

*This post discusses active research regarding the Petya threat. Radware's ERT research team is conducting ongoing research of this evolving malware endemic. This is a preliminary report and will be updated accordingly.*

## Abstract

On June 27, 2017, a global ransomware campaign targeting computers around the world with a new ransomware variant referred to as NotPetya<sup>1 2</sup> (also in use - Nyetya, GoldenEye). This attack comes just one month after the WannaCry outbreak infected computers in over 100 countries. This campaign has already targeted several countries around the world, including Ukraine, Russia, Denmark, Spain, India, Germany, United Kingdom, United States and France. Those that were infected include individuals to large corporations like financial institutions, utility companies, an airport, media outlets, transportation and a hospital. Organizations that were struck include Ukrainian government institutions, Merck, Deutsche Post, Maersk, Rosneft, and others.

Despite the extortion demand, analysis of this new version of Petya appears to support the fact that it is designed to wipe out data on infected computers/networks, leaving it useless and inoperative. This Radware threat advisory provides an overview of the threat, how it operates, how it spreads, and mitigation measures.

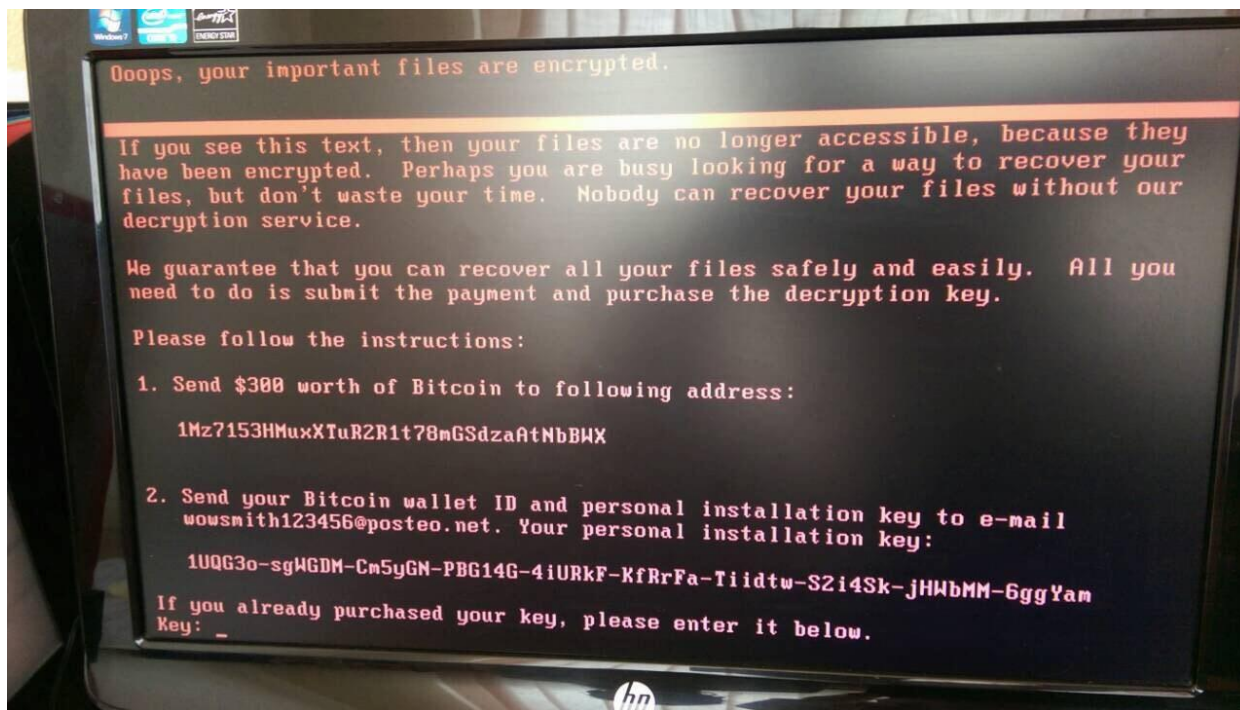


Figure 1: NotPetya infected computer – Source Hromadske.ua

## The Evolution of Petya Ransomware


In 2016, the ransomware programs Petya and Mischa emerged as part of an ongoing Darknet trend: ransomware affiliate programs. Its creators – allegedly a group who go by the name “Janus Syndicate” - offered their Ransomware-as-a-Service (RWaaS) on a Tor Hidden Service. It was created for the purpose of ransom attacks.

## Operation Mode

<sup>1</sup> <https://virustotal.com/fr/file/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745/analysis/>

<sup>2</sup> <https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmentId=100>

Petya was different from other ransomware variants because the malware did not target files on a victim's computer but instead targeted the Master File Tree tables (MFT) and the Master Boot Record (MRB) with a custom bootloader. The bootloader displayed a ransom note and prevented the system from ultimately booting. After security researchers published a way to recover files from Petya, a new variant appeared, referred to as "GoldenEye." This variant included an additional payload, Mischa. Mischa is a backup payload in the event Petya cannot gain administrative privileges and access the Master Boot Record. In this case, Mischa is deployed to encrypt files on the system (see Figure 2).

 **x0rz**  
@x0rz Follow

Petya was known to be RaaS (Ransomware-as-a-Service), selling on Tor hidden services. Looks like WannaCry copycat. Attribution will be hard.

