Malware

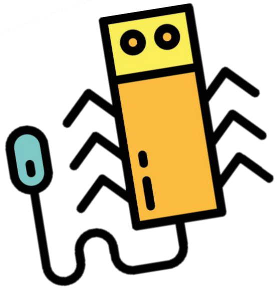
Malware (Malicious Software) is **any software or code specifically designed to disrupt, damage, or gain unauthorized access to computer systems, networks, or data**. It is used by cybercriminals to **steal sensitive information, encrypt files for ransom, spy on users, disrupt operations, or take control of systems remotely**.

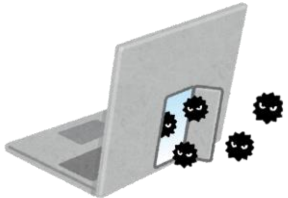
Malware can spread via **phishing emails, infected downloads, removable devices, software vulnerabilities, and network exploits**.

Types

- Virus
- Worm
- Trojan Horse
- Ransomware
- Spyware
- Adware
- Rootkit
- Metamorphic Malware
- Scareware

- Keylogger
- Botnet
- Fileless Malware
- Logic Bomb
- Backdoor
- RAT (Remote Access Trojan)
- Cryptojacking Malware
- Polymorphic Malware
- Bootkit





1. Virus

Definition

A **virus** is a type of **self-replicating malware** that attaches itself to legitimate files or programs and spreads when the infected file is executed.

How It Works

1. **Infection:** The virus **attaches itself** to a host file (e.g., EXE, DOC, DLL).
2. **Execution:** When the infected file is **opened or run**, the virus gets activated.
3. **Replication:** The virus **copies itself** to other files or system areas.
4. **Payload Execution:** Some viruses are harmless, but others can **delete files, steal data, or crash systems**.
5. **Spread:** The virus spreads through **USB drives, email attachments, file downloads, or network shares**.

Characteristics of a Virus

- **Needs a Host File:** Cannot spread without attaching to a file or program.
- **Requires User Action:** Needs the user to **run or open** an infected file.
- **Self-Replication:** Duplicates itself across files or systems.
- **Can Be Dormant:** Some viruses stay inactive until triggered by specific conditions.

Countermeasures

✅ **Use Antivirus Software:** Regularly scan for and remove viruses.

✅ **Update Software:** Keep OS and applications **patched** to prevent exploitation.

✅ **Avoid Suspicious Files:** Do not download or open unknown **email attachments**.

✅ **Use Application Whitelisting:** Restrict execution of unauthorized programs.

✅ **Regular Backups:** Maintain offline backups to recover lost data.

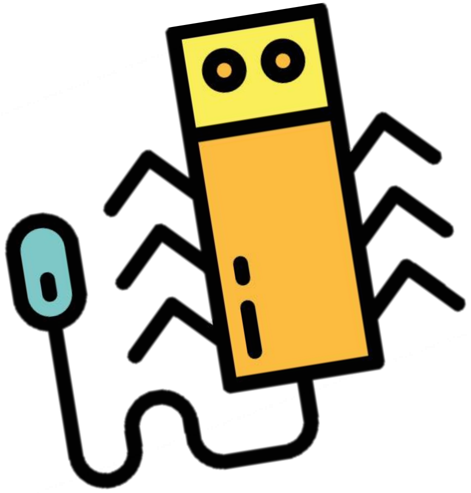
Recent Trending Viruses

1. Emotet Virus – Initially a banking Trojan, now used for malware delivery.

2. Sality Virus – A polymorphic virus that spreads via removable drives.

3. Ramnit Virus – A file-infecting virus that steals credentials and infects executable files.

2. Worm



Definition

A **worm** is a **self-replicating malware** that spreads across networks **without requiring user action**. Unlike viruses, worms do not need a host file and can **spread independently**.

How It Works

1. **Exploitation:** The worm **scans for vulnerabilities** in systems or networks.
2. **Infection:** Once it finds a target, it **gains access** and installs itself.
3. **Replication:** The worm **copies itself** to other systems, using exploits, emails, or removable drives.
4. **Payload Execution:** Some worms **steal data, install backdoors, or create botnets**.
5. **Spread:** The worm **self-propagates**, infecting other devices on the network.

