APPLE USERS, Beware the Fruitfly

BY MICHAEL REMER, PRESIDENT, COMPUTERCARE LLC

Apple has a pretty good reputation for avoiding the viruses and malware that have plagued Windows for years. While not completely invulnerable, the Apple OS is relatively unscathed when it comes to hackers seeking exploits in your computer's operating system.

This can be attributed to a number of things. For example: OS X is built on the Unix kernel, which is both stable and secure. There are more Windows users than Mac users – so it's easier for Windows-based malware to spread, and most of the tools used to create malware and viruses are actually created to be run in Windows. Even with this track-record and built in protections, the latest exploit was recently discovered in Apple's OS X.

The latest malware in OS X, named "Fruitfly" has actually been found to come from code that has been a part of the operating system for years. In fact, some code was found in the exploit that referenced a library that has not been used since 1998!

While there is evidence that points to this operating system vulnerability lying dormant for years, it is uncertain exactly how long it has been there, who created it or what its intended targets were. What we know about it so far is that most instances of attack have been at biomedical research institutions.

It was discovered that the malware was created to grab screenshots (taking a picture of what is on your screen) and take control of your webcam. Apple has released a patch for this malware and some antivirus programs will detect it as a back-door type Trojan.

So how was this exploit caught? Network administrators at the biomedical facility noticed abnormal outbound network traffic – that is they saw things leaving their network that were not authorized to do so. Until the patch is tested and installed, those same administrators will have to block traffic coming from those workstations, or disconnect them from the outside world entirely to prevent data from going out.

So what can you do? Well it's clearly a misconception that Apple devices do not require as much care and attention as Windows devices, and that extends to security as well as routine maintenance. It's imperative that all systems have business-grade malware and virus protection that is kept up-to-date. It's also important that you consider utilizing an intelligent network router and firewall that can provide you with detailed reports about network traffic, both inbound and outbound, and provide you with the ability to limit or block traffic to and/or from specific places both inside and outside your network.

Your technology partner can work with you to determine the best way to protect, update and monitor your devices, as well as create a backup and disaster recovery plan to address any future exploits and implement the appropriate hardware to protect your network, be that Apple, Microsoft or any other device type. B

» **MICHAEL REMER** is founder and president of ComputerCare LLC, an IT services company providing a full spectrum of IT solutions and services to small and medium businesses.