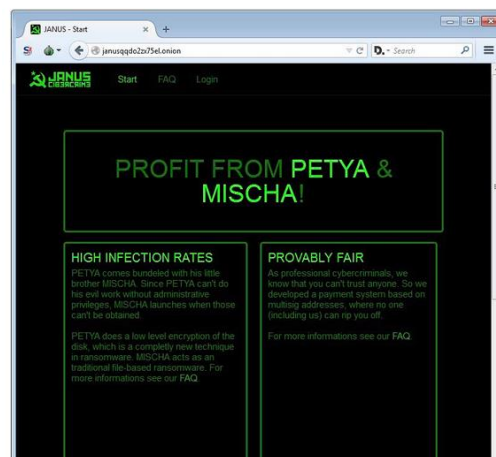


Figure 2: Petya & Mischa RWaaS on the Darknet

File types Mischa can encrypt:

.3ds .7z .accdb .ai .asp .aspx .avhd .back .bak .c .cfg .conf .cpp .cs .ctl .dbf .disk .djvu .doc .docx .dwg .eml .fdb .gz .h .hdd .kdbx .mail .mdb .msg .nrg .ora .ost .ova .ovf .pdf .php .pmf .ppt .pptx .pst .pvi .py .pyc .rar .rtf .sln .s ql .tar .vbox .vbs .vcb .vdi .vfd .vmc .vmdk .vmsd .vmx .vsdx .vsv .work .xls .xlsx .xvd .zip.

In the current attack, the new Petya variant (NotPetya/Nyetya<sup>3</sup>) is being used to control the reboot and the files for ransom purposes. To propagate, it leverages a spreading mechanism which is similar to what we saw during the WannaCry outbreak.

### Propagation

It has three different ways of propagating and moving laterally across networks once a machine is infected. The malware scans for vulnerable machines in the LAN and uses the EternalBlue exploit as well as Windows administration components such as Psexec and WMI to infect other devices in the network. NotPetya shares code with Mimikatz<sup>4</sup> and features a password-harvesting tool that gathers credentials from infected machines. It then hands off the credentials to Psexec and WMI and attempts to infect other machines in the network. For efficient propagation, NotPetya also leverages EternalBlue to infect systems that have not patched Microsoft's security update, MS17-010. Unlike WannaCry, NotPetya does not appear to have an external scanning element.

<sup>3</sup> <http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html>

<sup>4</sup> <https://twitter.com/omri9741/status/879786056966709248>



Figure 3: NotPetya appears to be sharing code with mimikatz

### Origin

Some reports suggest that the ransomware campaign may have originated from a malicious software update from MeDoc<sup>5</sup>. MeDoc is a popular accounting & workflow software from the Ukraine. MeDoc denies that they were the cause of the attack<sup>6</sup>.



Figures 4 & 5: Ukrainian police statements regarding MeDoc

This hypothesis, however, does not explain how Petya got into the networks of corporations in Western Europe and the United States. Others believe the Janus group may be behind this campaign and driven by financial gain. On the contrary, some speculate that the attack was not financially motivated, pointing at the relatively poor payment process, only one hardcoded BTC wallet, no command and control server, and a single point of contact via a public email that was eventually blocked by the host. These facts, combined with analysis of the

<sup>5</sup> <https://www.bleepingcomputer.com/news/security/petya-ransomware-outbreak-originated-in-ukraine-via-tainted-accounting-software/>

<sup>6</sup> <https://www.facebook.com/medoc.ua/posts/1904044929883085>

campaign, underscores the belief that this campaign was not financially motivated, but was intended to cause as much damage as possible by corrupting data and preventing access to information.

### Results

In this campaign, victims who are infected are instructed to make a payment of \$300 to a hardcoded BTC wallet found in the ransom note. The victim is expected to email the attacker with the transaction ID of the payment to receive their decryption key. The service provider Posteo<sup>7</sup> ultimately shut down the email address displayed in the ransom note, [wowsmith123456@posteo.net](mailto:wowsmith123456@posteo.net). Shutting down this email address makes it impossible to communicate with the authors or attempt to make a payment in exchange for the decryption keys if possible. There was only one Bitcoin address associated with this campaign, [1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX](https://blockchain.info/address/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX)<sup>8</sup>. At the time of writing there have been thirty payments received totaling \$7,705.

### What's Expected Next

Extortion is not new to humanity, and the cyber space is fertile grounds for it to prosper. The frequency of ransom attacks doubled the past year, but 2016 was the year where it became the primary motivation of cyber-attacks, particularly in Europe. In 2016, 49% of organizations reported having suffered either a ransomware infection or a DDoS threat for ransom, according to Radware's [2016-2017 Global Application & Network Security Report](#).

It is likely that as this trend continues, hackers will continue to customize new delivery methods for ransomware and more permutations will appear. It was just over a month ago when the WannaCry outbreak began leveraging the EternalBlue exploit.

### Recommended Precautions

1. Do not pay ransom!
2. Use backups for quick restoration
3. Patch Microsoft CVE's [MS-17-010](#)
4. Update AV and IPS malware signatures
5. Block port 445 for external communication
6. Implement private vLANs in your network switch so internal traffic only goes from endpoints to the servers (and back), and not between endpoints.

### Under Attack and in Need of Expert Emergency Assistance? Radware Can Help.

Radware offers a service to help respond to security emergencies, neutralize the risk and better safeguard operations before irreparable damages occur. If you're under DDoS attack or malware outbreak and in need of emergency assistance, [Contact us](#) with the code "Red Button".

### Learn More at DDoS Warriors

To know more about today's attack vector landscape, understand the business impact of cyber-attacks or learn more about emerging attack types and tools visit [DDoSWarriors.com](#). Created by Radware's [Emergency Response Team \(ERT\)](#), it is the ultimate resource for everything security professionals need to know about DDoS attacks and cyber security.

<sup>7</sup> <https://posteo.de/blog/info-zur-ransomware-petrwrappetya-betroffenes-postfach-bereits-seit-mittag-gesperrt>

<sup>8</sup> <https://blockchain.info/address/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX>