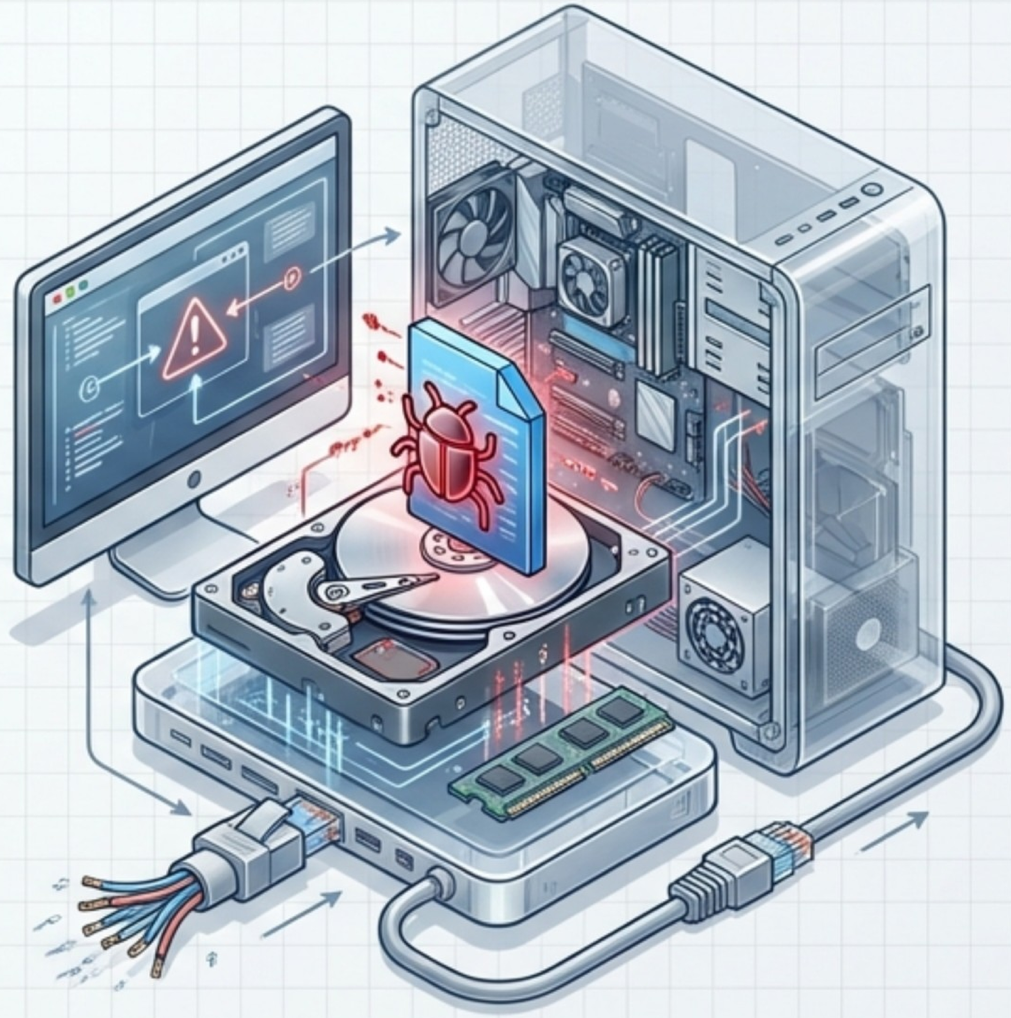
COMPREHENSIVE GUIDE TO MALWARE AND CYBER THREATS

A structural analysis of malicious software, propagation methods, and cybersecurity vulnerabilities.



Document Purpose: An educational deep-dive into the classifications of cyber attacks, covering definitions, operational mechanics, and key distinctions between threat types. Designed for students preparing for UGC NET Paper 1 ICT and general cybersecurity awareness.

