Date _____ Day _____

CHAPTER # 06

"Malware is any malicious software designed to disrupt, damage or gain unauthorized access to computer system."

- Threats malware posed to
  - ↳ Application programs,
  - ↳ Utility programs (editors, compilers)
  - ↳ Kernel-level programs

→ It is also used on
- ↳ Compromised or malicious websites & servers
- ↳ In especially crafted spam e-mails or other messages, which aim to trick users into revealing sensitive personal info.

→ Classification of Malware
- ↳ Malware is classified by "how it spreads" & "what it does".
- ↳ Modern malware often combines multiple meth
  - called **blended attacks**
    - ↳ uses multiple methods of infection & propagation to maximize speed & severity of attack.

Date _____ Day _____

- Classification based on how it Spreads
  - Viruses: Infect existing programs or files and spread when those are shared
  - Worms: Exploit software vulnerabilities to spread automatically accross networks
  - Trojans: Tricked users install them by thinking it as a safe program
  - Phishing or Social Engineering: Attackers convince user to install or share personal data

- Classification based on what it does
  - Corrupt files or damage system
  - Steal info (like pswds, credit card no. etc)
  - Take control of the sys to use it in a botnet or further attacks
  - Hides its presence (stealthing) to avoid detection
  - Theft of info from the sys / key logging

- PROPAGATION — INFECTED CONTENT - VIRUSES

→ The 1st category of malware propagation concerns parasitic software fragments that attach themselves to some existing executable code like

Date _____ Day _____

- an application
- utility program
- system program in the
- even in kernel (code which boots up computer)

→ ~~Computer virus infections forms the majori~~
→ Most viruses carryout their work that is specific to a particular operating system and/or to a particular hardware platform
  ↳ They are designed to exploit it's weakness
  ↳ Macro viruses however targets specific document types

→ A virus can infect some or all of the other files on that sys, with the executable content when it executes, depending on the access permissi it has
→ Viral infection can be prevented by blocking it entry on the first place

→ A computer virus (and many types of current malware) has three components
• Infection mechanism — The means by which vir spreads enabling it to replicate. Also referred as the infection vector

Date _____ Day _____

- Trigger — The event or condition that determines when the payload is activated or delivered, sometimes called logic bomb.
- Payload — What the virus does, besides spreading. The payload may involve damage or a small but noticeable activity

- Four Phases Of Virus

(1) Dormant Phase (Sleep Mode)
↳ The virus is inactive & waiting
↳ It activates later when a specific event happens – like a certain date or action
↳ Some virus skip this stage

(2) Propagation Phase (Spreading)
↳ The virus makes copies of itself and adds them to other programs or files
↳ These new infected files can then spread the virus further
↳ Many virus change slightly (morph) to avoid being detected

Date _____ Day

③ Triggering Phase (Activation)

↳ The virus gets activated & prepares to do what it was designed for

↳ This can happen after a certain no. of infections, a date or any specific event

④ Execution Phase (Attack)

↳ The virus performs it's actual task

↳ This could be harmless (like displaying a msg) or harmful (like deleting files)

▷ Macro Viruses

↳ A virus that attach themselve to documents and ~~and~~ uses the capabilities of the documents application to execute & spread.

↳ They infect every day files like .docx, .pdf, .xlsx etc.

↳ They spread quickly bcz people often share docs via email or file sharing

↳ They are simpler to write

↳ Ex: A word file may contain a hidden macro script that automatically runs when you open the doc.

Date _____ Day _____

• PROPAGATION — VULNERABILITY EXPLOIT — WORMS

→ "Worm" is a program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machine

→ Exploit software vulnerabilities in client / server programs
→ Can use network connection to spread from sys to sys
→ Spread thru shared media (USB drives, CD, DVD data disks)
→ Email worms spread in macro or script code included in attachements & instant messenger file transfers
→ Upon activation worm may replicate & propagate again
→ Usually carries some form of payload

▷ Worms Replication

• E-mail / Instant Messenger Facility — The worm sends copies of itself as attachements or links when someone opens the email or attachements, it infects their system.

Date _____ Day

- File Sharing / USB Drives — It hides in shared files or on removable devices like USBs. It runs ~~asa~~ as soon as the drive is plugged in

- Remote Execution — The worm takes adv of software bugs or vulnerabilities in network services to run itself on other sys.

- Remote File Transfer — It copies itself using services like shared folders or file transfer tools hoping someone on the other sys will open it.

- Remote Login — A worm logs onto a remote sys as a user and then uses cmds to copy itself from one sys to another, where it then executes.