Characteristics of a Worm

- **Self-Replicating:** Spreads without human intervention.
- **No Host File Needed:** Unlike viruses, worms **operate independently**.
- **Network-Based Propagation:** Exploits **network vulnerabilities** to spread.
- **Fast-Spreading:** Can infect **millions of devices** in hours.

Countermeasures

✅ **Patch Systems:** Keep OS and software updated to close security gaps.

✅ **Enable Firewalls:** Block unauthorized traffic and limit network access.

✅ **Disable Unused Ports:** Close open ports (e.g., SMB, RDP) to prevent exploitation.

✅ **Use Network Segmentation:** Separate networks to limit worm spread.

✅ **Monitor Network Traffic:** Detect **unusual spikes in connections** (e.g., scanning behavior).

Recent Trending Worms

1. **Morto Worm** – Spreads via RDP brute-force attacks.

2. **EternalBlue Exploit Worm (WannaCry & NotPetya)** – Used to spread ransomware via SMB vulnerabilities.

3. **SQL Slammer Worm** – Exploits Microsoft SQL Server vulnerabilities for rapid infection.

3. Trojan Horse (Trojan)

Definition

A **Trojan Horse** (or **Trojan**) is **malware disguised as legitimate software**. Unlike viruses and worms, a Trojan does not self-replicate but tricks users into downloading and executing it, allowing attackers to gain unauthorized access.

How It Works

1. **Disguised as Legitimate Software:** The Trojan is bundled with **fake software, cracked apps, or email attachments**.
2. **Execution:** The victim **installs or runs** the Trojan, believing it to be safe.
3. **Payload Execution:** Once activated, the Trojan performs malicious activities, such as **stealing data, opening backdoors, or installing additional malware**.
4. **Persistence:** Trojans often **modify system settings** to ensure they run after reboot.

Characteristics of a Trojan

- **Disguised as Legitimate Software** – Trick users into installing them.
- **No Self-Replication** – Unlike viruses, Trojans don’t spread automatically.
- **Can Open Backdoors** – Often used to install **spyware, ransomware, or botnets**.
- **Remote Control** – Attackers can control infected systems remotely.

Countermeasures

✅ **Use Reputable Software:** Download programs only from official sources.

✅ **Scan Email Attachments:** Do not open **unverified attachments or links**.

✅ **Use Endpoint Security Solutions:** Detect **Trojan signatures and behaviors**.

✅ **Monitor Network Traffic:** Identify **suspicious outbound connections**.

✅ **Block Unnecessary Services:** Disable **PowerShell, RDP, or scripting** if not needed.

Recent Trending Trojans

1. **TrickBot** – Banking Trojan that steals credentials and spreads ransomware.

2. **QakBot (Qbot)** – Trojan used for **financial fraud and data theft**.

3. **Zeus Trojan** – Designed to **steal banking information** via keylogging.

4. Ransomware

Definition

Ransomware is **malware that encrypts files or locks systems**, demanding payment (ransom) for decryption. It is one of the most **destructive** forms of cyber threats.

How It Works

1. **Infection:** Delivered via **phishing emails, malicious ads, or exploits**.
2. **Execution:** The ransomware **encrypts files** on the system.
3. **Ransom Demand:** The victim receives a **ransom note demanding payment (often in cryptocurrency).**
4. **Data Loss or Payment:** Victims either **pay or attempt recovery** (if backups exist).

Characteristics of Ransomware

- **Encrypts Files or Locks Systems** – Prevents access until ransom is paid.
- **Demands Cryptocurrency Payment** – Uses Bitcoin, Monero, etc., for anonymity.
- **Often Spread via Phishing** – Social engineering is a common method.
- **Uses Strong Encryption** – Many ransomware strains use **AES-256 or RSA encryption**.

Countermeasures

✅ **Regular Backups:** Keep **offline and cloud backups** to recover files.

