ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

Petya Ransomware

Compiled by ThaiCERT, a member of the Electronic Transactions Development Agency

Version 0.3 (28 June 2017)

TLP:WHITE

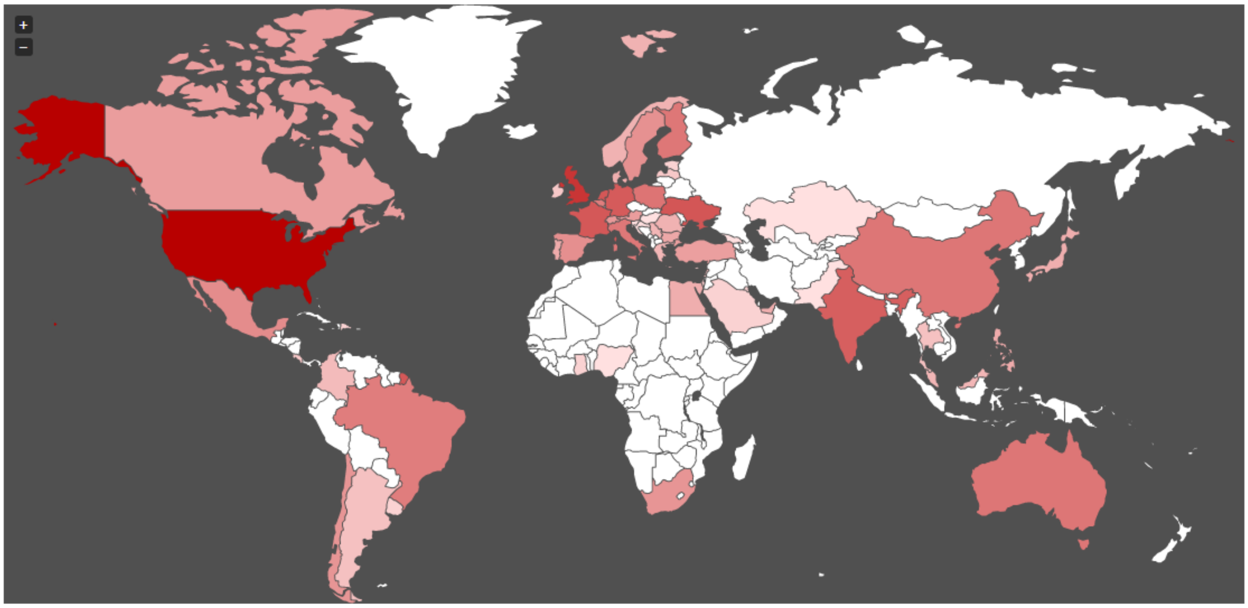

Figure 1: McAfee

Contents

Malware names

Petya, Petna, PetrWrap, NotPetya

Management summary

New Ransomware started spreading in the Ukraine on 27 June. Soon after, it spread worldwide.
This Ransomware uses the same mechanism to spread as WannaCry. As such, much of the same advice as given during the WannaCry outbreak can be given.
It also leverages the fact that many people (often needlessly) run their systems under accounts with admin privileges.

Vulnerable systems

Windows XP through 10.

Microsoft released a patch MS17-010 (ETERNALBLUE and ETERNALROMANCE) on 14 March:
<https://technet.microsoft.com/en-us/library/security/ms17-010.aspx>
Microsoft released a patch for the older unsupported Windows versions on 12 May:
<https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/>

Prevention

- Patch your systems
- Make backups
- Do not expose the SMB protocol to the outside world. Block TCP/445[1].
- The SMB spreading vulnerability can also be closed by completely disabling SMBv1 support. See <https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1,-smbv2,-and-smbv3-in-windows-vista,-windows-server-2008,-windows-7,-windows-server-2008-r2,-windows-8,-and-windows-server-2012>
- Try not to run your systems with admin privileges until needed.

Recovery

- You can recover from backups, and if those do not exist, try a program like Shadow Explorer in the hopes that the ransomware did not properly delete your Shadow Volume Copies. If a user did not click Yes at the UAC prompt, then there is a chance those are still available to recover from. A guide on recovery files from Shadow Volume Copies can be found at <https://www.bleepingcomputer.com/tutorials/how-to-recover-files-and-folders-using-shadow-volume-copies/>
- If the computer is shut down before the reload, MBR can be reestablished with "bootrec /FixMbr" command. (in Vista+, for Windows XP "fixmbr" can be used).
- Paying the ransom will **not** get your files back.

