“Perverse” malware infecting hundreds of Macs remained undetected for years

ars arstechnica.com/security/2017/07/perverse-malware-infecting-hundreds-of-macs-remained-undetected-for-years/

Dan Goodin

Enlarge

Tim Malabuyo

A mysterious piece of malware that gives attackers surreptitious control over webcams, keyboards, and other sensitive resources has been infecting Macs for at least five years. The infections—known to number nearly 400 and possibly much higher—remained undetected until recently and may have been active for almost a decade.

Further Reading

Newly discovered Mac malware found in the wild also works well on Linux

Patrick Wardle, a researcher with security firm Synack, said the malware is a variant of a malicious program that came to light in January after circulating for at least two years. Dubbed Fruitfly by some, both malware samples capture screenshots, keystrokes, webcam

images, and information about each infected Mac. Both generations of Fruitfly also collect information about devices connected to the same network. After researchers from security firm Malwarebytes discovered the earlier Fruitfly variant infecting four Macs, Apple updated macOS to automatically detect the malware.
The variant found by Wardle, by contrast, has infected a much larger number of Macs while remaining undetected by both macOS and commercial antivirus products. After analyzing the new variant, Wardle was able to decrypt several backup domains that were hardcoded into the malware. To his surprise, the domains remained available. Within two days of registering one of the addresses, close to 400 infected Macs connected to the server, mostly from homes located in the United States. Although Wardle did nothing more than observe the IP address and user names of Macs that connected to his server, he had the ability to use the malware to spy on the users who were unwittingly infected.

"This shows that there are people who are sick in the head who are attacking everyday Mac users for insidious goals," Wardle told Ars. Although the method of infection remains unknown, Wardle suspects it involves tricking users into clicking on malicious links, as opposed to exploiting vulnerabilities in apps or in macOS. "A lot of Mac users are overconfident in the security of their Mac. [The discovery] just goes to reiterate to everyday users that there are perhaps people out there trying to hack their computers."

Why?

Besides the means of infection being unknown, the exact purpose of the malware is also unclear. Wardle said he found no evidence the malware can be used to install ransomware or collect banking credentials. That largely removes the possibility that Fruitfly developers were motivated by financial profit. At the same time, the concentration of home users largely rules out chances the malware was designed by state-sponsored hackers to spy on targets.

"I don't know if it's just some bored person or someone with perverse goals," Wardle said. "If some bored teenager is spying on me, that would still be very emotionally traumatic. If it's turning on the webcam, that's for perverse reasons."

Wardle said the primary command-and-control server used by the malware had been shut down earlier but that many of the affected Macs had never been disinfected. As a result, the infected Macs reported to the backup server as soon as it became available. The researcher speculated that Fruitfly was therefore abandoned by its creators. As demonstrated by the backup servers, the Macs remained susceptible to spying by anyone who took the time to register one of the hardcoded domains.

Wardle has since reported all of his findings to law enforcement officials. He said all domains known to be associated with the malware are no longer available, a move that essentially neutralizes the threat. Apple representatives didn't respond to an e-mail seeking comment for this post.

While the backup server Wardle set up allowed him to discover the Macs that remained infected by the Fruitfly variant, it also allowed him to quickly analyze how the malware worked. Typically, researchers must undertake a painstaking process known as reverse engineering to document the inner workings. By infecting a lab computer and watching how it interacted with the backup server, the researcher was able to more easily understand how various commands worked. Wardle will speak about the process on Wednesday at the Black Hat Security Conference in Las Vegas, in a briefing titled Offensive Malware Analysis: Dissecting OSX/Fruitfly via a custom C&C Server.

One of the interesting aspects of the latest Fruitfly variant is that it flew under the radar for so long. The malware relies on functions that were retired long ago and uses a crude method to remain installed once a Mac is infected. Compared to newer, more sophisticated malware, Fruitfly is much easier to detect. And yet, for whatever reason, no one caught it until recently. Two pieces of Mac software developed by Wardle would have given victims a strong indication they were infected. One, called BlockBlock, would have warned of the suspicious launch agent used by the malware. A second tool, called Oversight, provides notification anytime an app attempts to access a Mac's webcam or microphone. A recent submission to the VirusTotal malware detection service shows that 19 of the top 56 AV- and endpoint-protection products now detect the malware.