Malware

Objective 2.4: Given a scenario, analyze indicators of malicious activity

- **Malware**
    - *Malware*
        - Malicious software designed to infiltrate computer systems and potentially damage them without user consent
    - Categories
        - Viruses
        - Worms
        - Trojans
        - Ransomware
        - Spyware
        - Rootkits
        - Spam
    - Threat Vector vs. Attack Vector
        - *Threat Vector*
            - Method used to infiltrate a victim's machine
            - Examples
                - Unpatched software
                - USB drive installation
                - Phishing campaigns
        - *Attack Vector*
            - *Means by which the attacker gains access and infects the system*
            - *Combines both infiltration method and infection process*

- Types of Malware Attacks
    - *Viruses*
        - Attach to clean files, spread, and corrupt host files
    - *Worms*
        - Standalone programs replicating and spreading to other computers
    - *Trojans*
        - Disguise as legitimate software, grant unauthorized access
    - *Ransomware*
        - Encrypts user data, demands ransom for decryption
    - *Zombies and Botnets*
        - Compromised computers remotely controlled in a network for malicious purposes
    - *Rootkits*
        - Hide presence and activities on a computer, operate at the OS level
    - *Backdoors and Logic Bombs*
        - Backdoors allow unauthorized access, logic bombs execute malicious actions
    - *Keyloggers*
        - Record keystrokes, capture passwords or sensitive information
    - *Spyware and Bloatware*
        - Spyware monitors and gathers user/system information, bloatware consumes resources without value
- Malware Techniques and Infection Vectors
    - Evolving from file-based tactics to modern fileless techniques
    - Multi-stage deployment, leveraging system tools, and obfuscation techniques

- Indications of Malware Attack
    - Recognizing signs like the following
        - Account lockouts
        - Concurrent session utilization
        - Blocked content
        - Impossible travel
        - Resource consumption
        - Inaccessibility
        - Out-of-cycle logging
        - Missing logs
        - Documented attacks

- **Viruses**
    - *Computer Virus*
        - Made up of malicious code that's run on a machine without the user's knowledge and this allows the code to infect the computer whenever it has been run
    - 10 Different Types of Viruses
        - *Boot Sector*
            - One that is stored in the first sector of a hard drive and is then loaded into memory whenever the computer boots up
        - *Macro*
            - Form of code that allows a virus to be embedded inside another document so that when that document is opened by the user, the virus is executed

- *Program*
  - Try to find executables or application files to infect with their malicious code
- *Multipartite*
  - Combination of a boot sector type virus and a program virus
  - Able to place itself in the boot sector and be loaded every time the computer boots
  - It can install itself in a program where it can be run every time the computer starts up
- *Encrypted*
  - Designed to hide itself from being detected by encrypting its malicious code or payloads to avoid detection by any antivirus software
- *Polymorphic*
  - Advanced version of an encrypted virus, but instead of just encrypting the contents it will actually change the viruses code each time it is executed by altering the decryption module in order for it to evade detection
- *Metamorphic*
  - Able to rewrite themselves entirely before it attempts to infect a given file
- *Stealth*
  - Technique used to prevent the virus from being detected by the anti-virus software
- *Armored*
  - Have a layer of protection to confuse a program or a person who's trying to analyze it
- *Hoax*
  - Form of technical social engineering that attempts to scare our end users

into taking some kind of undesirable action on their system

- **Worms**
  - *Worm*
    - Piece of malicious software, much like a virus, but it can replicate itself without any user interaction
    - Able to self-replicate and spread throughout your network without a user's consent or their action
  - Worms are dangerous for two reasons
    - Infect your workstation and other computing assets
    - Cause disruptions to your normal network traffic since they are constantly trying to replicate and spread themselves across the network
  - Worms are best known for spreading far and wide over the internet in a relative short amount of time
- **Trojans**
  - *Trojan*
    - Piece of malicious software that is disguised as a piece of harmless or desirable software
    - Claims that it will perform some needed or desired function for you
  - *Remote Access Trojan (RAT)*
    - Widely used by modern attackers because it provides the attacker with remote control of a victim machine
  - Trojans are commonly used today by attackers to exploit a vulnerability in your workstation and then conducting data exfiltration to steal your sensitive documents,

creating backdoors to maintain persistence on your systems, and other malicious activities

