

New WannaCryptor-like ransomware attack hits globally: All you need to know

wlvivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine

June 27, 2017



Numerous reports are coming out on social media about a new ransomware attack in Ukraine, which could be related to the Petya family.



Editor

27 Jun 2017 - 05:07PM

Numerous reports are coming out on social media about a new ransomware attack in Ukraine, which could be related to the Petya family.

Update (June 28 – 15:00 CEST): ESET researchers have confirmed that further affected systems had access to Ukraine networks through VPN. Presently, it has not been seen in the malware a functionality to spread outside of the LAN network.

Update (June 27 – 23.34 CEST): Shutting down the computer and not booting again could prevent the disk encryption, though several files can be already encrypted after the MBR is replaced and further infection through the network is attempted.

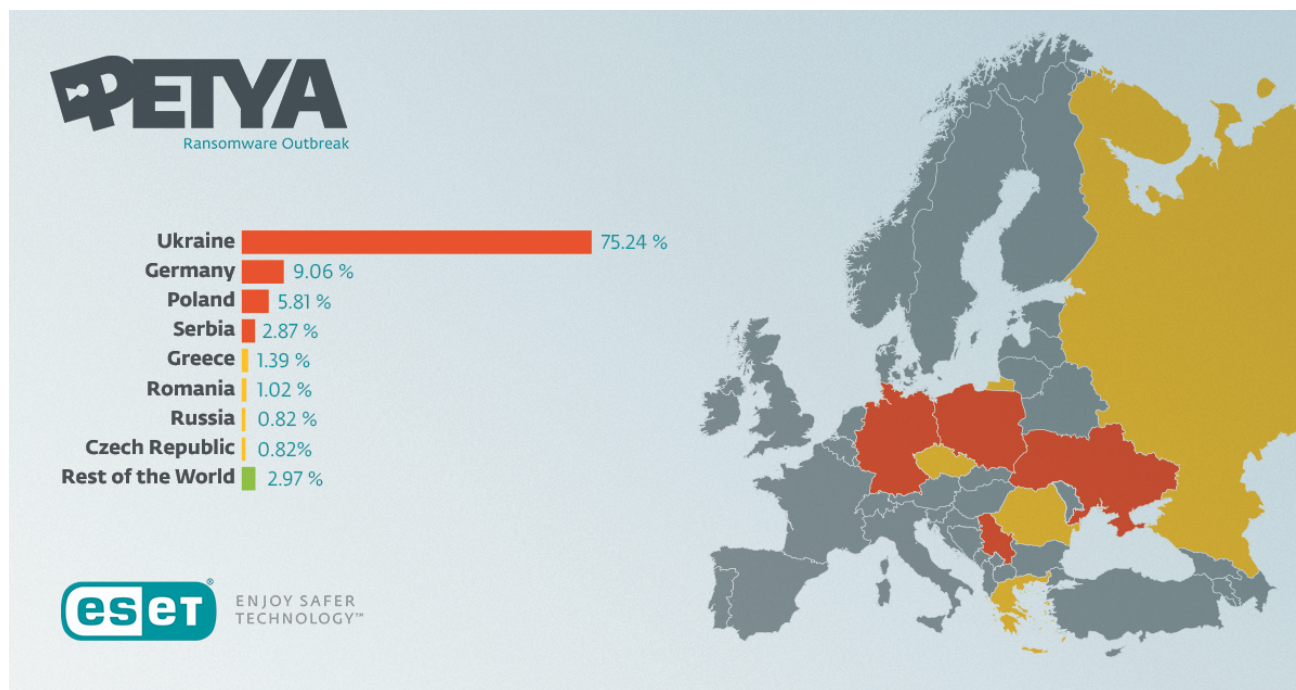
Update (June 27 – 22.28 CEST): Paying is no longer possible as the email to send the Bitcoin wallet ID and “personal installation key” has been shut down by the provider. Thus, people shouldn't pay for the ransom as they will not be able to receive the decryption key.

Update (June 27 – 21.20 CEST): ESET researchers have located the point from which this global epidemic has all started. Attackers have successfully compromised the accounting software M.E.Doc, popular across various industries in Ukraine, including financial institutions. Several of them executed a trojanized update of M.E.Doc, which allowed attackers to launch the massive ransomware campaign today which spread across the whole country and the rest of the world. M.E.Doc has today released a warning on its website.