[1] It is Good Practice to filter all NetBIOS traffic (TCP/137, TCP/139, TCP/445, UDP/137 and UDP/138), but WannaCry only leverages port TCP/445.

IoCs

SHA256 hashes

`f8dbabdfa03068130c277ce49c60e35c029ff29d9e3c74c362521f3fb02670d5` (signed PSEXEC.EXE)

`64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1` (main 32-bit DLL)

`027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745` (main 32-bit DLL)

`02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f` (64-bit EXE)

`eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998` (32-bit EXE)

Files

- c:\windows\dllhost.dat
- c:\windows\<malware_dll> (no extension)
- %TEMP%\<random name>.tmp (EXE drop)

Other indicators

- PIPE name: \\.\pipe\{df458642-df8b-4131-b02d-32064a2f4c19}
- Scheduled task running “shutdown -r -n”

Spreading

Petya uses the following mechanisms to spread to additional hosts.

1. An attack against the update mechanism of a third-party Ukrainian accounting software product called M.E. Doc appears to have been the initial vector.
2. Petya scans the local /24 to discover enumerate ADMIN$ shares on other systems, then copies itself to those hosts and executes the malware using PSEXEC. This is only possible if the infected user has the rights to write files and execute them on system hosting the share.
3. Petya uses the Windows Management Instrumentation Command-line (WMIC) tool to connect to hosts on the local subnet and attempts to execute itself remotely on those hosts. It can use Mimikatz to extract credentials from the infected system and use them to execute itself on the targeted host.
4. Petya finally attempts to use the ETERNALBLUE and ETERNALROMANCE exploit tool against hosts on the local subnet. This will only be successful if the targeted host does not have the MS17-010 patches deployed.

Encryption

The encryption used by the malware is AES-128 with RSA. This is different from previous variants, which used SALSA20.

What will be encrypted depends on the privileges the malware has on the system:

- If admin rights are available, the malware will “only” encrypt the MBR and MFT.
- In case the privileges are not high enough to rewrite MBR, the files are encrypted without a system reload. The list of file types that are encrypted: 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, sql, tar, vbox, vbs, vcb, vdi, vfd, vmc, vmdk, vmsd, vmx, vsdx, vsv, work, xls, xlsx, xvd, zip.

Command and Control

Petya contains no Command and Control mechanisms that we know of. After a host is infected, there is no communication from the malware back to the attacker.

Kill switch

From <https://twitter.com/0xAmit/status/879789734469488642>:
Create a read-only file called perfc with no extension in %windir%

Bleeping Computer describes how this can be done manually:
<https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/>

Deployment can also be automated with Group Policy Preferences, as described by Edd Watton:
<https://eddwatton.wordpress.com/2017/06/27/use-group-policy-preferences-to-deploy-the-notpetya-vaccine/>

Ransom

The setup of the payment part of the malware suggests that the ransom was only added as theatre – not to make any money but to cause as much damage as possible instead:

- There is only 1 bitcoin address that is used at every infection. As such, the perpetrator will be unable to distinguish who paid.
- Communication about payments was setup with plain text e-mail to a single address. Usually this is done in a more anonymous and resilient fashion (TOR). The e-mail address was taken down by the ISP immediately, leaving potential payers without any means to communicate and thus without any means to get their files back.

Malware analysis sources

<https://securelist.com/schroedingers-petya/78870/>

<https://securingtomorrow.mcafee.com/mcafee-labs/new-variant-petya-ransomware-spreading-like-wildfire/>

<https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/>

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

<https://blog.malwarebytes.com/cybercrime/2017/06/petya-esque-ransomware-is-spreading-across-the-world/>

<https://researchcenter.paloaltonetworks.com/2017/06/unit42-threat-brief-petya-ransomware/>

<https://www.fireeye.com/blog/threat-research/2017/06/petya-ransomware-spreading-via-eternalblue-exploit.html>

<http://blog.trendmicro.com/trendlabs-security-intelligence/large-scale-ransomware-attack-progress-hits-europe-hard/>

<https://blogs.forcepoint.com/security-labs/d%C3%A9j%C3%A0-vu-petya-ransomware-appears-smb-propagation-capabilities>

