“Petya” Ransomware Attack

Technical intelligence analysis
June 2017

Executive summary

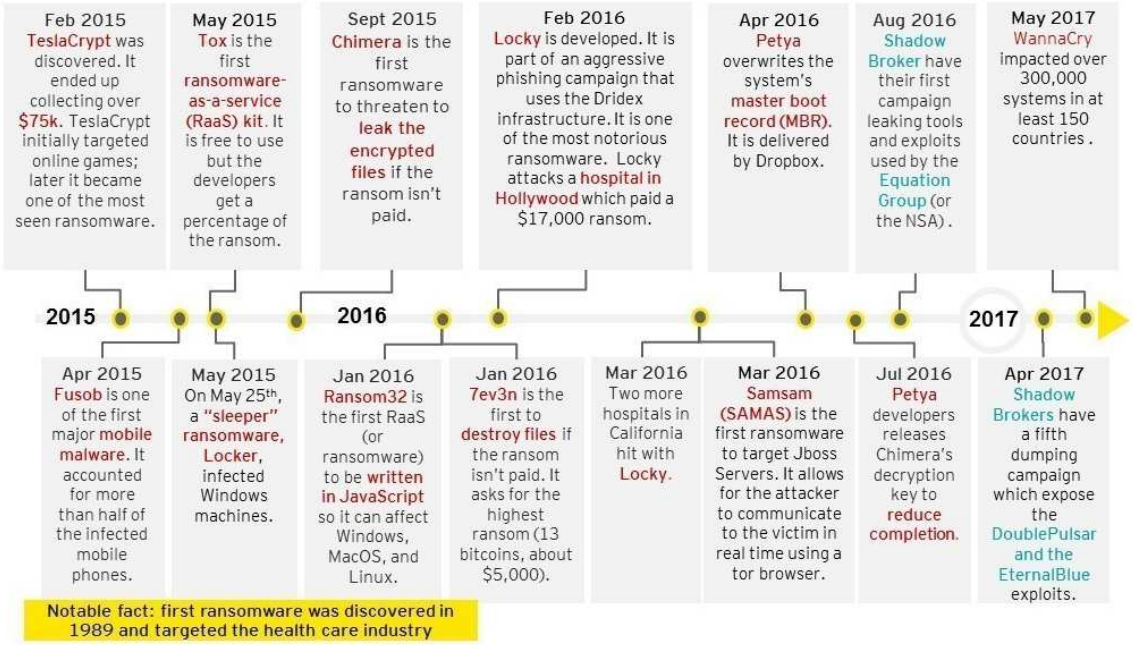
On 27 June 2017, a global ransomware attack campaign called Petya (also being called "NotPetya", and "Petna") impacted companies across a wide range of sectors including financial services, power and utilities, media, telecom, life sciences, transportation as well as government agencies.

While organizations in countries around the world were affected - including the United States, Netherlands, France, India, Spain and Russia - Ukraine seems to have been the first and hardest country hit by the attack due to the use of an auto-update feature of M.E.Doc software required for tax calculation by any company operating in the Ukraine. The ransomware successfully infected several of its banks as well as media outlets, energy companies, government agencies, airports and radiation monitoring equipment within the Chernobyl power plant.

It is the second major ransomware event in as many months after the WannaCry outbreak in May 2017. Although initially characterized as very similar to that attack, Petya is notably different, particularly in the way it spreads and encrypts victims' data. While WannaCry relied on its worm-like behavior to spread across the Internet, Petya was less virulent, and spread internally using a number of lateral movement techniques including the SMB vulnerability and credential harvesting. Once inside the network, Petya is more sophisticated and nefarious than WannaCry. It subsequently leverages several additional hacking tools to gather credentials from the infected computer's memory, before spreading to other machines using legitimate and well-known Windows system administration tools such as PsExec and WMIC. It does this for about an hour before rebooting and encrypting the system and/or the files.

