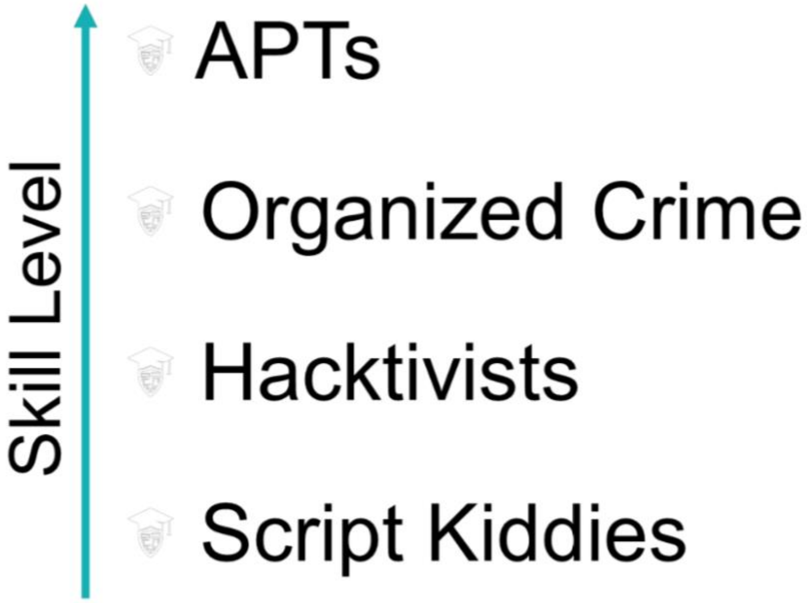
Sec+ 501 Get Certified Topic 6 – Comparing Threats, Vulnerabilities and Common attacks

CH 6 – THREAT ACTORS

- **Script Kiddies**
    - Hackers with little to no skill who only use the tools and exploits written by others
- **Hacktivists**
    - Hackers who are driven by a cause like social change, political agendas, or terrorism
- **Organized Crime**
    - Hackers who are part of a crime group that is well-funded and highly sophisticated
- **Advanced Persistent Threats**
    - Highly trained and funded groups of hackers (often by nation states) with covert and open-source intelligence at their disposal



