Computer Security Awareness

Protecting PNP Computer Systems and Data Against

“Ransomware”

Prepared by:

Web Service and Cyber Security Division
Information Technology Management Service
Philippine National Police

Situation : Compromised PNP Server

- On March 23, 2017, PNP Finance Service Data Management System (FSDMS) Information System could not be logged into.
- All files in the server were encrypted making the FSDMS computer system unusable.
- A “Ransom message” on the server’s screen was displayed informing the user that an amount must be paid in order to allow access and decrypt the files.

Related Terminologies

- **Malware** – software programs designed to alter, damage, steal or conduct unauthorized actions on a computer system and data.
- **Bitcoin** – a form of digital currency, created and held electronically used to buy things electronically.
- **Trojan** – a form of malware that pretends to be a legitimate software or file but deploys a host of malware to the infected computer system.

Related Terminologies

- **Phishing** – is the attempt to obtain sensitive information, by pretending to be a legitimate source, usually through email or fake/illegal websites.
- **Drive-by downloading** – the unintentional downloading and installation of malware such as RANSOMWARE by visiting illegal websites or opening email links or attachments from unknown senders .

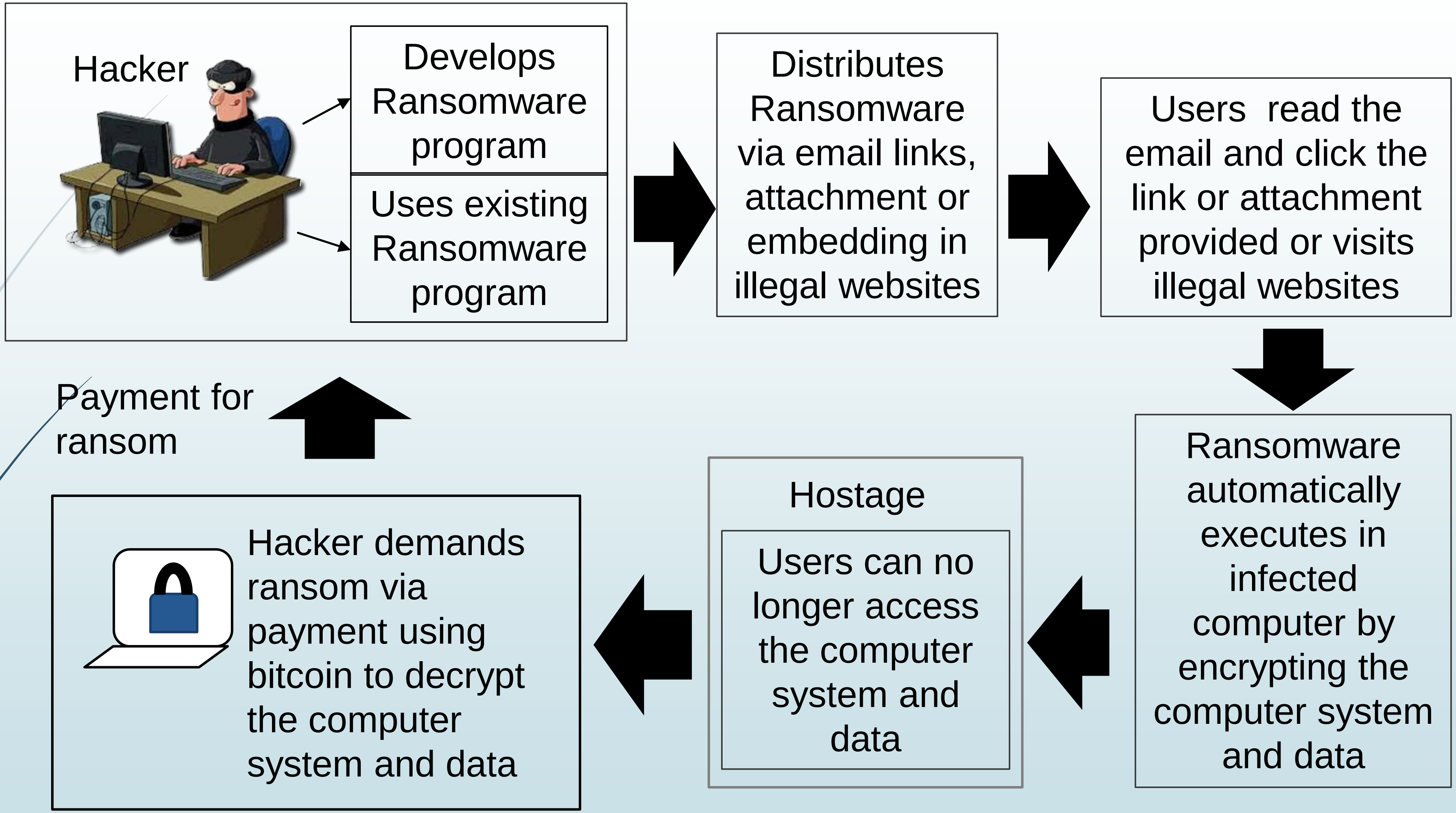
Related Terminologies