✅ **Disable Macros & Script Execution:** Prevent **automatic execution** of malicious scripts.

✅ **Patch Vulnerabilities:** Close security gaps (e.g., **SMB, RDP exploits**).

✅ **Use Endpoint Detection & Response (EDR):** Detect ransomware activity early.

✅ **Network Segmentation:** Isolate infected machines to stop ransomware spread.

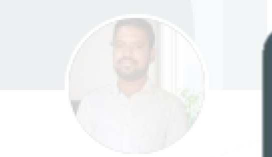
Recent Trending Ransomware

1. **LockBit 3.0** – Advanced ransomware targeting large enterprises.

2. **Black Basta** – Used in **double extortion attacks**.

3. **ALPHV/BlackCat** – A **ransomware-as-a-service (RaaS)** model targeting corporations.

5. Spyware



Definition

Spyware is **malware that secretly collects user data** without consent. It can track **keystrokes, browsing history, login credentials, and personal information**.

How It Works

1. **Infection:** Spread via **malicious downloads, Trojans, or bundled software**.
2. **Stealth Operation:** Runs in the background without user awareness.
3. **Data Collection:** Captures **keystrokes, screenshots, login credentials, and browsing activity**.
4. **Data Exfiltration:** Sends collected information to attackers.

Characteristics of Spyware

- **Operates Silently** – Runs **without user knowledge**.
- **Can Capture Keystrokes (Keyloggers)** – Records what the user types.
- **Steals Sensitive Data** – Collects **passwords, credit card details, and chats**.
- **Can Modify System Settings** – Changes browser settings, homepage, and DNS.

Countermeasures

✅ **Use Anti-Spyware Software:** Regularly scan for spyware.

✅ **Check Installed Applications:** Remove unknown or suspicious programs.

✅ **Block Unauthorized Data Transmission:** Use **firewalls & intrusion detection**.

✅ **Monitor Network Traffic:** Detect **anomalous outbound connections**.

✅ **Use Multi-Factor Authentication (MFA):** Protects against stolen credentials.

Recent Trending Spyware

1. **Pegasus Spyware** – Used for **surveillance and mobile device spying.**

2. **Agent Tesla** – Keylogger and credential-stealing spyware.

3. **RedLine Stealer** – Targets **browser-stored passwords and cryptocurrency wallets**.

6. Adware

Definition

Adware is **malware that delivers unwanted advertisements** on a user's device. While not always malicious, some adware collects **personal data** and redirects traffic to harmful sites.

How It Works

1. **Installation:** Often bundled with **freeware or cracked software**.
2. **Ad Injection:** Displays **pop-ups, banners, or forced redirects**.
3. **Data Collection:** Tracks user activity to **serve targeted ads**.
4. **Persistence:** Modifies browser settings, homepages, or search engines.

Characteristics of Adware

- **Displays Excessive Ads** – Often intrusive and hard to close.
- **Alters Browser Settings** – Redirects searches to **malicious websites**.
- **Slows Down System Performance** – Uses system resources for ad delivery.
- **Collects User Data** – Tracks **browsing habits and online behavior**.

Countermeasures

☑ **Avoid Freeware from Untrusted Sources:** Use only **verified applications**.

☑ **Check Installed Browser Extensions:** Remove **suspicious add-ons**.

☑ **Use Ad Blockers:** Prevents **malicious ads and pop-ups**.

☑ **Scan Regularly for Malware:** Detect and remove adware-infected programs.

Recent Trending Adware

1. **Fireball –** Adware that also acted as a **browser hijacker**.

2. **DeskAd Adware –** Injected unwanted ads into search results.

3. **Crossrider Adware –** Spread via fake browser extensions.

7. Rootkit

Definition

A **Rootkit** is **a stealthy malware** designed to gain **persistent privileged access** to a system while hiding its presence. Attackers use rootkits to **bypass security tools, modify system settings, and control devices remotely**.

