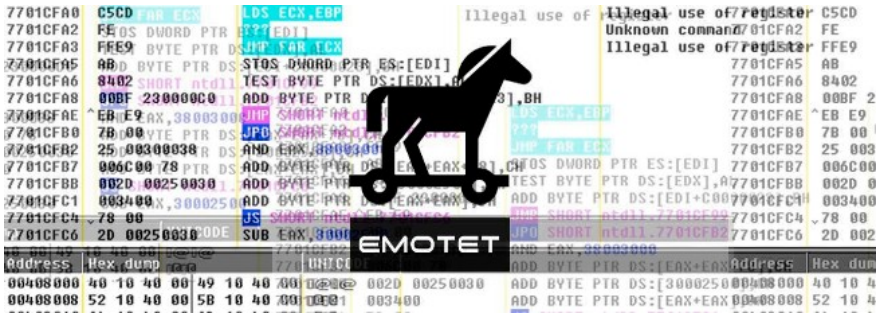
Microsoft warned the Emotet trojan back on a large scale, stealing the victim's banking information

After 5 months of silence, from February 2020 until now, the Emotet trojan has just officially returned with a larger scale.

Microsoft has officially issued a warning about a massive malware attack, targeting the victim's bank information. According to the software giant, both users and companies should be extremely wary of emails with file attachments.

Tens of thousands of emails with hundreds of malicious attachments were sent, according to Microsoft. If you click on these files, the Emotet trojan will be installed on the victim's computer.



Emotet is a dangerous trojan that steals victims' banking information
The Emotet banking Trojan was first discovered by security researchers in 2014. Initially, it was designed as a bank malware, attempting to penetrate a victim's computer to steal bank information. as well as other sensitive data. Later versions of Emotet added malware and spam distribution services, including the distribution of other banking trojans.

Emotet is equipped with functions to help avoid detection by virus scanning software. Besides, it can also spread itself to computers in the same network. The US Department of Homeland Security considers Emotet to be one of the most damaging and costly malware. Typically, it will cost about $ 1 million for each Emotet cleanup from the system of agencies, organizations and businesses.

Microsoft said the Threat Protection system had soon discovered this campaign. In addition, Office 365 ATP has long been able to detect malicious attachments and URL links in emails. Finally, Microsft Defender ATP will block malicious code from executing on the user's computer.