Malware Types and Their Impact

An in-depth look at how malware operates, spreads, and the damage it causes.

What is Malware?

Definition

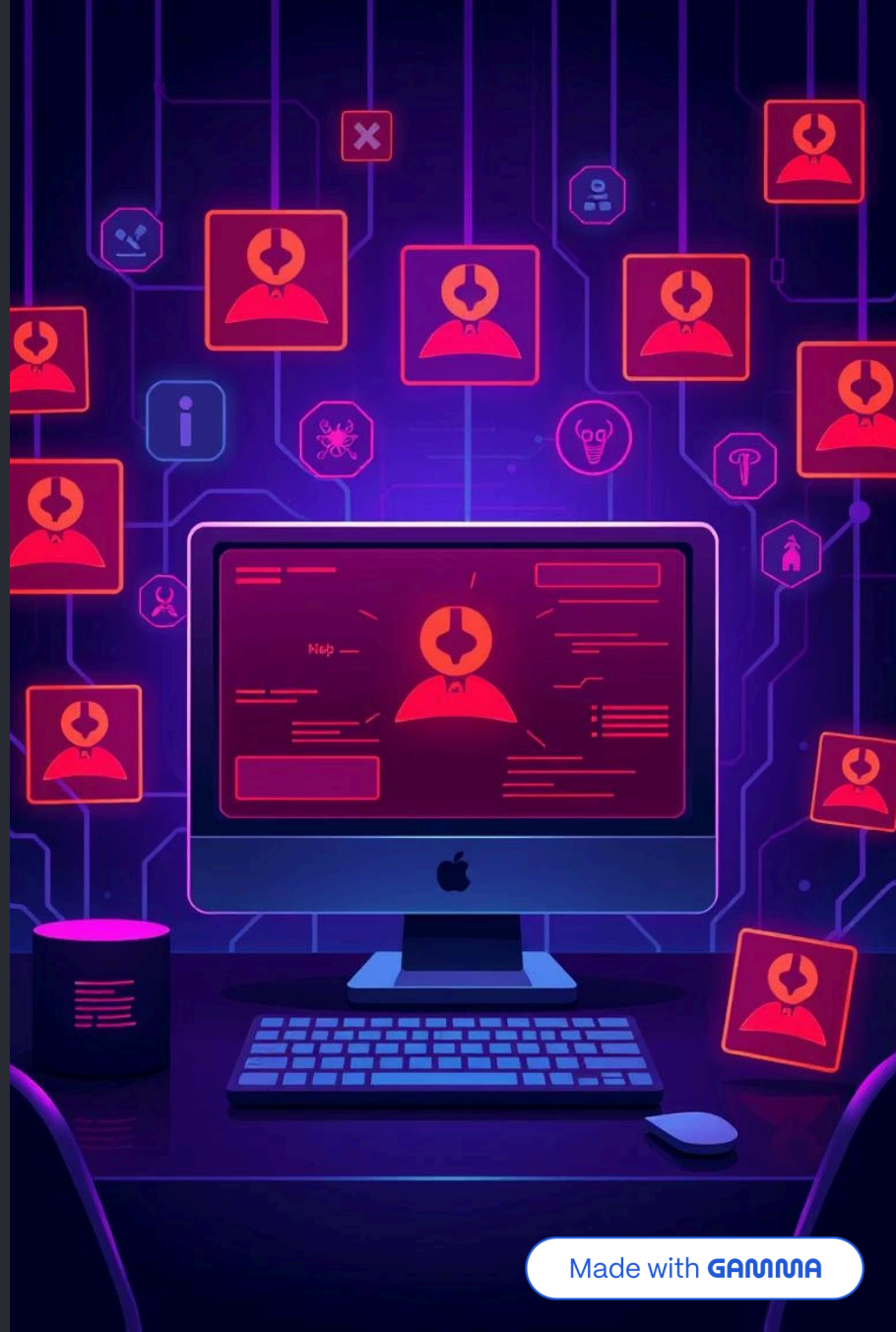