Finally, researchers are having moderate success with what they are calling a "vaccine" where placing a file in the Windows directory (C:\Windows\perfc.dat) has had moderate success in causing the malware to stop executing.

Recap of notable ransomware events



Overview of Petya

Petya is a type of ransomware, or extortive malware that encrypts files, disks, and locks computers. The malware demands a ransom of $300 to be paid to a bitcoin account in return for decrypting the files.

Petya is initially delivered with a tax software update. Petya spreads internally via SMB, the Server Message Block protocol operating over ports 445 and 139, typically used by Windows machines to communicate with file systems over a network. This ransomware scans for and propagates to other at-risk devices. Both DoublePulsar and the EternalBlue exploit the SMB vulnerability that was made public by the Shadows Brokers hacking group in April. If Petya finds that the computers on the network have applied the MS17-010 patch, it will laterally move using harvested credentials and PsExec and WMIC.

Researchers have found a work-around to prevent Petya from installing. Create a file called perfc.dat in the C:\Windows folder and make it read only. This is believed to work, because it indicates to Petya that is was already installed on this system at one point (most ransomware authors try to only infect each system once, so victims only need to pay once). The security vendor Malwarebytes' researcher verified that this method could potentially work to stop the infection, although their tests have shown that in many cases, it does not. Windows 10 systems seemed to have moderate success tests against Windows 7 consistently resulted in infections. Further details are in Appendix III.

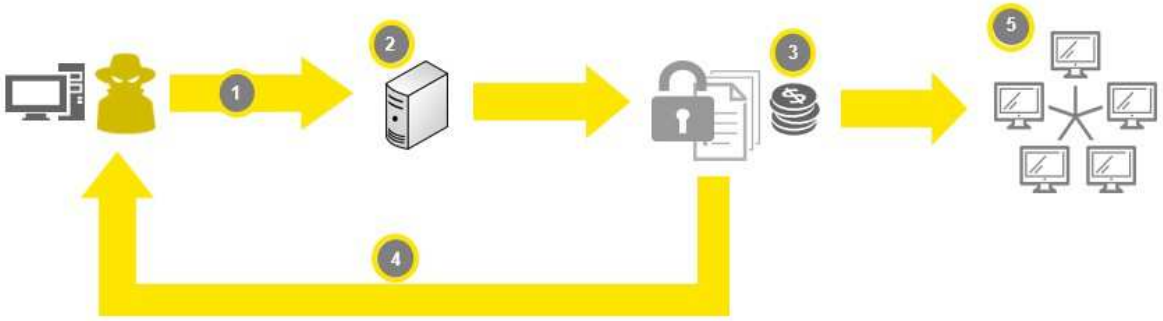


Figure 1 Petya Lifecycle

1. The attacker uses M.E.Doc software update as the initial attack vector. Further explained in Figure 2.
2. Installs Petya ransomware and possibly other payloads
3. Petya uses a two-layer encryption model that encrypts target files on the computer and encrypts NTFS structures, if it has admin privileges. If not, it just encrypts the files. It also collects passwords and credentials.
4. The ransom note includes a bitcoin wallet f where to send $300. It also includes the email, wowsmith123456@posteo[.]net, to send a bitcoin wallet number and a unique identifier number the ransom note lists. As of 27th of June the email hosting company has suspended this account thus it is recommended not to pay the ransom because victims will not be able to reach the attackers.

5. Petya spreads on the network using EternalBlue (MS17-010), the SMB based exploit released by the group Shadow Brokers. If the computers on the network are patched, the infected PC uses WMIC and PsExec with the locally available credentials.

