PNP Computer Security Bulletin CSB17-012

NotPetya Ransomware

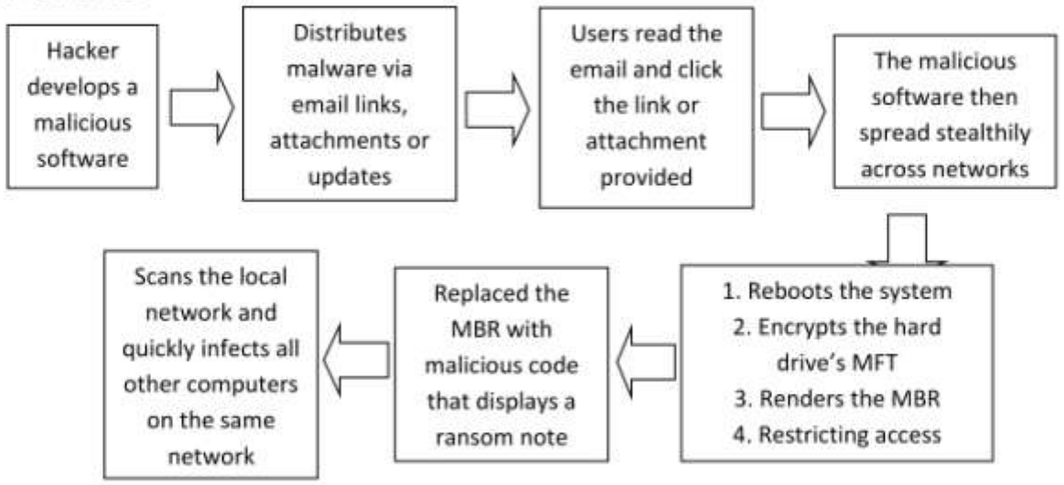
Risk/Impact Rating: **SERIOUS**

Revised: July 6 2017

Description:

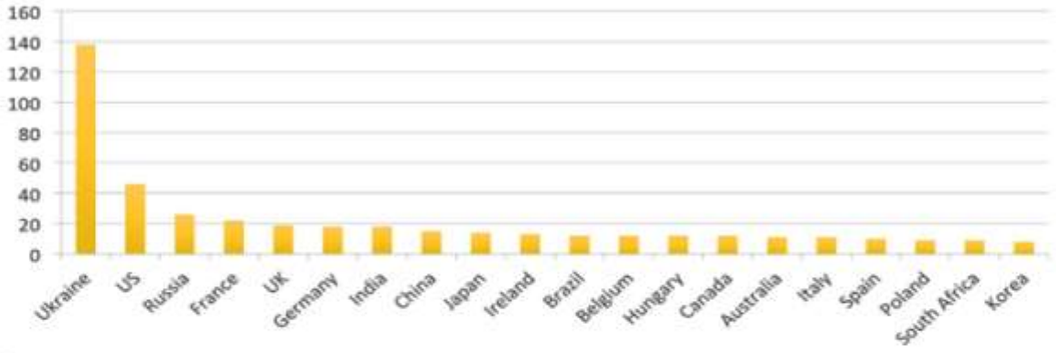
- This malware was not designed as a ransomware attack for financial gain. Instead, it was designed as a wiper pretending to be ransomware, to be destructive.
- It wipes computer outright, destroying all records from the targeted system called wiper malware (Comae Technologies Founder, Matt Suiche)
- NotPetya reboots victims' computers, encrypts the hard drive's master file table (MFT), and renders the master boot record (MBR) inoperable, restricting access to the full system by stealing the user's Windows credentials and location on the physical disk.
- It takes an encrypted copy of MBR and replaces it with its own malicious code that displays a ransom note, leaving computers unable to boot.
- Does not keep a copy of replaced MBR, leaving infected computers unbootable even if victims get the decryption keys
- After infecting one computer, it scans the local network and quickly infects all other computers (even fully patched) on the same network, using EternalBlue SMB exploit, WMIC and PSEXEC tools
- There is no possibility for the decryption key because it generates a random infection ID for each computer.
- If victims do pay for the ransom, they will never recover their files (Kaspersky researchers)
- The virus has possibly been spread through a malicious software update to a Ukranian tax accounting system called MeDoc. MeDoc was breached and the virus was spread via updates

How it works:



Note: Payment of ransom is no guarantee that hacker will send a key to unlock the infected computer

Top 20 countries based on numbers of affected organizations



By: www.symantec.com

Modus Operandi:

- Via email pretending to be from legitimate source and ask the reader to click on the link or open the attachment for software update.

Security Risks to PNP Computer Systems and Data:

- Data can be altered, damaged, deleted, and infused with additional computer viruses.
- Interfere with the normal functioning of the computer system or prevent its utilization.

Mitigation Measures:

- Apply the Microsoft patch for the MS17-010 SMB vulnerability dated March 14, 2017.
- Back up and test your data regularly
- Avoid opening e-mails from unverified or questionable sources.
- Avoid illegal websites or torrent sites.
- Use genuine software and patch/update.
- Scan your computer regularly using antivirus software.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching the end users.
- Run regular penetration tests as often as possible and practical.

If infected:

- Disconnect system from network immediately to avoid infecting other computers connected; or
- Reformat the computer and restore back-up; and
- Contact ITMS WSCSD for technical support assistance.

Warning: Once infected by Petya there is a high risk that the computer system cannot be restored to its working condition or recover the infected files.

For further inquiries, contact ITMS WSCSD:

- Telephone Number: **(02) 723-0401 local 4225**;
- E-mail address: **wscsditms@pnp.gov.ph**; and
- Chat Service: **www.itms.pnp.gov.ph**.

"Technology Runs Fast. ITMS Never Stops"