PNP Computer Security Bulletin CSB17-012

Petya Ransomware

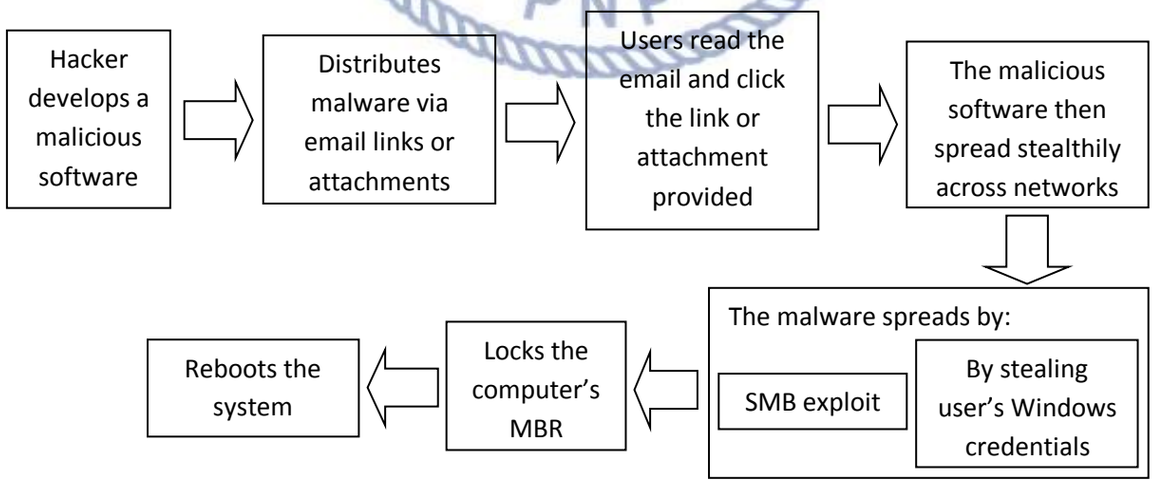
Risk/Impact Rating: **SERIOUS**

Revised: July 6 2017

Description:

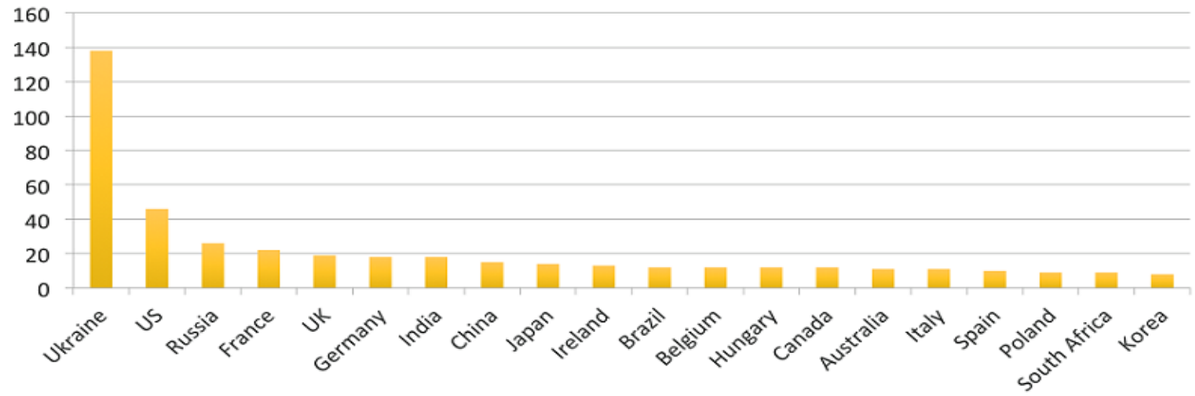
- Petya Ransomware encrypts the master boot records of infected Windows computers, making affected machines unusable.
- It exploit vulnerabilities in Server Message Block (SMB).
- It encrypts the victim's files with a dynamically generated, 128-bit key and creates a unique ID of the victim.
- It may not be possible for the attacker to decrypt the victim's file even if the ransom is paid.
- It spreads using the SMB exploit and by stealing the user's Windows credentials.
- Installs a modified version of the MImikatz tool, which can be used to obtain the user's credentials, which can be used to access other systems on the network.
- It also attempt to identify other hosts on the network by checking the compromised system's IP physical address mapping table.
- It scans for other systems that are vulnerable to the SMB exploit and installs the malicious payload.
- This Petya variant writes a text file on the C:\ drive with the Bitcoin wallet information and RSA keys for the ransom payment. It modifies the master boot record (MBR) to enable encryption of the master file table (MFT) and the original MBR, then reboots the system.

How it works:



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

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**.