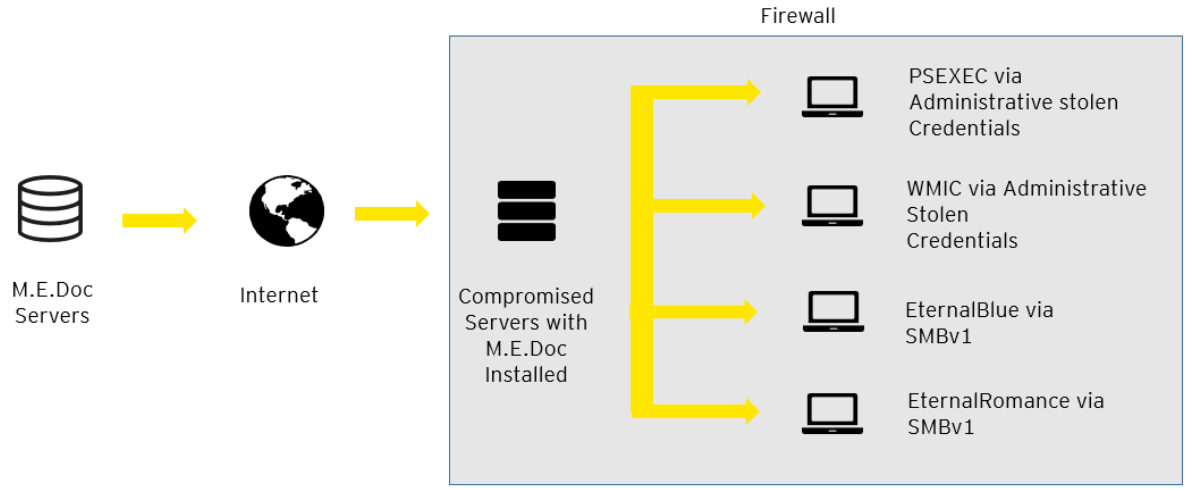


Figure 2. Initial Attack Vector

Global impact of Petya

There are approximately 20-30 publicly named companies among the likely thousands that were impacted by this ransomware.

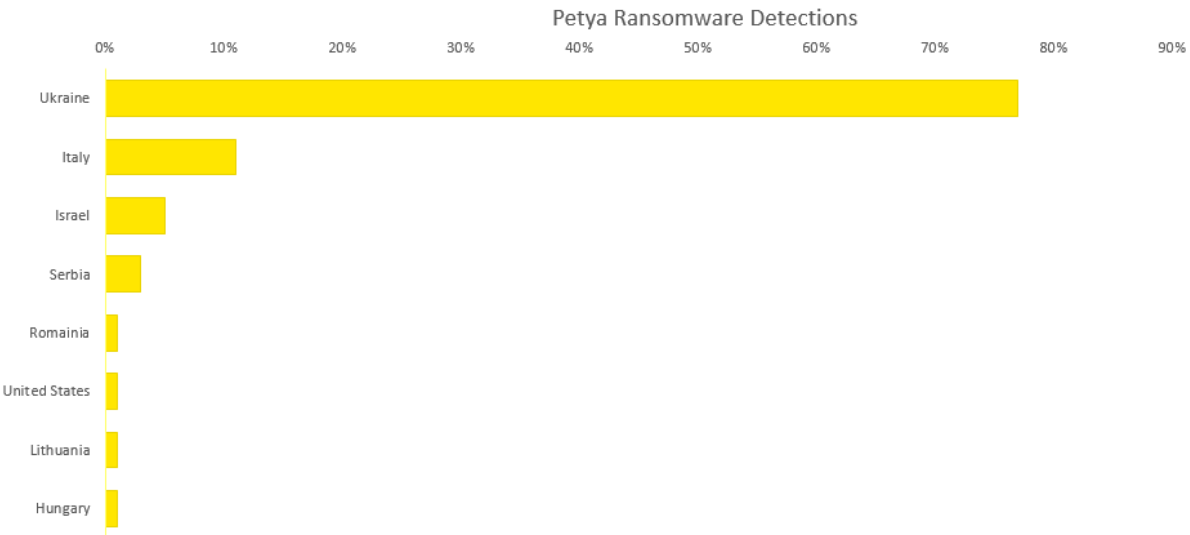


Figure 3. Petya Detection Rates according to ESET

Ukraine appears to be the heaviest hit by the Petya attack. This is because the initial attack vector used a Ukrainian tax software update as its vehicle. Since any company that does business in Ukraine must use this software, in theory, every Ukrainian business was affected.