- **Ransomware**
  - *Ransomware*
    - Type of malicious software that is designed to block access to a computer system or its data by encrypting it until a ransom is paid to the attacker
  - How can we protect ourselves and our organizations against ransomware?
    - Always conduct regular backups
    - Install software updates regularly
    - Provide security awareness training to your users
    - Implement Multi-Factor Authentication (MFA)
  - What should you do if you find yourself or your organization as the victim of a ransomware attack?
    - Never pay the ransom
      - Paying the ransom doesn't actually guarantee that you will ever get your data back
    - If you suspect ransomware has infected your machine, you should disconnect it from the network
    - Notify the authorities
    - Restore your data and systems from known good backups

- **Zombies and Botnets**
  - *Botnet*
    - Network of compromised computers or devices controlled remotely by malicious actors

- *Zombie*
  - Name of a compromised computer or device that is part of a botnet
  - Used to perform tasks using remote commands from the attacker without the user's knowledge
- *Command and Control Node*
  - Computer responsible for managing and coordinating the activities of other nodes or devices within a network
- Botnets are used
  - as pivot points
  - disguise the real attacker
  - to host illegal activities
  - to spam others by sending out phishing campaigns and other malware
- Most common use for a botnet is to conduct a DDoS (Distributed Denial-of-Service) attack
  - *Distributed Denial-of-Service (DDoS) Attack*
    - Occurs when many machines target a single victim and attack them at the exact same time
- Botnets are used by attackers to combine processing power to break through different types of encryption schemes
- Attackers usually only use about 20-25% of any zombie's power

- **Rootkits**
  - *Rootkit*
    - Designed to gain administrative level control over a given computer system without being detected

- Account with the highest level of permissions is called the Administrator account
    - Allows the person to install programs, delete programs, open ports, shut ports, and do whatever it is they want to do on that system
    - In a UNIX, Linux, or MacOS computer, this type of administrator account is actually called the root account
- A computer system has several different rings of permissions throughout the system
    - *Ring 3 (Outermost Ring)*
        - Where user level permissions are used
    - *Ring 0 (Innermost or Highest Permission Levels)*
        - Operating in Ring 0 is called "kernel mode"
        - *Kernel Mode*
            - Allows a system to control access to things like device drivers, your sound card, your video display or monitor, and other similar things
- If you login as the administrator or root user on a system, you have root permission and you will be operating at Ring 1 of the operating system
    - Remember, the closer the malicious code is to the kernel, the more permissions it will have and the more damage it can cause on your system
- When a rootkit is installed on a system, it tries to move from Ring 1 to Ring 0 so that it can hide from other functions of the operating system to avoid detection
- One technique used by rootkits to gain this deeper level of access is a DLL injection
    - *DLL Injection*
        - Technique used to run arbitrary code within the address space of another process by forcing it to load a dynamic-link library
    - *Dynamic Link Library (DLL)*
        - Collection of code and data that can be used by multiple programs simultaneously to allow for code reuse and modularization in software

development

- *Shim*
    - Piece of software code that is placed between two components and that intercepts the calls between those components and can be used redirect them
- Rootkits are extremely powerful, and they are very difficult to detect because the operating system is essentially blinded to them
    - To detect them, the best way is to boot from an external device and then scan the internal hard drive to ensure that you can detect those rootkits using a good anti-malware scanning solution from a live boot Linux distribution

- **Backdoors and Logic Bombs**
    - *Backdoor*
        - Originally placed in computer programs to bypass the normal security and authentication functions
        - Most often put into systems by designers and programmers
        - Remote Access Trojan (RAT) acts just like a backdoor in our modern networks
            - Can be placed by a threat actor on your computer to help them maintain persistent access to that system
    - *Easter egg*
        - a hidden feature or novelty within a program that is typically inserted by the software developers as an inside joke
        - Code often has significant vulnerabilities
    - *Logic Bombs*
        - Malicious code that's inserted into a program, and the malicious code will only execute when certain conditions have been met

- **Keylogger**
    - *Keylogger*
        - Piece of software or hardware that records every single keystroke that is made on a computer or mobile device
    - Keyloggers can be either software-based or hardware-based
        - *Software Keyloggers*
            - Malicious programs that get installed on a victim's computer
            - Often bundled with other software or delivered through social engineering attacks, like phishing or pretexting attacks
        - *Hardware Keyloggers*
            - Physical devices that need to be plugged into a computer
            - These will resemble a USB drive or they can be embedded within a keyboard cable itself
    - To protect your organization from keyloggers, ensure the following
        - Perform regular updates and patches
        - Rely on quality antivirus and antimalware solutions
        - Conduct phishing awareness training for your users
        - Implement multi-factor authentication systems
        - Encrypt keystrokes being sent to your systems
        - Perform physical checks of your desktops, laptops, and servers

