



Indian Computer Emergency Response Team

Ministry of Electronics and Information Technology
Government of India



CERT-In Advisory CIAD-2017-0033

Variants of Petya Ransomware spreading with EternalBlue

Original Issue Date: June 27, 2017

Description

It has been reported that variants of Petya ransomware with worm-like capabilities is spreading. The ransomware leverages etenalblue exploit, genuine psexec or wmic with appropriate credentials for a quick spread .

These mechanisms are used to attempt installation and execution of the dropped file C:\Windows\perfc.dat" on other devices to spread laterally. The dropped file, if managed to get the Administrator privileges, will encrypt the Master File Tree (MFT) tables for NTFS partitions and overrides the Master Boot Record (MBR) with a custom bootloader making the system unusable. Further the malware creates a scheduled task via schtasks /at to reboot the system one hour after infection. After the system is reloaded the malware downloads its code from MBR and encrypts data on the hard drive.

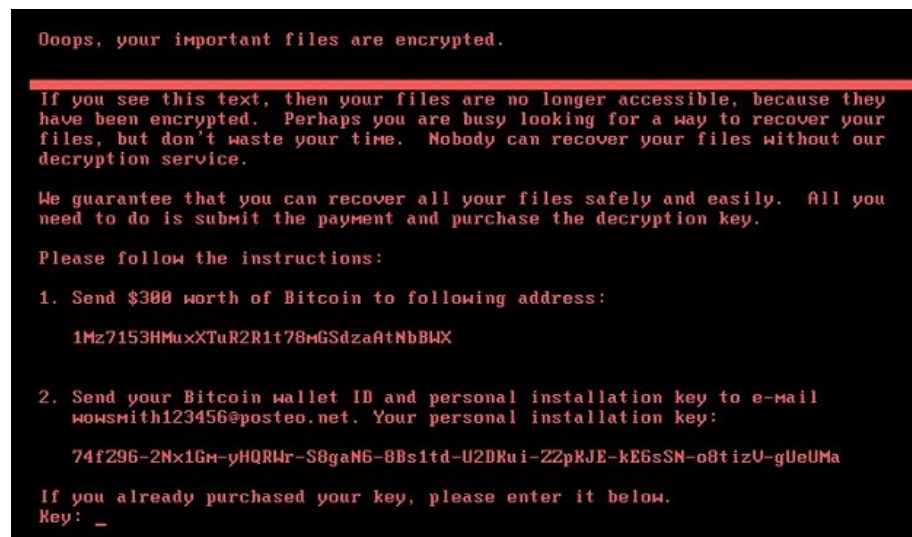
In case the fail to get the privileges rewrite MBR, the files are encrypted without a system reload. The list of file types that are encrypted:

3ds,7z,accdb,ai,asp,aspx,avhd,back,bak,c,cfp,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,vsd,xsv,work,xls,xlsx,xvd,zip.

The spreading mechanism thus far is by;

- EternalBlue - the same exploit used by WannaCry.
- Psexec - a legitimate Windows administration tool.
C:\WINDOWS\dlhost.dat \w.x.y.z -accepteula -s -d C:\Windows\System32\rundll32.exe C:\Windows\perfc.dat,#1 [dllhost.dat is psexec.exe]
- WMI - Windows Management Instrumentation, a legitimate Windows component.
Wbem\wmic.exe /node:"w.x.y.z" /user:"username" /password:"password" "process call create "C:\Windows\System32\rundll32.exe
"C:\Windows\perfc.dat\" #1" [there are unconfirmed reports about the usage of mimikatz/lsadump to get the system credentials]

There are open source reports about the usage of Microsoft Office HTA handler vulnerability [CVE-2017-0199] as one of the infection vector.



Sample RANSOM NOTE

The malware clears system logs using the following command:

"wevtutil cl Setup & wevtutil cl System & wevtutil cl Security & wevtutil cl Application & fsutil usn deletejournal /D %c:" to make further analysis more difficult.