Risk mitigation consideration

Organizations can mitigate their risk exposure by considering the following actions:

- Ensure that vulnerability management (including patch management and vulnerability scanning/remediation) is properly prioritized and is a mature, enterprise-level program
- Maintain backups that account for critical data and the rate of data generation
  - Align timeline and procedures for restoring system backups with your business continuity plan (BCP)
  - Review and test incident response and disaster preparedness plans to verify that they adequately address recovery from a ransomware event
- Implement endpoint monitoring, giving teams visibility into malicious behavior occurring at that level
- Properly apply network segregation to reduce the effects of lateral movement by malware
- Ensure that the organization has a comprehensive security awareness training program in place
- Maintain an effective enterprise incident response plan that is regularly tested and measured for effectiveness against ransomware, as well as regularly updated to reflect the current cyber threat environment
- Confirm that critical systems are not unnecessarily connected to/accessible from the internet
- Recommend the implementation of strong governance controls in terms of assessing the security and risk management maturity of third party vendors - at the beginning of an engagement, and then at subsequent periodic intervals.

How Petya works and why it was so successful

The initial vector of delivery for this malware was believed to be from the M.E.Doc software update. M.E.Doc is a Ukrainian tax software used by any country that does business in Ukraine. The malware was able to infect many systems because it was digitally signed and came with a legitimate looking software update. Once the system was infected, Petya used a two-layer encryption scheme. Firstly, it encrypts targeted files like other previous ransomware. Then if the ransomware can get system administrator privileges it encrypts MFT (Master File Tree) tables for NTFS partitions, which makes they file system unusable. If the ransomware does not have system administrator privileges, it will only do the normal first layer of encryption. This two layer model, makes it especially hard to try to decrypt without the ransomed key. Petya also overwrites the MBR (Master Boot Record) with a custom bootloader that shows a ransom note, shown in Figure 4, and prevents victims from booting their computer. Figure 5 is the screen shown when it is encrypting, so if it is seen shut down the computer.