⇒ Difference b/w Virus & Worm

→ - activated only when infected file/program is executed by user
- spreads thru infected files, emails or downloads

" A virus needs a host file & user action to spread, whereas a worm spreads automatically thru networks without user involvement "

- runs on its own
- spread thru network, USBs

Date _____ Day _____

Target Discovery

→ The first function in the propagation phase of worm is to find other sys to inject, process is called — scanning or fingerprinting.

→ Each infected host typically repeats the scanning so the worm spreads exponentially

→ Common Scanning Strategies

① Random Scanning

→ Probe random IP addresses accross the whole IPv4 space

→ Generates very large, noisy traffic accross the internet

→ Pros for attacker : Simple; can find vulnerable hosts anywhere

→ Cons for attackes : Eacy to detect by volume/ anomaly

② Hit-list Scanning

→ The attackes first compiles a long list of potential vulnerable machines. Once ready, each infected hosts uses portions of the list to infect quickly

→ Fast targeted spread & harder to detect

→ Requires effort to compile list.

Date _____ Day _____

(3) Topological
→ Uses info from the compromised host to discovers nearby or related hosts
→ Efficent & often gets into related network
→ Cons: Dependent on what compromised host revealed

(4) Local-Subnet Scanning
→ After breaching a host behind a firewall, the worm scans its local subnet to infect other machines that the firewall might protect

• WannaCry
→ Also known as WannaCrypt, WannaCryptor or WCry is a ransomware worm that spread quickly accross the world in May 2017, encrypting files on infected computer and demanding bitcoin to decrypt them.

→ It spreads as a worm by agressively scanning both local & random remote networks, attempting to exploit a vulnerability in the Server Message Block protocal file sharing service

Date _____ Day _____

→ The spread was only slowed by the accidental activation of a "kill-switch" domain by a UK security researcher.

▸ State of Worm Technology

Modern worms are much more advance than early ones

① Multipartform

- Old worms — Targeted only windows sys
- New worms — Can attack multiple OS — windows linux, macOS, even mobile devices

↳ The can also exploit document macros or scripts

② Multi-Exploit

- Modern worms don't rely on just one vulnerability
- They use many different entry points
  ↳ Webservers, browsers, email attachments.
- Makes more difficult to defend against

③ Ultrafast Spreading

- They used optimized scanning & infection methods
- The goal is to infect as many sys as possible before being detected

Date _____ Day _____

④ Polymorphic
- Each copy of the worm changes its code slig... to help evade antivirus detection because every copy looks different

⑤ Metamorphic
- Goes beyond just changing code — also chan... it's behaviour
- Can perform diff actions at diff time on diff systems.

⑥ Transport Vehicles
- Worm acts as delivery system for other malware
  ↳ DDoS bots, Rootkits, Spyware

⑦ Zero-Day Exploits
- The most dangerous worms uses zero-day vulnerabilities — flaws unknown to vendor.
- Which gives no time for defense or patching before the attack.

Date _____ Day _____

Mobile Code

→ Programs or scripts that are sent from a remote system and executed locally on a host machine with the same semantics accross platforms.

→ Executed on the local sys after being transmitted - often without explicit, informed user actions.

→ Often acts as a mechanism for a virus, worm or Trojan horse

Mobile Phone Worms

→ Communicate thru Bluetooth wireless connections or MMS

→ Target is the smartphone

→ Can completely disable the phone, delete data on the phone, or force the device to send costly messages

→ Eg: CommWarrior replicates by means of Bluetooth to other phones

Client Side Vulnerabilities :

Drive by Downloads

→ Malware gets installed on your machine just by visiting a webpage (no extra clicks)

→ The page contains exploit code that abuses browser or plugin bugs

→ This malware doesnot actively propagates as worm

Date _____ Day _____

does, but rather waits for unsuspecting users to visit the malicious webspage in order to spread to their sys.

- Watering Hole Attack
  - → Attacker compromise a website that a target group often visits (a "watering hole") to infect those visitors.
  - → The attacker researches their intended victim to identify websites they are likely to visit, then scan these website to find vulnerabilities
  - → Attack code may even be written in such a way which affects only certain users that visits the website, not all of them.
  - → This helps them remaining undetected.
- Malvertising
  - → Place malware on websites without actually compromising them.
  - → Malicious ads deliver malware to visitors
  - → Attacker buys ad slots or compromises ad network; ads contain exploit code or redirect to exploit pages
  - → the malware code may be dynamically generated

Date _____ Day _____

to either reduce the chance of detection or to only effect specific systems.

