WannaCry is a year old, EternalBlue is bigger than you think

Today 12/5, commemorating the 1st anniversary of WannaCry extortion's virulence broke out into a global 'pandemic'.

Today 12/5, commemorating the 1st anniversary of WannaCry extortion's virulence broke out into a global 'pandemic'.

It has been 1 year since the day of one of the biggest security incidents in history. But it is not over and over, according to the statistical data of the company providing ESET antivirus software, 'heart' of WannaCry, the EternalBlue vulnerability is growing and more popular than ever.

EternalBlue is said to be developed by the US National Security Agency, located in a toolkit stolen by The Shadow Brokers hacker group from NSA's server in 2016, then surfed online from August 8 to April 4. 2017

The beginning is fuzzy

EternalBlue is exploited and becomes the main mechanism for WannaCry blackmail to invade the computer, then ransomware like NotPetya or Bad Rabbit also exploit in the same way.

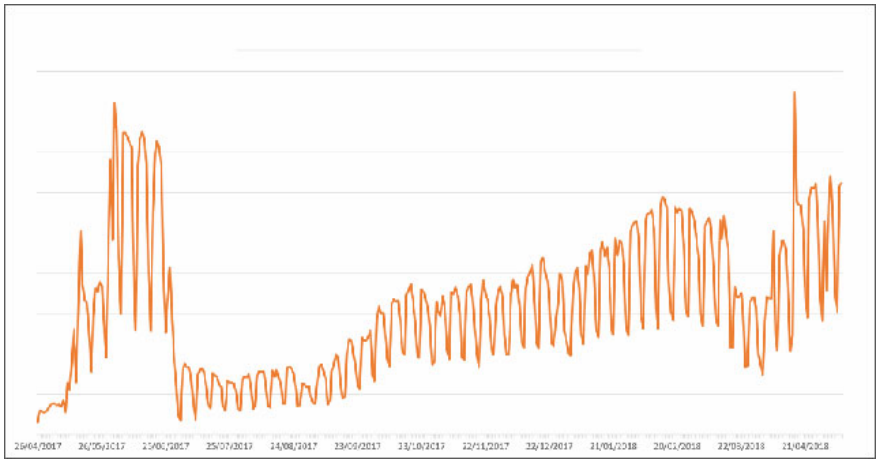
According to IBM X-Force, the WannaCry case alone caused $ 8 billion in losses across 150 countries. But the first version of EternalBlue was not perfect, only running on Windows 7, Windows Server 2008 and crashing on Windows XP.

EternalBlue caused great damage in the WannaCry case, but very few malicious authors knew how to use it, so the number of users of this vulnerability fell sharply.

1. What is Petya? What is NotPetya? Is it really ransomware or is it even more dangerous?
2. All about WannaCry, Ransomware has been confusing for the past few days

Become a best seller in the malware market

Things changed after WannaCry and NotPetya went through. Security researchers put EternalBlue on a lot of platforms, such as Windows 8 and Server 2012, even Windows 10, making the ability to exploit more, the EternalBlue variable into the item most wanted by malware authors.



ESET's number of EternalBlue discoveries for the 2017-2018 period

A few months later, EternalBlue encroached on both virtual money digging and government spy groups.

Living on unpatched systems

Although EternalBlue is no longer used as much to spread extortion code, most users do not know that it is still one of the biggest threats today. Not only because there are still people who are trying to exploit it for their malicious campaigns, but also because there are many devices that are easily poisoned.

According to Nate Warfield, from the Microsoft Security Response Center, many Windows machines are still "displaying" their SMB services online. EternalBlue is also one of the reasons why Microsoft disables SMBv1 (which is the EternelBlue object targeted) on the new OS.

1. Microsoft will turn off SMBv1 in Windows Starting this fall
2. Windows SMB users should close some ports to prevent WannaCry

EternalBlue will remain a threat for many more years

Krypto Logic, which blocked WannaCry's rampage, said that WannaCry's remnants still use EternalBlue to find new victims, scan millions of millions on the Internet to find EternalBlue unpatched and untapped computers.

They can block WannaCry from encrypting the file but the EternalBlue vulnerability used to spread WannaCry is still working properly. There are machines that have not installed the patch, EternalBlue is still successful and is a threat.

See more:

1. Digital pre-digging tool infects Windows computers via EternalBlue and WMI
2. Eternal Blues - NSA's EternalBlue vulnerability testing tool
3. Warning with 4 dangerous variants of WannaCry malware