Numerous reports are coming out on social media about a new ransomware attack in Ukraine, which could be related to the Petya family (subsequently being referred to as NotPetya and ExPetya, due to its particularly unique characteristics), which is currently detected by ESET as *Win32/Diskcoder.C Trojan*. If it successfully infects the MBR, it will encrypt the whole drive itself. Otherwise, it encrypts all files, like Mischa.

For spreading, it appears to be using a combination of the SMB exploit (EternalBlue) used by WannaCryptor for getting inside the network, then spreading through PsExec for spreading within the network.

This dangerous combination may be the reason why this outbreak has spread globally and rapidly, even after the previous outbreaks have generated media headlines and hopefully most vulnerabilities have been patched. It only takes one unpatched computer to get inside the network, and the malware can get administrator rights and spread to other computers.

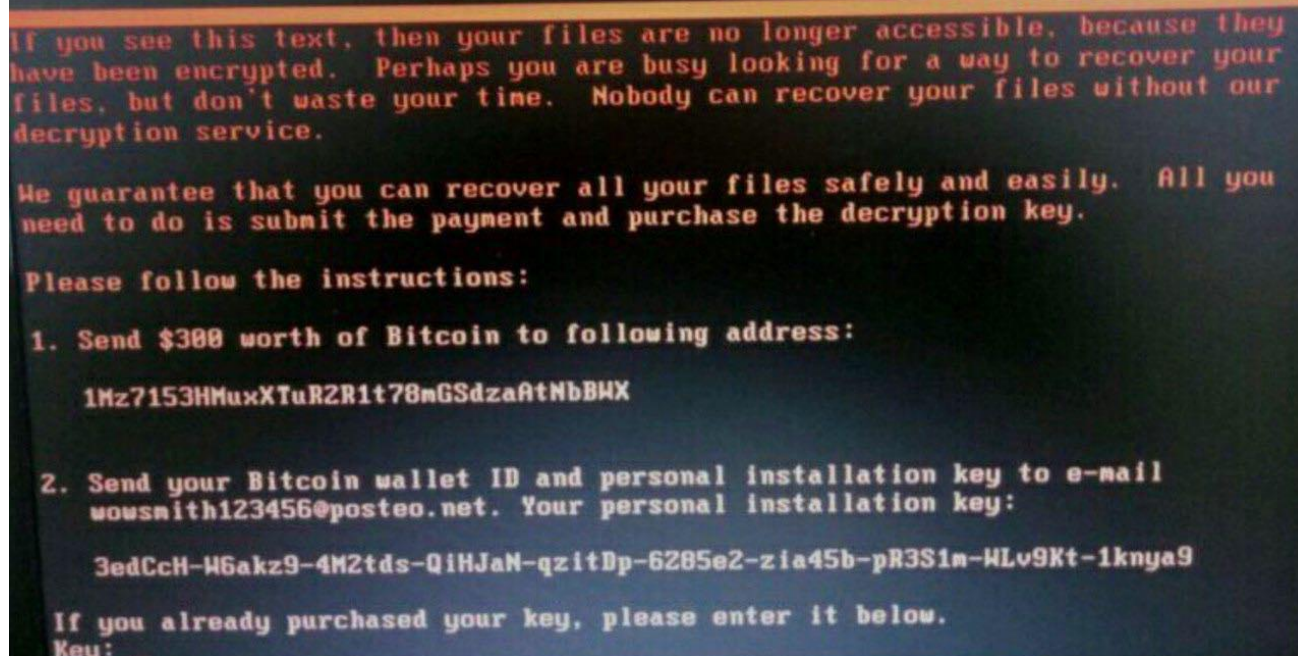


The journalist Christian Borys, for example, tweeted that the cyberattack has “allegedly hit” banks, power grid and postal companies, among others. Moreover, it appears that the government has also come under attack. Borys has also tweeted an image put up on Facebook by Ukraine’s deputy prime minister, Pavlo Rozenko, which shows a computer apparently being encrypted.

The National Bank of Ukraine has also put out a message on its website warning other banks of the ransomware attack.

It stated: “Currently, the financial sector strengthened security measures and counter hacker attacks all financial market participants.”

Forbes said that while there appear to be similarities with WannaCryptor – with others describing it as WannaCry-esque – it is likely to be a variant of Petya.

