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
- Malicious code
- Weak and default passwords
- Unpatched or outdated software vulnerabilities
- Removable media

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 a malicious website
- May appear to be from a position of authority or legitimate company:
  - Your employer
  - Bank or credit card company
  - Online payment provider
  - Government organization
- Asks you to update or validate information or click on a link
- Threatens dire consequence or promises reward
- Appears to direct you to a web site that looks real

Spear phishing specifically:

- Has a high level of targeting sophistication and appears to come from an associate, client, or acquaintance
- May be contextually relevant to your job
- May appear to originate from someone in your email address book
- May contain graphics that make the email look legitimate

Effects include, but are not limited to:

- Deceiving you into disclosing information
- Allowing adversary to gain access to your and/or your organization’s information

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

The following are suspicious indicators related to malicious code; malicious code may be distributed via:

- E-mail attachments
- Downloading files
- Visiting an infected website
- Removable media

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 (names, 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
- Hacker access and sabotaged systems

Countermeasures

The following countermeasures can be taken to guard against software vulnerabilities:

- Comply with the measures in your organization’s policies, including the Technology Control Plan (TCP)
- Stay current with patches and updates
- Conduct frequent computer audits
    - Ideally: Daily
    - At minimum: Weekly
- Do not rely on firewalls to protect against all attacks
- Report intrusion attempts
- Disconnect computer system temporarily in the event of a severe attack

If you suspect your information system has been compromised, report it to your FSO or security point of contact.

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:

- Leave removable media, such as thumb drives, at locations for personnel to pick up
- Send removable media to personnel under the guise of a prize or free product trial

Effects include, but are not limited to:

- Corrupt files and destroyed or modified information
- Hacker access and sabotaged systems

Countermeasures

The following countermeasures can be taken to guard against removable media vulnerabilities.

Contractors: Follow your organization's removable media policy

DoD personnel:

- Do not use flash media unless operationally necessary and government-owned
- Do not use any personally owned/non-Government removable flash media on DoD systems
- Do not use Government removable flash media on non-DoD/personal systems
- Encrypt all data stored on removable media
- Encrypt in accordance with the data's classification or sensitivity level
- Use only removable media approved by your organization
- Store in GSA approved storage containers at the appropriate level of classification

The DoD severely restricts or prohibits the use of removable media. Consult your security point of contact (POC) for current policy.

If you suspect you have been targeted via removable media, report it to your FSO or security point of contact.