<https://www.binarydefense.com/petya-ransomware-without-fluff/>

<https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/>

International advisories

<https://www.itnews.com.au/news/what-you-need-to-know-about-the-petya-notpetya-ransomware-466707>

<https://nakedsecurity.sophos.com/2017/06/27/breaking-news-what-we-know-about-the-global-ransomware-outbreak/>

<https://securityintelligence.com/petya-werent-expecting-this-ransomware-takes-systems-hostage-across-the-globe/>

<https://www.us-cert.gov/ncas/current-activity/2017/06/27/Multiple-Petya-Ransomware-Infections-Reported>

<https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know>

<https://www.auscert.org.au/bulletins/49286>

English news references

<https://www.nytimes.com/reuters/2017/06/27/business/27reuters-ukraine-cyber-attacks-ukrenergo.html>

<https://www.bleepingcomputer.com/news/security/wannacry-d-j-vu-petya-ransomware-outbreak-wreaking-havoc-across-the-globe/>

<https://www.anomali.com/blog/petya#When:15:17:00Z>

<https://www.arbornetworks.com/blog/asert/patching-not-enough-stop-petya/>

<http://blog.checkpoint.com/2017/06/27/global-ransomware-attack-spreading-fast/>

<http://www.csoonline.com/article/3203970/ransomware/petya-darwinism-applied-to-cyberspace.html>

<https://www.cyberscoop.com/petya-eternalblue-nsa-hacking-tool-ransomware/>

<https://www.cyberscoop.com/petya-ransomware-medoc-hacked-auto-update/>

<https://www.cyberscoop.com/massive-ransomware-outbreak-quickly-spreading-across-europe/>

<https://www.darkreading.com/attacks-breaches/petya-or-not-global-ransomware-outbreak-hits-europes-industrial-sector-thousands-more/d/d-id/1329231>

<https://blog.fortinet.com/2017/06/27/new-ransomware-follows-wannacry-exploits>

<https://www.helpnetsecurity.com/2017/06/27/petya-ransomware/>

<https://www.infosecurity-magazine.com/news/ukraine-businesses-petya-ransomware/>

<https://www.infosecurity-magazine.com/news/global-ransomware-attack-continues/>

<https://www.infosecurity-magazine.com/news/petya-ransomware-spreading-beyond/>

<https://www.itnews.com.au/news/massive-ransomware-outbreak-hits-servers-worldwide-466691>

<https://motherboard.vice.com/en_us/article/qv4gx5/a-ransomware-outbreak-is-infecting-computers-across-the-world-right-now>

<https://researchcenter.paloaltonetworks.com/2017/06/palo-alto-networks-protections-petya-ransomware/>
<http://www.reuters.com/article/us-cyber-attack-idUSKBN19I1TD?feedType=RSS&feedName=technologyNews>
<https://arstechnica.com/security/2017/06/a-new-ransomware-outbreak-similar-to-wcry-is-shutting-down-computers-worldwide/>
<http://securityaffairs.co/wordpress/60475/malware/petwrap-ransomware.html>
<http://news.softpedia.com/news/windows-pcs-under-attack-in-europe-pcs-at-chernobyl-nuclear-plant-infected-516696.shtml>
<http://thehackernews.com/2017/06/petya-ransomware-attack.html>
<https://www.theregister.co.uk/2017/06/27/ransomware_outbreak_hits_ukraine/>
<https://threatpost.com/complex-petya-like-ransomware-outbreak-worse-than-wannacry/126561/>
<https://threatpost.com/second-global-ransomware-outbreak-under-way/126549/>
<https://www.welivesecurity.com/2017/06/27/new-ransomware-attack-hits-ukraine/>
<http://www.zdnet.com/article/six-quick-facts-june-global-ransomware-cyberattack/>
<https://labs.bitdefender.com/2017/06/massive-goldeneye-ransomware-campaign-slams-worldwide-users/>
<https://twitter.com/kaspersky/status/879749175570817024>

E-mail shutdown

<https://www.bleepingcomputer.com/news/security/email-provider-shuts-down-petya-inbox-preventing-victims-from-recovering-files/>
<https://motherboard.vice.com/en_us/article/new8xw/hacker-behind-massive-ransomware-outbreak-cant-get-emails-from-victims-who-paid>