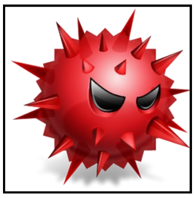
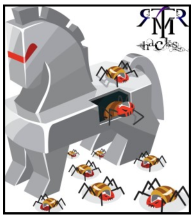
Cybersecurity Threats

Malware—Short for "Malicious Software". Malware is the generic term for all types of harmful software. Malware have varying ways of infecting systems and propagating themselves.



Virus—A virus is a form of malware that is capable of copying itself and spreading to other computers. Viruses often spreads to other compOuters by attaching themselves to various programs and executing code when a user launches one of those infected programs



Trojan Horse—A Trojan horse or Trojan, is a type of malware that disguises itself as a legitimate file or software. When your download and run the program, the Trojan horse will run in the background, allowing third-parties to access your computer.

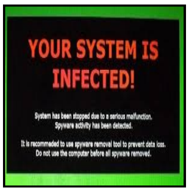
Spyware—Spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, screen recording, collecting mouse clicks and keystrokes via key loggers, data harvesting (account information, logins, financial data) and more.

Rootkits—A rootkit is a hidden malware that operates at the most basic level ("the root") of the operating system. It is used to obtain administrator-level access and create a backdoor to remotely access and control a computer without being detected by users or security programs.

Ransomeware—Ransomeware is a form of malware that essentially holds a computer system captive while demanding a ransom. The malware restrict user access to the computer either by encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the malware creator to remove the restrictions and regain access to their computer.

Cybersecurity Threats

Adware—Adware is a common type of malware that automatically delivers advertisements. Common examples of adware include pop-ups and ads displayed within the software. Often times, software and applications offer "free" version that come bundled with adware. Most adware is sponsored or authored by advertisers and serves as a revenue generating toll. While some adware is solely designed to deliver advertisements. It is not uncommon for adware to come bundled with spyware.


YOUR SYSTEM IS INFECTED!

System has been stopped due to a serious malfunction.
Spyware activity has been detected.

It is recommeded to use spyware removal tool to prevent data loss.
Do not use the computer before all spyware removed.

Scareware— Also known as "rogue security software, scareware uses pop-ups or alerts to notify the user that the computer is allegedly infected and recommends a fake security software to be downloaded and installed to fix the problem. However, instead of removing the supposed infection, it installs actual malware,

Bots— A bot is a malicious self-propagating malware designed to infect a host and connect back to a central server or servers that act as a command and control (C&C) center for an entire network of compromised devices or "botnet". With a botnet, attackers can launch broad-based "remote control", flood-type attacks against their target(s) known as Distributed Denial of Service or DDoS attacks.

Spam— Spam is the electronic sending if mass unsolicited message. The most common medium for spam is email, but it is not uncommon for spammers to use instant messages, texting, blogs, web forums, search engines and social media. While spam is not actually a type of malware, it is very common for malware to spread through spamming. This happens when computers that are infected with viruses, worms or other malware are used to distribute spam messages containing more malware.

Cybersecurity Threats

Bugs– Bugs are not malware but rather flaws that are usually a result of human error and typically exist in the source code or compilers of a program. These vulnerabilities can be exploited by cyber criminals to bypass a computer's security measures if left unpatched.

Phishing– Phishing uses deception, usually through spoofing of emails or typo squatting websites making the user believe that they are a legitimate person, company or site asking for personal and financial information such as passwords and credit cards details. While phishing attacks are sent to a general group of people, spear phishing on the other hand is a phishing attack that targets a specific person. Spear phishing high-level targets such as CEOs and other executives is also called "whaling". Phishing through voice call is called "vishing".

Social Engineering– Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. It is said that it is much easier to trick someone onto revealing a password for as system than to exert the effort of hacking into the system. Social engineering also uses all available information at their disposal such as publicly-viewable information in social media accounts.

Wi-Fi Eavesdropping– Wi-Fi eavesdropping is another method used by cyber criminals to capture personal information. With the right equipment, cyber criminals can "listen in" on information that's shared over an unsecured (not encrypted) public Wi-Fi.

Drive-by Downloads– The automatic download of software to a user's computer triggered simply by a website or viewing an HTML formatted email. The download occurs without the user's consent and often without any notice at all.

Cybersecurity Incident Response Quick Guide

A. In case of malware infection

1. Disconnect the computer/device from the network.
2. If it is detected by a security software, take not of the type of infection.
3. If it is undetected by a security software but the computer/device is possibly experiencing infection-like symptoms/effects, take note of this symptoms/effect.
4. Take note of the suspected source of the infection.
5. Make sure to quarantine the suspected source of the infection.
6. Report the incident immediately to the Directorate for Information Systems, OA-6 at contact number: VABEX 6610 and Cyber Security Flight, 952nd MIS, 950th CEISG at contact number 6729.
7. Update the security software and run a scan.

B. In case of ransomware infection

Symptoms: encrypted files, password-protected files, hacker initiated contact and tries to extort money.