- **Malicious email** – a suspicious email received from an unknown sender containing links or attachments.
- **Software** – a program or a set of instructions and applications used to manage and control various functions of a device such as a computer

What is Ransomware?

- 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 a legitimate file or software that automatically installs on the infected computer system.

How Ransomware works:



Hacker

Develops Ransomware program

Uses existing Ransomware program

Distributes Ransomware via email links, attachment or embedding in illegal websites

Users read the email and click the link or attachment provided or visits illegal websites

Ransomware automatically executes in infected computer by encrypting the computer system and data

Hostage

Users can no longer access the computer system and data

Hacker demands ransom via payment using bitcoin to decrypt the computer system and data

Payment for ransom

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 (infected the FSDMS)*** – designed to encrypt and block system files and demands payment in order to decrypt the computer system and data using a screen message.

Top 10 Ransomwares

(as of December 18, 2016)

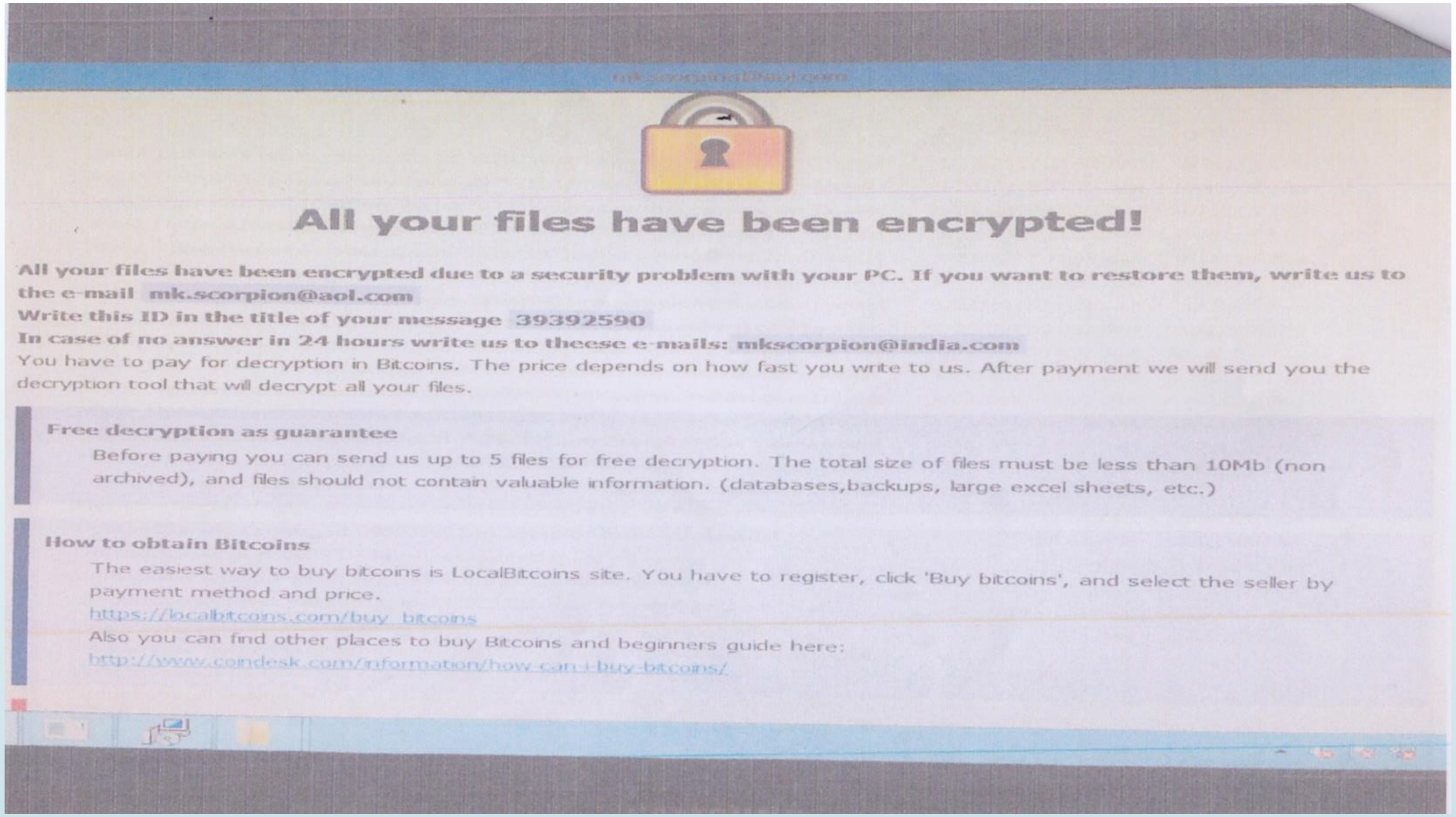
1. Locky > Crypto
   - Dharma
2. Teslacrypt > Crypto
3. Hddcryptor > Crypto
4. Crylocker > Locker
5. Cerber > Crypto
6. Petya and Mischa > Crypto
7. Chimera > Crypto
8. Jigsaw > Crypto
9. Samsam > Crypto
10. Cryptowall > Crypto