→ Attackers can place these ads for as little as few hrs, when they expect their intended victims to visit the targeted websites.

▸ Clickjacking

→ Attacker tricks you into clicking an invisible or disguised element so you perform actions you didn't intend.

→ Using layered iframes, transparency, CSS tricks to overlay malicious controls under legit UI.

→ Keystroke-hijacking is a related variant (invisible text fields).

PROPAGATION — SOCIAL ENGINEERING - SPAM EMIAL, TROJAN HORSE

→ Social Engineering — it's when attackers tricks user into helping infect their own systems, usually by clicking, downloading or sharing something harmfull

→ Spam (Unsolicited Bulk Email)

↳ Unwanted mass emails sent to thousands or millions of users

Date _____ Day _____

↳ Most are advertisements, scams or malware carriers

↳ Emails may have:
  ↳ Infected attachements
  ↳ Trojan programs or scripts that install secret
  ↳ Phishing links that lead to fake web.

→ Trojan Horse
↳ A malicious program disguised as something useful or safe — like a game, software update or utility tool.
↳ Attacker hides malicious code inside a normal looking program.
↳ It might
  ↳ Steal sensitive data
  ↳ Send info to the attacker
  ↳ Install other malware
↳ Types of Trojan Behavior
  • Adds malicious actions while still doing its normal job
  • Modifies the original program's function
    ↳ fake login app steals pswd
  • Replaces the original program completely
    ↳ fake "sys update" that install malware

Date _____ Day _____

→ Mobile Trojan

↳ A malicious app that looks useful or legitimate but secretly performs harmful activities on smartphone

↳ Spreds thru

↳ App stores or marketplaces

↳ Spam msgs

↳ Jailbroken iPhones

↳ Common Mobile Trojans

↳ Phishing Trojans — tricks user typing their banking info

↳ Ransomware ↳ — locks the phone & demand payment

↳ Fake Security app — claim to clean virus but actually install more malware

• PAYLOAD — SYSTEM CORRUPTION

① Data Destroying Malware

- Malware whose payload deliberately corrupts or erases data/files or overwrites disk areas.

② Ransomware

- Malware that encrypts user data & demands payments for ~~decriptio~~ decryption key.
- Spread vectors — spam attachments, drive-by downloads, worm propagation

Date _____ Day _____

③ Physical - damage / Industrial Malware
- Malware designed to cause physical harm equipment by altesing control code or comm

④ Logic Bombs
- Code that remains dormant until specific conditions are met, then executes destructive actions
- Triggers — dates, file existence, user identity, system state, software config

- PAYLOD — ATTACK AGEN — ZOMBIE, BOTS

→ Bot / Zombie / drone — a compromised host (PC, server, IoT device) secretly controlled by an attackers

→ Botnet — A cordinated network of many bots that the attacker controls to carry out large-scale actions

→ Typical Use of Botnets
① DDoS Attacks — overwhelm targets with traffic so that it denies legit requests
② Spamming — send massive vols of email
③ Sniffing — capture data on infected host

Date _____ Day _____

④ Keylogging — capture keystrokes
⑤ Propagation — distribute new malware / updates
⑥ Ad Fraud / Click Fraud — automate ad clicks or hijack browsers for revenue
⑦ House of Chat / IRC (Internet relay chat) networks — Similar to DDoS & voting / Gamming manipulation
⑧ Manipulating online polls / games
⑨ Install ransomware, crypto-miners, rootkits

• Remote Control Facility

→ worms = spread & act automatically
→ Bots = wait for cmds from an attackers via ~~CLI~~ system (C&C)
Command & control

Difference between worms & bot

→ How it works
↳ A computer or device gets infected
↳ The bot connects to a C&C server (attacker's control center)
↳ The attacker sends instruction
↳ Bots can be told to download new files or malware for new attacks
↳ Bots send stolen data or status update back to the controller

→ More recent botnets use communication channels via Protocols such as

Date _____ Day _____

- PAYLOD — INFORMATION THEFT - KEYLOGGER'S

↳ Types of malware designed to steal sensitive info.

- Keylogger
  - ↳ Records every key you press on your keyboard
  - ↳ Sends this data to attacker
  - ↳ Eg: If you type your bank's pswd attacker gets it

- Spware
  - ↳ When web started using on-screen keyboards or graphical pswd entry (so no actual typing), keyloggers stop working
  - ↳ Attackeers created spyware, which can:
    - ↳ Monitor browser activity & history
    - ↳ Redirect users to fake websites (phishing sites)
    - ↳ Modify data btw browser & real web (main-in-the-browser attack)
  - ↳ It catch everything you do

- Phishing Attack
  - ↳ An attack that uses fake emails or website to steal your confidential info

Date _____ Day _____

↳ Spear Phishing
↳ More adv. and personalized form of phishing
↳ The attacker researches the target, writes a customized email to look more convincing.

