WannaCry security note

Nokia Threat Intelligence Labs

May 2017

The WannaCry ransomware attack was a worldwide cyberattack on May 2017 caused by the WannaCry ransomware cryptoworm, which targeted computers running Microsoft Windows operating system by encrypting data and demanding ransom payments in Bitcoin cryptocurrency. WannaCry propagates using an exploit of Windows' Server Message Block (SMB) protocol. To date, Nokia has not observed a significant increase in this exploit in networks protected by NetGuard Endpoint Security (NES). Nokia will continue to monitor the situation and update customers as appropriate.
What does the WannaCry virus do?

It locks computers so that users cannot access their files or programs. Hackers ask for payment to release the computer. This type of virus is also known as ransomware. WannaCry and its variants like WannaCrypt and Wanna Decryptor target computers that use Microsoft's Windows operating system.

How does it infect computers?

By e-mail. Users receive a file, usually in a .zip format. When the user clicks on the file or opens it, the virus will automatically spread and lock up files and programs. Once the computer is fully infected, the user can access only two files: instructions on what to do next and the virus program itself. Other forms of ransomware lure users into clicking on a fake link in an e-mail or on a bogus website. It will then release a virus that corrupts the computer.

Ransomware is not new. Why the panic?

The speed and scale of WannaCry's spread has alarmed security experts.

Within hours of it being discovered on Friday, over 57,000 attacks were reported across 99 countries, with Russia, Ukraine and Taiwan reportedly the top targets. Operations in large organizations like Britain's National Health Service, global shipping company FedEx in the United States, and the Russian Interior Ministry have been affected.

Experts say the malicious software was spreading at a rate of five million e-mails per hour. This virus has been designed as a "worm", which means it can automatically spread to other computers in the same network.

EternalBlue (MS17-010) is a Windows SMB vulnerability. A patch for this vulnerability was released by Microsoft in mid-March, after a leaked NSA rootkit called DoublePulsar, which used the vulnerability, became publicly available.
How to protect one’s computer?

Microsoft has issued automatic Windows updates to defend its clients from this virus. Additional measures include using a reputable antivirus software and a firewall, backing up files in a separate system and setting a popup blocker. Beware of clicking links or files in e-mails or on suspicious websites. Users who receive a ransom note should disconnect the computer from the Internet and alert the authorities.

Who are these hackers?

No one has claimed responsibility so far. Experts speculate that it could be a large cyber-criminal gang or even state governments.

What do they want?

The hackers are asking for payment of US$300 to US$600 in bitcoin, a digital currency, to restore access. Users are warned that if they do not pay up in a few days, their files will be deleted. The hackers give instructions on how to buy bitcoin and which bitcoin address to send it to.

Governments have advised users not to pay the ransom, as it encourages these hackers.

Where did this virus come from?

The US National Security Agency was the first to discover a flaw in Microsoft's Windows operating system that allowed it to develop a way to hack or gain access to computers used by terrorists and enemy states. The flaw, and a tool to exploit it with malicious software, was made public last month by a hacker collective known as Shadow Brokers.
What has Nokia done?

The worm: A signature SID:2024216/Win32.Backdoor.DOUBLEPULSAR is already deployed to NetGuard Endpoint Security (NES) customers that detects the SMB-based infection attempts using the EternalBlue vulnerability. (The signature is deployed in an “inactive state”, meaning that detected infections will not contribute to Security Analytics infection rate, but triggers raw events that are available in the Security Analytics Portal.)

The IP addresses in the raw events identify which subscribers are infected and could be used by service providers to block infected devices: this could help prevent spread of the worm. The rule that detects this SMB infection associated with the ransomware has been deployed in passive mode since May 1st. The rule will be activated at all customers in the next signature update.

The ransomware: Threat Intelligence Labs has analyzed a copy of the ransomware, WannaCry. Two more signatures, SID:2024218 and SID:2024220 / Win32.Bot.WannaCry are under review and will be available with the next rules update.
What are the recommended actions?

Immediate steps for IT security would include:

1. Block SMB traffic (tcp port 445) where possible.
2. Patch all Windows computers as soon as possible.
3. Locate infected computers, quarantine, reimage and restore files from backups (if available).