[STUDENT SUMMARY] This document functions as a 'Slidedoc'—a visual textbook designed to clarify the hierarchy of cyber threats from basic viruses to complex polymorphic code

Table of Contents

01 Foundations of Threat:
Defining Malware and the Biological Virus Analogy.

02 Propagation Mechanisms:
The critical distinction between Viruses (User-Dependent) and Worms (Self-Replicating).

03 The Deceivers & Spies:
Trojan Horses, Spoofing, Spyware, and Keyloggers.

04 Extortion & System Control:
Ransomware mechanics, Rootkits, and Backdoors.

05 Social Engineering:
Phishing, Pharming, Smishing, and Vishing.

06 Triggered & Network Attacks:
Logic Bombs, DoS/DDoS, and Piggybacking.

07 Advanced Viral Architectures:
Technical classifications: Boot Sector, Polymorphic, and Multipartite viruses.

[Student Summary] The content is structured to build a mental model: first understanding the agent (Malware), then how it moves, how it tricks you, and finally how it hides.

Foundations of Threat: Malware & Viruses

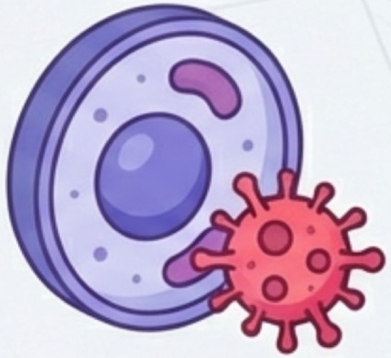
Core Summary

Malware (Malicious Software) is the umbrella term for any software designed with malicious intent to damage, disrupt, or steal data from a computer system.

Deep-Dive Analysis

- **The Parasite Analogy:** A virus functions like a biological parasite. It has no independent identity and cannot execute on its own. It requires a host—an authentic file or program—to reside upon.
- **Mechanism:** The virus attaches itself to files (often .exe). It remains dormant until the user executes that specific file.
- **Impact:** Once the host file is run, the virus executes, potentially corrupting data or spreading to other files.

> **VIRUS (Vital Information Resources Under Siege):** A type of malware that attaches itself to files/programs and spreads only when that specific file is shared and executed by a user.



Biological Host

Digital Host (.exe)

User Action Required.

[Student Summary] Remember: A virus is user-dependent. If you don't run the infected file, the virus sleeps. It needs your action to wake up.

Self-Propagation: Worms vs. Viruses

Core Summary

While viruses need a host, **Worms** are self-sufficient. They do not need to attach to a program; they are standalone programs that replicate autonomously across networks.

Feature	Virus	Worm
Dependency	Parasitic (Needs a host file).	Independent (Standalone program).
Activation	Requires human action (running a file).	Self-replicating (No human action needed).
Acronym/Motto	"Vital Information Resources Under Siege"	"Write Once, Read Many"
Spread Speed	Slower (dependent on file sharing).	Extremely fast (network propagation).

Deep-Dive Analysis: The 'I LOVE YOU' Worm (2000)

A classic example that spread via email. Unlike a virus that requires you to forward a file manually, a worm can seize control of your email system and send itself to everyone in your address book automatically.

[Student Summary] The critical distinction: Viruses wait for you to move them; Worms move themselves.

The Deceivers: Trojan Horses & Spoofing

Core Summary

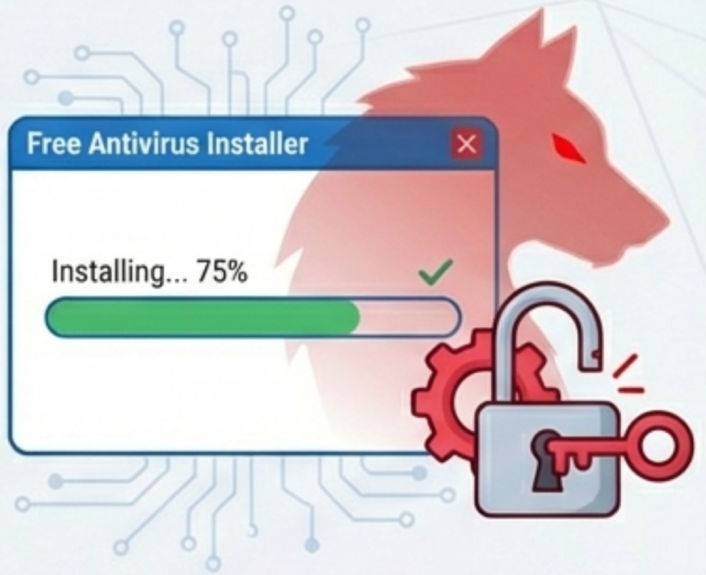
These threats rely on masking their true identity to trick the user into granting access.

Key Learning Points

- **Trojan Horse:** A non-replicating program containing malicious code that disguises itself as legitimate software.
- **Spoofing:** The act of pretending to be someone else (a bank, a person, or a network entity) to gain trust.

Deep-Dive Analysis

- **The 'Relative' Analogy:** Trojans are compared to 'relatives' or 'close friends'—they appear safe and familiar on the outside, but harbor harmful intent on the inside.
- **Scenario:** A user downloads a 'Free Antivirus' program. It looks functional, but in the background, it is stealing bank details.



Definition Box

Trojan Horse:

Named after the Greek myth; it does not replicate like a worm or virus. It relies entirely on **social engineering** to get installed.

[Student Summary] Trojans are the 'wolves in sheep's clothing' of the digital world—they look useful (like a free game) but exist solely to open the door for attacks.

Surveillance: Spyware & Keyloggers

Core Summary

Spyware is malware designed to secretly monitor and collect data on a user's activities without their consent.

Deep-Dive Analysis

- **The 'Free App' Trap:** Legitimate-looking apps (e.g., a Free Weather App) often request excessive permissions. Once granted, they track user activity and data.
- **Keyloggers:** A surveillance tool that records every keystroke made on the keyboard.

Definition Box
Keylogger: A specific sub-type of spyware that records every key pressed by the user, effectively stealing passwords and sensitive communications before they are even encrypted by the network.

[Student Summary] If Spyware is the camera in the corner of the room, Keyloggers are the person reading your diary over your shoulder.

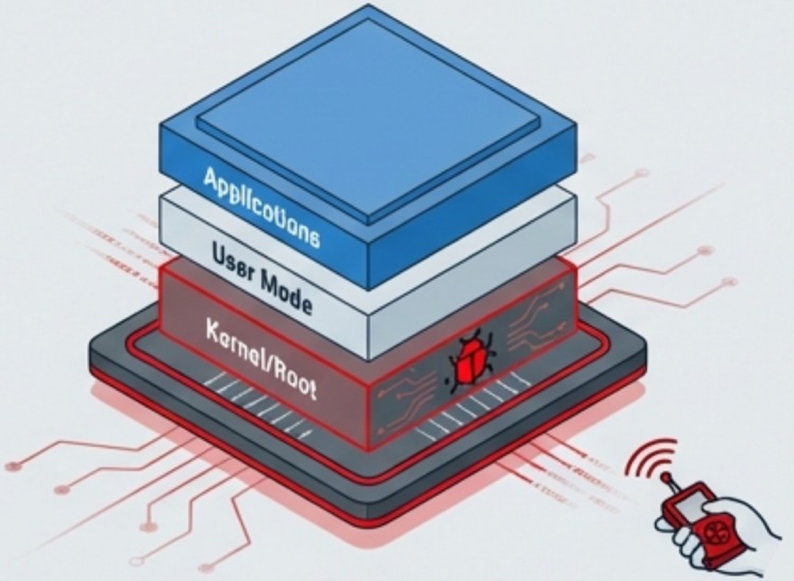
Extortion & System Control: Ransomware & Rootkits

Ransomware

- **Core Concept:** Locks the computer or encrypts files, demanding payment (often Bitcoin) for the decryption key.
- **Case Study: WannaCry Attack (2017)** - A massive global attack that demanded cryptocurrency to restore data access.

