PNP Computer Security Bulletin CSB18-03

Phishing

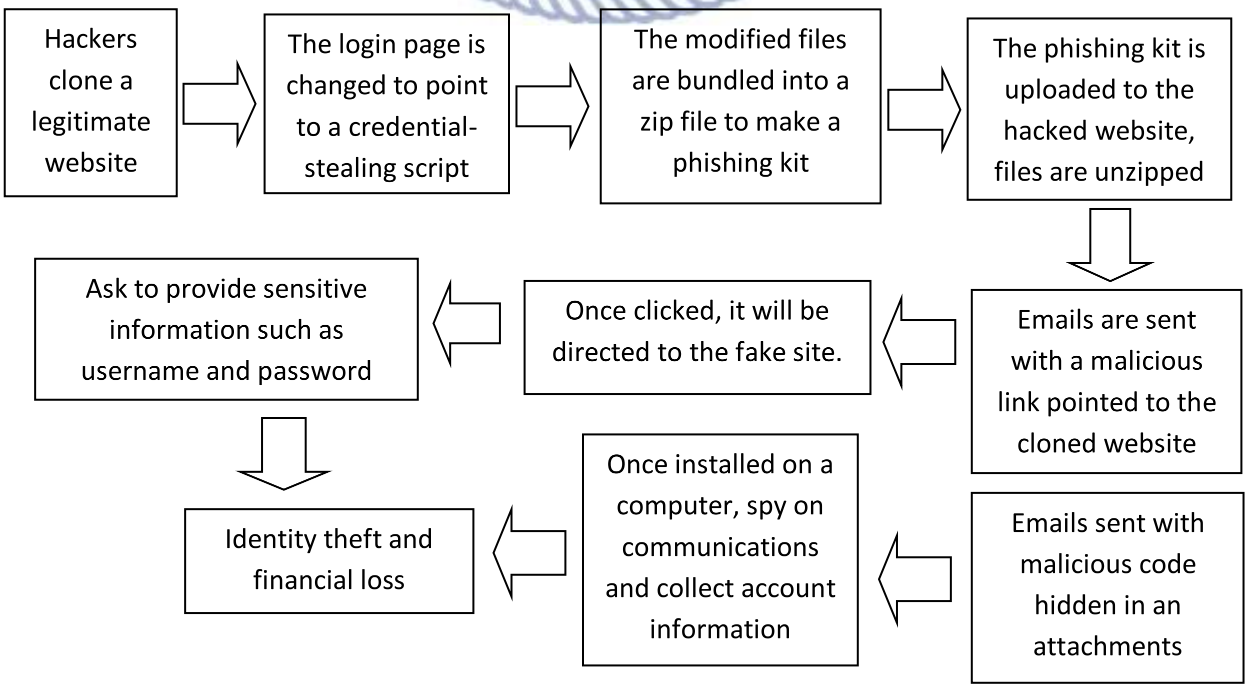
Risk/Impact Rating: **SERIOUS**

Revised: March 14, 2018

Description:

- Use of electronic mail messages, designed to look like messages from a trusted agent. These messages usually implore the user to take some form of action, such as validating account information. Also, use of malicious code that targets user account information.
- Rely on social networking techniques applied to email or other electronic communication methods, including direct messages sent over social networks, SMS text messages and other instant messaging modes.
- It may use social engineering and other public sources of information, including social networks to gather background information about the victim's personal and work history, interest and activities.
- A victim receives a message that appears to have been sent by a known contact or organization through a malicious file attachment that contains phishing software, or through links connecting to malicious websites.
- A phishing email can include corporate logos and other identifying graphics and data collected from the company being misrepresented.
- The use of subdomains and misspelled URLs are common tricks, as is the use of other link manipulation techniques.
- Attacker is asking to click or open an attachment to avoid a negative consequence or to gain something of value. It have bad grammar or spelling errors.
- Objective: install malware on the user's device or direct the victim to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

How it works:



Hackers clone a legitimate website

The login page is changed to point to a credential-stealing script

The modified files are bundled into a zip file to make a phishing kit

The phishing kit is uploaded to the hacked website, files are unzipped

Emails are sent with a malicious link pointed to the cloned website

Once clicked, it will be directed to the fake site.

Ask to provide sensitive information such as username and password

Emails sent with malicious code hidden in an attachments

Once installed on a computer, spy on communications and collect account information

Identity theft and financial loss

Modus Operandi:

- Via email or other electronic communication methods pretending to be from a legitimate source that trick users into clicking the malicious link or downloading attachments with malicious code.

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:

- Always check the spelling of the URLs in email links before clicking or entering sensitive information
- Avoid opening e-mails from unverified or questionable sources.
- Avoid posting personal data on social media
- Back up and test your data regularly
- Use genuine software and patch/update.
- Scan your computer regularly using antivirus software.
- Configure email client for security.
- Scan all emails and filter executable files from reaching the end users.
- Run regular penetration tests as often as possible and practical.

If infected:

- Report it to the network administrators;
- Contact your financial institution immediately and close any accounts that may have been compromised;
- Immediately change any passwords; or
- Report to ITMS ISSD for assistance.

References:

- *Avoiding Social Engineering and Phishing Attacks*. (2009, October 22). Retrieved January 24, 2017, from https://www.us-cert.gov/ncas/tips/ST04-014
- *Recognizing and Avoiding Email Scams*. (n.d). Retrieved from https://www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf
- *What is Phishing?.* (n.d). Retrieved from http://www.phishing.org/what-is-phishing
- *Recent Email Phishing Campaigns – Mitigation and Response Recommendations*. (2015, August 1). Retrieved Semptember 29, 2016, from https://www.us-cert.gov/ncas/alerts/TA15-213A
- *Technical Trends in Phishing Attacks*. (n.d). Retrieved from https://www.us-cert.gov/sites/default/files/publications/phishing_trends0511.pdf
- *How to recognize phishing email messages, links, or phone calls*. (n.d). Retrieved from https://www.microsoft.com/en-us/safety/online-privacy/phishing-symptoms.aspx
- Margaret Rouse. (2017, October). *Phishing.* Retrieved from http://searchsecurity.techtarget.com/definition/phishing

For further inquiries, contact ITMS ISSD:

- Telephone Number: **(02) 723-0401 local 4225**;
- E-mail address: **issditms@gmail.com**; and
- Website: **www.itms.pnp.gov.ph**.