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

By Dan Goodin

Published: 2017-01-18 · Archived: 2026-04-05 13:09:19 UTC

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.