How It Works

1. **Infection:** Delivered via **Trojan, phishing emails, or malicious downloads**.
2. **Privilege Escalation:** Gains **administrator (root) access** by exploiting vulnerabilities.
3. **System Manipulation:** Modifies **kernel, boot records, or firmware** to avoid detection.
4. **Hiding Malicious Processes:** Prevents antivirus tools from detecting its activities.
5. **Remote Control:** Attackers gain **backdoor access** to execute commands stealthily.

Characteristics of Rootkits

- **Stealthy & Persistent:** Hides itself from **antivirus and system logs**.
- **Operates at Low-Level:** Some rootkits modify the **kernel or firmware**.
- **Disables Security Tools:** Deactivates **antivirus, firewalls, and system monitoring**.

Countermeasures

✅ **Use Secure Boot & UEFI Firmware Protection:** Prevents unauthorized boot modifications.

✅ **Employ Behavior-Based Detection:** Identify abnormal privileged activities.

✅ **Use Rootkit Removal Tools:** (e.g., **GMER, TDSSKiller, Malwarebytes Anti-Rootkit**).

✅ **Reinstall OS (If Necessary):** Rootkits deeply embedded in firmware require a full system wipe.

Recent Trending Rootkits

1. **LoJax Rootkit** – The first UEFI rootkit used for persistent attacks.

2. **SYNFUL Knock** – Targets **Cisco routers** for remote control.

3. **Zacinlo Rootkit** – Targets Windows systems for **ad fraud and surveillance**.

8. Keylogger

Definition

A **Keylogger** (Keystroke Logger) is **malware that records keystrokes** to steal passwords, banking credentials, and personal information.

How It Works

1. **Infection:** Delivered via **malicious email attachments, Trojans, or phishing sites**.
2. **Keystroke Recording:** Captures **everything typed**, including passwords.
3. **Data Storage:** Logs keystrokes into hidden files or sends them to an attacker's server.
4. **Exfiltration:** The stolen data is transmitted via **email, FTP, or C2 servers**.

Characteristics of Keyloggers

- **Operates Silently:** Runs in **background without user knowledge**.
- **Records Sensitive Data:** Logs **usernames, passwords, credit card details**.
- **Can Be Software or Hardware-Based:** Some are installed on **USB devices or firmware**.

Countermeasures

✅ **Use Virtual Keyboards & 2FA:** Prevents keylogging attacks.

✅ **Monitor System Processes:** Detects **unauthorized logging applications**.

✅ **Use Anti-Keylogging Tools:** (e.g., **Zemana AntiLogger, SpyShelter**).

✅ **Enable Tamper-Proof Antivirus Protection:** Prevents stealth keyloggers from running.

Recent Trending Keyloggers

1. Agent Tesla – Widely used in **credential theft campaigns**.

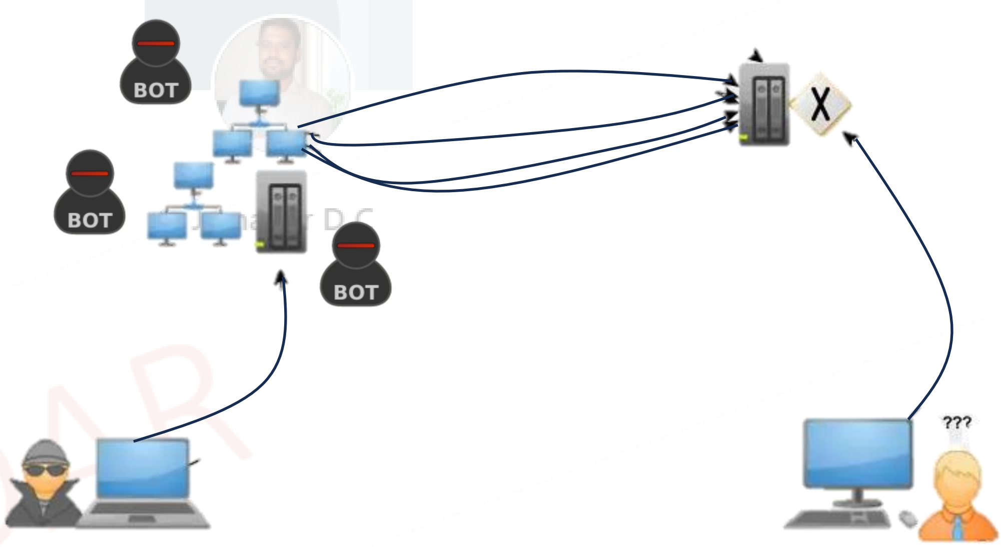
2. HawkEye Keylogger – Sold as a **malware-as-a-service (MaaS)**.

3. Olympic Vision Keylogger – Targets government organizations.

9. Botnet

Definition

A **Botnet** is a **network of compromised devices (bots) controlled by an attacker** to launch large-scale cyberattacks, such as **DDoS, spamming, or credential stuffing**.



How It Works

1.**Infection:** Devices are compromised via **malware, phishing, or exploits**.

2.**Connection to Command & Control (C2):** The infected device connects to a C2 server.

3.**Remote Control:** Attackers issue commands to thousands of infected devices.

4.**Attack Execution:** Botnets are used for **DDoS attacks, spam campaigns, or crypto mining**.

Characteristics of Botnets

- **Mass Infection:** Can control **millions of devices simultaneously**.
- **Used for Large-Scale Attacks:** DDoS, brute-force attacks, and credential stuffing.
- **Hard to Detect:** Bots operate **stealthily in the background**.

Countermeasures

✓ **Use Network Traffic Analysis:** Detect **anomalous communication patterns**.

✓ **Enable Firewall & IDS/IPS:** Blocks unauthorized traffic from botnets.

✓ **Patch Systems & Close Open Ports:** Prevents exploit-based infections.

✓ **Monitor for C2 Communication:** Detects suspicious connections to botnet servers.

Recent Trending Botnets

1. Mirai Botnet – Targets **IoT devices** for massive DDoS attacks.

2. Emotet Botnet – Originally a banking Trojan, now used for **malware distribution**.

3. Mantis Botnet – Used for **record-breaking DDoS attacks**.

10. Fileless Malware

Definition

Fileless Malware is a type of malware that **does not use traditional executable files** but instead **exploits legitimate system processes** (e.g., PowerShell, WMI).

How It Works

1. **Exploits Legitimate Tools:** Runs directly in **memory (RAM) without leaving a file**.
2. **Uses Living-Off-The-Land Binaries (LOLBins):** Executes via **PowerShell, WMI, or JavaScript**.
3. **Persistence:** Hides in **registry, scheduled tasks, or process memory**.

Characteristics of Fileless Malware

- **No Traditional Files:** Avoids detection by antivirus tools.
- **Uses Legitimate Windows Components:** Exploits **PowerShell, WMI, and script interpreters**.
- **Highly Stealthy & Persistent:** Can execute commands without leaving disk traces.

Countermeasures

✅ **Disable Unnecessary Scripting Tools (PowerShell, WMI, Macros):** Prevents execution.

✅ **Use Behavioral Analysis Solutions:** Detects suspicious process injections.

✅ **Monitor Registry & Memory Usage:** Identifies fileless attack patterns.

Recent Trending Fileless Malware

1. Kovter – Uses **registry persistence** for stealth execution.

2. FIN7 Fileless Attack – Uses **PowerShell and WMI scripting** for cybercrime.

3. Cobalt Strike Beacons – Fileless exploitation tool used in **advanced persistent threats (APTs)**.

11. Logic Bomb

Definition

A **Logic Bomb** is **malware that remains dormant until triggered by a specific condition** (e.g., a date, event, or system change).

How It Works

1. **Hidden Inside Software:** Planted in applications, scripts, or firmware.
2. **Trigger Activation:** Activates on a specific **date, system event, or action**.
3. **Payload Execution:** Deletes files, corrupts databases, or installs backdoors.

Characteristics of Logic Bombs

- **Dormant Until Triggered:** Does not activate until predefined conditions are met.
- **Planted by Insiders or APT Groups:** Often used for **insider threats**.
- **Highly Destructive:** Can **wipe data, disable security controls, or disrupt operations**.

Countermeasures

✓ **Monitor System Changes:** Detect unauthorized **scheduled tasks or scripts**.

