Apple users are careful with the kind of malware that is virtually undetectable on a Mac

If you think you are using a Mac and are completely immune to malware, you are wrong. Yes, even Mac users can stick to viruses and silently monitor users.

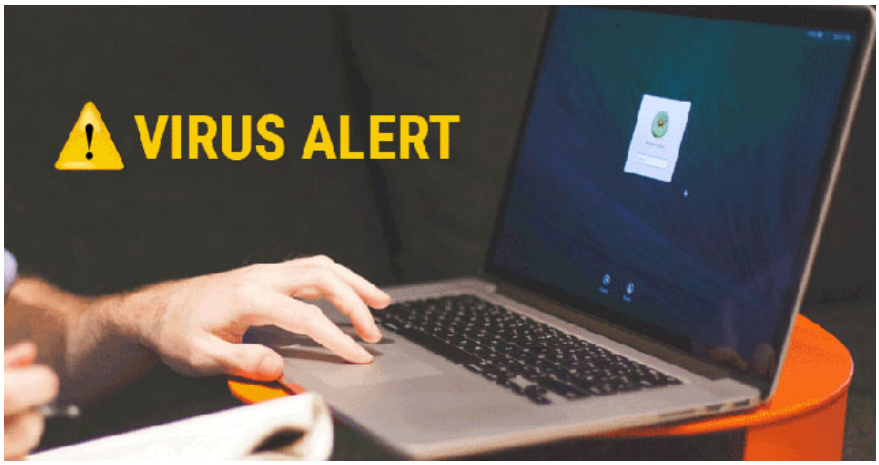
A few malware that can take control of webcams, monitors, mice, keyboards, and install malicious software has invaded hundreds of Macs for more than 5 years, and has just been discovered a few months ago. .

Named FruitFly, malware on this Mac was discovered earlier this year by Malwarebytes Thomas Reed researcher and Apple quickly released a security patch to resolve this dangerous malware. A few months later, Patrick Wardle, who was an NSA hacker and now the team leader at Synack network security company, discovered about 400 Macs infected with another variant of FruitFly malware (FruitFly 2).

Wardle thinks that the number of Macs infected with FruitFly may be higher because he can only access some servers used to control FruitFly. Although it is still unclear who is behind the FruitFly and how it gets into the Mac, researchers think the malware has been around for 10 years because some of its code dates back to 1998.

'FruitFly, the first malware on OS X / macOS of 2017, is very curious. Selected to target biomedical research centers, it is said to have worked without anyone knowing it for years. ' Wardle wrote in the opening of his talk.

Because FruitFly's infiltration is still unclear, like many other malware, FruitFly can be infected via malicious websites or fake emails or trapping applications.



Many Macs infected FruitFly malware

ruitFly is a spy malware that can execute shell command, move and click, capture webcam image, stop computer processes (kill process), get system runtime, get back screenshot pictures and even alert hackers when the victim works again on a Mac.

> 'The only reason I can think of why this malware has not been discovered is because it is used in attacks with very strict object selections, limited levels of infection,' Reed writes in a monthly blog. One. 'Although there is no evidence to connect this malware to any group, but since it is used at biomedical research, it is probably a result of some spying activity.'

Wardle can find FruitFly victims after registering the control server via Command and Control Center (C&C) which is used by the attacker. Then he saw about 400 Mac users infected with FruitFly since connecting to that server.

Since then, the researcher can see the IP address of the FruitFly infected victim, of which 90% of victims in the US. Wardle can even see the victim's name, it's easy to know exactly who is infected with malware.

Instead of taking control of the computer or spy on the victim's machine, Wardle contacted the police and transferred what he found. Wardle said surveillance is the main purpose of FruitFly, though it is unclear whether it is a government or a hacker group.

> 'It doesn't look like the behavior of cybercrime, there's no advertising, keyboard manipulation or ransomware,' Wardle said. 'What it does makes it more like interactive support, it can alert an attacker when the user is active on the machine, fake a mouse click or a keyboard'.

Because FruitFly's code also includes the Linux command shell, malware can work on the Linux operating system. So it will not be surprising if the Linux variant of FruitFly appears.