Sophisticated Emotet malware loader thriving on unsophisticated passwords

13 February 2020, by Nancy Cohen

Credit: CC0 Public Domain

Emotet has evolved. And that's not good. The worm is winning the attention of security watchers this month, as an exploit of Wi-Fi networks. It hops. It spreads. Its triggers are insecure passwords on routers and Windows PCs.

Specifically, according to its discoverers, it is "a new loader type that takes advantage of the wlanAPI interface to enumerate all Wi-Fi networks in the area, and then attempts to spread to these networks, infecting all devices that it can access in the process."

Paul Wagenseil, a senior editor who covers security at Tom's Guide, was one of several writers following this "newly-found variant of the feared Emotet Trojan."

Why did Wagenseil describe it as feared? "Emotet is a jack-of-all-trades strain of malware that began life in 2014 as a banking Trojan," he wrote, "but later added the abilities to steal personal information, install ransomware, form botnets and download other pieces of malware."

A security firm Binary Defense identified the variant. According to Binary Defense, "With this newly discovered loader-type used by Emotet, a new threat vector is introduced to Emotet's capabilities. Previously thought to only spread through malspam and infected networks, Emotet can use this loader-type to spread through nearby wireless networks if the networks use insecure passwords."

While Wagenseil described it as feared, James Quinn, malware analyst for Binary Defense, gave even more reasons to be aware of Emotet's powers:

"Emotet is a highly sophisticated trojan that typically also serves as a loader for other malware. A key functionality of Emotet is its ability to deliver custom modules or plugins that are suited for specific tasks, including stealing Outlook contacts, or spreading over a LAN."

And Sergiu Gatlan in *BleepingComputer* on Feb. 7 thought of even more reminders. "The Emotet Trojan ranked first in a 'Top 10 most prevalent threats' drawn up by interactive malware analysis platform Any.Run in late December," he wrote, "with triple the number of uploads for analysis when compared to the next malware family in their top, the Agent Tesla info-stealer."

Gatlan also reported that The Cybersecurity and Infrastructure Security Agency (CISA) had issued a warning "on increased activity related to targeted Emotet attacks...advising admins and users to review the Emotet Malware alert for guidance."

Binary Defense found that the Wi-Fi spreading behavior had been going unnoticed for almost two years.

How could that be?

TechRadar's Anthony Spadafora mentioned two reasons, due to (1) how rarely the binary was

dropped. He wrote, "According to Binary Defense, January 23rd 2020 marked the first time the company had observed the file being delivered by Emotet despite the fact that it was included in the malware since 2018." (2) Its ability to go on without being discovered could have been that "the module did not display spreading behavior on the virtual machines and automated sandboxes without Wi-Fi cards that researchers use to dissect new strains of malware."

Tom's Guide provided a detailed run-through of how Emotet operates.

Once Emotet is installed on a PC, "worm.exe" checks to see how many Wi-Fi networks are with range. The step fails on Windows XP but not later versions of Windows. Emotet attempts to crack access passwords of each nearby Wi-Fi network, "pulling them from a precompiled list of likely passcodes one after another until one works."

Then let the spreading begin:

"Once it's granted access to a network, Emotet sends the network name and password of the newly cracked network up to its command-and-control server, apparently adding the information to a master list of hacked Wi-Fi networks.

"Then the malware ditches its host PC's existing Wi-Fi connection and connects the PC to the newly linked network, after which Emotet scans for connected Windows machines. It then tries to brute-force the Windows usernames and user passwords on each newly infected machine, drawing from another precompiled list of likely text strings."

Wagenseil said that aside from weak Wi-Fi passwords, it also shows up in an infected email attachments.

Quinn's closing comments on his Binary Defense discussion included advice for using strong passwords to secure wireless networks so that malware like Emotet cannot gain unauthorized access to the network.

Quinn also underscored detection strategies for this threat that would include "active monitoring of endpoints for new services being installed and investigating suspicious services or any processes running from temporary folders and user profile application data folders." He also said that network monitoring was an effective detection, "since the communications are unencrypted and there are recognizable patterns that identify the malware message content."

More information:
www.binarydefense.com/emotet-e … -new-wi-fi-spreader/

APA citation: Sophisticated Emotet malware loader thriving on unsophisticated passwords (2020, February 13) retrieved 27 September 2021 from https://techxplore.com/news/2020-02-sophisticated-emotet-malware-loader-unsophisticated.html