1. Disconnect the computer/device from the network.
2. If it is detected by a security software, take not of the type of infection.
3. If it is undetected by a security software but the computer/device is possibly experiencing ransomeware attack, take note of the file being held for ransom.
4. Take note of the suspected source of the infection.
5. Make sure to quarantine the suspected source of the infection.
6. Report the incident immediately to the Directorate for Information Systems, OA-6 at contact number: VABEX 6610 and Cyber Security Flight, 952nd MIS, 950th CEISG at contact number 6729.
7. Update the security software and run a scan.

C. In case phishing/spear phishing attack

Symptoms: unusual information requests, unusual tone/language used in email as opposed to other emails by the same sender, unusual email attachments, misspelled URLs.

1. If even without opening the email, a message is already suspected to be a phishing attack, take not WITHOUT OPENING the sender's name, email address, and the subject of the email. Then, WITHOUT OPENING, highlight the message and send it to the spam folder.
2. If you have opened the message and see that it is a phishing attack, take note of of the same info mentioned above, and in addition, the kind of info being asked, the account/s that they are trying to breach and WITHOUT CLICKING, the URLs of the links provided. Then close the email and highlight the message and send it to the spam folder.
3. Report the incident immediately to the Directorate for Information Systems, OA-6 at contact number: VABEX 6610 and Cyber Security Flight, 952nd MIS, 950th CEISG at contact number 6729.

Cybersecurity Incident Response Quick Guide

D. In case of suspected Distributed Denial of Service (DDoS) attack

Symptoms: unusually slow network performance (opening files or accessing websites), unavailability of a particular website, inability to access any website, dramatic increase in the amount of spam you receive in your account.

1. Disconnect the computer/device from the network.
2. Report the incident immediately to the Directorate for Information Systems, OA-6 at contact number: VABEX 6610 and Cyber Security Flight, 952nd MIS, 950th CEISG at contact number 6729.

E. In case of password being changed/compromised

1. Disconnect the computer/device from the network.
2. Refrain from logging into other accounts.
3. Update the security software and run a scan to check for possible spyware.
4. Check the installed software on the computer/device to see if there are suspicious software installed that might be spyware.
5. Check if the computer/device itself if there are any hardware keyloggers attached.
6. Report the incident immediately to the Directorate for Information Systems, OA-6 at contact number: VABEX 6610 and Cyber Security Flight, 952nd MIS, 950th CEISG at contact number 6729.
7. Try to recover the hacked account through a known secure computer/device.

REPORT CYBER INCIDENTS IMMEDIATELY TO PREVENT FURTHER HARM TO THE NETWORK

Cybersecurity Best Practices

1. LOGOUT of your accounts and LOGOFF before leaving your computer.

2. Always UPDATE your Computer Security Software, Operating System, and other software you frequently use.

3. Turn on your PERSONAL FIREWALL.

4. Use STRONG PASSWORDS of AT LEAST (14) FOURTEEN CHARACTERS with a combination of upper and lower case letters, numbers, and symbols.

5. Change passwords AT LEAST (3) THREE MONTHS.

6. DO NOT POST PASSWORDS any where. Memorize them. Use COMPLEX YET EASILY MEMORABLE passwords such as acronyms, phrases, quotes, lyrics, etc.

7. DO NOT USE COMMERCIAL EMAIL SERVICES, especially when sending sensitive military information.

8. DO NOT OPEN suspicious emails, links or attachments.

9. LIMIT PERSONAL INFORMATION available and accessible online especially in Social Media Accounts.

10. Only use LICENSED SOFTWARE.

11. Make a BACKUP of your files.

12. Use ENCRYPTION if available.

13. AVOID connecting to PUBLIC WI-FI NETWORKS.

14. Enable ACCESS PROTECTION on your mobile devices such as PINs, Fingerprints, Passwords, or Pattern locks.

Contacts

AFP Computer Security Incidents Response Team (AFCSIRT)
Cyberspace Security Group (CSG), CEISSAFP, AFPGHQ

CATEX : (774) 5873
PLDT: (02) 911-6001 LOCAL 5873

Cyberspace Management Division (CMD)
ODCS for CEIS, J6, AFPGHQ
CATEX : (774) 6210
PLDT: (02) 911-6001 LOCAL 6210

Cybersecurity Division (CSD)
Network Enterprise and Communication Center (NETC) Army Signal Regiment
Philippine Army (PA)
PATEX: (765) 4491
PLDT: (02) 845-9555 local 4491

Cybersecurity Group (CSG)
Naval Information and Communication Technology Center (NICTC)
Philippine Navy (PN)
PNTEX: (764) 4392
PLDT: (046) 431-2120

952ND Information Systems Squadron
Philippine Air Force (PAF)
PAFTEX: (762) 6729
PLDT: (02) 853-4944

Anti-Cybercrime Group (ACG)
Philippine National Police (PNP)

References:

- Balikatan 2016 Cyber Security Pamphlet— :Incident Response Guide & Best Practices.
- https://icons8.com