Skill Level

APTs

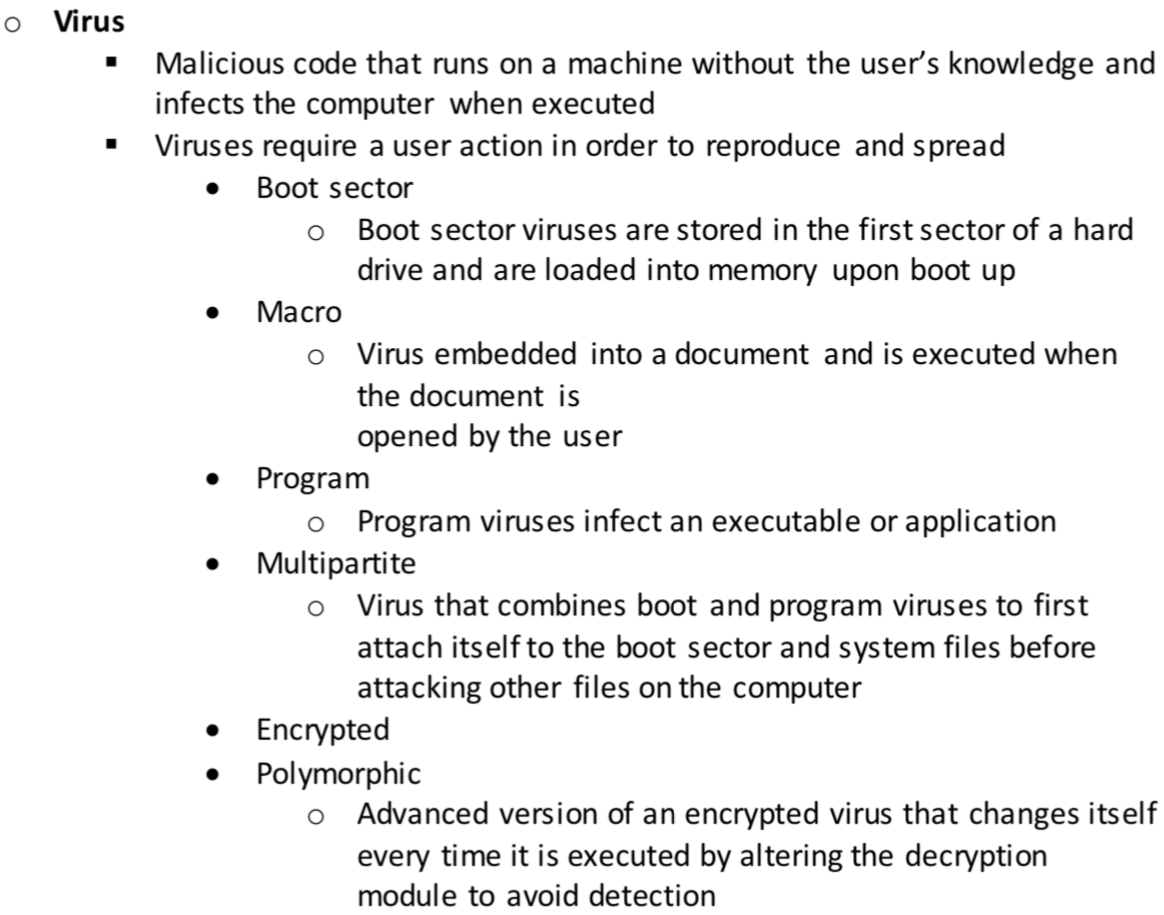
Organized Crime

Hacktivists

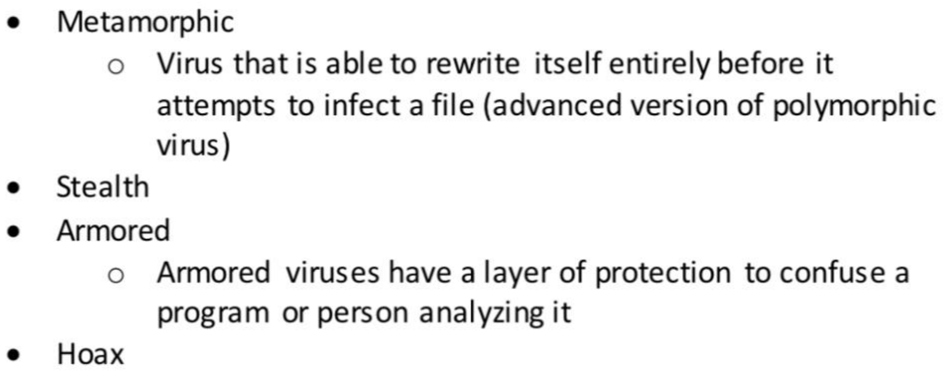
Script Kiddies

MALWARE ATTACKS

- **Remember this:**
    - **A DoS attack is an attack from a single source that attempts to disrupt the services provided by another system. A DDoS (Distributed Denial of Service) Includes multiple computers attacking a single target. DDoS attacks typically include sustained, abnormally high network traffic**



- **Virus**
  - Malicious code that runs on a machine without the user’s knowledge and infects the computer when executed
  - Viruses require a user action in order to reproduce and spread
    - Boot sector
      - Boot sector viruses are stored in the first sector of a hard drive and are loaded into memory upon boot up
    - Macro
      - Virus embedded into a document and is executed when the document is
        opened by the user
    - Program
      - Program viruses infect an executable or application
    - Multipartite
      - Virus that combines boot and program viruses to first attach itself to the boot sector and system files before attacking other files on the computer
    - Encrypted
    - Polymorphic
      - Advanced version of an encrypted virus that changes itself every time it is executed by altering the decryption module to avoid detection

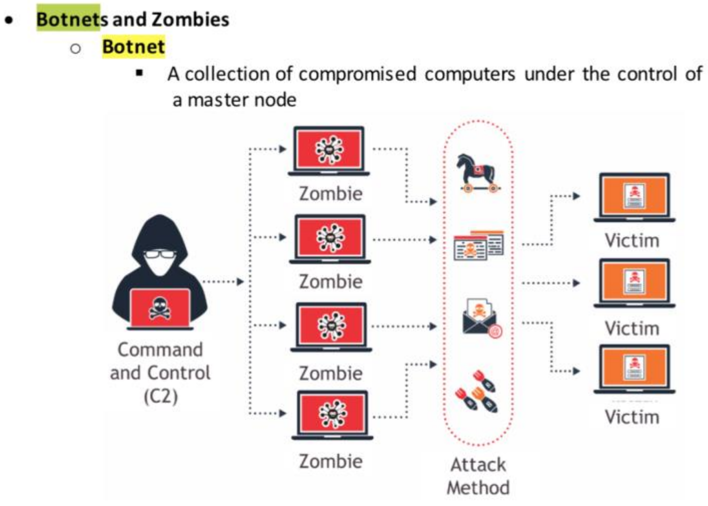


- Metamorphic
  - Virus that is able to rewrite itself entirely before it attempts to infect a file (advanced version of polymorphic virus)
- Stealth
- Armored
  - Armored viruses have a layer of protection to confuse a program or person analyzing it
- Hoax

- Worm: Self Replicating malware that travels throughout a network without assistance of a host application or user interaction. Resides in memory and can use different transport protocols to travel over the network. Consume network bandwidth.
- Logic Bomb: Executes in response to an event, such as when a specific application is executed or a specific time arrives
- Backdoor: Provides another way to access a system. Many types of malware create backdoors allowing attackers to access systems

from remote locations. Employees have also created backdoors in applications and systems.