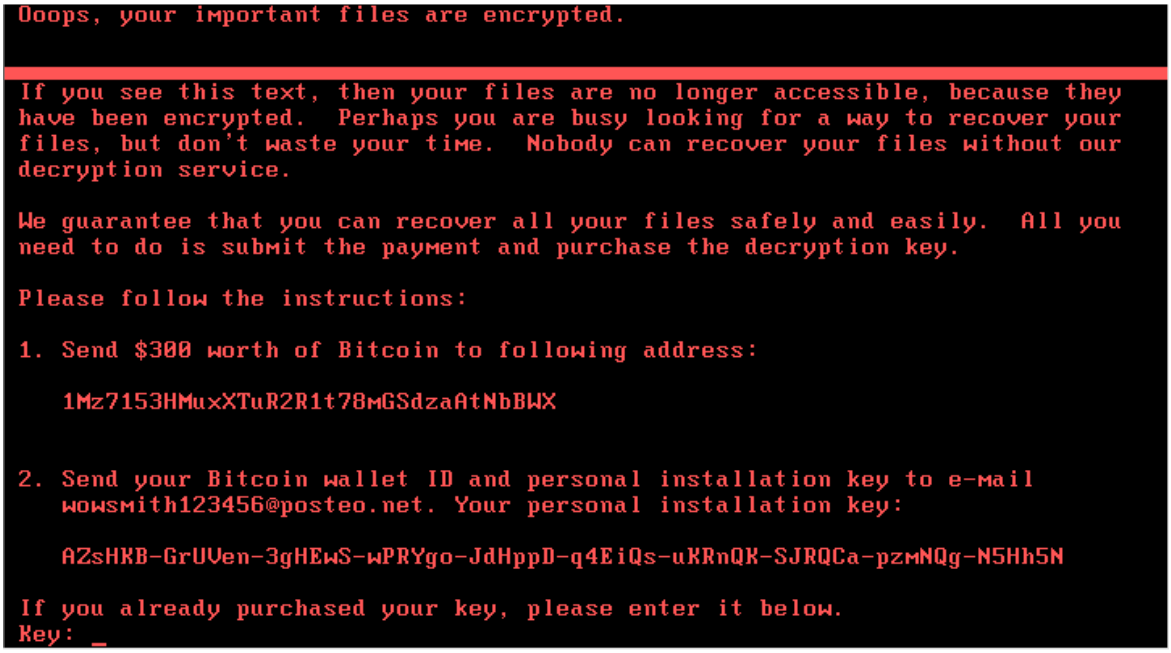


Figure 4. Petya Ransom Note

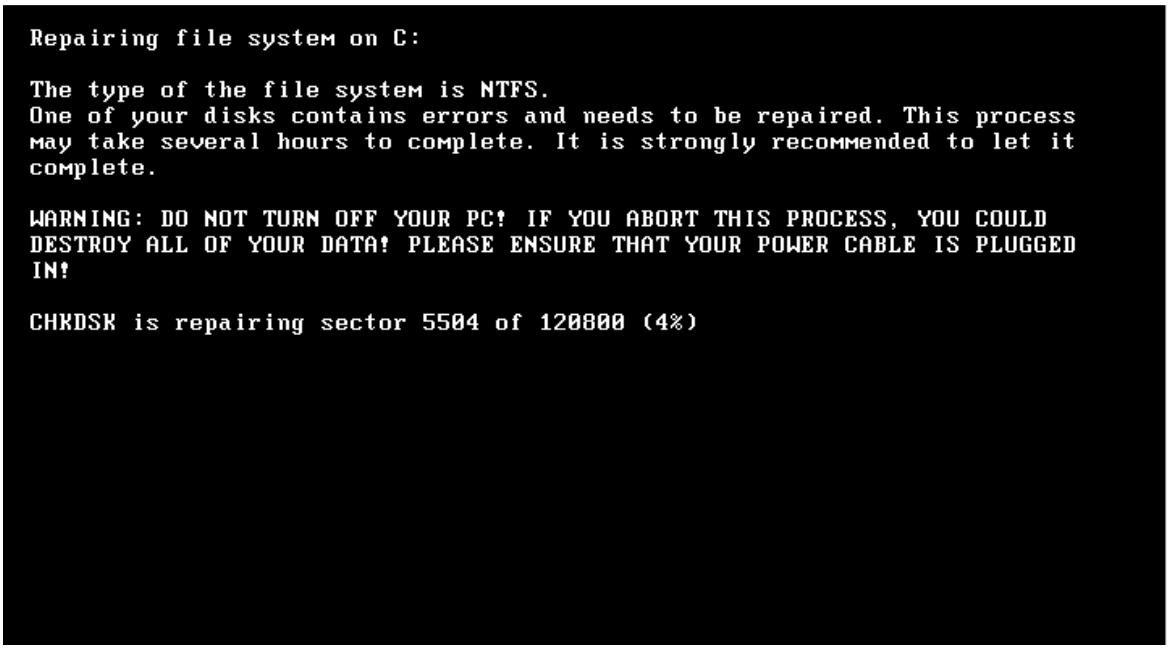


Figure 5. Petya Encryption Screen

The ransom note only uses one bitcoin address. But the author asks victims to email their bitcoin addresses and unique identifier included in the note, so the attacker knows who paid and sends the right decryption key. Unfortunately, for both the attacker and victims, the email provider has suspended the attacker's email account so currently there are no publicly known ways to get the decryption key.