✓ **Restrict Insider Access:** Limit **admin privileges and critical system access**.

✓ **Conduct Code Audits:** Review software and scripts for **hidden malicious logic**.

Recent Trending Logic Bombs

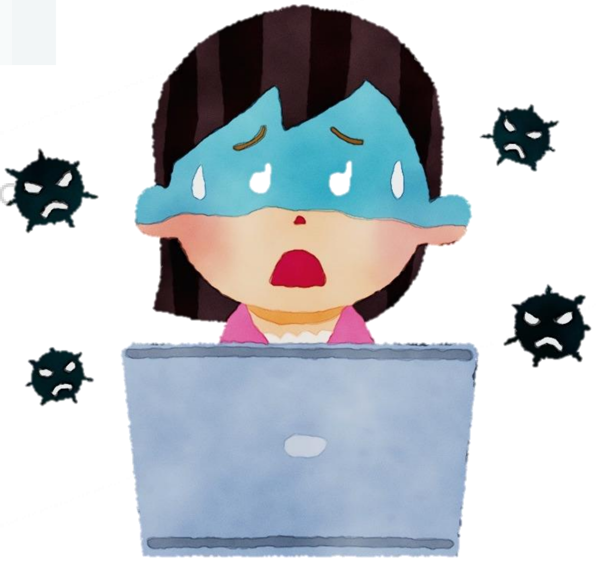
1. **Dark Seoul Logic Bomb** – Used in attacks against South Korean infrastructure.

2. **Sony Logic Bomb –** Allegedly used in insider sabotage cases.

12. Backdoor

Definition

A **Backdoor** is **malware that creates hidden access** to a system, allowing attackers to bypass authentication and security controls. Backdoors are often installed by **Trojans, rootkits, or attackers who exploit vulnerabilities**.



How It Works

1. **Infection:** Delivered via **Trojan, phishing, or software exploits**.
2. **Installation:** The backdoor modifies system settings to ensure persistence.
3. **Unauthorized Access:** Attackers use the backdoor to **remotely control** the system.
4. **Malicious Actions:** Attackers can **steal data, install additional malware, or manipulate files**.

Characteristics of Backdoors

- **Bypasses Authentication:** Allows attackers to access a system **without credentials**.
- **Operates Stealthily:** Hidden from **users and security tools**.
- **Provides Remote Access:** Enables **attackers to execute commands remotely**.
- **Can Be Installed via Exploits or Trojans:** Often injected into **compromised applications**.

Countermeasures

✅ **Regularly Patch Software:** Prevents attackers from exploiting known vulnerabilities.

✅ **Monitor Network Traffic:** Detects unauthorized **C2 (Command & Control) connections**.

✅ **Use EDR & SIEM Solutions:** Identify suspicious **remote access attempts**.

✅ **Restrict Administrative Privileges:** Prevent unauthorized **system modifications**.

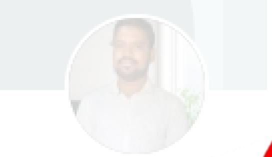
Recent Trending Backdoors

1. **Cobalt Strike Backdoor** – Used in **APT (Advanced Persistent Threat) campaigns**.

2. **RedLine Backdoor** – Targets **corporate networks for credential theft**.

3. **DoorDash Backdoor** – A Windows backdoor used in espionage attacks.

13. Remote Access Trojan (RAT)



Definition

A **Remote Access Trojan (RAT)** is a **type of Trojan malware** that provides **full remote control** of an infected device. Attackers use RATs for **spying, data theft, and further malware deployment**.

How It Works

1. **Infection:** Spread via **malicious email attachments, fake software, or cracked applications**.
2. **Installation & Persistence:** The RAT hides in **system processes** and ensures it survives reboots.
3. **Remote Control:** Attackers **send commands** via a Command & Control (C2) server.
4. **Exfiltration & Espionage:** Attackers **steal files, spy via webcams, log keystrokes, and manipulate data**.

