UNIT 1.2

Threats in Cyberspace

Who are the threats?

Some compare Cyberspace to the U.S. wild west era where the outlaws ruled the landscape and innocent people were often victims to various crimes. But what differentiates Cyberspace from that time in history is the anonymity of the attackers. It's important to classify the threat actors and understand their motives in cyberspace.

Now that we know the threats and their respective motives, we need to understand their methodologies. What are the indicators that a cyber breach has occurred and what countermeasures can we put into place to prevent these types of attacks. In this lesson we will discuss five common cyber threats:

1. Phishing
2. Malware
3. Weak or default passwords
4. Un-patched or outdated software
5. Removable media

- Phishing

This is a process where a malicious actor sends a convincing email to a set of targets. The goal is to get the target to disclose personal information, click on a malicious email attachment or malicious link. Spear-phishing is a targeted attack directed against a specific person or group.

- Indicators

Here are indicators related to phishing campaigns:

Typically email-based

FROM email addresses are not from legitimate domains

Bad grammar, spelling mistakes, bad translations

May contain malicious links or attachments

Appears to be from a position of authority (e.g. IRS, FBI, your boss)

Asks the user to update their information

Directs to a website that looks legitimate

- Malware (Malicious Software)

Malicious software or "malware" is used by adversaries to: damage a system, perform unwanted behavior, or establish a foothold for future malicious activity. The following are common types of malware:

Viruses

Malware that self-replicates, usually via removable storage media

Worms

Malware that does not require user interaction and may use stolen credentials to "worm" its way across a network to infect other systems.

Trojan

Malware designed to appear as legitimate software and usually requires user interaction to run (i.e. double-click to run)

Keyloggers

Malware designed to record user keystrokes and/or mouse-clicks

Spyware

Malware designed to record user activity to include: browser history, cookies, keystrokes. This software can also activate builtin cameras and microphones unbeknownst to the user

Rootkits

Malware designed to subvert the operating system and hide malicious activity

Backdoors

Malware designed for access into a target system only known by the attacker

- Indicators

Malware may come from the following sources:

E-mail attachments

Infected websites

Infected removable media (e.g. USB drive)

Malware can cause the following effects:

Destroyed or modified data

System or network disruptions/latency

Loss of personal data

Allow malicious actor access to system/network