Tonga National Computer Emergency Response Team

cert.to Advisory

Threat Name/Title: Petya/NotPetya/Petna

Original Issue Date: 28th June 2017

Updated: 29th June 2017

Severity Rating: High

Description:
There are early signs of a new ransomware outbreak, currently affecting a large number of countries across the globe, such as the UK, Ukraine, India, the Netherlands, Spain, Denmark, and others. This ransom uses the contact details of wowsmith123456@posteo.net and asks for a payment of $300 in Bitcoin.

The main culprit behind this attack is a new version of Petya, a ransomware that 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. Later, it was discovered this is a new strain altogether, which researchers have started referring to as NotPetya or Petna. Because our initial advisory and it's common name, we'll be using the name Petya through this advisory, but be aware this is a new ransomware strain that has some similarities with the original Petya, but is new in its own right.

According to several sources, the author of this new Petya strain appears to have taken inspiration from last month's WannaCry outbreak, and added a similar SMB work based on the NSA's ETERNALBLUE exploit. This has been confirmed by Payload Security, Avira, Emsisoft, Bitdefender, Symantec, and other security researchers. Later during the day, it was also discovered that Petya also used another NSA exploit called ETERNALROMANCE.

Information on Petya's distribution vectors is unknown at the moment, with two major theories. First, Petya appears to be spread via email spam in the form of boobytrapped Office documents. These documents use the CVE-2017-0199 Office RTF vulnerability to download and run the Petya installer, which then executes the SMB worm and spreads to new computers on the same network. Second, there's the train of thought that Petya is spreading via a malicious update of the MEDOC accounting software, very popular in Ukraine.

Unlike WannaCry, Petya is also spread via email spam in the form of boobytrapped Office documents. These documents use the CVE-2017-0199 Office RTF vulnerability to download and run the Petya installer, which then executes the SMB worm and spreads to new computers on the same network.

A past version of the Petya ransomware was decryptable, but we cannot confirm or deny at this stage that this version is also decryptable.

Email address associated with infections:
wowsmith123456@posteo.net

Bitcoin address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

Dynamic Analysis:

- Copies itself to C:\Windows\
- Drops a PE file to C:\Windows\dllhost.dat
- Attempts to connect to port 445 and initiate an SMB handshake, probably attempting to use ETERNALBLUE to spread itself.
- Creates a scheduled task file to induce a reboot at a specified time. Creates it using schtasks
- Uses wevtutil.exe to clear Setup, System, Security, and Application logs
- Uses fsutil.exe to delete the update sequence number (USN) change journal, which provides a log of all changes made to files on the volume, in this case "C:".

Targeted file 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.sln.sql.tar.vbox.vbs .vcb.vdi.vfd.vmc.vmdk.vmsd.vmx.vsdx.vsv.work.xls.xlsx.xvd.zip.

Ransom note name:
README.TXT

Ransom note text:
Send your Bitcoin wallet ID and personal installation key to e-mail
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because
they have been encrypted. Perhaps you are busy looking for a way to recover
your files, but don't waste your time. Nobody can recover your files without
our decryption service.
We guarantee that you can recover all your files safely and easily.
All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
Send $300 worth of Bitcoin to following address:

Does not encrypt files in this folder:
C:\Windows;

Recommendations:

- Clients should ensure that all versions of Windows are patched up to the latest currently available.
- Ensure Anti-virus software and associated signature files are up to date.
- Disable the outdated protocol SMBv1
- Isolate unpatched systems from the larger network
- Should you be impacted, clients can call cert.to hotline: 2378

Tonga National CERT contact details:
Tonga National CERT
Ministry of MEIDECC
Sanft Building
Nuku'alofa
Tel: 2378
email: cert@cert.to
web: www.cert.to

References:
https://www.bleepingcomputer.com/news/security/wannacry-d-j-vu-petya-ransomware-outbreak-wreaking-havoc-across-the-globe/#comments
https://exchange.xforce.ibmcloud.com/collection/Petya-Ransomware-Campaign-9c4316058c7a4c50931d135e62d55d89