- **Spyware and Bloatware**
    - *Spyware*
        - Malicious software that is designed to gather and send information about a user or organization without their knowledge

    - Spyware can get installed on a system in several different ways
      - Bundled with other software
      - Installed through a malicious website
      - Installed when users click on a deceptive pop-up advertisement
    - To help protect yourself against spyware, you should only use reputable antivirus and anti-spyware tools that are regularly updated detect and remove any potential threats
  - *Bloatware*
    - Any software that comes pre-installed on a new computer or smartphone that you, as the user, did not specifically request, want, or need
    - Other examples of bloatware are things like unnecessary toolbars or applications that promote certain services
    - Bloatware isn’t malicious, but it can
      - waste your storage space
      - slow down the performance of your devices
      - introduce security vulnerabilities into your systems
    - Remember, anytime a piece of software is installed, that is one more potential threat vector for an attacker to exploit if you don’t properly update that application
    - To remove bloatware, you can either do the following
      - Do a manual removal process
      - Use bloatware removal tools to uninstall the unwanted applications
      - Perform a clean operating system installation

- **Malware Attack Techniques**
    - *Malware Exploitation Technique*
        - Specific method by which malware code penetrates and infects a targeted system
    - Some malware focuses on infecting the system's memory to leverage remote procedure calls over the organization's network
        - Most modern malware uses fileless techniques to avoid detection by signature-based security software
        - Fileless Malware is used to create a process in the system memory without relying on the local file system of the infected host
    - How does this modern malware work?
        - When a user accidentally clicks on a malicious link or opens a malicious file, the specific type of malware being installed is known as a stage one dropper or downloader
            - *Stage 1 Dropper or Downloader*
                - Piece of malware that is usually created as a lightweight shellcode that can be executed on a given system
            - *Dropper*
                - Specific malware type designed to initiate or run other malware forms within a payload on an infected host
            - *Downloader*
                - Retrieve additional tools post the initial infection facilitated by a dropper
            - The primary function of a stage one dropper or downloader is to retrieve additional portions of the malware code and to trick the user into activating it

- *Shellcode*
  - Broader term that encompasses lightweight code meant to execute an exploit on a given target
- *Stage 2: Downloader*
  - Downloads and installs a remote access Trojan to conduct command and control on the victimized system
- "Actions on Objectives" Phase
  - Threat actors will execute primary objectives to meet core objectives like
    - data exfiltration
    - file encryption
- Concealment
  - Used to help the threat actor prolong unauthorized access to a system by
    - hiding tracks
    - erasing log files
    - hiding any evidence of malicious activity
  - *"Living off the Land"*
    - A strategy adopted by many Advanced Persistent Threats and criminal organizations
    - the threat actors try to exploit the standard tools to perform intrusions

- **Indications of Malware Attacks**
  - 9 Common Indicators of Malware Attacks
    - *Account Lockouts*
      - Malware, especially those designed for credential theft or brute force attacks, can trigger multiple failed login attempts that would result in a user’s account being locked out
    - Concurrent Session Utilization
      - If you notice that a single user account has multiple simultaneous or concurrent sessions open, especially from various geographic locations
    - Blocked Content
      - If there is a sudden increase in the amount of blocked content alerts you are seeing from your security tools
    - *Impossible Travel*
      - Refers to a scenario where a user's account is accessed from two or more geographically separated locations in an impossibly short period of time
    - Resource Consumption
      - If you are observing any unusual spikes in CPU, memory, or network bandwidth utilization that cannot be linked back to a legitimate task
    - Resource Inaccessibility
      - *Ransomware*
        - Form of malware that encrypts user files to make them inaccessible to the user
      - If a large number of files or critical systems suddenly become inaccessible or if users receive messages demanding payment to decrypt their data

- Out-of-Cycle Logging
  - If you are noticing that your logs are being generated at odd hours or during times when no legitimate activities should be taking place (such as in the middle of the night when no employees are actively working)
- Missing Logs
  - If you are conducting a log review as a cybersecurity analyst and you see that there are gaps in your logs or if the logs have been cleared without any authorized reason
- Published or Documented Attacks
  - If a cybersecurity research or reporter published a report that shows that your organization’s network has been infected as part of a botnet or other malware-based attack