Advance Notification of Cyber Threats against Petya Ransomware

Security Advisory AE-Advisory 17-38 **Criticality** Critical 

Advisory Released On 28 June 2017

Impact

Installs a ransomware on the infected device and might cause administrative level unauthorized access into networks and systems, or it might encrypt and lock all the data on a computer system making it inaccessible to the user.

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a new ransomware named currently named as "Petya Ransomware". On June 27, 2017, multiple organizations in Europe have detected a breach that have disabled, encrypted, and locked users from accessing their computers without paying a sum of Bitcoin. It is believed that Petya ransomware leverages that EternalBlue NSA exploit. The Petya ransomware shares similarities to the WannaCry ransomware but is also spreading via client-side attack using CVE-2017-0199. It is advised not to make any payments to the ransomware creator as the e-mail associated with the ransomware "wowsmith123456@posteo.net" has been shut down as well as there is no guarantee that paying the ransom will lead to the decryption of the files.

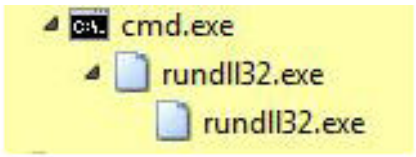
Advisory Details

Petya ransomware's initial distribution method seems to be over email where a malicious link is sent from an unknown address, once launched Petya does not attempt to encrypt the files but attempts to encrypts MFT (Master File Tree) tables for NTFS partitions and overwrites the MBR (Master Boot Record) with a custom bootloader that shows a ransom note and prevents victims from booting their computer. In addition, it has a fake Microsoft digital signature appended, that is copied from "Sysinternals". As well as that the ransomware can also spread via Windows Management Instrumentation Command-line (WMIC). Other than encrypting and locking the master file table, Petya ransomware attempts to steal credentials from the infected users and send them to a server controlled by the attackers.

Indicators of Compromise (IOCs)

Petya is quite similar to Wanacry since it relies on SMB to spread across a network. The malicious (.dll) file creates a task in (Task Scheduler) for the infected machine to shut down after 60 minutes of the infection.

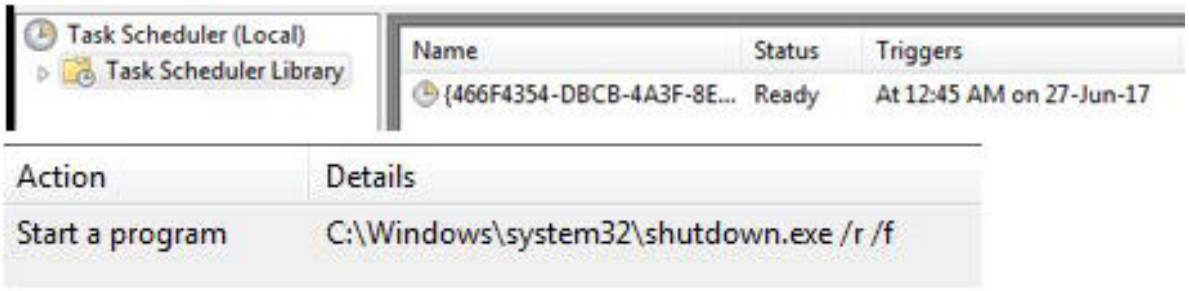
1



2

```
Hschtasks /Create /SC once /TN "" /TR "C:\Windows\system32\shutdown.exe /r /f" /ST 00:60
```

3



Once the system is rebooted, it will start encrypting files, encrypts MFT (Master File Tree) tables, overwrites the MBR (Master Boot Record) and shows the below message:

```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete. It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 8384 of 134624 (6%)
```

- myguy.xls
  EE29B9C01318A1E23836B949942DB14D4811246FDAE2F41DF9F0DCD922C63BC6

- BCA9D6.exe
  17DACEDB6F0379A65160D73C0AE3AA1F03465AE75CB6AE754C7DCB3017AF1FBD
- FileHash-SHA256
  027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745
- FileHash-MD5
  0df7179693755b810403a972f4466afb
- FileHash-SHA1
  34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d
- FileHash-MD5
  42b2ff216d14c2c8387c8eabfb1ab7d0
- FileHash-SHA256
  64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1
- FileHash-MD5
  71b6a493388e7d0b40c83ce903bc6b04
- FileHash-SHA256
  752e5cf9e47509ce51382c88fc4d7e53b5ca44ba22a94063f95222634b362ca5
- FilePath
  C:\Windows\dllhost.dat
- FileHash-MD5
  e285b6ce047015943e685e6638bd837e
- FileHash-MD5
  e595c02185d8e12be347915865270cca

