SECURITY ADVISORY

CYBER STASH

April, 2025

Evasive Malware Trends

Hijack Loader and SHELBY Campaigns

Context

In April 2025, cybersecurity researchers uncovered two advanced threats that highlight the growing sophistication of adversaries: an upgraded Hijack Loader variant and a newly discovered malware family named SHELBY (REF8685). Both demonstrate enhanced capabilities in evading detection, maintaining persistence, and misusing legitimate platforms.

The Hijack Loader—also known as DOILoader, SHADOWLADDER, and GHOSTPULSE—has evolved to include call stack spoofing, direct system calls via Heaven's Gate, and virtualisation-aware execution. These enhancements improve its ability to bypass sandboxes and endpoint protections while serving as a stealthy delivery mechanism for second-stage payloads such as Cobalt Strike.

Meanwhile, SHELBY exploits GitHub for Command-and-Control (C2) communications—a tactic designed to blend into legitimate network traffic. It uses a multi-stage chain with DLL side-loading and sandbox evasion to complicate detection and analysis.

These threats reinforce the need for organisations to strengthen their detection strategies against stealthy loaders, abuse of legitimate services, and evasive malware behaviours.

Mitigation

Defending against the evasive attacks that operate in-memory requires proactive measures:

Conduct periodic compromise assessments to detect fileless and in-memory attacks that evade traditional security controls.

Deploy adversary behaviour detection to identify Living-off-the-Land (LotL) tactics and other stealthy threat activity.

Enforce least-privilege access and monitor for abnormal process injections or direct system calls to reduce attack surfaces.

Reduce exposure to high-risk infrastructure by restricting network connections to and from high-risk Autonomous System Numbers (ASNs), geographic regions, and top-level domains (TLDs) frequently associated with malicious activity.

Technical Details

Hijack Loader (aka SHADOWLADDER / GHOSTPULSE / DOILoader)

The upgraded Hijack Loader in 2025 demonstrates a modular architecture and a variety of stealth-focused capabilities intended to avoid sandbox detection, bypass endpoint defenses, and persist on victim systems.

Core Functional Enhancements:

- **Modular Loader Framework:** The loader is designed as a modular malware framework. Modules are dynamically injected or loaded during execution, enabling adversaries to adjust functionality based on target environment.

- **Call Stack Spoofing (MITRE T1036):** Hijack Loader forges return addresses and stack frames during execution, masking the true origin of API/system calls. This technique disrupts stack-based detection heuristics used by EDR/XDR products and frustrates memory-based analysis tools like Sysmon or ETW telemetry.

- **Heaven's Gate Exploitation (MITRE T1055.012):** Executes 64-bit shellcode within a 32-bit process using Heaven's Gate — a known x64 technique that leverages the 0x33 segment selector. This allows malware to switch into 64-bit mode, bypassing hooks placed on 32-bit ntdll.dll functions by endpoint agents.

- **Direct Syscall Execution (MITRE T1106):** Hijack Loader directly invokes system calls without going through Windows APIs by resolving syscall numbers dynamically from the ntdll.dll export table. This undermines user-mode hooking and aids stealthy memory manipulation (e.g., VirtualAlloc, NtCreateThreadEx).

    1. Anti-Virtualization & Sandbox Evasion (MITRE T1497.001 / T1497.003): Performs checks for:
    2. MAC addresses associated with VM vendors (e.g., VMWare, VirtualBox)
    3. System uptime and CPU core count
    4. Artifacts like mouse movement or user interaction If a virtualized/sandbox environment is detected, execution is halted or alternate code paths are triggered.

- **Persistence via Scheduled Tasks (MITRE T1053.005):** A specific module (modTask) establishes persistence by registering a Windows Scheduled Task with obfuscated names and paths, enabling re-execution on reboot or time-triggered intervals.

SHELBY Malware (REF8685)

SHELBY is a newly emerged malware family discovered leveraging GitHub as a covert C2 channel. Its design focuses on stealth, sandbox awareness, and abuse of legitimate infrastructure.