- PAYLOAD — STEALTHING – BACKDOORS, ROOTKITS

- Backdoor (Trapdoor)
↳ A secret entry point that lets someone bypass normal authentication & get special access to the system
↳ How?
↳ Hard-coded special input sequence, secret acc
↳ Network backdoor: A non-standard port that accepts remote cmds.
↳ Maintenance hook is a backdoor used by programmers to debug & test programs

- Rootkit
↳ A collection of program installed on a sys to maintain covert ~~admin~~ access to the system
↳ Get the admin (↳ hidden root level access while hiding evidence of that access.
↳ It Sabotage the mechanism that monitor and

Date _____ Day _____

report on the process, files & registries on a computer → Persistence.

↳ ~~Activates each time the system boots.~~

↳ Classification

- ▷ Persistent — Stores code on disk and runs on boot
- ▷ Memory-based — lives only in RAM; gone after reboot, harder to detect
- ▷ User mode — intercepts user-space APIs & libraries
- ▷ Kernel mode — hooks kernel routine & sys calls
- ▷ Virtual Machine based — installs hypervisor below the OS & control from it.
- ▷ External / Firmware — lives in BIOS, system management mode or device firmware (survives OS reinstallation

• COUNTERMEASURES

→ Malware Countey Measure

↳ The Ideal soln is to prevent it from entering

• Four Key Elements

① Policy — Establish clear org. policies for malware prevention & response

② Awareness — Train users to recognize threats

Date _____ Day _____

③ Vulnerability Mitigation — Patch sys, close security gaps, manage configuration

④ Threat Mitigation — Use tools & strategies to detect, isolate & remove malware

- Preventive Measure
  - ↳ Keep sys fully patched & updated
  - ↳ Configure least priviledge access control
  - ↳ Reduces spread by limiting what malware can modify or infect
  - ↳ Combat social eng. through training
  - ↳ Informed users are less likely to execute malicious attachements.

- When Prevention Fails — Threat Mitigation Steps
  - ↳ Detection — Discovers the presence of malware
  - ↳ Identification — Determine the specific malware type / family
  - ↳ Removal — Eliminate malware & restore clean sys state.
    - ↳ Removal impossible then delete infected files or rebuild from clean backup or reinstall sys (worst case)

Date _____ Day _____

- Generations Of Antivirus

▷ 1st Generation : Simple Scanner
↳ Requires a malware signature to identify the malware
↳ Limited to detection of known malware

▷ 2nd Gen : Heuristic Scanners
↳ Use heuristic Rules to search for probable malware instances
↳ Another approach is integrity checking

▷ 3rd Gen : Activity traps
↳ Memory resident programs that identify malware by its action rather than its structure

▷ 4th Gen : Full Featured Protection
↳ Packages consisting of a variety of antivirus techniques used in conjuction
↳ Include scanning & activity trap components & access control capability.

Date _____ Day _____

- Sandbox Analysis
  - ↳ Means running suspicious software in a safe, fake env. (virtual machine) to see what it does — without risking a real sys.
  - ↳ The sandbox copies or simulates a real computer
  - ↳ Suspicious code runs inside it
  - ↳ Security expests ~~cutect~~ watch it's behaviour

- Host based Dynamic Malware Analysis
  - ↳ This method means watching how a program behaves while it is running on a real computer to see if it does anything harmful — and stopping it immediately if it does

  - ↳ Limitation
    - ↳ The malware must start running first before being detected therefore it might have done some damage before being fully blocked.
    - ↳ So it helps stop major harm but can have minor effects

Date _____ Day _____

- Perimeter Scanning
  - ↳ Means checking for malware at the boundary (perimeter) of an org.'s network — for eg on firewalls, email servers
  - ↳ It helps to catch malware before it enters or leaves the network
  - ↳ Types of Monitors
    - Ingress Monitors (Incoming Traffic)
      - ↳ Check data comming into the orgs from internet
      - ↳ Detect malware trying to enter, using signatures, heuristics or anomaly detection
    - Egress Monitors (Outgoing Traffic)
      - ↳ Check data leaving orgs
      - ↳ Detect if internal PC's are leaking data
  - ↳ Helps detect worm activity, spam or botnet traffic
  - ↳ Limitation — Can only detect for malware in transit, not observe how malware behaves after infecting a system

Page No.