Source: https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/top-10-ransomware-strains-2016/

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.

A sample screenshot of a ransomware



All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail mk.scorpion@aol.com

Write this ID in the title of your message 39392590

In case of no answer in 24 hours write us to theese e-mails: mkscorpion@india.com

You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 5 files for free decryption. The total size of files must be less than 10Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

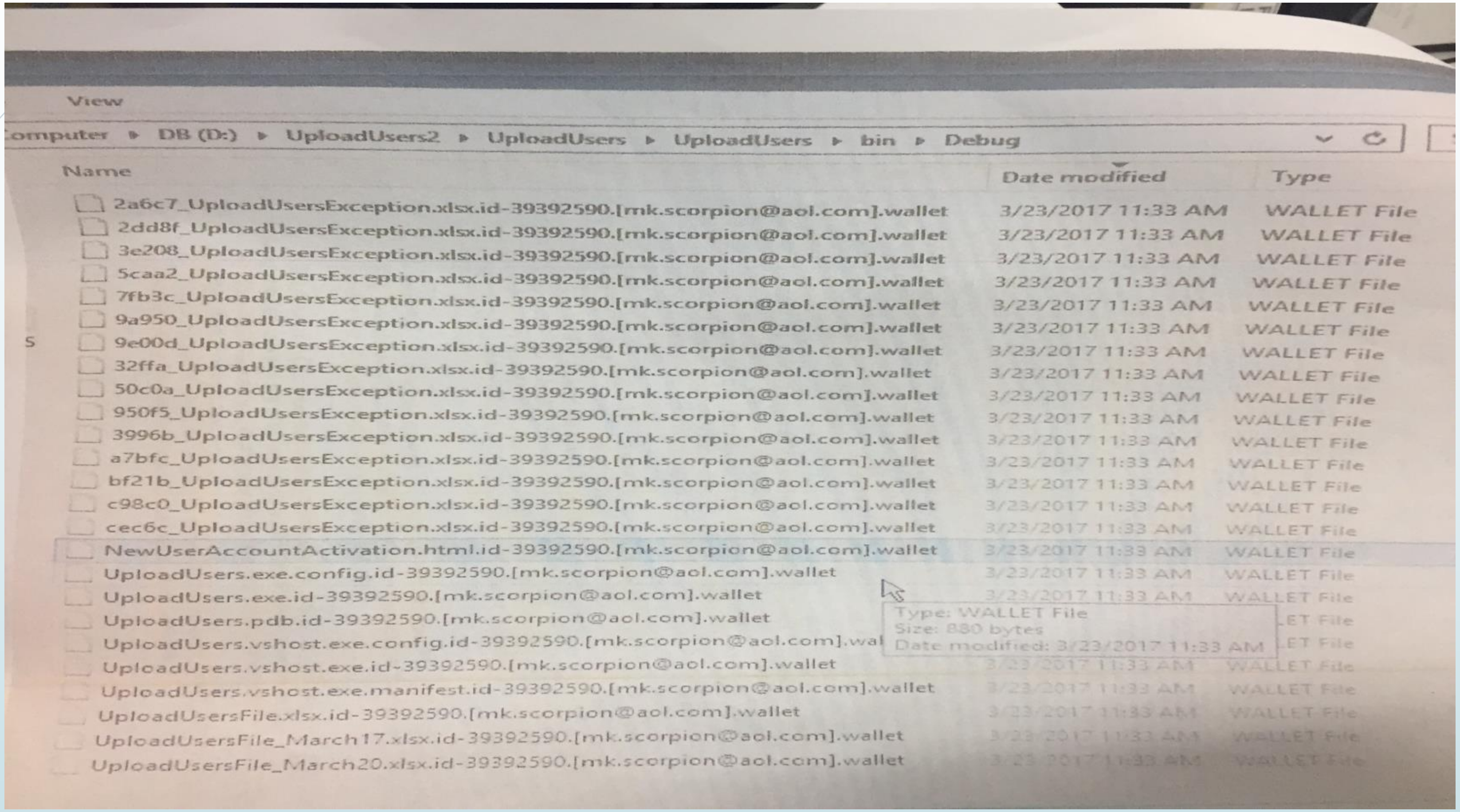
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

Warning pop up on the screen with instructions on how to pay for the decryption key.

INFORMATION TECHNOLOGY MANAGEMENT SERVICE · PNP ·

WEB SERVICES and CYBER SECURITY DIVISION

A sample screenshot of Ransomware



View
omputer ▸ DB (D:) ▸ UploadUsers2 ▸ UploadUsers ▸ UploadUsers ▸ bin ▸ Debug

Name	Date modified	Type
2a6c7_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
2dd8f_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
3e208_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
5caa2_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
7fb3c_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
9a950_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
9e00d_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
32ffa_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
50c0a_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
950f5_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
3996b_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
a7bfc_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
bf21b_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
