Common Cyber Threats: Indicators and Countermeasures

* Common Cyber Threats
  + If you suspect you may have been a target of any of the threats included here, or have been targeted by any other cyber threat, report it to your FSO or security point of contact immediately.
  + Common cyber threats include:
    - Phishing and Spear Phishing
      * The Threat
        + Phishing is a high-tech scam that uses e-mail to deceive you into disclosing personal information. It puts your personal information and your organization’s information at risk. Spear phishing is a type of targeted phishing that appears to be directed towards a specific individual or group of individuals.
      * Indicators
        + The following are suspicious indicators related to phishing and spear phishing:

Uses e-mail

May include bad grammar, misspellings, and/or generic greetings.

May include maliciously-crafted attachments with varying file extension or links to.

May appear to be from a position.

* + - * Countermeasures
        + The following countermeasures can be taken to guard against phishing and spear phishing:

Watch out for phishing and spear phishing

Delete suspicious e-mails

Contact your system security point of contact with any questions.

Report any potential incidents

Look for digital signatures

Configure Intrusion Detection Systems (IDS) to block malicious domains / IP addresses.

Ensure anti-virus software and definitions are up to date.

* + - * Do Not
        + Open suspicious e-mails
        + Click on suspicious links or attachments in e-mails
        + Call telephone numbers provided in suspicious e-mails
        + Disclose any information
      * If you suspect you may have been a target of phishing, report it to your Facility Security Officer (FSO) or security point of contact.
    - Malicious Code
      * The Threat
        + Malicious code is software that does damage and/or creates unwanted behaviors. Malicious code includes

Viruses

Trojan horses

Worms

Keyloggers

Spyware

Rootkits

Backdoors

* + - * Indicators
        + Effects include, but are not limited to:

Corrupt files and destroyed or modified information

Compromise and loss of information

Hacker access and sabotaged systems

* + - * Countermeasures
        + The following countermeasures can be taken to guard against malicious code. To guard against malicious code in email:

View e-mail messages in plain text

Do not view e-mail using the preview pane

Use caution when opening e-mail

Scan all attachments

Delete e-mail from senders you do not know

Turn off automatic downloading

* + - * + To guard against malicious code in websites.

Block malicious links / IP addresses

Block all unnecessary ports at the Firewall and Host

Disable unused protocols and services

Stay current with all operating system service packs and software patches

* + - * + If you suspect your information system has been compromised, report it to your FSO or security point of contact.
    - Weak and Default Passwords
      * The Threat
        + The use of weak and default passwords creates easily exploitable system vulnerabilities.
      * Indicators
        + The following are indicators of weak passwords; weak passwords include those that use:

Words found in the dictionary

Readily available information significant to you (name, dates, cities, etc.)

Lack of character diversity (e.g., all lower-case letters)

* + - * + Effects include but are not limited to, hackers:

Exploiting users’ habit of repeating passwords across sites and systems

Cracking passwords to less secure sites

Accessing your and your organization’s information

* + - * Countermeasures
        + The following countermeasures can be taken to guard against password compromise, when creating a password:

Combine letters, numbers, special characters

Do not use personal information

Do not use common phrases or words

Do not write down your password, memorize it

Change password according to your organization’s policy

Enforce account lockout for end-user accounts after a set number of retry attempts

Do not save your passwords or login credentials in your browser

Never share your password

* + - * + If you suspect your password has been compromised, report it to your FSO or security point of contact.
    - Unpatched or Outdated Software Vulnerabilities
      * The Threat
        + Unpatched or outdated software provide vulnerabilities and opportunities for adversaries to access information systems.
      * Indicators
        + The following is a list of suspicious indicators related to unpatched and outdated software:

Unauthorized system access attempts

Unauthorized system access to or disclosure of information

Unauthorized data storage or transmission

Unauthorized hardware and software modifications

* + - * + Effects include but are not limited to:

Corrupt files and destroyed or modified information

Hard drive erasure and loss of information.

* + - * Countermeasures
    - Removable Media
      * The Threat
        + Removable media is any type of storage device that can be added to and removed from a computer while the system is running. Adversaries may use removable media to gain access to your system. Examples of removable media include:

Thumb drives

Flash drives

CDs

DVDs

External hard drives

* + - * Indicators
        + The following is a list of suspicious indicators related to removable media. Adversaries and hackers may.
        + Hacker access and sabotaged systems.
      * Countermeasures
        + The following.

