What Is Petya and NotPetya Ransomware?

Petya ransomware began spreading internationally on June 27, 2017. Targeting Windows servers, PCs, and laptops, this cyberattack appeared to be an updated variant of the Petya malware virus. It used the Server Message Block vulnerability that WannaCry employed to spread to unpatched devices, as well as a credential-stealing technique, to spread to non-vulnerable machines. Petya was a global cyberattack felt around the world, but it primarily targeted Ukraine during its June 2017 run.

How does the Petya virus spread and infect devices?

Petya exploits the vulnerability CVE-2017-0144 in Microsoft's implementation of the Server Message Block protocol. After it exploits the vulnerability, this attack encrypts the master boot record, among other files. It sends a message to the user to conduct a system reboot, after which the system is inaccessible. This makes the operating system incapable of locating files and there is no way to decrypt the files, which makes Petya a wiper rather than ransomware, which it was first

believed to be.

The new variant has further increased its capabilities by adding a spreading mechanism similar to what we saw in WannaCry in May 2017. A set of critical patches was released by Microsoft on March 14 to remove the underlying vulnerability in supported versions of Windows, but many organizations may not have yet applied these patches.

How do I protect myself from Petya?

The best way to protect yourself from Petya is through proactive measures. The Petya virus is said to spread via phishing or spam emails, so make sure you check an email's content for legitimacy. Hover over a link and see if it goes to a trusted URL. Or, if you are unsure about an email's content or source, do a quick online search and look for other instances of this campaign, and what those instances could tell you about the email's legitimacy. You should also do a complete backup of your device. If a machine becomes infected with the Petya virus, data could become unrecoverable. You can back up your data stored on an external hard drive, in the cloud, or another third-party storage option. Most importantly, always apply system and application updates whenever they are available, as Petya—and attacks like it—rely on unpatched vulnerabilities to breach systems.

Trellix Threat Labs
Research Report: April 2022

Read Report

What is the difference between Petya and NotPetya?

Petya malware has been around for quite some time, with the June 2017 attack unleashing a new variant. This variant is called NotPetya by some due to changes in the malware's behavior. Petya and NotPetya use different

keys for encryption and have unique reboot styles and displays and notes. However, both are equally as destructive.

The history and evolution of Petya ransomware

Petya was discovered in March 2016 by security researchers who noted that although the malware achieved fewer infections than other currently active strains, the virus was still unique in its operation, alerting many in the industry to keep a watchful eye on the advanced attack. Later in 2016, another Petya variant emerged that contained an additional capability to be used if the virus could not gain administrator access to a machine.

Fast forward to June 2017, and the latest strain of Petya emerged, taking down organizations across the globe in a matter of hours. The updated capabilities of the new variant have some security professionals naming the virus NotPetya.

What should I do next?

If you have already taken the proactive measures outlined above, you should be protected from Petya/NotPetya. If you have been impacted by Petya, or another type of ransomware, head to NoMoreRansom.org. And remember, never pay the ransom: If you are dealing with Petya, you will not get your files back.

More Ransomware Articles

What Is Stuxnet?

Malware vs. Viruses

What Is Fileless Malware?

What Is Malware?

What Is Ransomware?

Copyright © 2022 Musarubra US LLC