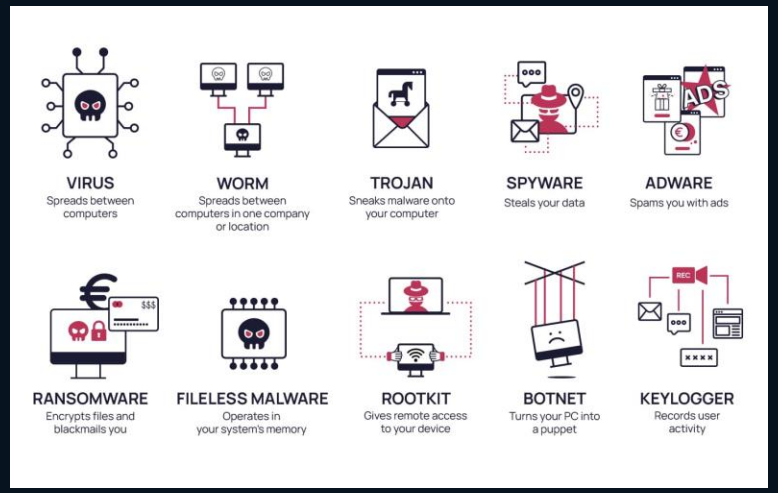
Malware

Introduction



- Malware, or malicious software, is an all-encompassing term for software that intentionally inflicts damage on its users who typically have no idea that they are running it.
- Malware includes:
  - Computer viruses, worms
  - Trojans
  - Ransomware
  - Scareware
  - Spyware
  - cryptocurrency miners
  - adware,
  - and other programs
- It is intended to exploit computer resources for nefarious purposes.

Computer Viruses

- What is a Virus?
  - Malware that inserts its code into files/programs to spread.
  - Requires a host (like biological viruses) to replicate.
- How Do Viruses Spread?
  - Infected files: Documents, executables, boot sectors.
  - Removable media: USB drives, shared networks.
  - Human action: Running infected programs or opening malicious files.
- Impact of Viruses
  - Performance issues (slowdowns, crashes).
  - Data corruption/deletion.
  - Dormant threats: Some operate silently.
  - Declining but not dead: Modern malware favours worms/Trojans.
- Protection Tips
  - Use antivirus software (real-time scanning).
  - Avoid unknown file sources.
  - Regularly update OS/apps.
  - Scan external devices before use.

Computer Worms: Self-Propagating Malware

- **Key Characteristics**
  - Standalone malware that **doesn't need a host file**
  - **Self-replicates** automatically across networks/systems
  - Spreads by exploiting **security vulnerabilities**
- **How Worms Spread**
  - Through **network connections** (LAN/Internet)
  - Via **email attachments** or malicious links
  - Using **unpatched software vulnerabilities**
- **Primary Impacts**
  - **Network congestion**: Slows Internet/LAN traffic
  - **Resource depletion**: Consumes bandwidth & system resources
  - **Secondary payloads**: May deliver other malware
- **Protection Measures**
  - Keep all systems **patched and updated**
  - Use **firewalls** to block unauthorized traffic
  - Implement **network segmentation**
  - Educate users about **suspicious emails/links**

Trojans: Deceptive Malware

- What is a Trojan?
  - Malware disguised as harmless software (e.g., games, utilities) or hidden in legitimate apps.
  - Named after the Trojan Horse (stealthy infiltration).
- How Do Trojans Spread?
  - Social Engineering Attacks:
    - Fake downloads, malicious email attachments, and pirated software.
    - Phishing links, fake updates, or compromised websites.
  - Human-Dependent: Unlike viruses/worms, they do not self-replicate.
- Common Payloads (Harm Caused)
  - Data theft (passwords, banking info)
  - Remote system control (backdoor access)
  - Ransomware deployment
  - Turning devices into botnets
- How to Stay Protected?
  - Avoid suspicious links/attachments.
  - Download software only from trusted sources.
  - Use antivirus + firewall.
  - Keep systems & apps updated.

Ransomware: Digital Extortion Malware

- **What is Ransomware?**
  - Malware that **demands payment** (often in crypto) to:
    - **Decrypt files** (e.g., WannaCry)
    - **Prevent data leaks** (threatens to publish stolen data)
    - **Permanently delete files** (no recovery option)
- **How It Spreads**
  - **Trojans** (fake software/emails)
  - **Viruses/Worms** (e.g., WannaCry exploited Windows vulnerabilities)
- **Targeted campaigns**: Criminals research victims to maximize ransom demands.
- **Notable Example: WannaCry (2017)**
  - **Impact**: 150+ countries, 300K+ computers, $4 billions in damages.
  - **Origin**: Likely state-sponsored (North Korea).
  - **Propagation**: Worm-like spread via unpatched Windows systems.
- **Protection & Response**
  - **Prevention**:
    - Regular **backups** (offline/cloud)
    - Patch **OS/software** promptly
    - Train users to **avoid suspicious links/attachments**
  - **If infected**:
    - Isolate systems, **do not pay** (no guarantee of recovery)
    - Report to the authorities

Scareware: Fear-Based Malware

- **What is Scareware?**
  - Malware that **uses fear tactics** to trick users into:
    - Buying **fake security software**
    - Paying for **unnecessary "system repairs"**
    - Downloading **malicious programs**
- **How It Works**
  - Displays **fake alerts/warnings** (e.g., "Virus Detected!")
  - Claims **urgent action** is needed (e.g., "Your PC is infected!")
  - Offers a **"solution"** (malicious or useless software)
- **Common Examples**
  - **Fake antivirus** pop-ups ("Your computer is at risk!")
  - **Browser lockers** ("Your PC has 5 viruses! Call this number!")
  - **Tech support scams** (e.g., "Microsoft" calling about a virus)
- **How to Avoid Scareware**
  - **Ignore unsolicited pop-ups** (never click "Fix Now")
  - **Never call the provided numbers**
  - **Use a trusted antivirus** (e.g., Windows Defender, Malwarebytes)
  - **Keep software updated** (prevents fake update scams)

Spyware: Covert Data Collection

- **What is Spyware?**
  - Malware that **secretly gathers data** without consent, including:
    - Keystrokes (**keyloggers**)
    - Camera/microphone access
    - Screen activity & browsing history
- **Common Delivery Methods**
  - **Bundled with free software** (e.g., pirated apps)
  - **Phishing links** or malicious attachments
  - **Exploiting unpatched vulnerabilities**
- **How to Protect Yourself**
  - **Avoid sideloading apps** (use official app stores)
  - **Review app permissions** (disable camera/mic access when unused)
  - **Use anti-spyware tools** (e.g., Malwarebytes, Spybot)
  - **Cover webcams** & disable unused microphones

Spyware (Malicious)	Legitimate Tracking
Installed **without consent**	Disclosed in **terms of service** (e.g., cookies, app permissions)
Hidden operations (e.g., background recording)	**Limited scope** (e.g., Uber location tracking only during rides)
Used for **fraud/theft**	Used for **analytics/targeted ads**

Cryptocurrency miners

- **What Are Cryptominers?**
  - Malware that **steals device processing power** (CPU/GPU) to mine cryptocurrency **without the owner's consent**.
  - Generates **crypto rewards for attackers** by solving complex math problems.
- **Why Are They Popular?**
  - **Low-cost, high-reward** for attackers:
    - No ransom demands or data theft required.
    - Easy to deploy at scale (e.g., via infected websites or malware).
  - **Proliferation**: Surged in 2017 with crypto price spikes; remains common even during market dips.
- **How They Spread**
  - **Infected downloads** (fake software, pirated apps).
  - **Malicious ads/websites** (in-browser mining via scripts).
  - **Exploiting vulnerabilities** (e.g., unpatched servers, smartphones).
- **Targets & Impact**
  - **Computers, servers, and even Android phones**.
  - **Slows devices**, increases power usage, and causes overheating.
  - **Financial motive**: Attackers profit directly from mined crypto
- **How to Stay Protected**
  - **Monitor device performance** (unusual CPU spikes = red flag).
  - **Use ad-blockers** (stop in-browser miners).
  - **Keep software updated** (patch exploits).
  - **Install anti-cryptomining tools** (e.g., Malwarebytes, NoCoin browser extension).