Rootkits

- **Core Concept:** 'Root' refers to the admin/core level of the system. These tools hide deep in the OS to allow hackers remote control.
- **Mechanism:** They modify the OS to hide their own existence, allowing an attacker to execute commands as if they were the system administrator.



[Student Summary] Ransomware is a digital kidnapping of your files; Rootkits are a secret tunnel into the heart of your operating system.

Social Engineering: Phishing, Pharming & Variants

Core Summary: Attacks that target human psychology rather than software vulnerabilities.

	Phishing	Pharming
Method	Uses fake **Communications** (Emails, SMS).	Uses fake **Infrastructure** (DNS, Website Redirection).
User Action	User clicks a link in a message.	User types a correct URL but gets redirected.
Analogy	Casting a line (fishing) for a victim.	**Farming** a large crop (redirecting traffic) for victims. 
Example	Email: 'Your SBI account is blocked, click here.'	Typing 'amazon.com' but landing on a fake site.

Mobile Variants & Advanced Tactics

- **Smishing:** Phishing via SMS (e.g., 'You won a lottery' text).
- **Vishing:** Phishing **via Voice calls** (e.g., a fake bank call asking for OTP).
- **Spear Phishing:** Targeted attacks using specific research on an individual.

[Student Summary] Phishing tricks you with a lure (email); Pharming tricks you with the destination (fake website). Both want your credentials.

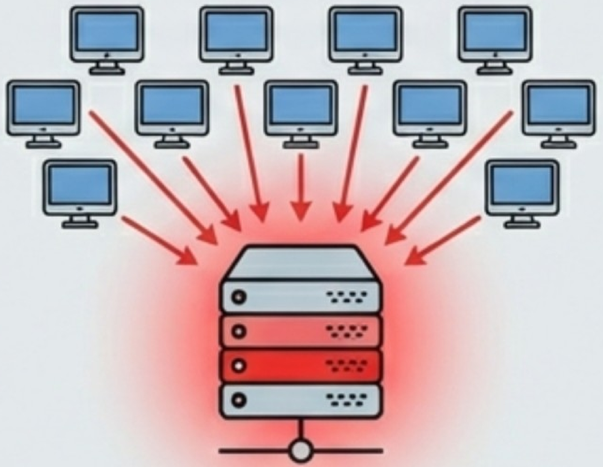
Triggered & Network Attacks

Logic & Time Bombs

- **Logic Bomb:** Malicious code that triggers when conditions are met (e.g., 'If name removed from payroll, delete database').
- **Time Bomb:** A variant triggered by a specific date (e.g., Jan 1, 2026). Dormant until that moment.

Denial of Service (DoS & DDoS)

- **DoS:** Overloading a server with traffic.
- **DDoS (Distributed):** Using a network of infected computers (**Botnets/Zombies**) to flood a target simultaneously.



Piggybacking

- **Definition:** Unauthorized use of someone else's WiFi or internet session.
- **Man-in-the-Middle:** Intercepting communication on unsecured networks.

[Student Summary] Logic bombs are conditional threats waiting for a trigger; DoS attacks are brute-force attempts to crash a digital service through traffic overload.

Advanced Virus Architectures (Part I)

Boot Sector Virus

- **Target:** The Master Boot Record (MBR). Infects code that runs immediately when the computer is turned on (Bootstrapping).
- **Severity:** Extremely high; loads before the OS.

