SCSC, CYBER SECURITY FORUM

Petya Ransomware FAQ

27/06/2017

The purpose of this FAQ is to provide verified information about the Petya Ransomware infection.

As the infection is ongoing and analysis is in the early stages, We may release additional information as appropriate. Given the rapidly developing nature of threats of this kind SCSC cannot take responsibility for the use of information and recommendations in this advisory.

How does the Petya infection spread?

Multiple distribution methods have been reported. Petya's previous initial infection vector has been phishing emails containing weaponized Rich Text Format (RTF) documents designed to exploit CVE-2017-0199. If successful, the Petya Ransomware component is downloaded as a Windows Dynamic Link Library (DLL).

Server Message Block (SMB) exploitation has been observed for internal propagation as well as PSEXEC and Windows Management Instrumentation Command-line (WMIC). Multiple sources have attributed the SMB activity to the use of the ETERNALBLUE exploit, but further analysis is required to confirm the exact nature of the SMB exploitation.

How does the Ransomware work?

Unlike traditional Ransomware, Petya encrypts the master file table (MFT) of the hard drive and overwrites the master boot record (MBR) with a custom boot loader. These operations restrict access to the necessary information required to boot the operating system and locate files on the disk.

What steps are recommended to mitigate risk for this attack?

- Incorporate blocking for the IOCs in this document
- Apply security updates for MS17-010
- Block inbound connections on port 445
- Restrict the use of PSEXEC through group policy

How can risk be mitigated for Ransomware in general?

- Train and sensitize users to report phishing and suspicious system activity
- Keep host-based and enterprise anti-virus solutions updated
- Patch third-party applications as soon as possible
- Remove local administrative rights
- Deploy a File Integrity Monitoring solution
- Test and validate data backup processes
- Block access to C2 servers
- Check encrypted file ownership to identify users
- Recall known phishing emails from mailboxes and block by sender, subject, or attachment
- Deploy Group Policy Objects to block executable files and disable macros
- Set file shares to read-only mode

Potential IOCs?

**********Bitcoin wallet ID for ransom payment

wowsmith123456@posteo[.]net

********** Bitcoin wallet for payment

https://blockchain.info/address/1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

********** Possible malware sample
files: https://yadi.sk/d/S0-ZhPY53KWc84
https://yadi.sk/d/Zpkm88sp3KWc8v
Archive password: virus

********** Possible callout IP
addresses: 185.165.29.78 84.200.16.242
111.90.139.247 95.141.115.108

********** Possible outbound
connections: COFFEINOFFICE[.]XYZ
hxxp://french-cooking[.]com

********** Analysis:
https://virustotal.com/fr/file/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745/analysi s/
https://www.hybrid-analysis.com/sample/027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745?environmen tId=100

********** Vulnerabilities:
MS17-010
- -

********** Has sysinternal utilities signature
https://twitter.com/ppeepuppy/status/879706271535972353

********** List of extensions targeted
https://twitter.com/MrCarlMcDade/status/879706580127809536

********** Indicates possible usage of PSEXEC, on windows that means the admin$ and c$ shares.
https://twitter.com/rikvduijn/status/879726410201526272

********** It is confirmed that the sample 027cc... contains PSEXEC:
https://twitter.com/NVISO_Labs/status/879724733696274432