- Trojan: Appears to be something useful but includes malicious component such as installing a backdoor on a user's system. Many Trojans are delivered via drive-by downloads. Can also infect systems from fake antivirus software, pirated software, games, or infected USB drives.
- RAT:
    - Provides the attacker with remote control of a victim computer and is the most commonly used type of Trojan from remote locations. Often delivered via drive-by downloads. Can collect/log keystrokes, usernames and passwords, incoming and outgoing email, chat sessions and browser history
- Ransomware: Malware that takes control of a user's system or data. Criminals then attempt to extort payment from victim. Ransomware often includes threats of damaging a user's system or data if the victim does not pay the ransom. Ransomware that encrypts the user's data is sometimes called crypto-malware.
- Spyware: Monitor's a user's computer and often includes a keylogger.
- Adware
    - Displays advertisements based upon its spying on you
- Grayware
    - Software that isn't benign nor malicious and tends to behave improperly without serious consequences



- Botnets and Zombies
    - Botnet
        - A collection of compromised computers under the control of a master node

- Bot – software robot.
- Botnet – usually used in DDOS and can download additional malware, adware, or spyware such as keyloggers.
- Rootkit:
    - Software designed to gain administrative level control over a system without detection
    - DLL injection is commonly used by rootkits to maintain their persistent control
    - Group of programs/ single program in rare instances – hide fact that the system has been infected or compromised by malicious code.
- **Remember this:**
    - **Rootkits have system-level or kernel access and can modify system files and system access. Rootkits hide their running processes to avoid detection with hooking techniques. Tools that can inspect RAM can discover these hidden hooked processes.**

SOCIAL ENGINEERING

- Social engineering uses social tactics to trick users into giving up information or performing actions they wouldn't normally take. Social engineering attacks can occur in person, over the phone, while surfing the internet and via email.
- Impersonation – Impersonate others
- Shoulder surfing
    - When a person uses direct observation to obtain authentication information. Looking over a person's shoulder.
    - Screen filters help prevent shoulder surfing by obscuring view for people unless they are directly in front of monitor.
- Hoax: Message tells of impending doom from a virus or other security threat but which simple doesn't exist.
- Tailgating: Following one person closely behind another without showing credentials.
- Mantrap:
    - Area between two doorways that holds people until they are identified and authenticated

- Dumpster Divers: Search through trash looking for information. Shredding or burning papers instead of throwing them away mitigates this threat.
- Watering hole attack: Malware is placed on a website that you know your potential victims will access.
- **Remember this:**
  - **Spam is unwanted email. Phishing is malicious spam. Attackers attempt to trick users into revealing sensitive information or clicking on a link. Links within email can also lead unsuspecting users to install malware.**
- Beware email from friend impersonation
- **Remember this:**
  - **Spear phishing attack targets specific groups of users. Could target employees within a company or customers of a company. Digital signatures provide assurance to recipients about who sent an email, and can reduce success of spear phishing. Whaling targets high-level executes like CFO, CTO, CEO etc.**
- Vishing: Form of phishing that uses the phone system or VOIP .some vishing attempts are fully automated. Others start automated but an attacker takes over at some point during the call.
- Steps in an attack:
  - 1. Attacker uses open source intelligence to identify a target.
    - E.G: Social media sites and news outlets
  - 2. Attacker creates a spear phishing email with a malicious link. Can include malware hosted on another site and encourage user to click link.
    - E.G: Cosy Bear and Fancy Bear
  - 3. Attacker sends spear phishing email to recipient from a server in the neutral space.
  - 4. If user clicks on link, takes user to website that looks legitimate.
  - 5. Malicious link tricks user into entering credentials, website sends information back to attacker. If malicious link installs malware such as a Rat the attacker uses it to collect information on the user’s computer.

  - 6. Attacker uses credentials to access targeted systems.
  - 7. Attacker installs malware on targeted systems
  - 8. Malware examines all the available data on these systems, such as emails and files on computers and servers.
  - 9. Malware gathers data of interest and typically divides it into encrypted chunks
  - 10. Encrypted chunks are exfiltrated out of the network and back to attacker.
- Protecting Systems from malware:
  - Spam filter on mail gateways
  - Anti-malware software on mail gateways and all systems
  - Firewalls
  - Detection tools/UTM’s
  - DEP - Data Execution Prevention
    - Security feature that prevents code from executing in memory regions marked as non-executable.
  - Advanced malware tools
  - Spam filters
  - Educate Users
    - Helps prevent incidents
- Remember this:
  - Antivirus software detects and removes malware, such as viruses, Trojans and worms.
  - Signature based antivirus software detects known malware based on signature definitions and patterns.
  - Heuristic-based software detects previously unknown malware based on behaviour such as zeroday exploits.
- Directory Traversal
  - Method of accessing unauthorized directories by moving through the directory structure on a remote server
- Arbitrary Code Execution
  - Occurs when an attacker is able to execute or run commands on a victim computer
- Remote Code Execution(RCE)
  - Occurs when an attacker is able to execute or run commands on a remote computer

- Check File Integrity
    - E.G: Hash Integrity check
- Why Social Engineering works: Psychological factors
    - Authority
        - Impersonating
        - Whaling
        - Vishing
    - Intimidation
    - Consensus – People are often more willing to like something that other people like. Some attackers take advantage of this by creating web sites with fake testimonials that promote a product.
    - Scarcity – People are often encouraged to take action when they think there is a limited quantity.
        - E.G: Apple Iphones when first released
    - Urgency
    - Trust