Malware

- Software that has malicious repercussions
- Creates threat vector and attack vector
- Threat vector
    - How they access the system
    - Ex. unhardened system
    - Vulnerabilities of what COULD be exploited
- Attack Vector
    - How they access AND affect the system
    - The METHOD of exploiting each vulnerability
- An unpatched vulnerability is a threat vector
- A threat actor can scan for machines lacking the patch to exploit
- Once gained access, the actor can then run malware on the machine for something such as a financial incentive
- Viruses
- Worms
- Trojans
- Viruses and Trojans
- Ransomware
- Zombies and Botnets
- Rootkits
- Backdoors and logic bombs
- Keyloggers
- Spyware and Bloatware
- Malware attack techniques
- Indications of Malware Attacks

Viruses

- Malicious code running on a machine without user knowledge and infects when ran
- Virus wants to reproduce and spread
- 10 types
    - Boot sector
        - Stored in first sector
        - Hard disk and then memory whenever machine boots
        - Need antivirus that looks for this
    - Macro
        - Code that allows virus to be within a doc and executes when opened
        - Word docs, powerpoint presentations, excel spreadsheets, etc.
        - A macro can help in spreadsheets to make calculations faster
    - Program
        - Finds executables or app files to infect their code
        - Infections every time the application is opened
    - Multipartite
        - Combo of boot sector and program
        - Infects in the boot sector and loads every time of boot

        - Each boot also causes application infection as well
        - So just removing the virus from the program, the virus will still return
    - Encrypted
        - Encrypts its own code or payloads to hide from antivirus
    - Polymorphic
        - Changes virus code appearance by chanfind decryption module
        - Harder to detect than encrypted virus
    - Metamorphic
        - Writes itself entirely before infecting again
        - Advanced version of polymorphic
    - Stealth
        - Technique to avoid detection by antivirus
        - Ex. modify payloads
    - Armored
        - Layer of protection to create confusion
    - Hoax
        - Technical and social engineering
        - Scaring users to do something undesirable on their system
        - Not a virus
        - Virus is not originally there until you download it yourself or allow another to do it

Worms

- Malicious software that can replicate without user intervention
- Virus requires an action
    - Opening a file
    - Clicking a link
    - Connecting a storage drive to your system
- Takes advantage of vulnerabilities of the OS
- Scans the network to look for machines with vulnerabilities to replicate on and can then travel across networks and across the world
- Dangerous
    - Infects workstation and assets
    - Disrupts normal traffic from replicating
        - Consumes power (processing, compute, memory, capacity)
        - Slows the network
        - Can cause a DOS attack
- Can create bots out of machines and connect them in a botnet

Trojans

- Malicious software disguised to be harmless, even performing normal functions
- Tetris copy passed on a disk at a school and passed a trojan
- Remote access trojan
    - Provides attacker with remote control over a machine
- Commonly used to expose a vulnerability and extract data

- Use antimalware solution to check things for trojans before running them on your computer

Ransomware

- Digital equivalent of kidnapping but with digital assets
- Software that encrypts data and ransoms the key for a payment
- Demands can go to the multi millions of dollars
- Colonial pipeline attack
    - Pipeline had to shutdown
    - Carried half of nations fuel supply
    - 5-days
    - Ransomware attack
    - Demanded 4.4M in bitcoin
- Dusseldorf hospital attack
    - Patients had to transfer to other hospitals
    - Woman rerouted but died in the process
        - Attackers were held liable
    - Attackers provided the decryption key after finding out what happened
- 4 best practices
    - Back up regularly
        - Stored physically and cloud based to make sure not connected to the main system
    - Software update regularly
        - Updated antivirus keeps you patched and in good shape
        - Many exploits look for unpatched machines
    - Security awareness training to end users
        - Be skeptical of unsolicited emails
    - Implement MFA
        - Extra layer of security
- Never pay the ransom of the attack
    - Does not always assure you will get your data back
    - Makes you look ;lole someone who will always pay
- Isolate and disconnect machine if you think its infected
- Notify the authorities
    - Consult your orgs incident response process
- Restore your data from known good backups

Botnets and Zombies

- Botnet
    - Network of compromised computers controlled remotely used for malicious attacks
- Zombies
    - Compromised computer that is part of a botnet (remote commands)
- C2 Node
    - Controls all zombies in a botnet
- Botnets can be used to perform illegal actions and not lead back to the person behind it

- Common use
    - DDOS attack
    - Distributed denial of service
    - All machines in a botnet attacks a victim at the same time
    - C2 node tells all zombies to attack a server and crashes it as a result. Users and customers will suffer
- Botnets can be used for crypto mining
    - Store coins in victims digital wallet
- Combines processing power to break through different encryption schemes
- Zombies will typically use fractional of processing power to keep a low profile
    - 20-25% of processing power