Malware = **malicious software**

Purpose

Designed to harm, disrupt, or exploit systems

Uses

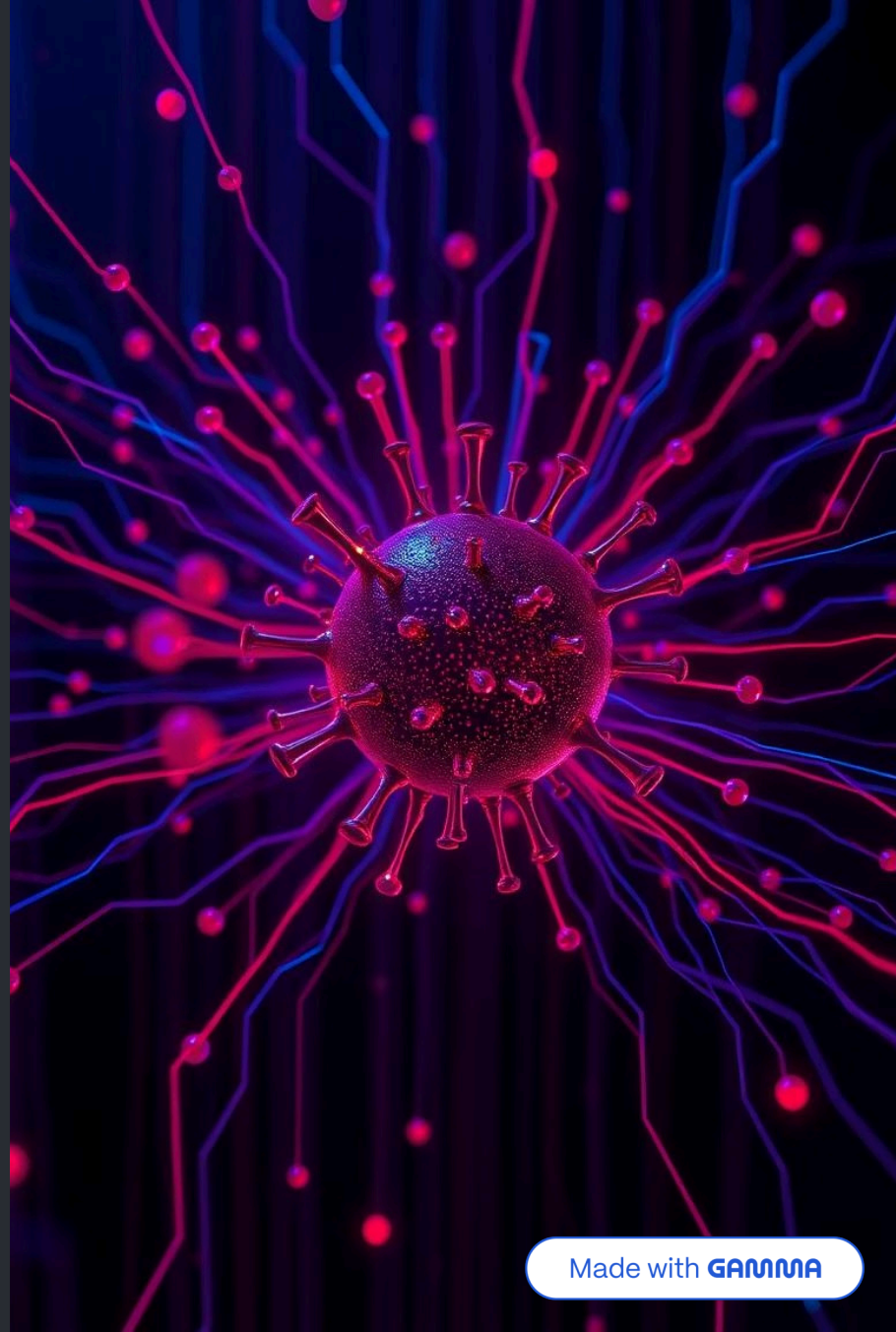
- Data theft
- Espionage
- Ransomware
- Sabotage



Common Malware Types

Virus

- Attaches itself to clean files and spreads through legitimate applications.
- Activates when the infected file is executed.
- Can delete files, reformat systems, or render devices inoperable.
- *Examples:* ILOVEYOU, Melissa



Worm

- Self-replicates and spreads without needing to attach to programs.
- Exploits vulnerabilities in operating systems or networks.
- Causes network congestion and resource exhaustion.
- *Examples:* Blaster, Conficker

Trojan Horse

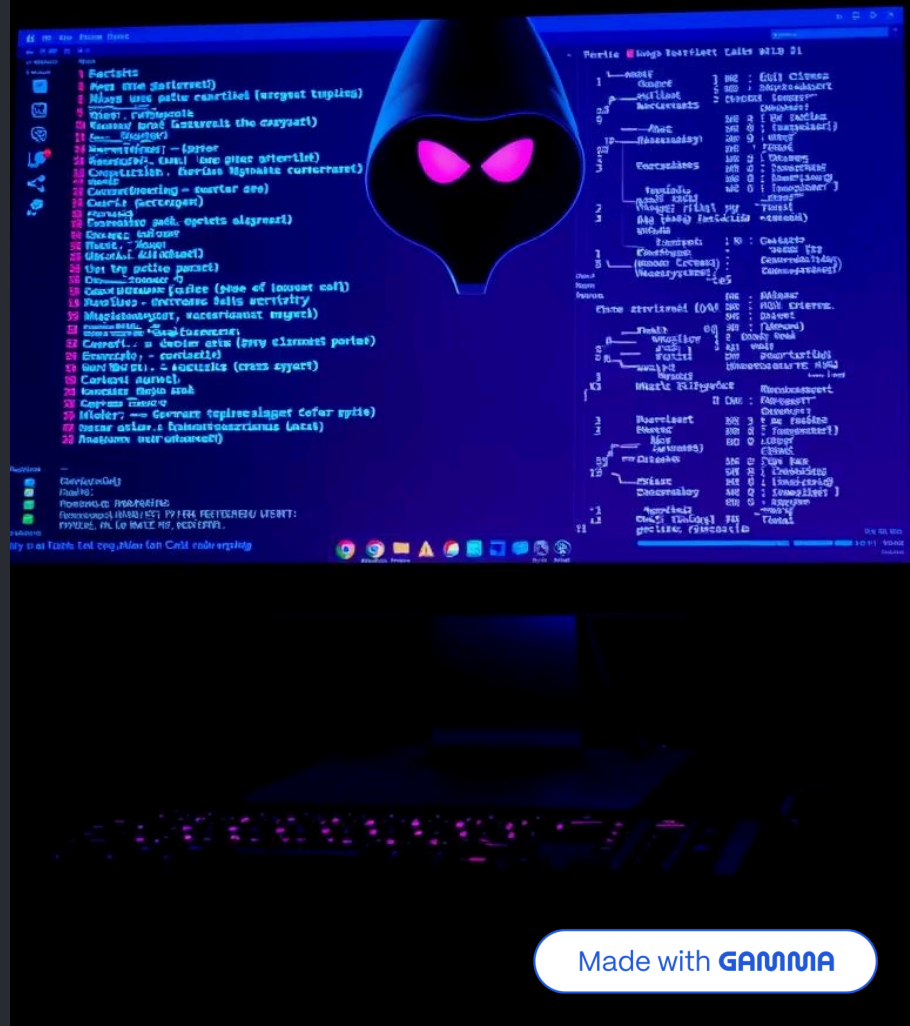
- Appears as a legitimate program but contains malicious code.
- Creates backdoors for attackers or steals information.
- Often used to install additional malware.
- *Examples:* Zeus, Emotet

Ransomware

- Encrypts the victim's data and demands ransom to decrypt it.
- Targets both individuals and organizations.
- Significant financial losses and operational downtime.
- *Examples:* WannaCry, Ryuk, Petya

