Find bug in Emotet malware, prevent it from spreading for 6 months

According to researcher James Quinn of the security firm Binary Defense, like other software, malicious code also has vulnerabilities, error codes. Hackers can exploit software vulnerabilities to cause harm, security experts can also decompile the source code of malicious code to find the vulnerability to exploit and defeat the malicious code.

In the case of Emotet, security researchers found an error code that allowed them to install a kill-switch that made it impossible to spread. Kill-switch took effect, stopping Emotet from February 6, 2020 to August 6, 2020. After that, Emotet updated the source code, patched it and continued to distribute it.

Emotet is a very dangerous malicious code, it spread through spam email system controlled by botnet. After infecting a victim's system, Emotet can commit various destructive acts, including stealing information and deploying ransomware to encrypt the victim's important data and then ransom.

How is the kill-switch Emotet created?

Emotet first appeared in 2014 and continuously updated with new features and attack methods. Earlier this February, the new update of Emotet added a way to take advantage of infected devices to spread to nearby WiFi shared devices.

Also in this update, Emotet has added a new retention mechanism. It creates a file to store the malicious code on the victim's system, using a random system filename with the .exe or .dll extension from the system32 directory.

Emotet malware has a bug

Based on this mechanism, Binary Defense created a kill-switch to limit the spread of Emotet. The first version of the kill-switch came out about 37 hours after the Emotet update was deployed. Researchers used PowerShell scripts to generate registry key values ??for each victim and set the data to these values ??to null.

Thus, when malicious code checks the registry for a file to infect other computers, it will load an empty exe file. Therefore, the malicious code cannot be deployed on other machines.

EmoCrash

Quinn even created an upgraded version of the kill-switch called EmoCrash. According to Quinn's description, EmoCrash can exploit the cache overflow vulnerability discovered in the Emotet installation process to circumvent the Emotet installation process to help prevent this malware more effectively.

Instead of resetting the registry value, EmoCrash redefines the architecture of the system to create the registry setting value for the serial number for the drive, using it to store an 832 byte buffer.

This tiny buffer can destroy an Emotet and can even be pre-deployed like a vaccine or deployed as soon as the Emotet is spreading. EmoCrash has been quietly deployed to systems and organizations at risk of being attacked by Emotet in April 2020.

On July 17, 2020, Emotet began re-booting the malicious email spam system after a few months trying to avoid being prevented. However, it was not until August 6, 2020 that this malicious code completely fixed its bug code.

Now, with the new Emotet release, the Binary Defense security researchers' containment method is no longer in effect. However, according to Quinn, they have been very successful at stopping Emotet from spreading for six months.

Experts recommend that users should not click on links or attachments in emails sent from strange users. Besides, attachments and emails sent from acquaintances also need to be scanned for viruses before clicking.