When Petya installs it bundles a tool called "LSADump," which can gather passwords and credential data from Windows computers and domain controllers on the network. Petya propagates laterally using three methods. First, it tries using the exploit EternalBlue. If the machines on the network have the patch applied, it uses the stolen credentials to use PsExec and WMIC to infect new computers on the network. It first send a broad cast to the local network than it tried to connect to all the IPs on the infected machines subnet on ports 139 and 445.

What we expect next

CTI expects to see further variants and copycats of Petya without the kill switch.

Over the coming days and weeks, we anticipate that cyber criminals will release malware variants that leverage other and newer exploits, especially once more organizations patch systems to prevent EternalBlue. We expect that there could be more weaponization of the Equation Group's exploits that were leaked by Shadow Brokers.

We also expect that cyber criminals will try to copy the highly-effective worm-like propagation techniques of Petya and WannaCry, creating malware that can move laterally within an infected system without the need for human intervention.

CTI expects to see more supply chain based attacks. In order to prevent this type of attack, an active defense and considerable review of network hygiene is necessary. Verification and increased security in third party vendors is vital.

On a positive note, every wide-scale attack reinforces the importance of cyber security and the reality that cyberattacks are a major business risk. Hopefully, a result from this attack will result in practicing better computing and security processes, as well as understanding and effectively prioritizing remediation efforts.

Appendix I: What you can do about Petya and general ransomware?

If you notice the screen shown in Figure 4 or 5 on your computer, then you are possibly a victim of this ransomware. Following the steps below immediately can help to reduce the impact.

- Disconnect all network connections and external storage immediately
- Shut down the computer and inform your IT teams
- Do not pay any ransom to the hacker, as this fuels the illegal ecosystem and there is no guarantee that you will get the data back
- Safeguard and keep your backups ready before experts assist you

Company-level recommendations:

- A kill switch has been discovered by PT Security, create file "C:\Windows\perfc.dat" to stop the ransomware from executing – this is a preliminary recommendation
- Block SMB port access and RDP (Remote Desktop Protocol) to all computers from the internet; Port 445 and 139 for SMB and 3389 for RDP should be blocked
- Block SMB for the time being within the company through a group policy or other endpoint security solution
- Stop granting any privilege escalation requests to users who want to run an unknown program as an administrator
- Ensure that all Windows OS and Microsoft software are patched, especially the MS17-010; any unsupported or outdated operating systems should either be upgraded or reconfigured to stop SMB and RDP
- Issue a notice to all employees to not open unknown attachments and emails; if in doubt, they should read emails on their mobile devices without opening the attachments
- Disable office macros through a group policy
- Enable scanning of all attachments at your endpoints and email gateways; see a list of file hashes and IP addresses to block and observe at the end of this advisory
- Disable uPNP on all your gateways, firewalls, routers and proxy servers
- Maintain backups that account for critical data and the rate of data generation
  - Align timeline and procedures for restoring system backups with your business continuity plan (BCP)
  - Review the organization's incident response and disaster preparedness plans to verify that they adequately address recovery from a ransomware event
- Endpoint monitoring: tools that give a team visibility into the behavior occurring on the endpoint are tremendously useful in combating ransomware
  - Antivirus tools lag behind in detection of ransomware due to their nature
  - Endpoint monitoring solutions allow visibility into processes and network traffic running on endpoints
  - Endpoint monitoring solutions can block rogue processes pending further verification
- Email filtering: Filtering extensions in email will stop a lot of malware attacks in its tracks
  - Recommend blocking executable and zip file attachments, and filtering all other attachments for manual review
  - It is safer to block attachments and use a secure transfer option than to allow attachments that may harbor malicious software
- Security awareness training: In the long run, it doesn't matter what tools are implemented if a user is actively clicking on malicious attachments or taking actions that violate the acceptable use policy for a network
  - Security awareness training is an effective method of reducing the susceptibility of people to ransomware campaigns

- Maintain an effective enterprise incident response plan that is tested and measured for effectiveness against ransomware, as well as updated to reflect the current cyber threat environment
  - Confirm critical systems are not unnecessarily connected to/accessible from internet
- Ensure vulnerability management is a robust and mature enterprise-level program

