**Module 07: Malware Threats**

**Common Techniques Attackers Use to Distribute Malware on the Web**

* **Black hat Search Engine Optimization (SEO):** Ranking malware **pages highly** in search results
* **Social Engineered Click-jacking:** Tricking users into **clicking on innocent-looking** webpages
* **Spear-phishing Sites:** Mimicking legitimate institutions in an attemp to **steal login credentials**
* **Malvertising:** Embedding malware in ad-networks that display across hundreds of legitimate, high-traffic sites
* **Compromised Legitimate Websites:** Hosting embedded malware that spreads to unsuspecting vistors
* **Drive-by Downloads:** Exploiting flaws in browser software to install malware just by visiting a web page.
* **Spam Emails:** Attaching the malware to emails and tricking victims to click the attchment.

**Components of Malware**

* **Crypter**
* **Downloader**
* **Dropper:** A type of Trojan that covertly install other malware files on to the system
* **Injector:** A program that injects its code into other vulnerable running processes and…
* **Exploit**
* **Obfuscator:** A program that conceals its code and intended purpose via various tevchniques
* **Packer:** A program that allows all files to bundle together into a single executable file via compression to bypass security software detection
* **Payload**
* **Malicious Code:** It can take the forms of Java Applets, ActiveX Controls, Browser Plug-ins, Pushed Content

**APT (Advanced Persistent Threats)**

* Defined as a **type of network attack**, when an attacker gains unauthorized access to a target network and remains undetected for a long period of time
* **Obtain sensitive info** rather than sobotaging the org and its network
* **Lifecycle:** Preparation->Initial Intrusion->Expansion->Persistence->Search and Exfiltration->Cleanup

**Trojan**

* Get activated when a user perform certain **predefined** actions
* Create a **covert communication** channel between..

**Infect Systems Using a Trojan**

* Create a new Trojan packet:
  + Trojan Horse construction kits help attacker…
  + Tools in these kits can be dangerous and can backfire if not properly executed
  + DarkHorse Trojan Virus Maker creates user-specified Trojans
* Employ a **dropper** or **downloader** to install the malicious code on the target system
  + **Droppers:** Used to camouflage the malware payloads. Consist of one or more types of malware features. **Emotet dropper** and **Dridex dropper** are some of the famous droppers
  + **Downloads:** A program that can download and install harmful program. Do not carry malware of itself, so it could pass through the AV scanner. **Godzilla Downloader** and **Trojan.Downloader** are some of the famous downlaoders.
* Employ a **wrapper** to bind the Trojan to a legitimate file
  + Bind a Trojan executable with genuine looking .EXE applications.
  + When the user runs the wrapped .EXE, it first installs the Trojan in the background and then runs the wrapping application
  + **Tools:** IExpress Wizard, Elite Wrap
* Employ a **crypter to encrypt** the Trojan
  + A software used to **hide virus, keyloggers** or **tools**. Not easily get detected by AV
  + BitCrypter can be used to encrypt and **compress 32bit executable** and **.NET** apps
  + **Tools:** SwayzCryptor, AegisCrypter
* **Propagate the Trojan** by various methods
  + Use covert channels to **deploy and hide malicious trojans in an undetected protocol**
  + Covert channels operate on **a tunneling method** to evade firewalls
  + Attackers can **create covert channels** using Tools such as **Ghost Tunnel, ELECTRICFISH -A North Korean tunneling tool**
  + **Evade AV:**
    - Break the trojan file into multiple pieces and zip them.
    - Write own Trojan and embed it into an app.
    - Change the syntax. Change the content of the trojan using hex editor and change the checksum and encrypt the file.
    - Never use downloaded trojan
* **Deploy the Trojan on the victim’s machine** by executing dropper or downloader on the target machine
  + Deploy a trojan through **emails, covert channels, proxy servers, USB/flash Drives**
  + **Covert Channels** are method used to deploy and hide malicious trojans in an undetectable protocol, they rely on **tunneling**.
* Execute the **damage routine**

**Exploit Kits**

* An exploit kit or crimeware toolkit is a platform to **deliver explolits and payloads** such as trojans, spyware…
* Come with **pre-written** exploit codes and can be easily used by an attacker
* RIG Explit Kit: RIG EK was used by attackers for distributing…

**Stage of Virus Lifecycle**

* Design
* Replication
* Launch
* Detection
* Incorporation
* Execution of the damage routine

**Type of virus**

* 1. System or Boot Sector Virus
* 2. File Virus
* 3. Multipartite Virus
* 4. Macro Virus
* 5. Cluster Virus
* 6. Stealth/Tunneling Virus
* 7. Encryption Virus
* 8. Sparse Infector Virus
* 9. Polymorphic Virus10. Metamorphic Virus
* 11. Overwriting File or Cavity Virus
* 12. Companion Virus/Camouflage Virus
* 13. Shell Virus
* 14. File Extension Virus
* 15. FAT Virus
* 16. Logic Bomb Virus
* 17. Web Scripting Virus
* 18. Email Virus
* 19. Armored Virus
* 20. Add-on Virus
* 21. Intrusive Virus
* 22. Direct Action or Transient Virus
* 23. Terminate and Stay Resident Virus (TSR) System

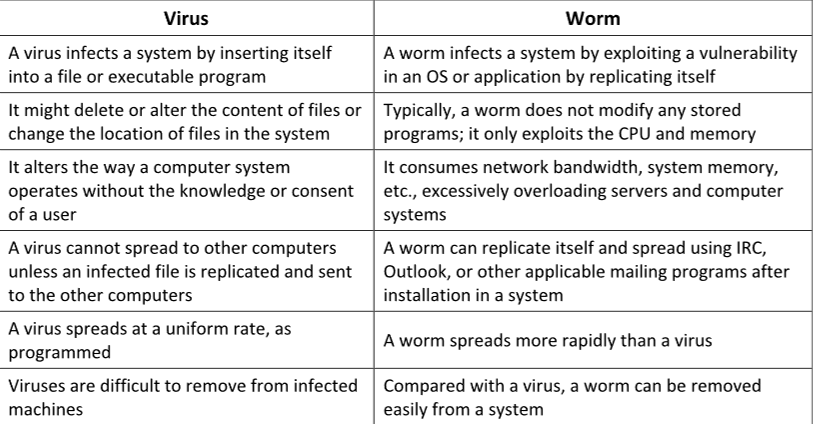
**Randomware:**

* Dharma
* eCh0raix
* SamSam

**Infect Systems Using a Virus**

* Creating a Virus
* Propagating and Deploying a Virus
  + Virus Hoaxes
  + Fake Antivirus

**Computer Worms**

* Mailicous programs that independently replicate, execute, and spread across the network connections, comsuming available computing resources without human interaction.
* Differences from a virus: 
* Worm Makers: Internet Worm Maker Thing

**Fileless Malware**

* Also known as non-malware, **infects legitimate software, applications**, and other protocols
* Leverage vulnerabilities to infect the system
* Reside in the system’s RAM, **injecting malicious code** into the running processes.
* Reason for using it:
  + Stealthy in nature
  + **Living-off-the-land:** Exploit default system tools
  + **Trustworthy:** Uses tools that are frequently used and trusted
* Taxonomy:
  + Type1: No file activity performed
  + Type2: No files written on disk, but some files used indirectly
  + Type3: File required to achieve fileless persistence
* How does Fileless malware work
  + **Point of Entry:** 
    - Memory Exploits
    - Malicious Document
  + **Code Execution:** 
    - Code injection
    - Script-Based
  + **Persistence:** Registry, WMI, Scheduled Task
  + **Achieving Objectives:** Recon, Credential Harvesting, Data Exfiltration, Cyber Espionage
* Launching Fileless Malware
  + **Memory Exploits:** Inject a malicious payload into the RAM, exploit different Win APIs.
  + **Malicious Document:** Trick users into downloading a file consisting of malicious macro code.
  + **Script-Based:** Allow attackers to communicate and infect the applications or OS without being traced
  + **Exploiting System Admin Tools:** Exploit system admin tools such as Certutil, WMIC, and Regsvr32 to launch fileless infections. Exploit cmd tools such as **Regsvr32**, and **runddl32** to run malicious DLLs.
  + **Through Phishing:** Use social engineering techniques. Fileless malware exploits vulnerabilities in system tools to load and run malicious payloads to compromise the sensitive info stored in the process memory.
* Main Persistence with Fileless Techniques
  + **Do not use disk files** to spread its infection or main persistence
  + Adopt unique methods such as **developing load points** to restart infecteted payload
  + Save the malicious payload **inside the registry t**hat hold data for configuration, application files, and settings, which executes itself with evetry restart
* **Fileless Malware:** Divergent is a type of fileless malware that **depends mostly on the registry** for the….It also employs a key in the register to **maintain persistence** and exploits PowerShell to inject itself on to the other processes.
* **Obfuscation Techniques:**
  + Insert characters
  + Insert Parentheses
  + Insert caret symbol
  + Insert double quotes
  + Using custom environment variables
  + Using pre-assigned environment variables

**Sheep Dip Computer**

* Refer to the analysis of suspect files, incoming messages, etc…
* Is installed with port monitors, files monitor…Connect to a network only under strictly controlled conditions

**Antivirus Sensor Systems**

* A collection of computer software that detects and analyzes **malicious code threats** such as viruses, worms, and trojans.
* They are used along with **sheep dig computer.**

**Malware Analysis**

* A process of **reverse engineering** a specific piece of malware to determine the origin…
* **Static Malware Analysis:** Also known as **code analysis without executing** it.
  + **File fingerprinting:** Hash
  + **Local and online malware scanning:** AV software, VirusTotal
  + **Perform string search:** Embedded strings of readble text, using **BinText**
  + **Identify packing/obfuscation methods: PEid tool**
  + **Finding the PE info:** Metadata of PE files, PE explorer
  + **Identify file dependencies:** Dependency Walker
  + **Malware disassembly:** IDA, OllyDbg
* **Dynamic Malware Analysis: Behabioral analysis** involves executing the malware code
  + Require a safe environment such as **virtual machines** and **sandboxes**
  + **System Baseline**: Take a snapshot of the system, compare
  + **Host Integrity Monitoring:** 
    - **Port:** netstat, TCPView
    - **Process:** Process Monitor
    - **Registry:** jv16 PowerTools
    - **Service:** Windows Service Monitoring Tools
    - **Startup:** Autoruns for Windows, **C:\ ProgramData\Microsoft \Windows\Start Menu\Programs\Startup**
    - **Event Logs:** Splunk is a SIEM (Security Information and Event Management) tools that…
    - **Installation:** Mirebusoft Install Monitor
    - **File and Folders:** PA File Sight
    - **Drivers:** DriverView, **run->msinfo32->Software Environment->System Drivers**
    - **Network traffic:** SolarWinds NetFlow Traffic Analyzer
    - **DNS/Resolution:** DNSQuerySniffer
    - **API Calls:** API Monitor

**Virus Detection Methods**

* **Scanning**
* **Integrity Checking**
* **Interception:** Monitor the OS requests written to the disk
* **Code Emulation:** effective in dealing with encrypted and polymorphic virus
* **Heuristic Analysis:** can be static or dynamic

**Emotet**

* A banking Trojan which can function both as a trojan by itself or as the downloader and dropper of other banking trojans
* It is a **polymorphic malware** as it can change its own identifiable feartures to evade **signature-based** detection

**Countermeasures against Fileless Malware**

* Disable PDF readers to automatically run JS
* Disable macros and use only digitally signed trusted macros
* Tools: AlienBault USM Anywhere, McAfee End Points Security