Attack Surface & Methods

* When looking at the number of breaches per asset category, servers have typically been on top – that.

Insider Threat

* Insiders / contractors are the most likely perpetrators of security incidents reported in South America.
* 57% of respondents consider employees the most likely source of an attack
* The majority of employees perpetrated their acts while in the office right under the noses of coworkers.
* 72% of security incidents at financial services organizations involved a current or former employee.
* Third parties with trusted access were responsible for 41% of the detected security incidents at financial services organizations.

GROUP

Read ------------- Write / Read ------------- Admin

Corporate Espionage, Activists, Hacktivists & Nation States

* Compromises attributed to competitors were highest in Asia Pacific.
* Almost half (47%) of respondents from China point to competitors as the source of security incidents, higher than any other nation.
* Automotive firms saw an 84% increase in security incidents from activists / hacktivists.
* Attacks by nation-states jumped 80% at technology companies, explaining increase in IP theft perhaps.

Policies & Procedures

* One in three companies do not have a written information security policy (“WISP”).
* 77% of organizations have a password policy or standard.
* 59% of organizations have a.

Current IT Security Methods

IAM

* Identity and access management (“IAM”) is the discipline for managing access to enterprise resources. It is a foundational element of any information security program and one of the security areas that users interact with the most.

IAM life cycle

* Strategy and governance
  + User access request and approve – Provision / de-provision – Enforce – Report and audit – Review and certify – Reconcile – Repeat.
* Provision / de-provision
  + Definition objective:
    - Granting users appropriate entitlements and access in a timely manner.
    - Revoking access in a timely manner when no longer required due to termination or transfer.
  + Common challenges
    - Time lines to grant / remove access is excessive.
    - Inefficient and error-prone manual provisioning.

Two – Factor Authentication (the problem)

* To use many of the services on the Internet today, such as email, online banking or online shopping, you must first prove you are who you say you are. This process of proving your identity is known as authentication. Authentication is done by using something you know (such as your password), something you have (such as your smartphone), or something unique to you (such as a retinal scan or fingerprint). Traditionally, one of the most common ways of authenticating has been a username and a password. The problem with using just a password for authentication is simple: all an attacker needs to do is guess or compromise your password and they gain instant access to your online account and information. If you use the same username and password for multiple accounts, the harm can.

Data Breach

* A data breach is an incident wherein information is stolen or taken from a system without the knowledge or authorization of the system’s owner. A small company or a large organization may suffer a data breach. Stolen data may involve sensitive, proprietary, or confidential information, such as credit card numbers, customer data, trade secrets or matters of national security.

Breach methods observed across industries

* Based on data breach incidents recorder between January 2005 and April 2015, personally identifiable information [PII] was the most stolen record type while financial data came in second.
  + Hacking or malware – 25.0%
  + Portable device loss – 24.0%
  + Unintended disclosure – 17.4%
  + Insider leak – 12.0%
  + Physical loss – 11.6%
  + Stationary device loss – 5.4%
  + Payment card fraud – 1.4%
  + Unknown – 3.2%

The NIST Internal / Interagency Report NISTIR 7298 (Glossary of Key Information Security Terms, May 2013) defines the term computer security as follows:

* “Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.”

Data and services

* Confidentiality
* Integrity
* Authenticity
* Availability
* Accountability

Key Security Concepts

* Confidentiality
  + Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
* Integrity
  + Guarding against improper information modification or destruction, including enduring information nonrepudiation and authenticity.
* Availability
  + Ensuring timely and reliable access to and use of information.

Levels of Impact

* Low
  + The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
* Moderate
  + The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
* High
  + The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Assets of a Computer System

* Hardware
* Software
* Data
* Communication facilities and networks

Vulnerabilities, Threats and Attacks

* Categories of vulnerabilities
  + Corrupted (loss of integrity)
  + Leaky (loss of confidentiality
  + Unavailable or very slow (loss of availability)
* Threats
  + Capable of exploiting vulnerabilities
  + Represent potential security harm to an asset.
* Attacks (threats carried out)
  + Passive – Attempt to learn or make use of information from the system that does not affect system resources
  + Active – attempt to alter system resources or affect their operation
  + Insider – initiated by an entity inside the security parameter
  + Outsider – initiated from outside the perimeter

Countermeasures

* Means used to deal with security attacks
  + Prevent
  + Detect
  + Recover
* May itself introduce new vulnerabilities
* Goal is to minimize residual level of risk to the assets
* Residual vulnerabilities may remain