How to prevent EternalRocks malicious code

EternalRocks is a malicious code that is even more dangerous than WannaCry, exploiting up to seven NSA vulnerabilities and they work on computers.

After the cyberattack from WannaCry, cyber security researchers have discovered more EternalRocks malicious code, supposedly more powerful than WannaCry.

The way EternalRocks works is to exploit vulnerabilities in the SMB file sharing protocol on the Windows operating system, thereby spreading to computers. However, while WannaCry only took advantage of two vulnerabilities, EternalBlue and DoublePulsar, EternalRocks exploited seven vulnerabilities.

1. EternalRocks - more dangerous malicious code than WannaCry exploits up to seven NSA vulnerabilities

1. Malicious code EternalRocks attack the computer

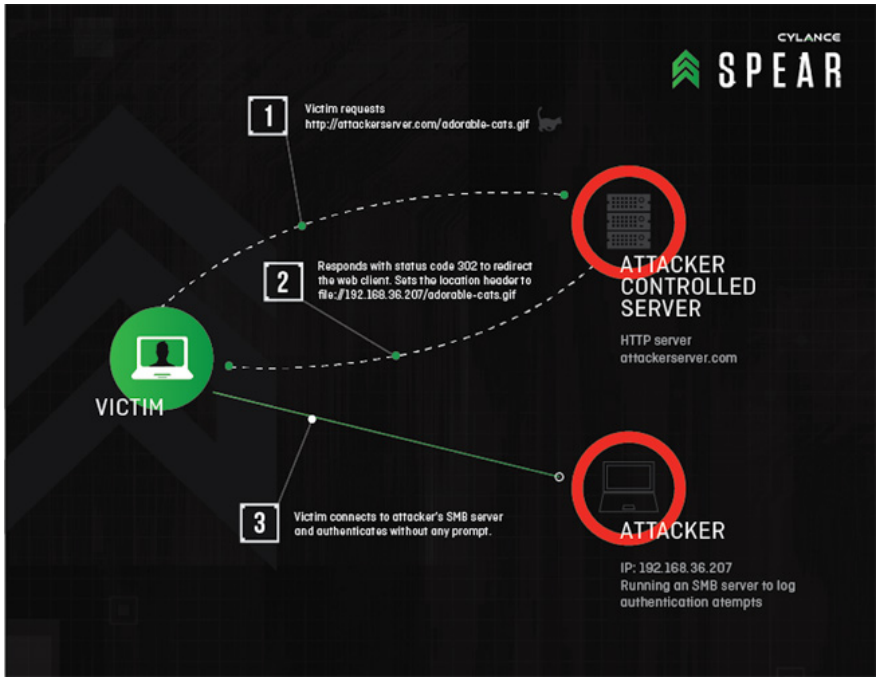
The way EternalRocks works is similar to Wanna Cry, which is to exploit the vulnerability in the data sharing protocol on Windows computers that is Microsoft Windows Server Message Block.

More dangerous, this malicious code secretly makes software or antivirus programs, malware detection difficult to detect. The seven vulnerabilities that EternalRocks exploits and uses indicate that the level of danger of this type of malware affects the network security system.

1. EternalBlue: SMBv1 exploit tool.
2. EternalRomance: SMBv1 exploit tool.
3. EternalChampion: SMBv2 exploit tool.
4. EternalSynergy: SMBv3 exploit tool.
5. SMBTouch: SMB reconnaissance tool.
6. ArchTouch: SMB reconnaissance tool.
7. DoublePulsar: SMB reconnaissance tool.

DoublePulsar ArchTouch, SMB Touch are 3 SMB reconnaissance tools to scan SMB ports. Meanwhile, 4 vulnerabilities, EternalBlue, EternalChampion, EternalSynergy and EternalRomance, increase the chances of Windows computers being more vulnerable.

Cyber ??security expert Miroslav Stampar said EternalRocks has control over all affected computers, in order to expand the scale of attacks to most computers worldwide.



2. How to prevent EternalRocks malicious code

Until now, EternalRocks is still in a "hidden" state and "dormant" so the way to prevent and destroy EternalRocks like Wanna Cry has not been found by cyber security researchers. However, users should use preventive methods before becoming one of the victims of EternalRocks.

You can use the ways to prevent WannaCry malicious code that the Network Administrator introduced in the previous articles. We need to update antivirus software, detect malicious code for the computer. In particular, you need to update the latest Windows patches that Microsoft provides.

1. Microsoft released an emergency patch to prevent ransomware from attacking
2. With the NMR's 15 free Ransomware decoding tools, you won't need to ransom the file anymore
3. How to remove / fix ransomware WannaCry

You can also close port 445 on Windows to prevent malicious code. Readers refer to the article How to close the port / Port 445 on Windows 2000 / XP / 2003 to Windows 10 to prevent ransomware WannaCry.

You finished reading the article "**How to prevent EternalRocks malicious code**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.