

Stealthy Mac Malware Delivered via Pirated Apps

Legitimate Mac software applications are being trojanized with malware and uploaded to Pirate Bay. From here, software pirates are downloading the apps and unknowingly infecting themselves. One example involves a stealthy implementation of XMRig cryptojacking malware; but the process could be used for other malware.

XMRig on Macs is not new. Trend Micro analyzed a sample in February 2022: “We suspected that the Mach-0 sample arrived packaged in a DMG (an Apple image format used to compress installers) for Adobe Photoshop CC 2019 v20.0.6. However, the parent file was not successfully sourced.”

More recently, Apple security firm Jamf detected something similar: an XMRig implementation executing under the guise of the Apple-developed video editing software Final Cut Pro. In both cases, i2p (Invisible Internet Project) was used for outbound communication. This raised numerous questions: if the infections were connected a year apart, are they part of something larger, and why have other infections not been detected?

In looking for the source of the malware, Jamf researchers turned to a Pirate Bay mirror to seek torrents of Final Cut Pro. They found one with a matching hash to the trojanized version they discovered in the wild. But they found more – a series of Apple Mac applications including Final Cut Pro, Logic Pro, and Photoshop, all uploaded to Pirate Bay by wtfisthat34698409672. This includes various versions of Final Cut Pro, allowing the researchers to analyze the malware development over time.

The researchers discovered three generations of the malware. The first generation, starting from August 2019, is a fairly standard implementation of malware. “The malware is still coming out of the pirated application, but it gets installed and it runs – it doesn’t worry about remaining stealthy,” Jamf’s macOS detections expert Jaron Bradley told *SecurityWeek*. It was new, it wasn’t being detected yet, and the author was more concerned about his or her own anonymity – hence the use of Pirate Bay for incoming and i2p for outgoing.

The second generation, starting from April 2021 and still undetected via VirusTotal as of February 13, 2023, was different. There were some additional hidden files, but no attempt at persistence. Instead, the malware opens with the

application, and stops operating when the app is closed – the probability is a desire for greater stealth. A giveaway for the presence of cryptomining is unexpected device overheating – and for this to occur with no ‘legitimate’ apps running would be very suspicious.

The third generation attempts greater stealth. There are no hidden executables, just one large binary with components base64 encoded and compressed with LZMA. New versions of the trojanized Mac apps began appearing on Pirate Bay within 24 hours of Apple’s application update releases. The malicious processes are disguised as legitimate processes.

An example of the malware’s stealth activity can be seen in a short script that monitors the activity of Activity Monitor. “The script runs a continuous loop that checks the list of running processes every 3 seconds, looking for the Activity Monitor,” say the researchers. “If it finds the Activity Monitor, it immediately terminates all of its malicious processes... until the next time the victim launches the application.” So, a user’s suspicions will not be confirmed.

But it’s worth noting that the whole process of delivering malware via major pirated applications is a stealth maneuver – pirates tend to keep their practices under wraps and not do things that might bring awareness to their unethical behavior. This, coupled with the techniques within the malware explain why this particular distribution has been largely undetected since at least 2019.

Apple is aware of this type of problem and has repeatedly improved its operating system to prevent the use of pirated software. This has developed into the traditional leapfrog race between developers and criminals – and it is not always clear who has the upper hand. For example, the latest Mac Ventura release appears to be partially successful in blocking these pirate apps.

But, say the researchers, “At the time of writing, the pirated Photoshop uploaded by wtfisthat34698409672 still successfully launches both the malicious and working components on the latest version of macOS Ventura 13.2 and earlier. This seems to be due to a minor difference in how the executable in the working copy of Photoshop is called compared to how the Final Cut and Logic Pro executables are launched. These could likely be restored to working order with minor adjustments from the malware author.”

This is not a malware ‘campaign’ in the traditional sense – it is a methodology for malware delivery that has been successful for many years. This example used the cryptojacking XMRig, but it could easily be used to deliver other malware. This example focused on the use of Pirate Bay – but there are other sources for pirated software that may have been similarly trojanized.

Related: Microsoft Details Recent macOS Gatekeeper Bypass Vulnerability

Related: Apple Updates Advisories as Security Firm Discloses New Class of Vulnerabilities

Related: Apple Patches Over 100 Vulnerabilities With Release of macOS Ventura 13

Related: Jamf to Acquire Wandera for \$400 Million to Bring Zero Trust to Apple Ecosystem

<https://www.securityweek.com/stealthy-mac-malware-delivered-via-pirated-apps/>