Solution

Entities are recommended to follow the following steps to attempt to prevent the infection and spread of the Petya Ransomware:

- Apply caution when opening unknown files and unknown e-mails
- Block any emails coming from source e-mail "wowsmith123456@posteo.net".
- Block SMB ports or services at firewall level when it's not needed:
  - Deny port 137 name services.
  - Deny port 138 datagram services.
  - Deny port 139 session service.
  - Deny port 445 session service
- Apply MS17-010 patch as well as that CVE-2017-0199
- Disable WMIC if possible
- Have offline backups
- Use Network analytics tools to detect any outgoing Tor connections
- Migrate from older Windows operating systems to the latest patched operating systems.
- Apply vendor patches as soon as they are available
- Block access to the following domains :
  - (Tor) hxxp://mischapuk6hyrn72.onion/
  - (Tor) hxxp://petya3jxfp2f7g3i.onion/
  - (Tor) hxxp://petya3sen7dyko2n.onion/
  - (Tor) hxxp://mischa5xyix2mrhd.onion/MZ2MMJ
  - (Tor) hxxp://mischapuk6hyrn72.onion/MZ2MMJ
  - (Tor) hxxp://petya3jxfp2f7g3i.onion/MZ2MMJ
  - (Tor) hxxp://petya3sen7dyko2n.onion/MZ2MMJ
  - hxxp://benkow.cc/71b6a493388e7d0b40c83ce903bc6b04.bin
  - hxxp:/coffeeinoffice.xyz
  - hxxp://french-cooking.com/

- Block IPs associated with the ransomware:
  - 95.141.115.108
  - 185.165.29.78
  - 84.200.16.242
  - 111.90.139.247
- Apply patches MS17-010 patch and CVE-2017-0199
- Disable Server Message Block v1 (SMBv1)
- Update Anti-Virus hastes

  a809a63bc5e31670ff117d838522dec433f74bee

  bec678164cedea578a7aff4589018fa41551c27f

  d5bf3f100e7dbcc434d7c58ebf64052329a60fc2

  aba7aa41057c8a6b184ba5776c20f7e8fc97c657

  0ff07caedad54c9b65e5873ac2d81b3126754aac

  51eafbb626103765d3aedfd098b94d0e77de1196

  078de2dc59ce59f503c63bd61f1ef8353dc7cf5f

  7ca37b86f4acc702f108449c391dd2485b5ca18c

  2bc182f04b935c7e358ed9c9e6df09ae6af47168

  1b83c00143a1bb2bf16b46c01f36d53fb66f82b5

  82920a2ad0138a2a8efc744ae5849c6dde6b435d

- Monitor and if possible, block RTF attachments sent via e-mail
- Follow @TheUAETRA on Instagram and Twitter for the latest updates
- Signature-Based Detection for YARA

```
rule ransomware_PetrWrap {
meta:
copyright = "Kaspersky Lab"
description = "Rule to detect PetrWrap ransomware samples"
last_modified = "2017-06-27"
author = "Kaspersky Lab"
hash = "71B6A493388E7D0B40C83CE903BC6B04"
version = "1.0"
strings:
$a1 =
"MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n
2JmURWV/uHB0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GR
KxEEFLCy7vP12EYOPXknVy/+mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDD
mdrRIiUEUw6o3pt5pNOskfOJbMan2TZu" fullword wide
$a2 =
".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djv
u.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.mail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.p
hp.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" fullword wide
$a3 = "DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS
PLUGGED" fullword ascii
$a4 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" fullword ascii
$a5 = "wowsmith123456@posteo.net." fullword wide
condition:
uint16(0) == 0x5A4D and
filesize < 1000000 and any of them }
```

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae