'Petya' ransomware attack: what is it and how can it be stopped?

Companies have been crippled by global cyberattack, the second major ransomware crime in two months. We answer the key questions

Companies have been crippled by global cyberattack, the second major ransomware crime in two months. We answer the key questions

Olivia Solon in San Francisco and Alex Hern in London

07.17 BST01.24 BST

Many organizations in Europe and the US have been crippled by a ransomware attack known as “Petya”. The malicious software has spread through large firms including the advertiser WPP, food company Mondelez, legal firm DLA Piper and Danish shipping and transport firm Maersk, leading to PCs and data being locked up and held for ransom.

It’s the second major global ransomware attack in the past two months. In early May, Britain’s National Health Service (NHS) was among the organizations infected by WannaCry, which used a vulnerability first revealed to the public as part of a leaked stash of NSA-related documents released online in April by a hacker group calling itself the Shadow Brokers.

The WannaCry or WannaCrypt ransomware attack affected more than 230,000 computers in over 150 countries, with the NHS, Spanish phone company Telefónica and German state railways among those hardest hit.

Like WannaCry, “Petya” spreads rapidly through networks that use Microsoft Windows, but what is it, why is it happening and how can it be stopped?

Ransomware is a type of malware that blocks access to a computer or its data and demands money to release it.

When a computer is infected, the ransomware encrypts important documents and files and then demands a ransom, typically in Bitcoin, for a digital key needed to unlock the files. If victims don’t have a recent back-up of the files they must either pay the ransom or face losing all of their files.

The ransomware takes over computers and demands $300, paid in Bitcoin. The malicious software spreads rapidly across an organization once a computer is infected using the EternalBlue vulnerability in Microsoft Windows (Microsoft has released a patch, but not everyone will have installed it) or through two Windows administrative tools. The malware tries one option and if it doesn’t work, it tries the next one. “It has a better mechanism for spreading itself than WannaCry,” said Ryan Kalember, of cybersecurity company Proofpoint.

Most major antivirus companies now claim that their software has updated to actively detect and protect against “Petya” infections: Symantec products using definitions version 20170627.009 should, for instance, and Kaspersky also says its security software is now capable of spotting the malware. Additionally, keeping Windows up to date – at the very least through installing March’s critical patch defending against the EternalBlue vulnerability – stops one major avenue of infection, and will also protect against future attacks with different payloads.

For this particular malware outbreak, another line of defence has been discovered: “Petya” checks for a read-only file, C:\Windows\perfc.dat, and if it finds it, it won’t run the encryption side of the

crackIAS.com

software. But this "vaccine" doesn't actually prevent infection, and the malware will still use its foothold on your PC to try to spread to others on the same network.

Strictly speaking, it is not. The malware appears to share a significant amount of code with an older piece of ransomware that really was called Petya, but in the hours after the outbreak started, security researchers noticed that "the superficial resemblance is only skin deep". Researchers at Russia's Kaspersky Lab redubbed the malware NotPetya, and increasingly tongue-in-cheek variants of that name – Petna, Pneytna, and so on – began to spread as a result. On top of that, other researchers who independently spotted the malware gave it other names: Romanian's Bitdefender called it Goldeneye, for instance.

The attack appears to have been seeded through a software update mechanism built into an accounting program that companies working with the Ukrainian government need to use, according to the Ukrainian cyber police. This explains why so many Ukrainian organizations were affected, including government, banks, state power utilities and Kiev's airport and metro system. The radiation monitoring system at Chernobyl was also taken offline, forcing employees to use hand-held counters to measure levels at the former nuclear plant's exclusion zone. A second wave of infections was spawned by a phishing campaign featuring malware-laden attachments.

The "Petya" ransomware has caused serious disruption at large firms in Europe and the US, including the advertising firm WPP, French construction materials company Saint-Gobain and Russian steel and oil firms Evraz and Rosneft. The food company Mondelez, legal firm DLA Piper, Danish shipping and transport firm AP Moller-Maersk and Heritage Valley Health System, which runs hospitals and care facilities in Pittsburgh, also said their systems had been hit by the malware.

Crucially, unlike WannaCry, this version of 'Petya' tries to spread internally within networks, but not seed itself externally. That may have limited the ultimate spread of the malware, which seems to have seen a decrease in the rate of new infections overnight.

It initially looked like the outbreak was just another cybercriminal taking advantage of cyberweapons leaked online. However, security experts say that the payment mechanism of the attack seems too amateurish to have been carried out by serious criminals. Firstly, the ransom note includes the same Bitcoin payment address for every victim – most ransomware creates a custom address for every victim. Secondly, the malware asks victims to communicate with the attackers via a single email address which has been suspended by the email provider after they discovered what it was being used for. This means that even if someone pays the ransom, they have no way to communicate with the attacker to request the decryption key to unlock their files.

It is not clear, but it seems likely it is someone who wants the malware to masquerade as ransomware, while actually just being destructive, particularly to the Ukrainian government. Security researcher Nicholas Weaver told cybersecurity blog Krebs on Security that 'Petya' was a "deliberate, malicious, destructive attack or perhaps a test disguised as ransomware". Pseudonymous security researcher Grugq noted that the real Petya "was a criminal enterprise for making money," but that the new version "is definitely not designed to make money.

"This is designed to spread fast and cause damage, with a plausibly deniable cover of 'ransomware,'" he added, pointing out that, among other tells, the payment mechanism in the malware was inept to the point of uselessness: a single hardcoded payment address, meaning the money can be traced; the requirement to email proof of payment to a webmail provider, meaning that the email address can be – and was – disabled; and the requirement to send an infected machine's 60-character, case sensitive "personal identification key" from a computer which can't even copy-and-paste, all combine to mean that "this payment pipeline was possibly the worst of all

crackIA2.com

options (sort of ‘send a personal cheque to: Petya Payments, PO Box … ’)”.

Ukraine has blamed Russia for previous cyber-attacks, including one on its power grid at the end of 2015 that left part of western Ukraine temporarily without electricity. Russia has denied carrying out cyber-attacks on Ukraine.

The ransomware infects computers and then waits for about an hour before rebooting the machine. While the machine is rebooting, you can switch the computer off to prevent the files from being encrypted and try and rescue the files from the machine, as flagged by @HackerFantastic on Twitter.

If machine reboots and you see this message, power off immediately! This is the encryption process. If you do not power on, files are fine. pic.twitter.com/IqwzWdlrX6

If the system reboots with the ransom note, don’t pay the ransom – the “customer service” email address has been shut down so there’s no way to get the decryption key to unlock your files anyway. Disconnect your PC from the internet, reformat the hard drive and reinstall your files from a backup. Back up your files regularly and keep your anti-virus software up to date.

END

Downloaded from **crackIAS.com**

© **Zuccess App** by crackIAS.com