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

While ransomware WannaCry has stirred up the internet world over the past few weeks to exploit only two vulnerabilities, the new malware uses seven vulnerabilities.

Network security researchers have confirmed the emergence of a new malicious code called EternalRocks, which exploits seven NSA vulnerabilities that have been leaked by Shadow Brokers hacker group. Experts describe this computer worm as "the end of the world" that can cause vibration.

Earlier this month, ransomware WannaCry caused many organizations to stop working when they invaded more than 300,000 computers in more than 150 countries around the world. While WannaCry only exploited two vulnerabilities, EternalBlue and DoublePulsar, EternalRocks exploited **7 vulnerabilities** : **EtenalBlue, DoublePulsar, EternalChampion, EternalRomance, EternalSynerg, ArchiTouch** and **SMBTouch.** All of them were leaked tools from the Shadow Brokers group.

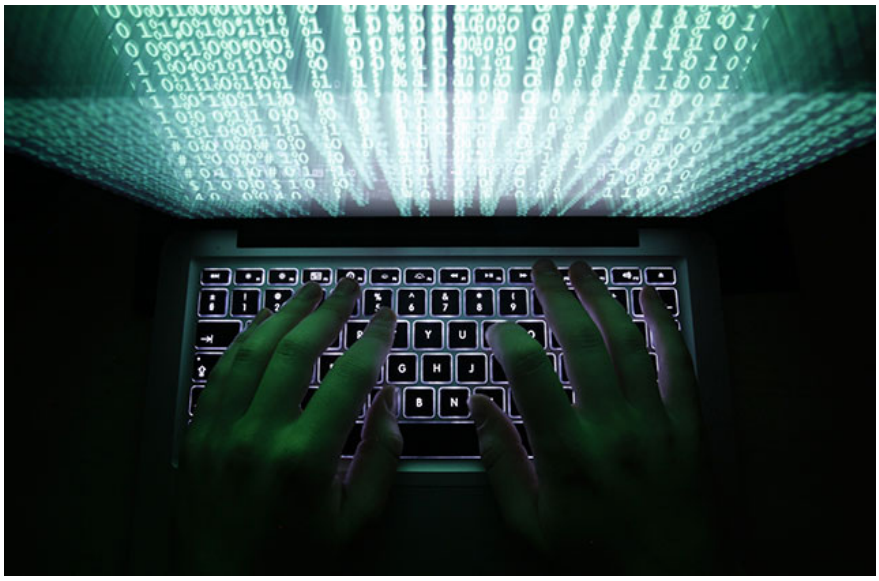
Miroslav Stampar, cyber security expert at Croatia's CERT, was the first to discover EternalRocks on Wednesday. He wrote a description on GitHub that the first evidence for its appearance dates from May 3. You can find out about Stampar's EternalRocks report on GitHub at: https://github.com/stamparm/EternalRocks

Most tools exploit vulnerabilities through file-sharing technology on PCs called Microsoft Windows Server Message Block, which is how WannaCry infects very quickly without anyone knowing. Microsoft patched these vulnerabilities in March, but many un-updated computers are still infected.

Unlike WannaCry, just a blackmail, EternalRocks stays dormant and hidden on the computer.**EternalRocks uses a two-stage installation process** , in which the second stage will have a slight delay. At the first stage, EternalRocks will infect the system, download the Tor anonymous browser and connect to the C&C (Command and Control) server located in the Tor network. Within 24 hours, it will not calm down. But then, in the second phase, C&C server started responding, downloading and copying. It also means that security experts who want to know more information to study malicious code will be delayed by 1 day. EternalRocks will then scan and find machines that have vulnerabilities to continue to penetrate.

Mr. Micharl Patterson, CEO at security company Plixer said: " *By delaying it, malicious code works stealthily and makes the race to detect and prevent it more difficult . "*

Stampar said the malware even named after WannaCry to fool cyber security experts. Like the dangerous variants of WannaCry, **EternalRocks has no kill switch** , the tool has helped prevent the early WannaCry, so it is not easy to block it.



While infecting more and more computers, EternalRocks is still lying dormant. Stampar warned it could attack at any time, similar to the way WannaCry surprised the cyber security community when simultaneously infecting thousands of computers. Because of its characteristics, users also do not know if the device is infected with EternalRocks. It is unclear what kind of attack EternalRocks will have, Plixer said that it might turn into ransomware or trojans to attack.