Exclusive: Apple, Macs hit by hackers who targeted Facebook

reuters.com/article/us-apple-hackers/exclusive-apple-macs-hit-by-hackers-who-targeted-facebook-idUSBRE91I10920130219

Jim Finkle, Joseph Menn

Technology News
Updated

By Jim Finkle, Joseph Menn

6 Min Read

BOSTON/SAN FRANCISCO (Reuters) - Apple Inc was recently attacked by hackers who infected Macintosh computers of some employees, the company said Tuesday in an unprecedented disclosure describing the widest known cyber attacks targeting Apple computers used by corporations.

The Apple logo hangs in a glass enclosure above the 5th Ave Apple Store in New York, September 20, 2012. REUTERS/Lucas Jackson

Unknown hackers infected the computers of some Apple workers when they visited a website for software developers that had been infected with malicious software. The malware had been designed to attack Mac computers.

The same software, which infected Macs by exploiting a flaw in a version of Oracle Corp's Java software used as a plug-in on Web browsers, was used to launch attacks against Facebook, which the social network disclosed on Friday.

The malware was also employed in attacks against Mac computers used by "other companies," Apple said, without elaborating on the scale of the assault.

Twitter, which disclosed that it had been breached February 1 and that hackers might gave accessed some information on about 250,000 users, was hit in the same campaign, according to a person close to the investigation.

Another person briefed on the case said that hundreds of companies, including defense contractors, had been infected with the same malicious software. Though this person said that the malware could have originated from China, there was no proof.

"This is a new campaign. It's not like the other ones you read about where everyone can tell it's China," the first person said.

Investigations into the breaches are ongoing. It was not immediately clear when the attacks had begun, the extent to which the hackers had succeeded in stealing data from targeted systems, or whether all infected machines have been identified.

The malware was distributed at least in part through a site aimed at iPhone developers, which might still be infecting visitors who haven't disabled Java in their browser, the person close to the case said. There is a version that infects computers running Microsoft Windows as well.

Related Coverage

Security firm F-Secure wrote that the attackers might have been trying to get access to the code for apps on smartphones, seeking a way to infect millions of end-users. It urged developers to check their source code for unintended changes.

Apple disclosed the breach as tensions are heating up over U.S. allegations that the Chinese military engages in cyber espionage on U.S. companies.

U.S. cyber security firm Mandiant reported over the weekend that it has uncovered evidence that the Chinese military is behind a slew of cyber attacks on U.S. businesses. The White House said it has repeatedly raised concerns about Chinese cyber theft with Beijing.

The breaches described by Apple mark the highest-profile cyber attacks to date on businesses running Mac computers. Hackers have traditionally focused on attacking machines running the Windows operating system, though they have gradually turned their attention to Apple products over the past couple of years as the company gained market share over Microsoft Corp.

"This is the first really big attack on Macs," said the source, who declined to be identified because the person was not authorized to discuss the matter publicly. "Apple has more on its hands than the attack on itself."

Charlie Miller, a prominent expert on Apple security who is co-author of the Mac Hacker's Handbook, said the attacks show that criminal hackers are investing more time studying the Mac OS X operating system so they can attack Apple computers.

For example, he noted, hackers recently figured out a fairly sophisticated way to attack Macs by exploiting a flaw in Adobe Systems Inc's Flash software.

"The only thing that was making it safe before is that nobody bothered to attack it. That goes away if somebody bothers to attack it," Miller said.

NATIONAL SECURITY

Cyber security attacks have been on the rise. In last week's State of the Union address, U.S. President Barack Obama issued an executive order seeking better protection of the country's critical infrastructure from cyber attacks.

White House spokesman Jay Carney told reporters on Tuesday that the Obama administration has repeatedly taken up its concerns about Chinese cyber theft with Beijing, including the country's military. There was no indication as to whether the group described by Mandiant was involved in the attacks described by Apple and Facebook.

An Apple spokesman declined to specify how many companies had been breached in the campaign targeting Macs, saying he could not elaborate further on the statement it provided.

"Apple has identified malware which infected a limited number of Mac systems through a vulnerability in the Java plug-in for browsers. The malware was employed in an attack against Apple and other companies, and was spread through a website for software developers," the statement said.

"We identified a small number of systems within Apple that were infected and isolated them from our network. There is no evidence that any data left Apple," it continued.

The statement said Apple was working closely with law enforcement to find the culprits, but the spokesman would not elaborate. The Federal Bureau of Investigation declined to comment.

Apple said it plans to release a piece of software on Tuesday that customers can use to identify and repair Macs infected with the malware used in the attacks.

Editing by Andre Grenon, Edwin Chan and Richard Chang

Our Standards: The Thomson Reuters Trust Principles.

for-phone-onlyfor-tablet-portrait-upfor-tablet-landscape-upfor-desktop-upfor-wide-desktop-up