

What is Petya? What is NotPetya? Is it really ransomware or is it even more dangerous?

According to a new analysis, NotPetya is designed like ransomware but it is malware that erases the hard drive, completely removes the data on the computer, destroying all records from target systems.

If I say that the global devastating global malware outbreak is not due to any ransomware contamination, what do you think?

1. Petya's "extortion" malicious code is raging, this is a remedy to prevent

What is Petya?

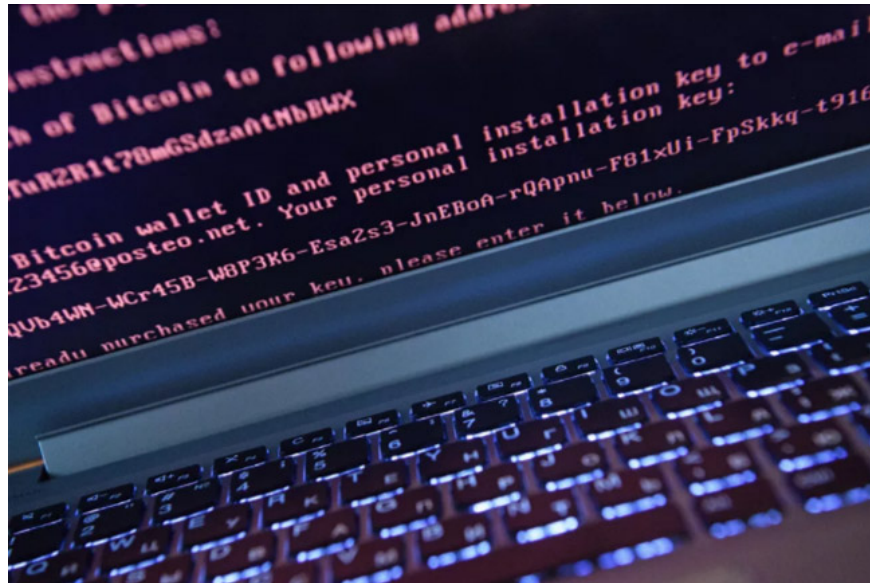
Petya is a ransomware variant that was first discovered in 2016. It represents a big step forward in ransom, more complex than everything that happened before. However, its influence is quite limited, especially when people find a way to stop Petya soon after.

What is NotPetya?

The types of ransomware that are spreading throughout the world are not Petya. Although it is similar to Petya, it is a new type of ransomware that has never been seen before. That's why Kaspersky called it NotPetya. Other names for NotPetya include Petrwrap, Petna, Pneytna, ExPetr, and GoldenEye.

But because NotPetya is quite similar to Petya, the last few days, the name Petya is used most commonly. It works like any other ransomware, encrypts all your files and requires a ransom to decrypt the file. The ransom in this case is worth \$ 300 in the form of Bitcoin.

Yes, "ransomware" NotPetya has begun to infect computers in a number of countries, including Russia, Ukraine, France, India and the United States on Tuesday and has asked for a non-designed \$ 300 ransom. for the purpose of restoring computers.



According to a new analysis, NotPetya is designed like ransomware but it is malware that erases the hard drive, completely removes the data on the computer, destroying all records from target systems.

Matt Suiche, founder of Comae Technologies, looked at the malware's activity, saying after analyzing the virus, known as NotPetya, his team discovered that it was "software malicious Wiper" rather than ransomware.

Security experts even believe that the real attack has been disguised to attract the world's attention from a state-sponsored attack on Ukraine to spread malware.

Suiche writes: "We believe ransom is actually to attract the attention of the media, especially after the WannaCry incident, in order to attract the attention of some more hacker groups than the attackers because national purpose".

Will Petya be faulty or is it too smart?

NotPetya is a type of malware, unlike other traditional ransomware tools, does not encrypt files on a system that is targeted one by one.

Instead, NotPetya restarts the victim computer and encrypts the Master File Table (MFT) of the hard drive and renders the Master Boot Record (MBR) inactive, limiting access to the entire system by collecting information about file names, sizes and locations on the hard drive.

Then, NotPetya retrieves an encrypted copy of the MBR and replaces the MBR with its own malicious code, showing the ransom notification, making the computer unbootable.

However, the new variant of Petya does not keep a copy of the MBR that has been replaced, possibly by mistake or intentional, so that the infected computer cannot boot even if the victim has obtained the decryption key.

In addition, after infecting one computer, NotPetya scans the local network and quickly infects all other computers (even computers that have full patches installed) on the same network, using the EternalBlue SMB, WMIC and PSEXEC instruments.

According to former NSA expert David Kennedy, NotPetya will find the passwords stored in memory, the file system on the infected computer to spread to other systems. Kennedy also emphasized: 'This case will definitely be big, not kidding'.

NotPetya also misused the PsExec tool to infect. This is a tool designed to perform some operations on the system. NotPetya used PsExec to execute its malicious code. If the infected computer NotPetya has administrative rights in the network, all other computers will "get hit". Another similar method used by NotPetya is with the Windows Management Instrumentation (WMI) tool.

Security expert from ESET firm Robert Lipovsky said it was the combination of these three methods that made NotPetya spread rapidly, even though the whole world updated the patch after the WannaCry case, but only one machine in the system was needed. If the network is not patched, both the network can be compromised, gain administrative rights and then spread to all other computers on the network.

Therefore, NotPetya can infect EternalBlue-patched machines, on all Windows versions, including Windows 10. This indicates that NotPetya is more dangerous, more professional than WannaCry, because WannaCry is primarily infected. on older Windows versions.

A Microsoft spokesman said Windows Defender could detect and block NotPetya. Currently the company is also looking for appropriate measures to protect customers and investigate to clarify the problem.

Don't pay the ransom, because if you pay, you won't get the file back

So far, nearly 45 victims have paid a total of \$ 10,500 in the form of Bitcoin to NotPetya creators in the hope of retrieving locked files, but unfortunately, they still cannot retrieve the data they need. This is because the email address is set up by the attacker to contact the victim and send the decryption key blocked by the German service provider immediately after the attack. That is, even if the victim pays the ransom, it will never recover the data. Kaspersky researchers also said so.

"Our analysis shows that there is little hope for victims to recover their data. We analyzed Petya's source code at a very deep level and we found that after the code The drive, the creator of NotPetya, could not decipher the victim's drive, "the security company said.

"To decrypt the victim's drive, ID settings are required. In previous versions of ransomware similar to Petya / Mischa / GoldenEye, this installation ID contains the necessary information to recover."

If the researchers' claims are correct, the new variant of NotPetya is a destructive malware designed to shut down and disrupt services worldwide, the malware has been successful in public. its work.

However, this is still speculation, NotPetya mainly focuses on many objects in Ukraine, including Kiev's subway, Boryspil airport, electricity supplier, central bank and state telecommunications.

Other countries infected with Petya include Russia, France, Spain, India, China, the United States, Brazil, Chile, Argentina, Turkey and South Korea.

How did Petya spread to the first computer?

According to research conducted by Talos Intelligence, a small Ukrainian company called MeDoc may be the main source of global ransomware boom yesterday.

The researchers said the virus could be spread through a malware update to the MeDoc tax accounting system, although MeDoc denied claims in a long post on Facebook.

"At the time of updating the program, the system cannot be infected directly from the update file," excerpts from MeDoc's article. "We can show that users of the MEDoc system cannot be infected at the time of updating the program."

However, some security researchers and even Microsoft have agreed with Talo's findings, saying that MeDoc has been targeted and the virus has spread through updates.

You finished reading the article "**What is Petya? What is NotPetya? Is it really ransomware or is it even more dangerous?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.