c98c0_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
cec6c_UploadUsersException.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
NewUserAccountActivation.html.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
UploadUsers.exe.config.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
UploadUsers.exe.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
UploadUsers.pdb.id-39392590.[mk.scorpion@aol.com].wallet		ET File
UploadUsers.vshost.exe.config.id-39392590.[mk.scorpion@aol.com].wal		ET File
UploadUsers.vshost.exe.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
UploadUsers.vshost.exe.manifest.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
UploadUsersFile.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
UploadUsersFile_March17.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File
UploadUsersFile_March20.xlsx.id-39392590.[mk.scorpion@aol.com].wallet	3/23/2017 11:33 AM	WALLET File

Type: WALLET File
Size: 880 bytes
Date modified: 3/23/2017 11:33 AM

Files when infected by ransomware

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.

Offense Committed Using Ransomware

Under R.A. 10175 “Cybercrime Prevention Act of 2012”

- **Data Interference** – the intentional alteration, damaging, deletion of data and transmission of viruses.
- **System Interference** – the intentional inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, and transmission of viruses.

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.

Mitigation Measures (continued)

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, you may contact ITMS WSCSD thru the following:

- Telephone Number: **(02) 7230401 local 4225**;
- E-mail address: **wscsditms@pnp.gov.ph**; and
- Chat Service: **www.itms.pnp.gov.ph**

THANK YOU

INFORMATION TECHNOLOGY MANAGEMENT SERVICE · PNP

WEB SERVICES
and CYBER SECURITY DIVISION