Rootkits

- Software that gains administrator level control without detection
- Install programs
- Delete programs
- Open and shut ports
- Rings of permissions
    - Ring 3
        - Most common for endpoint users
        - Outermost ring
    - Ring 0
        - Kernel Mode
        - Access to device drivers, sound card, monitor
        - Trusted and most powerful ring
    - Ring 1
        - Easier to do things than ring 3
        - This is where the root login occurs
- The closer the permissions that are gained in a rootkit (closer to ring 0) the more damage an attacker can do on your system
- DLL injection (dynamic link library)
    - Runs arbitrary code within an address space of another process by forcing it to load a dynamic link library
    - Collection of code and data and can be used in multiple programs at once
    - DLLs are ran each time a machine boots up
    - Rootkits can be hidden within a DLL
- Shim
    - Software between two components and redirects the communications between them
    - Rootkit intercepts coms between OS and DLL then redirects the call to embedded malicious code
- Conduct an external system scan

Backdoors and logic bombs

- Backdoor

        - Bypass normal security and auth fxns
        - Common in the 80s and 90s
        - Way for programmers to do maintenance and repairs instead of going through everything
        - Modern networks consider this a breach of best practices
    - RAT can help an intruder maintain persistent access on your system
        - Callback to remote system and bypass your security
    - Easter Egg
        - Insecure coding practices used by programmers as a joke
        - Google Easter Egg
            - Do a barrel roll
        - Most are harmless
        - Can provide vulnerabilities
        - Typically are added to a program at the end of development and not vetted as much as the rest of the normal code
    - Logic bomb
        - Malicious code that runs when conditions are met
        - Jurassic park
            - Power shuts down at a certain time so person can sneak into lab and steal dino eggs
    - Never include backdoors, easter eggs, or logic bombs

Keylogger

- Stealth and potential to cause damage
- Software or hardware that records all keystrokes
- Passwords and web searches
- Simple and effective to get sensitive data
- Software based
    - Installed on a victim computer
    - Phishing
    - Pretexting
    - Evades antivirus
    - Transmits keylogs back to another computer
- Hardware based
    - External drive or embedded in the keyboard
- Lots of risk to system and privacy
    - Usernames, passwords, credit card numbers
- Updates and patches
    - Make sure no vulnerabilities to be exploited
- Antivirus solutions
    - Detection becomes more likely
- Training
    - Keyloggers often are transmitted through phishing attempts
- Implement MFA
    - Threat actor needs to go through an extra step

- Encrypt keystrokes
    - Scrambles data before sending to the system
- Physical checks for hardware based keyloggers

Spyware and Bloatware

- Spyware
    - Software that gathers info without user knowledge
    - Passwords, browsing habits
    - Installed by
        - Bundled with other software
        - Malicious website
        - Pop up ads being clicked
    - Invades privacy and slows system performance
    - Use reputable antivirus software, read through EULA to ensure company is not collecting your data without your knowledge , download from trusted sources
    - Update and patch your OS
- Bloatware
    - Software preinstalled on your system that you didn't request
    - Takes up storage and uses RAM
    - Typically not malicious
    - Introduces new vulnerabilities to your system if the code has bugs
    - Remove any software that you don't need or use
        - Manually Remove It
            - Windows based devices allow you to use the control panel for this
        - Bloatware removal tools
            - Can be more comprehensive
        - Perform clean OS install

Malware Attack Techniques

- Method malware uses to attack a system
- Different tactics for different malware types
- Some malware infects memory to leverage remote procedure calls over a network
- Modern methods use fileless techniques to avoid signature based detections
    - Directly executes the software via script or shellcode
- Creates process in system memory without relying on local file system on a host
- How does it work
    - Dropper and downloader (stage 1)
        - Lightweight shell code that can be executed on a system
        - Dropper
            - Runs other malware forms within a payload on a host
        - Downloader
            - Retrieves tools post dropper infection
        - Shellcode
            - Lightweight code
            - Executes an exploit
        - Goal is to retrieve additional portions and get user to activate the malware

- Downloader (stage 2)
    - Downloads RAT and uses C2
    - Then move from one device to another and try to find high-value targets and take over as many as possible
- Actions on objectives phase
    - TA executes objectives that will help them meet their core objectives
- Concealment
    - Prolong unauthorized access to a system by hiding tracks, erasing logs, etc.
- Malware delivered
    - Code injection
        - Disguises code by running it with a legit process
        - More challenging to detect
    - Living off the land
        - Threat actors tries to exploit tools to perform intrusions
            - Ex. powershell to conduct malicious activities

Indications of Malware Attacks

- 9 common
    - Account lockouts
        - Some malware causes lockouts
        - Unusual surge of locked out accounts across a network
    - Concurrent Session Utilization
        - Users should only have one session open at a time
        - Multiple and at different locations is suspicious
    - Block content
        - Sudden increased from blocked content
    - Impossible Travel
        - User account accessed from two or more locations within an impossible time frame
    - Resource Consumption
        - Crypto miners, botnets and worms can consume a lot
        - Notice any unsolicited resource consumption
    - Resource Inaccessibility
        - Large number of files suddenly inaccessible or held for ransom
    - Out of cycle logging
        - Logs are being generated at odd hours
        - Unauthorized data transfers or system mods by an attacker
    - Missing logs
        - Can be used to hide tracks of a threat actor
    - Published and documented attacks
        - Publishing shows that your org is part of a botnet
    - First recognize the indications if you have any hope to defend against them