**Comp and Network Security Week 2**

* Threats and attacks on Endpoints
  + Malware is software that enters computer without users knowledge then performs harmful or unwanted actions
    - General term for a broad variety of damaging software
  + Evolving to become less detectable
  + Imprison
    - Malware that take away the freedom of users to do what they want. Imprisons the user.
    - Ransomware: prevents a user endpoint device from working properly until a fee is paid
  + Cryptomalware
    - Type of malware that imprisons users and encrypts all files on the device so they cannot be opened
    - The fee for the unlock key increases over time. Some new crypto-malware encrypt all files on a network or attached device
  + Launch
    - Malware that infects a computer to attack other endpoint devices: Include Virus, Worm, Bot
    - Virus
      * Two types: file based virus, file-less virus
      * File based is malicious code that is attached to a file and reproduces itself on the computer automatically
      * File-less viruses don’t attach to files, rather use native services services and processes that are part of the OS. Loads code directly into the computers RAM
      * An armored file-based virus goes to great lengths to avoid detection. Split infection and mutation
      * First, virus unloads payload to perform malicious action, then it replicates itself by inserting its code into another file
    - Worm
      * Malicious program that uses computer networks to replicate (referred to as a network virus)
      * Enters computer through the network and then takes advantage of a vulnerability in an app or an OS on the host computer
      * Can leave behind a payload like a virus
      * Worms can delete files or allow remote access to an attacker
    - Bot
      * Malware that allows the infected computer to be remotely controlled by an attacker
      * The infected computer is knows as a bot or zombie
      * When many bot computers are gathered into a logical network, they create a botnet controlled by a bot herder
  + Snoop
    - * Spyware: tracking software that is deployed without the consent or control of user
      * Keylogger: silently captures and stores each keystroke that a user types
        + The threat actor can search the captured text for information such as passwords, credit card number, or private information
        + Can be software or small hardware
  + Deceive
    - * Attempts to deceive the user, includes potentially unwanted programs (PUPs), Trojans, and remote access trojans (RATs)
      * Potentially Unwanted Program (PUP)
        + Software the user doesn’t want on their computer. Examples are ads that obstruct the screen, pop ups, etc
      * Trojan
        + An executable program that acts as its performing a benign activity, but is malicious
      * Remote Access Trojan (RAT)
        + Has the basic functionality of a trojan but also allows the attacker to remotely access the victims computer
    - Evade
      * + Attempts to help malware evade detection
        + Backdoor

Gives access to a computer, program, or service that bypasses normal security protections

* + - * + Logic Bomb

Computer code added to a legitimate program but lies dormant and avoids detection until a logical event triggers it

* + - * + Rootkits

Malware that can hide its presence and the presence of other malware on the computer. It does this by accessing lower layers of the OS

* + Application Attacks
    - Look for vulnerabilities in applications
    - Common targets are Internet Web Server
    - Scripting
      * In cross-site scripting (XSS) attack, a website that accepts user input without validating it and uses the input as a response can be exploited
      * Can trick a valid website into feeding a malicious script to another user’s web browser
    - Injection
      * Introduce new input to exploit vulnerabilities
      * SQL injection inserts statements to manipulate a database server
      * By entering crafted SQL statements as user input, info from the database can be extracted or manipulated
    - Request Forgery
      * A request that has been fabricated
      * Cross-site request forgery (CSFR)
        + Takes advantage of authentication token that website sends to user's web browser. If a user is authenticated on a website and is tricked into loading another webpage, the new page inherits the identity and privileges of the victim
      * Server-site request forgery (SSRF)
        + Takes advantage of relationships between web servers. They exploit how a server processes info received from another server
        + Some web apps can read or write information to a specific URL. IF an attacker can modify that URL, they can extract sensitive information, or inject untrusted input
    - Replay
      * Replay attacks are commonly used against digital identitites
      * After intercepting and copying data, the threat actor retransmits selected and edited portions of the copied communications later to impersonate the legitimate user
      * Many digital identity replay attacks are between a user and an authentication server
    - Attacks on Software
      * Directly focused on vulnerabilities in the software apps
      * Memory Vulnerabilities
        + Some memory attacks are called resource exhaustion because they ‘deplete’ parts of the memory
        + A buffer overflow attack occurs when a process attempts to store data in Ram beyond the boundaries of a fixed-length storage buffer. The extra data overflows into adjacent memory locations
        + Integer overflow attack is when an attacker changes the value of a variable to something outside the range that the programmer intended
      * Improper Exception Handling
        + Result of poor coding from software devs
        + Software that allows user to enter data but has improper input handling, does not filter or validate user input
        + Also NULL pointer/object reference, when an app sees a pointer as NULL, it usually crashes or ends the program
      * Attacks on External Software Components
        + Targeting external software components like: Application Program Interface (API), Device Driver, Dynamic-link library (DLL)
  + Adversarial Artificial Intelligence Attacks
    - AI is technology that imitates human abilities
    - Subset of AI is machine learning (ml): Defined as teaching a technology device to learn by itself
    - Almost all email systems use AI to block phishing attacks
    - Ai can predict and prevent future attacks
    - Risks in using AI and ML in Cybersecurity
      * Security of ML algorithms
        + These could be attacked and compromised, allowing them to be altered
      * Tainted data training
        + Attackers can attempt to alter the training data to produce false negatives to cloak themselves