New malware can infect iPhones via Mac computers (Update)

November 6 2014

A person in Singapore uses an iPhone to order a taxi

A newly discovered family of malware has the capacity to infect iPhones via Apple computers, posing a security threat to devices that have been largely resistant to cybercriminals, researchers said.

The researchers at Palo Alto Networks, a cybersecurity firm, said the malware shows "characteristics unseen in any previously documented

threats targeting Apple platforms."

It represents "a potential threat to businesses, governments and Apple customers worldwide," they said.

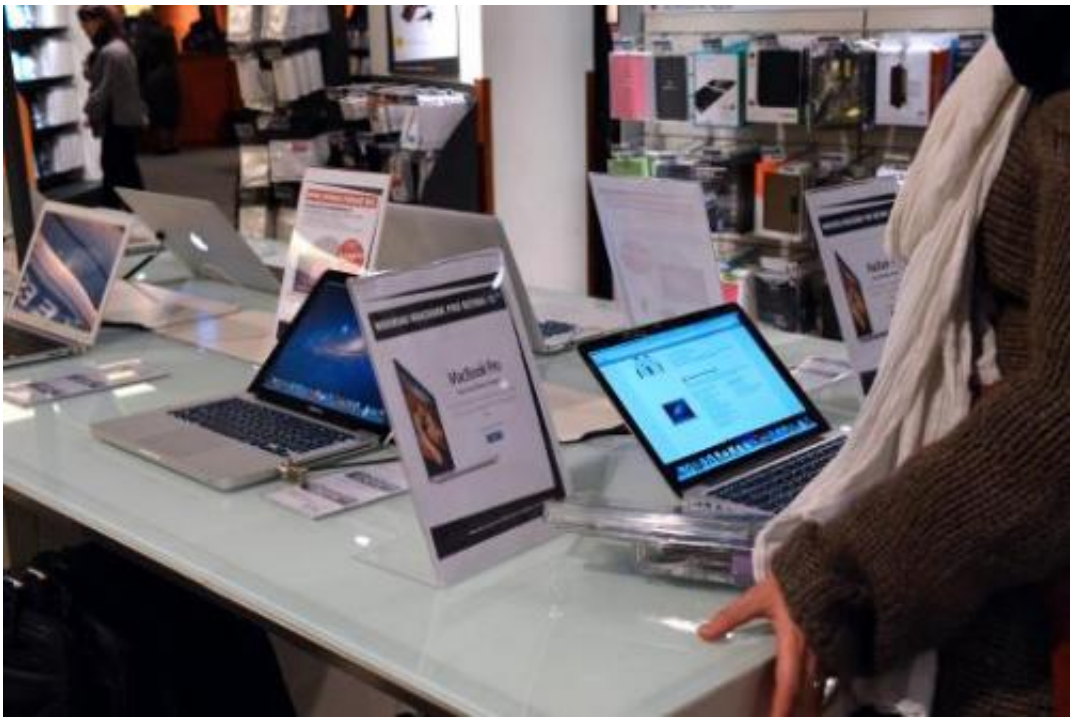
The malware, dubbed WireLurker, "is capable of stealing a variety of information from the mobile devices it infects and regularly requests updates from the attackers command and control server," according to a report by the security firm, which added that "its creator's ultimate goal is not yet clear."

Apple said it had taken steps to block the malicious software.

Although hackers have been able to target "jailbroken" iPhones, which have been modified to accept unauthorized software, this new threat appears to pose a threat to devices that have not been modified, the security researchers said.

"WireLurker is unlike anything we've ever seen in terms of Apple iOS and OS X malware," said Palo Alto's Ryan Olson.

"The techniques in use suggest that bad actors are getting more sophisticated when it comes to exploiting some of the world's best-known desktop and mobile platforms."



A Mac Book Pro computer on display at a FNAC store on November 27, 2012 in Paris

According to the researchers, WireLurker malware first infects a Mac computer, which uses the OS X operating system, and then installs itself on iOS devices—iPads or iPhones—when they are connected to the computers via USB ports.

The malware was traced back to a third-party Chinese app store, which had 467 infected applications downloaded over 356,104 times, potentially affecting hundreds of thousands of users.

"WireLurker monitors any iOS device connected via USB with an infected OS X computer and installs downloaded third-party applications or automatically generated malicious applications onto the device, regardless of whether it is jailbroken," a report by the security firm said.

"This is the reason we call it 'wire lurker.' Researchers have demonstrated similar methods to attack non-jailbroken devices before; however, this malware combines a number of techniques to successfully realize a new breed of threat to all iOS devices."

Apple, in a statement to AFP, said it had acted to block the malware.

"We are aware of malicious software available from a download site aimed at users in China, and we've blocked the identified apps to prevent them from launching," the company said.

"As always, we recommend that users download and install software from trusted sources."

Another security researcher, Jonathan Zdziarski, said the new malware suggests a potentially large security issue for Apple devices.

"The bigger issue here is not WireLurker itself," Zdziarski said in a blog post.

"The real issue is that the design of iOS' pairing mechanism allows for more sophisticated variants of this approach to easily be weaponized," he said.

"While WireLurker appears fairly amateur, an NSA or a GCHQ, or any other sophisticated attacker could easily incorporate a much more effective (and dangerous) attack like this."