Employee recommendations:

- If your computer reboots and you see the image on Figure 4 on your screen its high recommended that you power off your computer immediately.
- Disconnect from the internet and take a backup of all your data on an encrypted, removable hard drive; disconnect the hard drive and keep it at a secure location after the backup is completed
- Do not open attachments from unknown sources, and do not download or open unauthorized software
- Do not check your personal email on a company computer, as most free email services will not have advanced security scanning of attachments
- If you suspect any unusual hard drive activity on your computer, immediately shut it down and notify your IT administrator
- Do not enable macros on office documents

IT administrator recommendations:

- Disconnect all network shares from idle computers and servers or use a share software to decrease this risk
- Recheck network shares with write permissions
- Periodically scan network shares with security solutions
- Change passwords of and safeguard all common domain administrator accounts; refrain from logging in using these accounts; and use these accounts to only authorize specific actions as per standard operating procedures
- Make sure backup solutions provide write access to only accounts that are hard configured in the backup solution
- User accounts should only have read access
- Enable volume shadow copy if possible through group policy and enforce it
- Update the endpoint security solution and enable anti-malware or anti-ransomware modules
- Prevent privilege escalation of unknown programs and processes
- Create a manual signature on your endpoint security solution and monitor for file hashes and extensions specific in this advisory; in case of any such findings on a user computer, disconnect it from the network and shut it down

Read about more recommendations here.

Appendix II: Indicator of compromise (IOCs) for Petya

Hashes

0df7179693755b810403a972f4466afb
42b2ff216d14c2c8387c8eabfb1ab7d0
71b6a493388e7d0b40c83ce903bc6b04
e285b6ce047015943e685e6638bd837e
e595c02185d8e12be347915865270cca
a809a63bc5e31670ff117d838522dec433f74bee
bec678164cedea578a7aff4589018fa41551c27f
d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
aba7aa41057c8a6b184ba5776c20f7e8fc97c657
0ff07caedad54c9b65e5873ac2d81b3126754aac
51eafbb626103765d3aedfd098b94d0e77de1196
078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
7ca37b86f4acc702f108449c391dd2485b5ca18c
2bc182f04b935c7e358ed9c9e6df09ae6af47168
1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
82920a2ad0138a2a8efc744ae5849c6dde6b435d
415FE69BF32634CA98FA07633F4118E1
101CC1CB56C407D5B9149F2C3B8523350D23BA84
FE2E5D0543B4C8769E401EC216D78A5A3547DFD426FD47E097DF04A5F7D6D206
0487382A4DAF8EB9660F1C67E30F8B25
736752744122A0B5EE4B95DDAD634DD225DC0F73
EE29B9C01318A1E23836B949942DB14D4811246FDAE2F41DF9F0DCD922C63BC6
A1D5895F85751DFE67D19CCCB51B051A
9288FB8E96D419586FC8C595DD95353D48E8A060
17DACEDB6F0379A65160D73C0AE3AA1F03465AE75CB6AE754C7DCB3017AF1FBD
027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1
f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5
02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f
eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998

IPs

84.200.16.242
111.90.139.247
185.165.29.78

File names

Order-20062017.doc
myguy.xls
BCA9D6.exe

Targeted extensions

.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, .sin, .sql, .tar, .vbox, .vbs, .vcb, .vdi, .vfd, .vmc, .vmdk, .vmsd, .vmx, .vsdx, .vsv, .work, .xls, .xslx, .xvd, .zip

Appendix III: Petya 'Vaccine'

Different researchers have discovered that the ransomware can be stopped from executing by having the following files as read-only on the operating system folder under "c:\windows".
c:\windows\perfc
c:\windows\perfc.dll
c:\windows\perfc.dat

The Security Vendor Malwarebytes' researcher verified that" Petya has a "vaccine" that could potentially work to stop the infection, although their tests have shown that in many cases, it does not. Windows 10 systems seem to have a fighting chance by using this method but based on their tests, Windows 7 gets infected every time.