A screenshot of a ransomware message displayed in a terminal window. The text is in a red, monospaced font on a dark background. The message reads: "If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service. We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key. Please follow the instructions: 1. Send \$300 worth of Bitcoin to following address: 1Hz7153HMuxXTuR2R1t78mGSdzaAtNbBX 2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key: 3edCch-W6akz9-4M2tds-QiHJaN-qzItDp-6285e2-zia45b-pR3S1m-4Lv9Kt-1knya9 If you already purchased your key, please enter it below. Key:"/>

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:
1Hz7153HMuxXTuR2R1t78mGSdzaAtNbBX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
3edCch-W6akz9-4M2tds-QiHJaN-qzItDp-6285e2-zia45b-pR3S1m-4Lv9Kt-1knya9

If you already purchased your key, please enter it below.
Key:

An image, similar to the one witnessed by WannaCryptor victims, reportedly showing the ransomware message is making the rounds online, with one from [Group-IB](#) showing the following message (paraphrased):

“If you see this text, then your files are no longer accessible, because they have been encrypted ... We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment [\$300 bitcoins] and purchase the decryption key.”

However, a spokesman said that “there is no effect on power supplies”, although it may be too early to ascertain this.

It appears that the ransomware attack is not specific to Ukraine. The [Independent](#) said that Spain and India may also have been affected, as well as the Danish shipping company Maersk and the British advertising company WPP.



On the latter's homepage, the following message reads: "The WPP web site is currently unavailable due to important routine maintenance normal service will resume shortly.

"We apologise for any inconvenience this may cause. In the meantime if you would like to contact WPP, please email the site Editor at the following address ..."

WPP has since confirmed on [Twitter](#) that it has been the victim of an attack: "IT systems in several WPP companies have been affected by a suspected cyberattack. We are taking appropriate measures & will update asap."

There are also reports that payments are being made in response to the attack, at the BTC address linked [here](#).

For more on Petya, check out [this insightful piece](#) from 2016, which notes of the crypto-ransomware:

"Petya took an approach different from that of other crypto-ransomware. Instead of encrypting files individually, it aimed at the file system.

"The target is the victim's master boot record (MBR), which is responsible for loading the operating system right after system boot."

In order to prevent this kind of threat, we recommend that you read our [support article](#) and keep in mind the following steps:

1. Always have your systems fully patched
2. Use a proper [security solution](#)

3. Do not use the same account/credentials for workstations and server administration
4. Disable default ADMIN\$ or communication to admin shares – users can use ESET Smart Security for home and ESET Endpoint Security 6+ for business where network attack protection is present (Option: IDS and advanced options->allow incoming connections to admin shares in SMB)
5. Disable SMB1 when possible – issues with XP, 2003 that do not know SMB2+

This is currently a breaking story. Further updates to come, as listed above. For a snapshot of recent major ransomware attacks and what else to do, see the infographic below:

Protect Your Business from Ransomware

How not to fall victim to #WannaCryptor or #Petya



2017

Recent ransomware outbreaks which have infected **hundreds of thousands** of computers **in more than 150 countries** have proven that the year 2017 is the year of locked & lost data.



Malware is often spread via email or by drive-by downloads from compromised websites or even via software updates. After it encrypts all your precious data, the ransomware generates a pop-up message asking you to pay.

2017: The Year of Ransomware

#WANNA  CRYPTOR

Infected more than **230.000 computers** in **150 countries**.
Used the **Eternal Blue** vulnerability in unpatched systems.

#PETYA

The outbreak began in Ukraine.
Attackers used a compromised update of the **M.E.Doc accounting software** to spread the malware.

If you are tempted to pay the ransom, keep in mind that there is **NO GUARANTEE** your files will be returned to you or that the malware will be removed



HOW TO PROTECT YOURSELF

BEFORE YOU GET INFECTED...

- 1 **Back up** your company data.
- 2 Install **the latest security updates & patches**.
- 3 Use a reputable **business security software suite**.

IF YOU HAVE SUSPICIONS...

- 1 **Immediately turn off** the affected computer.
- 2 Try **System Restore**.
- 3 Set the **BIOS** clock back.
- 4 And – in particular – **DON'T PAY**.





Learn more about the **#Petya** outbreak on
[ESET.com/int/business/ransomware-attacks/](https://www.eset.com/int/business/ransomware-attacks/)



ENJOY SAFER
TECHNOLOGY™

27 Jun 2017 - 05:07PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion
