Malware Family Classification & Differentiation

By

Vibhuti Naik

Intern ID: 2046

Malware Family Classification & Differentiation

Introduction

- The modern threat landscape is composed of hundreds of specialized malware families.
- While often grouped under the broad term "malware," these threats differ significantly in their operational goals, infection vectors, and monetization strategies.
- This report provides a framework for differentiating major malware families ranging from high-pressure extortion (Ransomware) to silent resource theft (Cryptojackers).

Malware Families

Below is the list of malware families, strains, and threat actor tools spanning several decades of cybersecurity history categorized based on their use cases.

1. Extortion & Destruction:

These threats focus on locking data, leaking it, or destroying systems entirely.

Category	Description	Examples
Ransomware (Modern/RaaS)	Sophisticated "Big Game Hunting" groups that encrypt and leak data.	LockBit, Conti, REvil, BlackCat, Hive, Cl0p, Akira, Medusa, Play, Royal.
Ransomware (Classic/Historic)	The foundational strains that defined the encryption-for-pay model.	CryptoLocker, WannaCry, Locky, TeslaCrypt, Ryuk, GandCrab, Maze.
Wipers	Malware designed to delete data and make	NotPetya, Shamoon, HermeticWiper,

	systems unbootable (often state-sponsored).	WhisperGate, IsaacWiper, AcidRain.

2. Information & Asset Theft:

These focus on stealthily extracting value, whether through credentials, banking access, or hardware resources.

Category	Description	Examples
Banking Trojans	Intercept financial transactions and steal banking portal credentials.	Zeus, Dridex, TrickBot, Emotet, QakBot, Gozi, IcedID, Carberp.
InfoStealers	Rapidly harvest passwords, cookies, and crypto wallets from browsers.	RedLine, Vidar, Raccoon, Lumma, Stealc, AgentTesla, FormBook.
Cryptojackers	Silently use the victim's CPU/GPU to mine cryptocurrency for the attacker.	XMRig, Coinhive, LemonDuck, Smominru, WannaMine.
Skimmers (MageCart)	Malicious scripts injected into websites to steal credit card data at checkout.	MageCart, WebSkimmer, SilentSkimmer.

3. Access, Control & Persistence:

These tools provide the "bridge" for attackers to enter a network and maintain control**.**

Category	Description	Examples
RATs (Remote Access Trojans)	Provide full remote desktop-like control over a victim's machine.	njRAT, DarkComet, Remcos, AsyncRAT, NanoCore, PoisonIvy.
Loaders & Droppers	Minimalist malware used to "load" heavier payloads like Ransomware later.	SmokeLoader, GootLoader,

		BazarLoader, Bumblebee, Pikabot.
Botnets & Worms	Self-spreading or network-controlled armies of infected devices.	Conficker, Mirai, Necurs, Andromeda, Mozi, StormWorm.
C2 & Offensive Frameworks	Legal/Grey-area security tools used by hackers for network lateral movement.	CobaltStrike, Metasploit, Sliver, BruteRatel, Empire.

4. Specialized & High-Target Threats:

Advanced threats targeting specific platforms or infrastructure.

Category	Description	Examples
APT & ICS Malware	Nation-state tools targeting industrial systems or high-level espionage.	Stuxnet, Triton, BlackEnergy, Sunburst (SolarWinds), Havex, Pegasus.
Mobile Malware	Specifically designed for Android or iOS (Banking overlay attacks/Spying).	FluBot, Anubis, TeaBot, Joker, SpyNote, AhMyth, SharkBot.
Classic Viruses & Filers	Older, "file-infecting" malware that attaches to legitimate programs.	Sality, Virut, Parite, Ramnit.

5. Deception & Fraud:

Lower-level threats that rely on tricking the user or abusing web protocols.

Category	Description	Examples from your list
Adware & Fraud	Hijacks browsers to show ads, click links, or redirect traffic.	Shlayer, Bundlore, Fireball, DNSChanger, ClickFraud.

Scareware / FakeAV	Tricks users into believing their PC is infected to sell fake "cleanup" software.	FakeAV, RogueSecurity, Scareware.

Differentiating Factors

To differentiate such a vast list, here are the five core factors: the malware's Intent (what it wants), Action (how it does it), Spread (how it travels), Stealth (how it hides), and Monetization (how the hacker gets paid).

