Ransomware asks Apple Mac victims to pay up

March 8 2016, by Nancy Owano

Hackers got malicious code named 'KeRanger' into Mac machines by infecting the open-source program Transmission used to transfer files at a file-sharing network

Ransomware on the OS X platform was discovered affecting Apple Mac users. Claire Reilly, CNET news writer based in Sydney, said on Sunday that it was spread through "torrenting" software. Researchers at Palo

Alto Networks made the discovery on Friday.

Researchers found a popular BitTorrent client for Apple's OS X software for Macs infected with the ransomware. That software in question is Transmission. What is Transmission? Reilly said Mac users can install it on Apple's OS X and use it to access shared files in torrent swarms.

The Palo Alto Networks team called the ransomware KeRanger. What happens if the user becomes victim? Designed to infect a computer, the ransomware can "put the owner in a bind, locking up files or functionality and essentially bricking the device until the user pays to have the problem neutralized. This particular piece of ransomware brings with it a $400 ransom note," said Reilly.

A user was at risk if having installed one of the infected versions of Transmission. Though an executable file embedded in the software would run on the system, the user would not see any sign of a problem. After three days, KeRanger would connect with servers over Tor and begin encrypting certain files on the Mac's system, said CNET.

(Palo Alto Threat Intelligence Director Ryan Olson said in a Reuters report that the victims whose machines were compromised but not cleaned up could start losing access to data on Monday, which is three days after the virus was loaded onto Transmission's site.)

KeRanger asked victims to pay one bitcoin (about $400) to a specific address to retrieve their files," said CNET.

Jim Finkle in Reuters said on Monday said that ransomware was one of the fastest-growing types of cyber threats, encrypting data and then typically asking for ransoms "in hard-to-trace digital currencies to get an electronic key so they can retrieve their data."

The Palo Alto Networks team notified both Apple and the Transmission Project on March 4. CNET's Reilly said Apple responded: Apple revoked the security certificate exploited by KeRanger and updated its XProtect antivirus software.

Who is at risk? "If you directly downloaded the Transmission installer from the official website on March 4-5, 2016, you may have been infected by KeRanger. Even if you downloaded it elsewhere or at another time, Palo Alto Network's security experts advise taking extra precautions," said Reilly.

Transmission responded to news of the ransomware. It has removed the affected versions of the BitTorrent installer from its website, said CNET. (According to *Ars Technica*, "Olson also said that the rogue version was only live on the Transmission website for 36 to 48 hours.")

Transmission is self-described as "a fast, easy and free BitTorrent client ."

A notice on Transmission's site: "Read Immediately!!!! Everyone running 2.90 on OS X should immediately upgrade to and run 2.92, as they may have downloaded a malware-infected file. This new version will make sure that the "OSX.KeRanger.A" ransomware … is correctly removed from your computer. Users of 2.91 should also immediately upgrade to and run 2.92. Even though 2.91 was never infected, it did not automatically remove the malware-infected file."

Interestingly, a number of readers' comments indicated that they felt this was not worth big headlines to fuss over Mac users' vulnerability to malware.

"The torrent site is easily corrected, and Transmission is up and running the next day without a hitch. This kind of attack is an annoyance more

than anything else; of no real consequence at all in the larger picture," said one comment on CNET. "This kind of attack will hit at most a couple of hundred users, will affect less than a dozen, and will be out of commission within 24 hours if not sooner… really not a big deal."

Still, in an interview Sunday, Olson said he expected more Mac ransomware to proliferate, reported *Ars Technica*'s Cyrus Farivar. Olsen also told *Ars*:

"It is a little bit surprising because ransomware has been so incredibly popular for Windows, and mobile platforms," he said. "It's now of the most popular criminal business models. The fact that it hasn't made it to Mac shows that it's had a great amount of success on the Windows side. But the fact that [the malware] was distributed through a legit application demonstrates that we will see this again."

Finally, what would a readers' comments section be without the classic kind of warning such as this appearing on CNET: "Want a no brainer? Don't do anything stupid on your computer and you won't get a virus. Crazy idea."

Citation: Ransomware asks Apple Mac victims to pay up (2016, March 8) retrieved 19 May 2024 from https://techxplore.com/news/2016-03-ransomware-apple-mac-victims.html