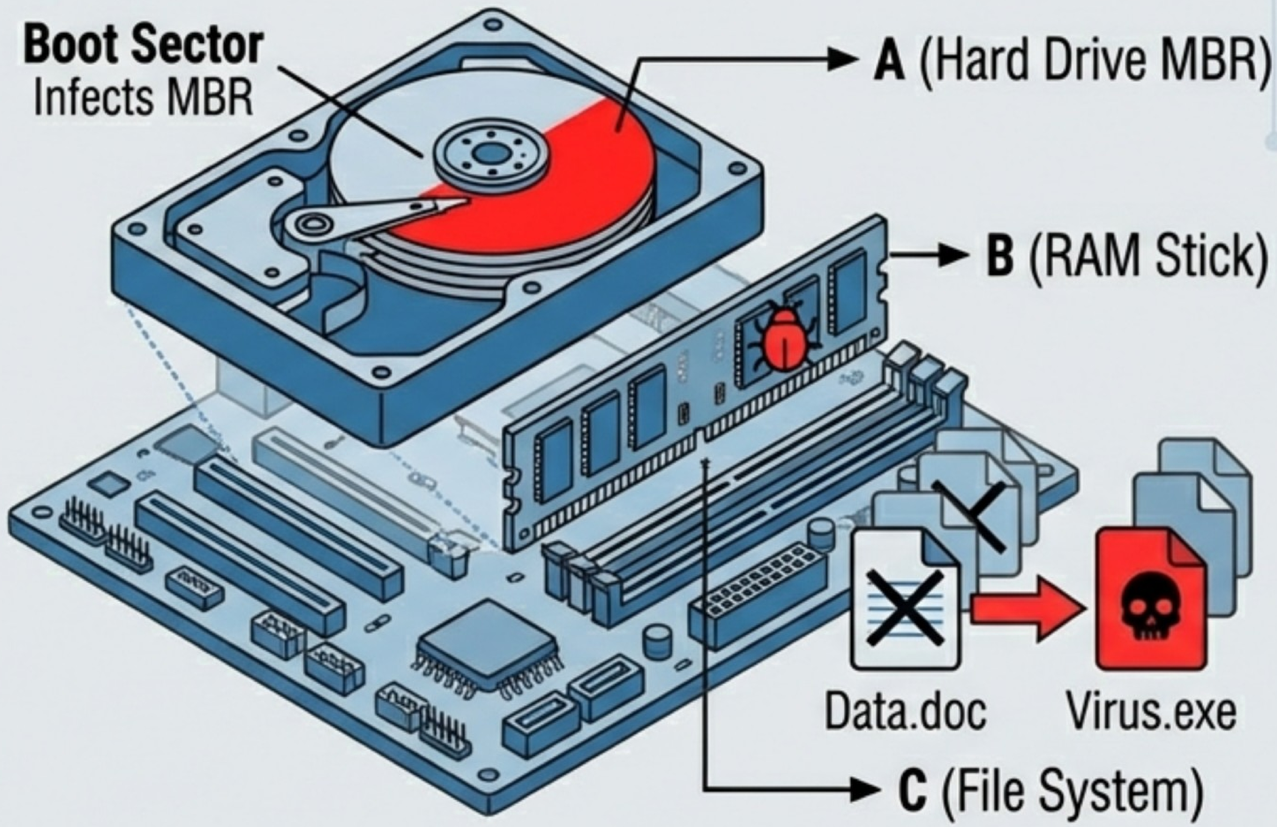
Overwrite Virus

- **Mechanism:** Writes its own malicious code *over* the original file's data, destroying the original content.

Resident Virus

- **Target:** Computer Memory (RAM). Embeds in volatile memory, remaining active even after the infected file is closed.

System Architecture View



[Student Summary] These classifications define the virus's home: Boot Sector viruses live in the startup sequence, while Resident viruses live in the system's active memory.

Advanced Virus Architectures (Part II)

Macro Virus

- **Context**: Microsoft Office (Word, Excel).
- **Mechanism**: Mimics legitimate automation scripts/macros.

Web Scripting Virus

- **Context**: Online Browsing.
- **Mechanism**: Hides within web page code (videos, ads) to infect via browser.

