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

arstechnica.com/security/2017/01/newly-discovered-mac-malware-may-have-circulated-in-the-wild-for-2-years/

Dan Goodin

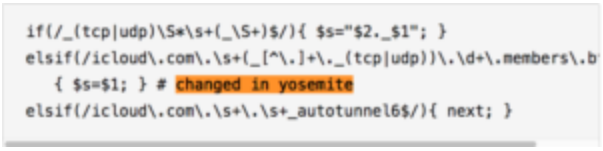
A newly discovered family of Mac malware has been conducting detailed surveillance on targeted networks, possibly for more than two years, a researcher reported Wednesday.

The malware, which a recent Mac OS update released by Apple is detecting as Fruitfly, contains code that captures screenshots and webcam images, collects information about each device connected to the same network as the infected Mac, and can then connect to those devices, according to a blog post published by anti-malware provider Malwarebytes. It was discovered only this month, despite being painfully easy to detect and despite indications that it may have been circulating since the release of the Yosemite release of OS X in October 2014. It's still unclear how machines get infected.

"The first Mac malware of 2017 was brought to my attention by an IT admin, who spotted some strange outgoing network traffic from a particular Mac," Thomas Reed, director of Mac offerings at Malwarebytes, wrote in the post. "This led to the discovery of a piece of malware unlike anything I've seen before, which appears to have actually been in existence, undetected for some time, and which seems to be targeting biomedical research centers."

Ancient artifacts

The malware contains coding functions that were in vogue prior to the first release of OS X in 2001. Open source code known as libjpeg, which the malware uses to open or create JPG-formatted image files, was last updated in 1998. It's possible Fruitfly wasn't developed until much later and simply incorporated those antiquated components. Still other evidence—including a comment in the code referring to a change made in Yosemite and a launch agent file with a creation date of January 2015—suggests the malware has been in the wild for at least two years.



Enlarge

"The only reason I can think of that this malware hasn't been spotted before now is that it is being used in very tightly targeted attacks, limiting its exposure," Reed wrote. "There have been a number of stories over the past few years about Chinese and Russian hackers targeting and stealing US and European scientific research. Although there is no evidence at this point linking this malware to a specific group, the fact that it's been seen specifically at biomedical research institutions certainly seems like it could be the result of exactly that kind of espionage."

Another intriguing finding: with the exception of Mac-formatted Mach object file binary, the entire Fruitfly malware library runs just fine on Linux computers. Reed said Malwarebytes has yet to spot a Linux variant, but he said he wouldn't be surprised if one existed. He said he has also come across Windows-based malware that connected to the same control server used by the Mac malware.

Despite its functionality, Fruitfly remains unsophisticated compared to some malware. Its control servers are simply the IP address 99.153.29.240 and the dynamic DNS address eidk.hopto.org. Its method for keeping Macs infected even after they're rebooted—a hidden file and a launch agent—is also outdated because it's so easy to detect and remove. People who work with Macs inside research labs should consider checking their machines for infections. Besides the update automatically pushed by Apple, Malwarebytes also detects the infection, although it's known as OSX.Backdoor.Quimitchip.