NEW WAVE OF RANSOMWARE AFFECTING BUSINESSES: WHAT TO DO?

28Jun2017

Press Release

Since yesterday, 27 June 2017, critical infrastructure and business systems are being targeted with a new wave of ransomware, which is an updated version of Petya. The attack has caused infections worldwide and has not yet been stopped.

Immediately after the first reported infections, Europol has set up an urgent coordination cell and is currently actively monitoring the spread of the ransomware. We are in close contact with law enforcement authorities from infected countries and key industry partners to assess the impact of this attack, coordinate actions and join forces. At this stage, it is not yet possible to say how many victims have been infected.

Europol's Executive Director, Rob Wainwright, said: *"This is another serious ransomware attack with global impact, although the number of victims is not yet known. There are clear similarities with the WannaCry attack, but also indications of a more sophisticated attack capability, intended to exploit a range of vulnerabilities. It is a demonstration of how cybercrime evolves at scale and, once again, a reminder to business of the importance of taking responsible cyber security measures."*

How does it work?

Despite existing since 2016, Petya ransomware differs from typical ransomware as it does not just encrypt files, it also overwrites the Master Boot Record (MBR)[1]. This renders the machine unusable and prevents users from recovering any information from it. Unlike the previous Wannacry incident, this attack does not include any type of "kill switch".

What to do?

<u>If you have been infected:</u>

1. **Do not pay.** You will not only be financing criminals, but it is unlikely that you will regain access to your files. This is particularly relevant in the case of Petya, as the email account used to manage ransom demands has been blocked, thus disabling attackers' access to

the only communication channel known at the moment.

2. **Report it to your local police.** Make sure that you **keep a copy of the phishing email** received from the attackers and provide it to the police. This will help law enforcement with their investigation.

3. **Disconnect the infected device from the internet.** If the infected device is part of a network, try to isolate it as soon as possible, in order to prevent the infection from spreading to other machines. You can then format the hard drive, reinstall the operating system and apps, run any available updates and, finally, restore the locked files from your back-up device.

If you have not been infected:

1. **Keep all apps and operating system up to date**, making sure that you install all Microsoft patches as soon as they are made available. If the device offers the option of automatic updates, take it.

2. **Back-up your data.** Even if you are affected by ransomware, you can easily retrieve your files. It is best to create two back-up copies: one to be stored in the cloud and one to store physically.

3. Use **robust security products** to protect your system from all threats, including ransomware.

4. **Do not use high privileges accounts** (accounts with administrator rights) for daily business.

5. **Do not click on attachments** or links that accompany suspicious or unexpected emails, even if they seem to be coming from a trusted party such as such as a bank or an online store. Trust no one.

For more tips and for the latest available decryption keys, visit https://www.nomoreransom.org/

--

[1] The MBR, the most important data structure on the disk, is created when the disk is partitioned. The MBR contains a small amount of executable code called the master boot code, the disk signature, and the partition table for the disk. https://technet.microsoft.com/en-us/library/cc976786.aspx

CRIME AREAS Cybercrime

TARGET GROUPS General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

Source URL: https://www.europol.europa.eu/newsroom/news/new-wave-of-ransomware-affecting-businesses-what-to-do