PNP Computer Security Bulletin CSB18-01

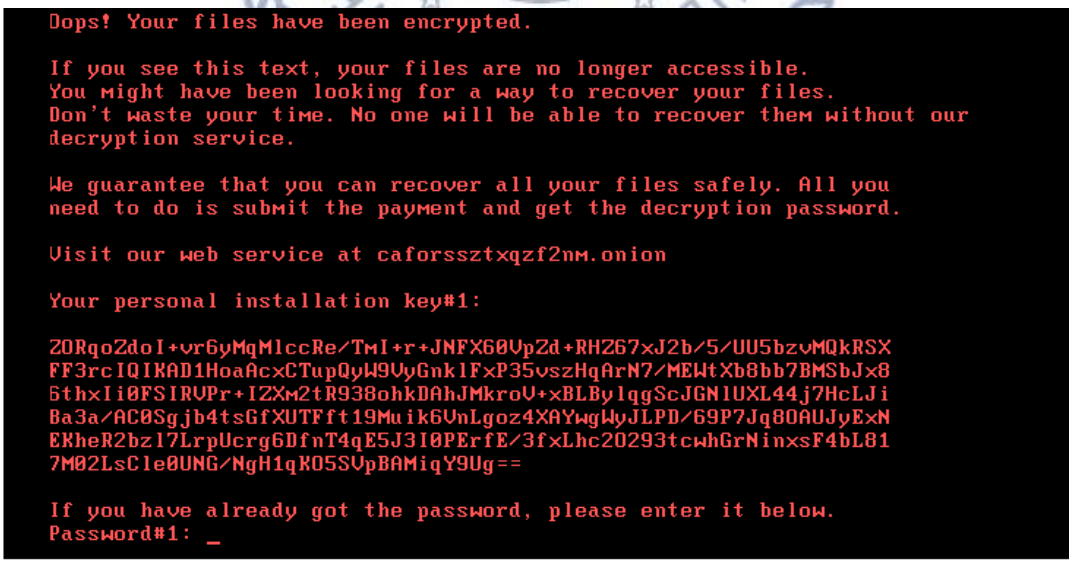
Bad Rabbit Ransomware

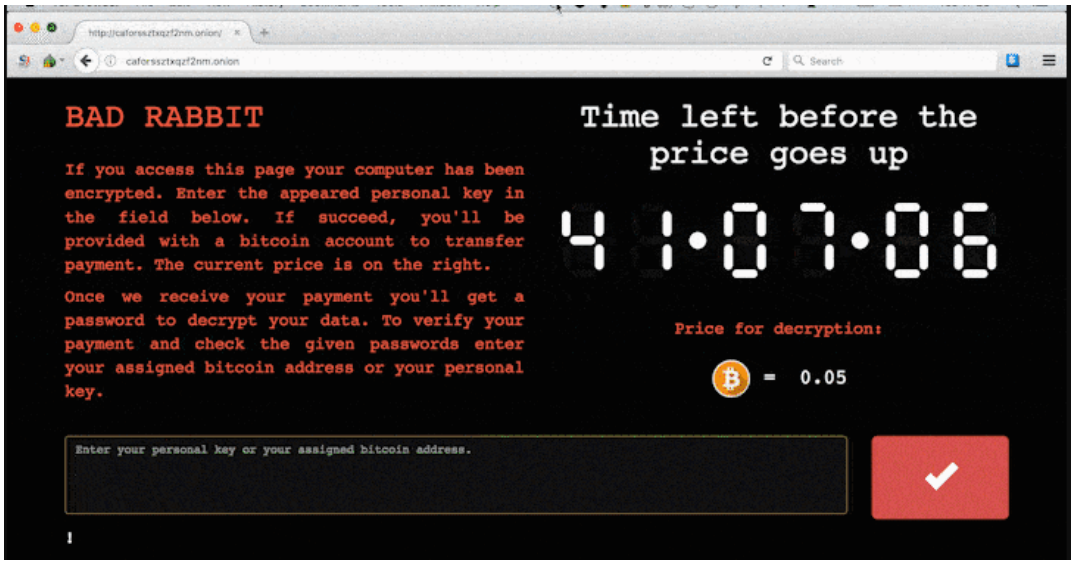
Risk/Impact Rating: **SERIOUS**

Created: January 8, 2018

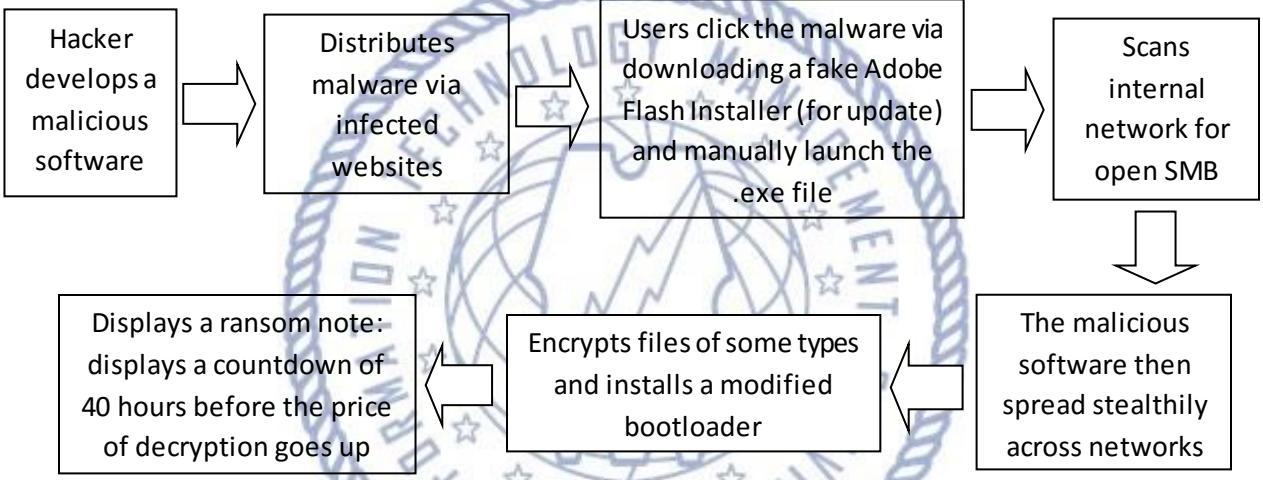
Description:

- Targeted attack: Corporate Networks.
- Infected several big Russian media outlets. Some in Ukraine, Turkey and Germany.
- Some of the code used was spotted in NotPetya Ransomware.
- It uses EternalRomance exploit to move laterally on the local network.
- Encrypts files of some types and installs a modified bootloader, thus preventing the PC from booting normally.
- The malefactors behind it potentially have the ability to decrypt the password, which is needed to decrypt files and allow the computer to boot the operating system.
- Ask for a ransom payment of 0.05 bitcoin, (~ $285) to unlock systems.
- Ransom note: Asks victim to log into a Tor onion website to make the payment, which displays a countdown of 40 hours before the price of decryption goes up.





How it works:



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

Modus Operandi:

- Via Adobe Flash updates, tricking users into clicking the malware by falsely alerting the user that their Flash player requires an 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:

- Back up and test your data regularly
- Avoid opening e-mails from unverified or questionable sources.
- Avoid illegal websites or torrent sites.

- Never download any app from third-party sources and read even before installing apps from official stores.
- 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.
- Block the execution files c:\windows\infpub.dat and c:\windows\cscc.dat
- Disable WMI Service.

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 Bad Rabbit there is a high risk that the computer system cannot be restored to its working condition or recover the infected files. However, if for some reason, Bad Rabbit didn't encrypt the whole disk, it is possible to retrieve the files from the shadow copies (if the shadow copies were enabled prior to the infection)

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**.