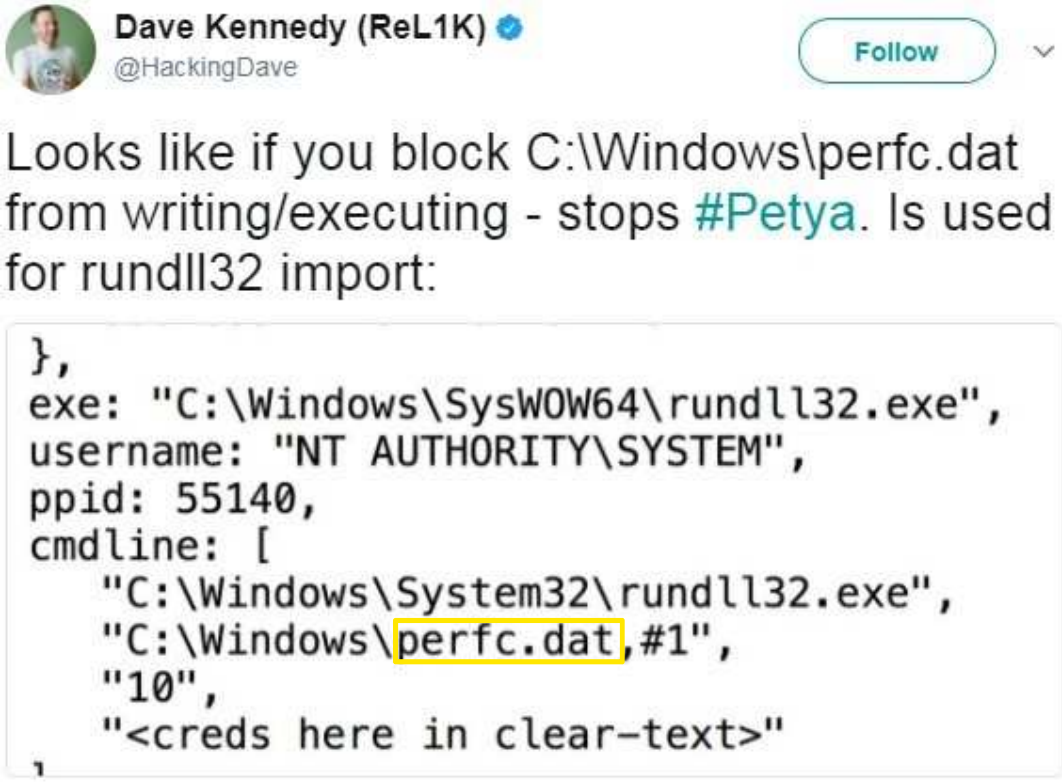


Figure 6. Twitter screenshot Dave Kennedy

perfc

Figure 7. Twitter screenshot PT Security

Appendix IV: Sourcing

- *Bleeping Computers*, https://www.bleepingcomputer.com/news/security/wannacry-d-j-vu-petya-ransomware-outbreak-wreaking-havoc-across-the-globe, accessed 27 June 2017
- *The Hacker News*, http://thehackernews.com/2017/06/petya-ransomware-attack.html, accessed 27 June 2017
- *Bleeping Computers, https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak, accessed 27 June 2017*
- *Krebs on Security*, https://krebsonsecurity.com/2017/06/petya-ransomware-outbreak-goes-global, accessed 27 June 2017
- *GitHub,* https://gist.github.com/vulnersCom/65fe44d27d29d7a5de4c176baba45759, accessed 27 June 2017
- *McAfee*, https://securingtomorrow.mcafee.com/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire, accessed 28 June 2017
- *We Live Security*, https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine, accessed 28 June 2017

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no.
ED None

ey.com/cybersecurity
ey.com/ransomware