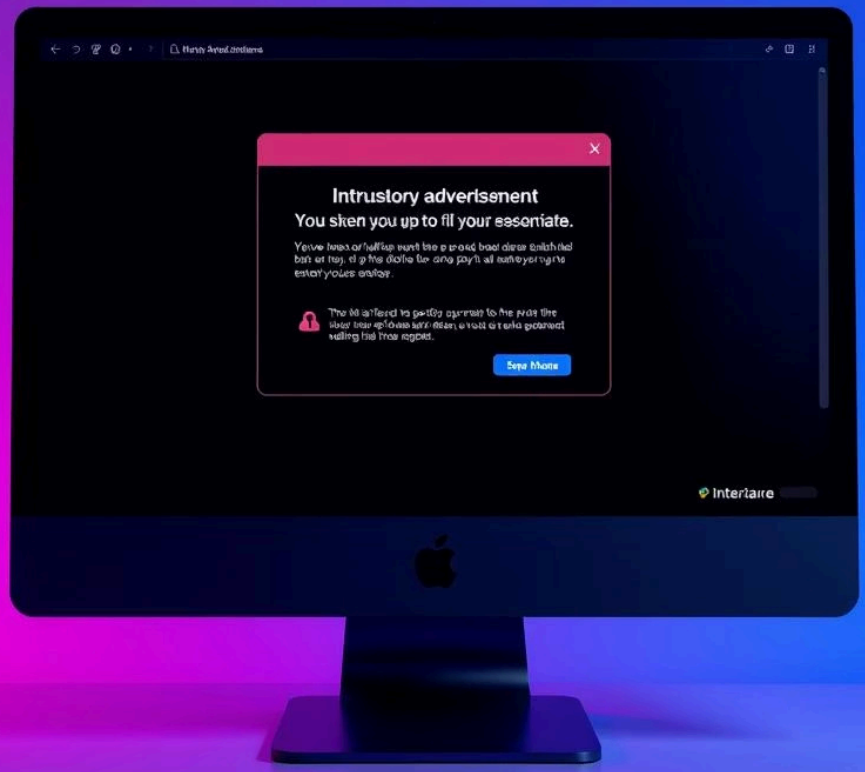
Spyware

- Monitors user activities without consent.
- Captures keystrokes, screen data, and browser history.
- Used for identity theft and surveillance.
- *Examples:* FinFisher, DarkHotel



Adware

- Displays intrusive advertisements.
- Slows down systems and collects user data.
- Sometimes bundled with freeware.
- *Examples:* Fireball, Gator