Adware: Advertising-Supported Software

Legitimate Adware	Malicious Adware (Adware Malware)
User **knowingly installs** it (e.g., free ad-supported apps)	Installed **without consent** (often bundled with pirated software)
Clearly disclosed in terms	Hidden, difficult to remove
Generally non-harmful	May track behavior, slow devices, or redirect to scams

- **What is Adware?**
  - Software that **displays ads** to generate revenue, existing in two forms (see the table)
- **How Malicious Adware Spreads**
  - Bundled with **free downloads** (games, utilities)
  - **Fake updates** or browser extensions
  - Exploiting **unpatched vulnerabilities**
- **Risks of Malicious Adware**
  - Excessive **pop-up ads** & browser redirects
  - **System slowdowns** (high CPU/RAM usage)
  - **Privacy risks** (tracking browsing habits)
- **How to Protect Against Adware**
  - **Read EULAs** (End-user license agreement) before installing free software
  - Use **ad-blockers** (uBlock Origin, AdGuard)
  - Avoid **pirated software** and shady download sites
  - Regularly **scan for adware** (Malwarebytes, AdwCleaner)

Zero-Day Malware: The Invisible Threat

- **Zero-Day Malware is a:**
  - Malware that exploits **unknown vulnerabilities** (not yet patched by vendors).
  - Highly effective because:
    - No defences exist yet.
    - Attacks occur **before vendors can issue fixes**.
- **Who Creates Zero-Day Malware?**
  - **Nation-state actors** (cyber armies, espionage).
  - **Well-funded criminal groups** (selling exploits for $1M+ on the dark web).
  - **Advanced Persistent Threats (APTs)** (long-term targeted attacks).
- **Why is it Dangerous?**
  - **No prior detection**: Bypasses antivirus & firewalls.
  - **High success rate**: Victims have no time to prepare.
  - **Used in targeted attacks**: Espionage, sabotage, or data theft.

Zero-Day Malware: The Invisible Threat

- **Famous Examples:**
  - **Stuxnet** (sabotaged Iranian nuclear facilities)
  - **WannaCry** (exploited Windows SMB zero-day).
- **How to Reduce Risk**
  - **Advanced threat detection** (AI/behaviour-based tools).
    - Traditional security solutions often rely on recognizing known signatures of malware or attack patterns. **The AI models** is a behavior-based tools come into play.
  - **Network segmentation** (limit lateral movement).

    Network segmentation is a security practice that divides a network into smaller, isolated segments.
  - **Patch ASAP** (when vendors release fixes).
    - Software and hardware vulnerabilities are constantly being discovered. Vendors regularly release patches or updates to fix these flaws. Applying these patches promptly is a fundamental security practice.
  - **Assume breaches** (zero-trust security models).
    - The traditional security model often operates on the assumption that everything inside the network perimeter is trustworthy. The "assume breach" or "zero-trust" model flips this assumption.

Fake Malware: The Bluff Attack

What is Fake Malware?

- **No actual infection**—just scare tactics to trick users into:
  - Paying for **fake "security services"**
  - Downloading **real malware** (disguised as a "fix")
  - Sharing **personal/financial info**

Common Delivery Methods

- **Fake pop-ups**:
  - *"Virus detected! Call tech support NOW!"*
  - *"Your PC is at risk—click here to scan!"*
- **Phishing emails**:
  - *"Urgent: Your device is hacked—pay to unlock!"*

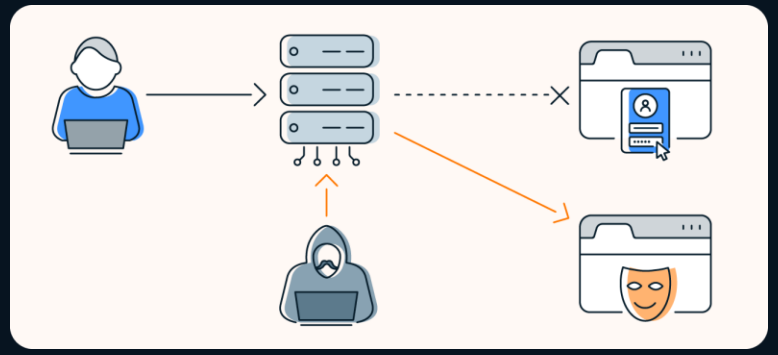
How It Works

- Displays **alarming (but fake) warnings**.
- Pressures users into **quick action** (e.g., paying a fee).
- May lead to **real malware** if users click links.

How to Spot & Avoid It

- **Never trust unsolicited alerts**—close pop-ups via Task Manager (Ctrl+Shift+Esc).
- **Do not call provided numbers**—scammers impersonate Microsoft/Apple support.
- **Use real antivirus** (Windows Defender, Malwarebytes).
- **Check for actual threats**—run a legitimate scan.

Poisoned Web Service Attacks



- **Hijacked servers** deliver malware to visitors via:
  - Compromised **web pages** (e.g., injected malicious scripts).
  - Exploited **user-generated content** (e.g., comments, forms).
- **How It Works**
  1. **Server Compromise** (Direct Attack):

     Hackers breach a site (e.g., www.abc123.com) and **modify its code** to infect visitors.
  2. **Cross-Site Scripting (XSS)** (No Breach Needed):

     Attackers post **malicious scripts** in comments/forms.

     When loaded, the script **steals cookies/session data** or delivers malware.
- **Real-World Risks**
  - **Drive-by Downloads** (malware installs silently).
  - **Credential Theft** (via session hijacking).
  - **Fake Redirects** (phishing/scam sites).
- **How to Stay Protected**
  - **Use ad-blockers** (stop malicious scripts).
  - **Keep browsers updated** (patch XSS vulnerabilities).
  - **Avoid suspicious sites** (check for HTTPS & trust seals).
  - **Disable JavaScript** for untrusted sites (if possible).

The CIA Triad: Core Principles of Cybersecurity

- CIA Triad is the Foundational model for cybersecurity. Stands for**: Confidentiality, Integrity, Availability**.
- **Confidentiality:**
  - Ensures data is accessible only to authorized users.
  - Tools: Encryption, Access Controls, Multi-Factor Authentication (MFA).
- **Integrity:**
  - Ensures data is accurate and unaltered.
  - Tools: Hashing, Digital Signatures, Checksums.
- **Availability:**
  - Ensures systems/data are accessible when needed.
  - Tools: Redundancy, Backups, DDoS Protection.
- Why is the CIA Triad Important?
  - Protects sensitive data (e.g., financial, personal, government).
  - Prevents tampering, breaches, and downtime.
  - Basis for compliance (e.g., GDPR, HIPAA).

The CIA Triad: Core Principles of Cybersecurity

Real-World Examples

- Confidentiality: Healthcare records (HIPAA).
- Integrity: Blockchain transactions.
- Availability: Cloud server redundancy (AWS/Azure).

Challenges & Threats

- Confidentiality: Phishing, Data leaks.
- Integrity: Malware, Insider threats.
- Availability: Ransomware, DDoS attacks.

Conclusion

- CIA Triad is the backbone of cybersecurity.
- Balancing all three principles is key to robust security.
- Visuals to Include:
- CIA Triad diagram.

Questions