Characteristics of RATs

- **Gives Full Remote Access:** Attackers can **control the system like an admin**.
- **Hard to Detect:** Operates stealthily, avoiding detection by antivirus software.
- **Can Install Additional Malware:** Often used to deploy **ransomware or keyloggers**.
- **Records Audio & Video:** Can activate **webcams and microphones** for spying.

Countermeasures

☑ **Block Untrusted Applications:** Use **whitelisting** to restrict execution.

☑ **Monitor Network Traffic:** Identify **C2 communication patterns**.

☑ **Check for Unusual System Processes:** Look for hidden **remote administration services**.

☑ **Disable Unused Ports & Services:** Prevent remote exploitation via **RDP, SSH, or Telnet**.

Recent Trending RATs

1. NanoCore RAT – Used in **corporate espionage and financial fraud**.

2. AsyncRAT – A stealthy RAT used for **long-term remote control**.

3. DarkComet RAT – A popular RAT used for **keylogging and webcam spying**.

14. Cryptojacking Malware

Definition

Cryptojacking is malware that **hijacks system resources** to mine cryptocurrency without user consent. It slows down infected devices and increases electricity costs.

How It Works

1. **Infection:** Delivered via **malicious websites (drive-by mining), Trojans, or browser-based scripts**.
2. **Execution:** The malware secretly runs a **cryptocurrency mining algorithm** in the background.
3. **Resource Hijacking:** Uses **CPU and GPU power** to mine coins for attackers.
4. **Stealth Mode:** Ensures persistence by **avoiding detection and disabling security tools**.

Characteristics of Cryptojacking

- **Consumes High CPU/GPU Resources:** Slows down **computers, servers, and IoT devices**.
- **Runs in the Background:** Often unnoticed by users.
- **Uses JavaScript in Browsers:** Some cryptojackers don't require downloads.
- **Targets Cloud Platforms:** Compromised cloud servers are used for large-scale mining.

Countermeasures

✅ **Use Endpoint Protection:** Detects cryptojacking malware.

✅ **Monitor System Performance:** Identify **unusual CPU/GPU usage**.

✅ **Block Unauthorized Websites:** Prevents browser-based mining scripts.

✅ **Enforce Cloud Security Policies:** Restrict unauthorized mining activities.

Recent Trending Cryptojacking Malware

1. **Kinsing Malware** – Targets **Docker & Kubernetes for cryptojacking**.

2. **LemonDuck Malware** – A cross-platform **cryptojacker & botnet**.

3. **Crackonosh** – Found in **pirated games, mining Monero (XMR)**.

15. Polymorphic & Metamorphic Malware

Definition

- **Polymorphic Malware** changes its **code structure or encryption** every time it infects a new system.
- **Metamorphic Malware** rewrites its entire **codebase** without affecting its functionality, making detection extremely difficult.

How It Works

1. **Infection:** Delivered via **email attachments, downloads, or exploits**.
2. **Code Mutation:** The malware **alters its structure** or **completely rewrites itself** after every execution.
3. **Evasion:** Since it constantly changes, **signature-based detection** fails to identify it.
4. **Payload Execution:** It performs its **malicious activity (data theft, ransomware, spying)** while evading antivirus software.

Characteristics of Polymorphic & Metamorphic Malware

- **Constantly Evolves:** Each instance is **unique**, bypassing signature-based defenses.
- **Uses Encryption & Obfuscation:** Ensures **hidden execution**.
- **Difficult to Remove:** Some variants re-infect the system if not fully eliminated.

Countermeasures

✅ **Use Heuristic & Behavioral Analysis:** Detects malware based on **activity patterns**.

✅ **Employ AI-Powered Threat Detection:** AI-driven security tools can recognize **malware evolution**.

✅ **Sandbox Analysis:** Run suspicious files in **isolated environments** for behavior study.

Recent Trending Polymorphic & Metamorphic Malware

1. **ZCryptor Ransomware** – A polymorphic ransomware strain.

2. **Shikitega Malware** – A polymorphic Linux malware with **multi-stage payloads**.

3. **Storm Worm** – A metamorphic malware used in **spam email campaigns**.