NIC-CERT

Advisory for Petya Ransomware Variant June 2017

A. Description

Petya ransomware and its variants are spreading by exploiting SMBv1 EternalBlue exploit, similar to ransomware WannaCry. It combines both a client-side attack (CVE-2017-0199) and a network based threat (MS17-010).

B. Mode of Operation

Current variant of Petya spread as a DLL file, which must be executed by another process before it make any changes to the system. Once executed, it overwrites the Master Boot Record and creates a scheduled task to reboot the system. On rebooting the malware displays a ransom note for payments. It encrypts the Master File Tree (MFT) table of NTFS.

Initial attack may originate by downloading malicious file through email and then executing it. Petya uses any of the three mechanisms to spread to the host network

1. Scans the local network for ADMIN$ shares with write and execute permission. It copies itself on such hosts and executes the malware using PSEXEC.
2. It uses the Windows Management Instrumentation Command-line (WMIC) tool to connect to hosts on the local subnet and attempts to execute remotely on such hosts.
3. It uses the vulnerability as mentioned by MS17-010 to spread to hosts on the local subnet.

C. Affected Systems

All Windows System (XP/Vista/7/8/10)

D. Recommendations to protect from Petya Ransomware

1. Apply patches for EternalBlue (MS17-010), CVE-2017-0199 and Keep your system updated.
2. Petya Ransomware is taking advantage of WMIC and PSEXEC tools to infect fully-patched Windows computers; it is advised to disable WMIC (Windows Management Instrumentation Command-line).
3. Use and keep your Antivirus Program updated.
4. Always exercise caution when opening uninvited documents sent over an email and clicking on links inside those documents unless verifying the source to safeguard against malware infections.
5. Keep regular Backup of your Files.

E. References

1. http://www.telegraph.co.uk/news/2017/06/27/ukraine-hit-massive-cyber-attack1/

2. https://researchcenter.paloaltonetworks.com/2017/06/unit42-threat-brief-petya-ransomware/
3. https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how
4. http://blog.checkpoint.com/2016/04/11/decrypting-the-petya-ransomware/