by the mono framework included in the bundle. This framework allows the execution of Microsoft .NET applications across platforms such as OSX.

Once run, the malware collects the following system information:

- ModelName
- ModelIdentifier
- ProcessorSpeed
- ProcessorDetails

- NumberofProcessors
- NumberofCores
- Memory
- BootROMVersion
- SMCVersion
- SerialNumber
- UUID

Under the */Application* directory, the malware also scans for all the basic and installed apps and sends all the information to the C&C server:

- App Store.app
- Automator.app
- Calculator.app
- Calendar.app
- Chess.app
- Contacts.app
- DVD Player.app
- Dashboard.app
- FaceTime.app
- Font Book.app
- Image Capture.app
- iTunes.app
- Launchpad.app
- Mail.app
- Maps.app
- Messages.app
- Mission Control.app
- Notes.app
- Photo Booth.app
- Photos.app
- Preview.app
- QuickTime Player.app
- Reminders.app
- Safari.app
- Siri.app
- Stickies.app
- System Preferences.app
- TextEdit.app
- Time Machine.app
- UtilitiesiBooks.app

It downloads the following files from the Internet and saves it to the directory *~/Library/X2441139MAC/Temp/*:

- hxxp://install.osxappdownload.com/download/mcwnet
- hxxp://reiteration-a.akamaihd.net/INSREZBHAZUIKGLAASDZFAHUYDWNBYTRWMFSOGZQNJYCAP/FlashPlayer.dmg
- hxxp://cdn.macapproduct.com/installer/macsearch.dmg

Figure 4. Downloaded files saved in the directory

These .DMG files are mounted and executed as soon as they are ready, as well as displaying a PUA during execution.

Figure 5. One of the adwares downloaded posing as a popular app

This malware runs specifically to target Mac users. Attempting to run the sample in Windows displays an error notification.

Figure 6. Error notification when installer is executed in Windows

Currently, running EXE on other platforms would have no impact on non-Windows systems such as MacOS. A mono framework installed in the system is required to compile or load these executables and libraries. In this case, however, the bundling of the said framework with the malicious files becomes a workaround to enable EXE files to run on Mac systems. As for the native library differences between Windows and MacOS, the mono framework supports DLL mapping to support Windows-only dependencies to their MacOS counterparts. Overall, this technique may be done to overcome a malicious user's Objective-c coding limitations.

Conclusion

We suspect that this specific malware can be used for future inter-platform attacks, where a single executable can perform its payload on different operating systems. We believe that the cybercriminals are still studying the development and opportunities from this malware bundled in apps and available in torrent sites. We will continue investigating how cybercriminals can use this information and routine. Users should avoid or refrain from downloading files, programs, and software from unverified sources and websites, and install a multi-layered protection for their individual and enterprise systems.

Trend Micro Solutions

The following Trend Micro products detect and block this threat:

Trend Micro Antivirus for Macproducts
Trend Micro Smart Protection Suitesproducts

Indicators of Compromise

Main Executables		
File	**SHA256**	**Detection**
setup.dmg	c87d858c476f8fa9ac5b5f68c48dff8efe3cee4d24ab11aebeec7066b55cbc53	TrojanSpy.MacOS.
Installer.exe	932d6adbc6a2d8aa5ead5f7206511789276e24c37100283926bd2ce61e840045	TrojanSpy.Win32.V
OSX64_MACSEARCH.MSGL517	58cba382d3e923e450321704eb9b09f4a6be008189a30c37eca8ed42f2fa77af	Adware.MacOS.M
chs2	3cbb3e61bf74726ec4c0d2b972dd063ff126b86d930f90f48f1308736cf4db3e	Adware.MacOS.GI
Installer (2)	e13c9ab5060061ad2e693f34279c1b1390e6977a404041178025373a7c7ed08a	Adware.MacOS.GI
macsearch	b31bf0da3ad7cbd92ec3e7cfe6501bea2508c3915827a70b27e9b47ffa89c52e	Adware.MacOS.M
C&C server		
hxxp://54.164.144.252:10000/loadPE/getOffers.php		