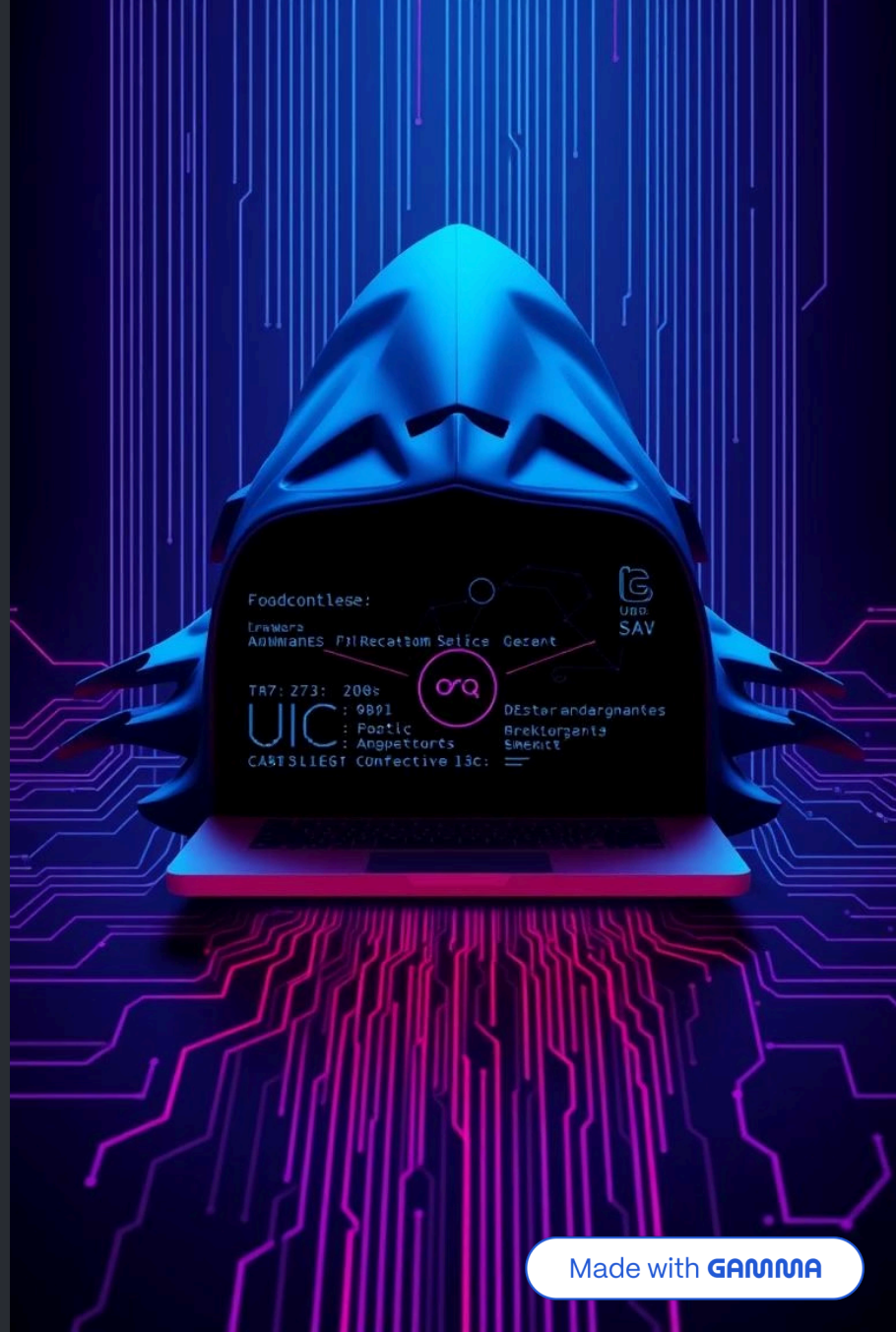


Keylogger

- Records every keystroke on the infected device.
- Captures passwords, credit card numbers, and personal information.
- Can be hardware- or software-based.
- *Examples:* Agent Tesla, Ardamax

Rootkit

- Provides privileged access to the attacker.
- Hides the presence of other malware.
- Extremely difficult to detect and remove.
- *Examples:* Necurs, ZeroAccess

