PNP Computer Security Bulletin CSB17-010

RANSOMWARE

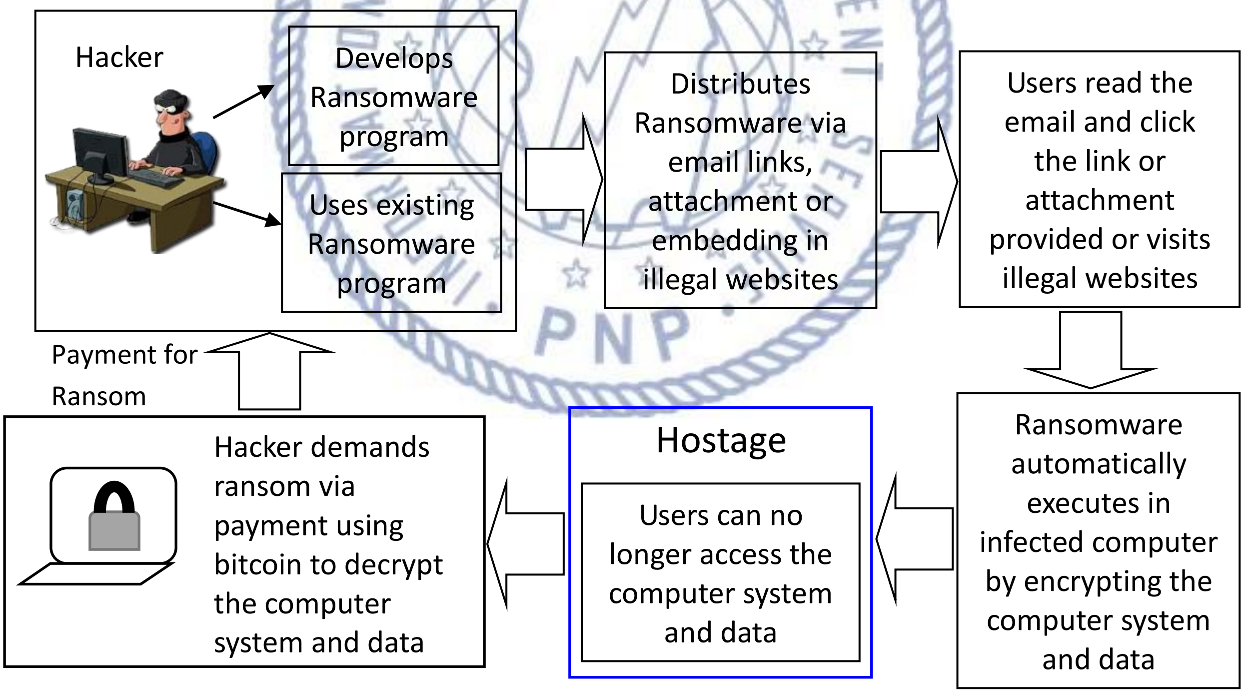
Risk/Impact Rating: **SERIOUS**

Revised May 16, 2017

Description:

- **Ransomware** is a type of malware that infects computer systems and data rendering them unusable for "ransom";
- Holds computer files for "ransom" by encrypting or preventing access to operating system such as Windows;
- Spreads through phishing emails or drive-by downloading websites; and
- Uses a Trojan, disguised as legitimate file or software that automatically installs on the infected computer system.

How Ransomware works:



Note: Payment of ransom is no guarantee that hacker will send a decryption key to unlock the infected computer system and data.

Two (2) Kinds of Ransomware

- **Locker ransomware** – locks the operating system, making it impossible to access the computer and/or any software or files and demands payment in order to unlock the computer system and data.
- **Crypto ransomware** – designed to encrypt and block system files and demands payment in order to decrypt the computer system and data using a screen message.

Modus Operandi on Ransomware Propagation

- Via email pretending to be from a legitimate source and ask the reader to click the link or download the attachment provided.
- Ransomware links are also provided in social media messages from unknown sources.
- Using hidden links in illegal websites and online games.

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

- 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.

If infected:

- Disconnect system from network immediately to avoid infecting other computers connected.
- Use Ransomware decryptors for many types of Ransomware.
- Restore latest backup of computer system and data.
- Contact ITMS WSCSD for technical support assistance.

Warning: Once infected by ransomware 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**.