1. Primary Operational Objective

Category	The "Differentiator"	Examples
Ransomware	**Extortion.** It wants you to know it's there. It encrypts your files and demands money for the key.	LockBit, Conti, REvil
Banking Trojan	**Financial Fraud.** It waits for you to visit a bank site, then injects fake fields to steal logins or 2FA.	Zeus, Dridex, TrickBot
InfoStealer	**Bulk Data Theft.** It performs a "smash and grab" of browser cookies, passwords, and crypto wallets.	RedLine, Lumma, Vidar
Wiper	**Destruction.** Unlike ransomware, there is no key. It simply deletes or overwrites data to cause chaos.	NotPetya, Shamoon
RAT (Remote Access)	**Total Control.** It gives the hacker a "live" window to see your screen and control your mouse.	njRAT, DarkComet
Cryptojacker	**Resource Hijacking.** It stays silent but uses 100% of your CPU to mine Bitcoin/Monero for the hacker.	XMRig, Coinhive

2. How They Interact With the Victim

- **Overt (Loud):** Ransomware is the loudest. It changes your wallpaper and leaves a text file. It *wants* to be noticed so you pay.
- **Covert (Silent):** InfoStealers and Spyware (like **Pegasus**) strive for zero visibility. If you notice them, they have failed.
- **Man-in-the-Browser:** Banking Trojans specifically modify the code of the website *inside* your browser while you are looking at it.

3. Method of Infection (The "Vector")

- **Worms (Self-Propagating):** They move automatically through network holes (like WannaCry or Conficker). No human click is needed.
- **Trojans (Deceptive):** They hide inside "cracks," "free movies," or "fake invoices." They require you to run the file.
- **Loaders/Droppers:** These are "delivery men." They don't steal anything themselves; they just open a back door to download the *actual* malware later.

4. Technical Sophistication & Target

- **Commodity Malware:** Sold on the dark web for $50–$500. Used by low-level "script kiddies" (e.g., AsyncRAT, AgentTesla).
- **APT / Nation-State Tools:** Multi-million dollar codebases built by governments for sabotage (e.g., Stuxnet for nuclear plants, **Trident** for power grids).
- **Mobile Specific:** Threats like FluBot use "Overlay Attacks" on Android to draw a fake screen over your real banking app.

5. The "Business Model"

- **Direct Payment:** Ransomware (Pay the ransom).
- **Account Takeover (ATO):** Banking Trojans (Drain the bank account).
- **Selling Access:** Botnets and Loaders (Hackers sell access to your PC to *other* hackers).

- **Market Sales:** Stealers (The stolen passwords are sold in bulk on "logs" markets).

Comparative Analysis Table

This table separates the most prominent families from your list based on the framework above.

Threat Category	Visibility	Key Action	Differentiating Factor	Examples
Ransomware	Overt	Data Encryption	Demands a ransom; leaves a note; highly disruptive.	LockBit, Conti, REvil, WannaCry
InfoStealers	Covert	Data Exfiltration	"Smash and grab" of browser data/passwords; usually exits quickly.	RedLine, Lumma, Vidar, AgentTesla
Banking Trojans	Covert	Browser Injection	Specifically targets financial URLs; modifies web pages in real-time.	Zeus, Dridex, TrickBot, Emotet
RATs	Covert	Remote Control	Provides a "live" interactive session for the hacker.	njRAT, Remcos, DarkComet
Wipers	Overt	Data Destruction	No decryption key; objective is total system failure/chaos.	NotPetya, Shamoon, HermeticWiper

Loaders	Covert	Software Delivery	Does nothing but download *other* malware; the "gatekeeper."	SmokeLoader, GootLoader, IcedID
Cryptojackers	Covert	CPU Hijacking	Uses hardware to mine crypto; performance degradation is the only sign.	XMRig, Coinhive, LemonDuck
Botnets	Mixed	Task Execution	Connects to a C2 server to perform mass DDoS or Spam attacks.	Mirai, Conficker, Mozi

Technical Deep-Dive: The "Evolutionary" Differences

To understand why the list is so long, we must look at how these families differ technically:

A. Modular vs. Monolithic

- **Modular (e.g., Emotet, TrickBot):** These are "Swiss Army Knives." They can change their function on the fly. Today they are a Banking Trojan; tomorrow they download Ransomware.
- **Monolithic (e.g., Locky, WannaCry):** They have one job (encrypt files). Once they run, their purpose is fulfilled.

B. User-Mode vs. Kernel-Mode

- **User-Mode (e.g., RedLine):** Runs like a normal app. Easier to build, easier for Antivirus to catch.
- **Kernel-Mode/Rootkits (e.g., ZeroAccess, Sality):** Hides deep inside the Operating System. It can "lie" to the Antivirus, saying its files don't exist.

C. File-Based vs. Fileless

- **File-Based (e.g., Zeus):** Leaves a .exe or .dll on the hard drive.
- **Fileless (e.g., PowerGhost, DarkGate):** Lives only in the computer's RAM (Memory). It disappears the moment the computer is restarted, making forensic investigation very difficult.

Conclusion

While the names of malware change weekly (e.g., from *GandCrab* to *REvil* to *BlackCat*), the differentiating factors remain the same. Modern defense requires understanding that a "Virus" is no longer just a program that breaks things—it is a specialized tool in a multi-stage criminal business model.