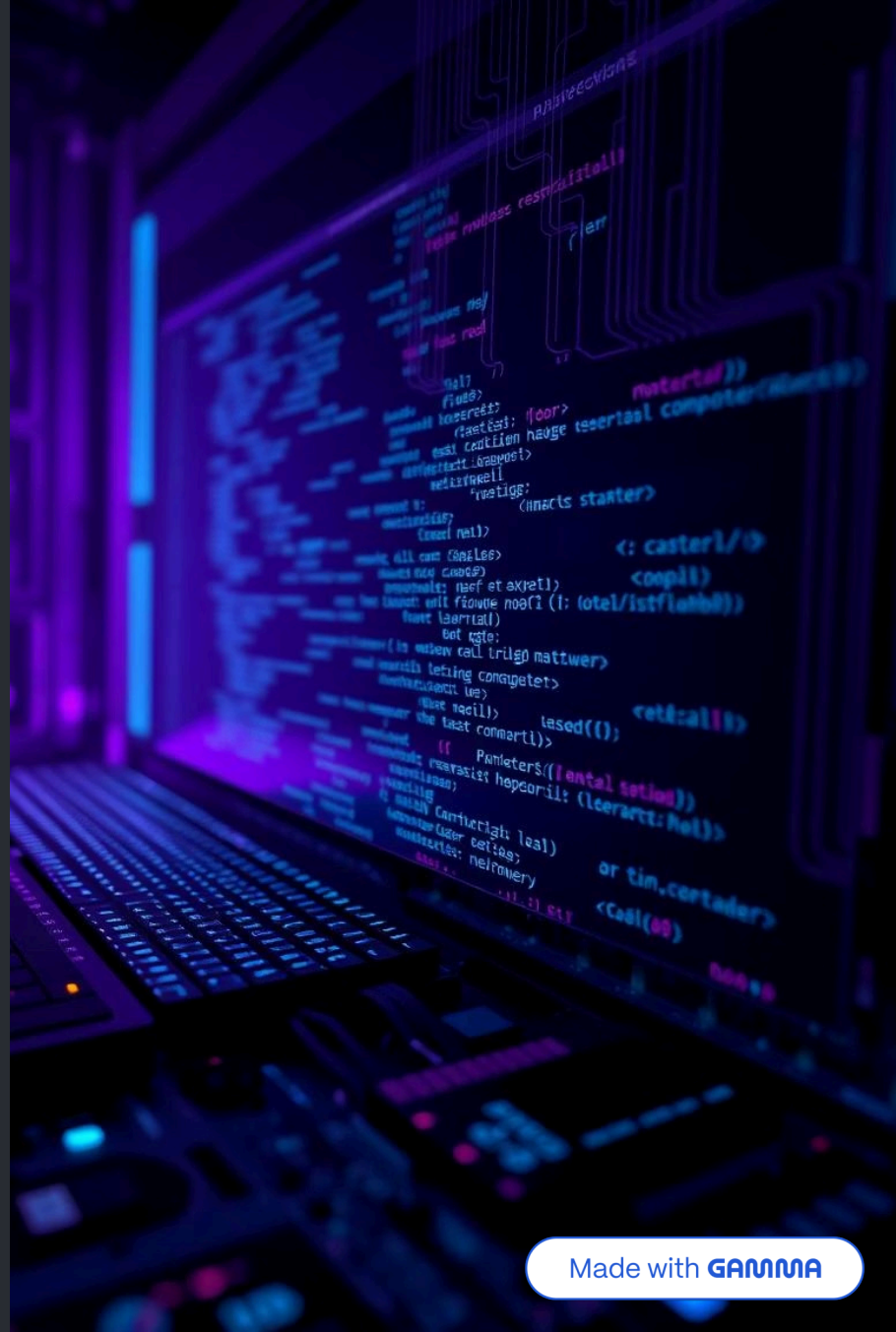


Botnet

- Networks of infected devices controlled remotely.
- Used in DDoS attacks, spamming, and crypto-mining.
- Each infected machine is called a 'bot' or 'zombie'.
- *Examples:* Mirai, Cutwail

Fileless Malware

- Resides in memory and doesn't write to disk.
- Uses legitimate system tools (like PowerShell).
- Harder to detect by traditional antivirus tools.
- *Examples:* Astaroth, Kovter



Malware Infection Vectors

Phishing Emails

Malicious attachments or links

Drive-by Downloads

From compromised or malicious websites

Removable Media

Infected USB drives or external devices

Unpatched Software

Exploits known vulnerabilities

Social Engineering

Tricks users into installing malware

Impacts of Malware Attacks

Data Breaches

Stolen sensitive information

Financial Loss

Ransom and fraud costs

Downtime

System crashes and freezes

Legal Issues

Violations of data protection laws

Reputation Damage

Loss of customer trust

Notable Real-World Malware Cases

WannaCry (2017)

Ransomware exploiting SMB protocol

Emotet Trojan

Email spread; dropped other malware

SolarWinds Attack

Fileless backdoor in trusted software

Detection & Prevention Techniques

1 **Antivirus & EDR Tools**

Essential for threat detection

2 **Regular Patching**

Fix vulnerabilities promptly

3 **Network Segmentation**

Limit malware spread potential

4 **User Training**

Phishing and safe practice awareness

5 **Incident Response Plan**

Prepare for quick mitigation

Conclusion & Recommendations

- Malware is evolving; so must defenses
- Adopt layered security: tech + training
- Continuous system monitoring
- Respond quickly to threats
- Stay updated on emerging malware

Thank You

Questions? Ready to enhance your cybersecurity defenses.