Polymorphic Virus

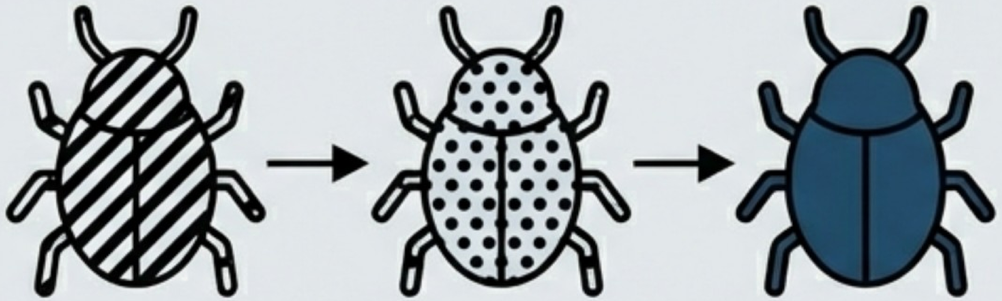
The Shape-Shifter

- **Mechanism**: Changes its code signature (encryption) every time it replicates to evade antivirus detection.

Multipartite Virus

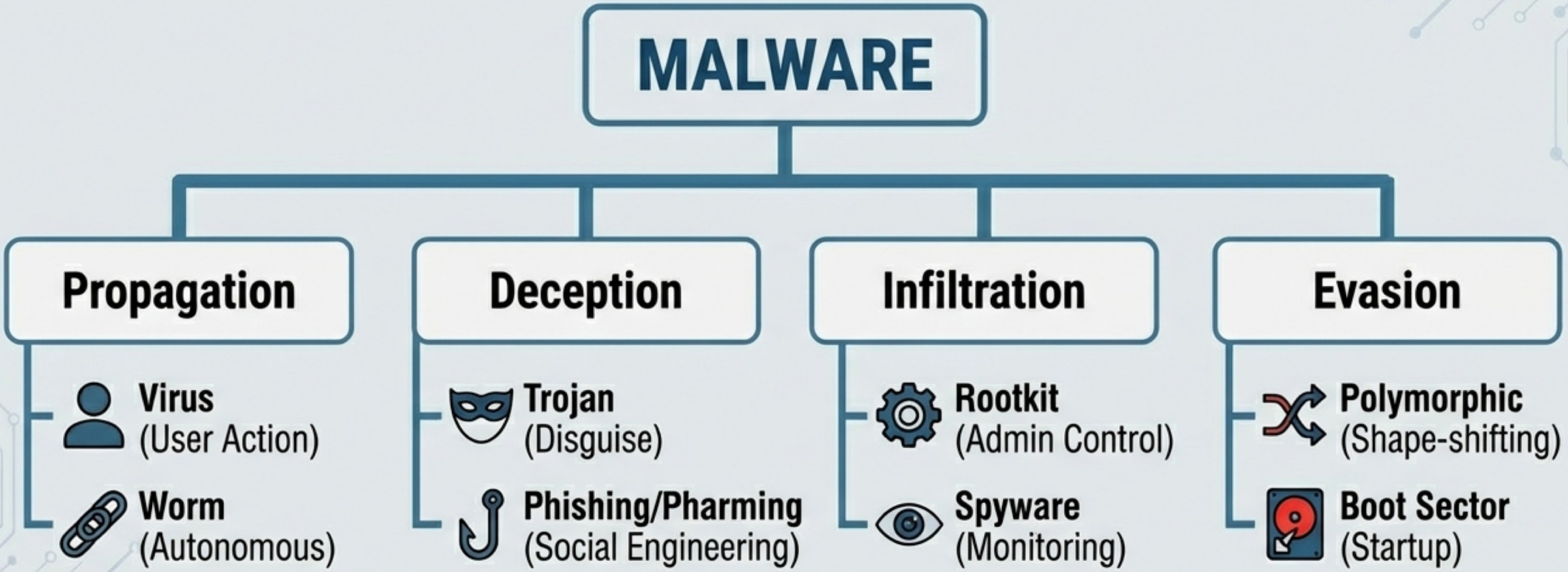
The Hybrid

- **Mechanism**: Attacks multiple points (Boot Sector AND Files) simultaneously.



[Student Summary] Polymorphic viruses are the hardest to catch because they change their ‘fingerprints’ with every infection.

Summary & Key Takeaways



[Student Summary] Success in cybersecurity topics relies on understanding the *method* of attack: Is it tricking you (Social Engineering), copying itself (Worm), or hiding in the memory (Resident Virus)?