Potential Indicators of compromises

ip 95.141.115.108
ip-dst 185.165.29.78
ip-dst 84.200.16.242

ip-dst 111.90.139.247
 domain coffeinoffice.xyz
 domain french-cooking.com
 domain sundanders.online
 url http://french-cooking[.]com/myguy[.]exe
 url http://84[.]200[.]16[.]242/myguy[.]xls
 url http://84[.]200[.]16[.]242/Profoma[.]xls
 url http://84[.]200[.]16[.]242/Lucky[.]exe
 url http://185.165.29.78/~alex/svchost.exe
 sha256 02ef73bd2458627ed7b397ec26ee2de2e92c71a0e7588f78734761d8edbdcd9f
 sha256 eae9771e2eeb7ea3c6059485da39e77b8c0c369232f01334954fbac1c186c998
 sha256 64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1
 sha256 027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
 sha256 fe2e5d0543b4c8769e401ec216d78a5a3547dfd426fd47e097df04a5f7d6d206
 sha256 ee29b9c01318a1e23836b949942db14d4811246fdae2f41df9f0dcd922c63bc6
 md5 9B853B8FE232B8DED38355513CFD4F30
 md5 CBB9927813FA027AC12D7388720D4771
 md5 a809a63bc5e31670ff117d838522dec433f74bee
 md5 bec678164cedea578a7aff4589018fa41551c27f
 md5 d5bf3f100e7dbcc434d7c58ebf64052329a60fc2
 md5 aba7aa41057c8a6b184ba5776c20f7e8fc97c657
 md5 0ff07caedad54c9b65e5873ac2d81b3126754aac
 md5 51eafbb626103765d3aedfd098b94d0e77de1196
 md5 078de2dc59ce59f503c63bd61f1ef8353dc7cf5f
 md5 7ca37b86f4acc702f108449c391dd2485b5ca18c
 md5 2bc182f04b935c7e358ed9c9e6df09ae6af47168
 md5 1b83c00143a1bb2bf16b46c01f36d53fb66f82b5
 md5 82920a2ad0138a2a8efc744ae5849c6dde6b435d
 sha256 22053C34DCD54A5E3C2C9344AB47349A702B8CFDB5796F876AEE1B075A670926
 sha256 1FE78C7159DBC3B59FF8D410BD9191868DEA1B01EE3ECCD82BCC34A416895B5
 sha256 EEF090314FBEC77B20E2470A8318FC288B2DE19A23D069FE049F0D519D901B95
 filename C:\0487382a4daf8eb9660f1c67e30f8b25.hta
 filename petwrap.exe
 filename C:\027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745.bin.dll
 filename Order-20062017.doc
 filename myguy[1].hta
 filename myguy.xls
 filename dllhost.dat
 named pipe {df458642-df8b-4131-b02d-32064a2f4c19}

emails wowsmith123456@posteo.net
 emails wowsmith123456@posteo.net
 emails iva76y3pr@outlook.com
 emails carmellar4hegp@outlook.com
 emails amanda44i8sq@outlook.com

Recommendations

- In order to prevent infection, users and organizations are advised to apply patches to Windows systems as mentioned in Microsoft Security Bulletin [MS17-010](#).
- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Block SMB ports on Enterprise Edge/perimeter network devices [UDP 137, 138 and TCP 139, 445] or Disable SMBv1.
<https://support.microsoft.com/en-us/help/2696547>
- Applocker policies to block execution of files having name perfc.dat as well as psexec.exe utility from sysinternals
- A quick fix to prevent by creating the files (perfc, perfc.dll, and perfc.dat) to already exist on the Windows machine, under C:\Windows, with READONLY permissions. A brief description is here:
<https://www.bleepingcomputer.com/news/security/vaccine-not-killswitch-found-for-petya-notpetya-ransomware-outbreak/>
- Yara Rules for Petya detections can be seen here [\[kaspersky.yara\]](#) and here [\[florian.yaya\]](#)
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser.
- Restrict execution of powershell /WSHSCRIPT/ PSEXEC / WMIC in enterprise environment Ensure installation and use of the latest version (currently v5.0) of PowerShell, with enhanced logging enabled. script block logging, and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis.

- Establish a Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA%, %PROGRAMDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations. Enforce application whitelisting on all endpoint workstations.
- Deploy web and email filters on the network. Configure these devices to scan for known bad domains, sources, and addresses; block these before receiving and downloading messages. Scan all emails, attachments, and downloads both on the host and at the mail gateway with a reputable antivirus solution.
- Disable macros in Microsoft Office products. Some Office products allow for the disabling of macros that originate from outside of an organization and can provide a hybrid approach when the organization depends on the legitimate use of macros. For Windows, specific settings can block macros originating from the Internet from running.
- Configure access controls including file, directory, and network share permissions with least privilege in mind. If a user only needs to read specific files, they should not have write access to those files, directories, or shares.
- Maintain updated Antivirus software on all systems.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Network segmentation and segregation into security zones-help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
- Disable remote Desktop Connections, employ least-privileged accounts.
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems, Check regularly for the integrity of the information stored in the databases.
- Restrict user's abilities (permissions) to install and run unwanted software applications.
- Employ data-at-rest and data-in-transit encryption.
- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies.

References

<https://isc.sans.edu/forums/diary/Checking+out+the+new+Petya+variant/22562/>
<https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know>
<https://securelist.com/petrwrap-the-new-petya-based-ransomware-used-in-targeted-attacks/77762/>
<http://blog.talosintelligence.com/2017/06/worldwide-ransomware-variant.html>

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,

New Delhi - 110 003
India