Execution Chain Overview:

- **Multi-Stage Infection:** The infection chain begins with a benign-looking .NET executable that side-loads a malicious DLL named HTTPS-ervice.dll, using DLL search order hijacking (T1574.002). This method exploits trusted binaries to load unsigned payloads from attacker-controlled directories.
- **Sandbox Detection (MITRE T1497):** The payload includes anti-analysis routines that:
    1. Detect hardware acceleration (GPU, RAM size)
    2. Check for common sandbox tools and processes
    3. Monitor for human-like input delays This enables it to either evade or delay execution in automated analysis environments.
- **GitHub-Based Command and Control (MITRE T1071.001 / T1573.002):**
    1. Connects to attacker-controlled GitHub repositories over HTTPS (legitimate SSL).
    2. Retrieves encrypted payloads (often base64-encoded blobs or JSON-structured C2 commands).
    3. Sends back system telemetry using push mechanisms or encoded commit messages. This use of GitHub evades network-level detection, as GitHub traffic is rarely blocked in enterprise environments.
- **DLL Functionality (HTTPService.dll):** The side-loaded DLL is responsible for:
    1. Establishing persistence by modifying the registry or installing scheduled tasks
    2. System reconnaissance (OS version, domain membership, AV product info)
    3. Downloading and executing follow-up payloads (e.g., Cobalt Strike beacon or infostealers)
    4. Encrypted communication with the C2 server

Common Traits Across Both Campaigns

The following 3 adversary techniques have been observed in relation to these campaigns:

1. **Obfuscation and Code Protection (MITRE T1027):** Both Hijack Loader and SHELBY use packed or obfuscated payloads. The .NET stubs are frequently protected with .NET Reactor, complicating reverse engineering through control flow obfuscation and anti-decompiler stubs.
2. **Data Exfiltration via Covert Channels:** By abusing platforms like GitHub, threat actors hide in plain sight. This avoids detection by traditional IDS/IPS and DNS tunnelling detection tools, which may not flag HTTPS traffic to trusted domains.
3. **Fileless Techniques & In-Memory Execution (MITRE T1055 / T1105):** Payloads are frequently decrypted and injected directly into memory using reflective PE loading or manual mapping, leaving minimal disk artifacts behind.

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to these two campaigns:

Tactic	Technique	Technique ID	Details
Initial Access	Phishing: Spear phishing Attachment	T1566.001	Malicious documents or executables sent via email to gain initial access.
Execution	DLL Side-Loading	T1574.002	The SHELBY malware uses a benign .NET binary to side-load a malicious HTTPService.dll.
	Command and Scripting Interpreter: PowerShell	T1059.001	Likely used in payload execution and environment manipulation.
Persistence	Scheduled Task/Job: Scheduled Task	T1053.005	Hijack Loader's modTask module creates scheduled tasks for persistence.
Defence Evasion	Virtualization/Sandbox Evasion	T1497	Both Hijack Loader and SHELBY implement checks to detect VM or sandbox environments.
	Indicator Removal on Host	T1070	Techniques like stack spoofing make it harder to trace malicious activity.
	Process Injection	T1055	Hijack Loader uses Heaven's Gate technique to inject code into remote processes.
	Obfuscated Files or Information	T1027	Use of obfuscation in the payload and .NET Reactor for protection.
Command and Control	Application Layer Protocol: Web Protocols	T1071.001	Communication over HTTPS with GitHub as a covert C2 channel.
	Encrypted Channel	T1573.002	Encrypted payloads and instructions are stored in GitHub repositories.

Cyber Threat Intelligence

The emergence of the enhanced Hijack Loader and the newly identified SHELBY malware marks a notable escalation in the sophistication of modern cyber threat actors. Hijack Loader—active since 2023 and also known as DOILoader, SHADOWLADDER, and GHOSTPULSE—has evolved from a basic dropper into a modular, evasive malware delivery framework. Frequently used in initial access campaigns by financially motivated actors and Malware-as-a-Service (MaaS) affiliates, it delivers second-stage payloads such as Cobalt Strike, IcedID, and SystemBC. Typically propagated via phishing, malvertising, or compromised websites, it targets sectors including finance, healthcare, legal, and government.

Recent enhancements—such as call stack spoofing, direct system calls, and anti-virtualisation logic—highlight its growing ability to evade advanced endpoint detection and response solutions.

In parallel, SHELBY (REF8685) is a novel malware family leveraging GitHub as its command-and-control (C2) platform. By embedding encrypted payloads and instructions within HTTPS traffic to a trusted domain, it bypasses traditional perimeter defences. Its use of DLL side-loading, scheduled task persistence, and .NET Reactor obfuscation indicates a high level of adversary sophistication, likely tied to a financially motivated group exploiting cloud infrastructure and secure coding practices.

Together, these campaigns exemplify the professionalisation of cybercrime and underscore the urgent need for adaptive, intelligence-driven defence strategies to counter stealthy, infrastructure-abusing threats.

Geopolitical Context and Strategic Implications

The rise of Hijack Loader and SHELBY reflects a broader shift in the cyber threat landscape, where financially motivated groups increasingly adopt techniques once reserved for state-aligned actors. Their ability to bypass controls using legitimate platforms like GitHub aligns with tactics seen in regions where cybercrime enforcement is weak or politically constrained.

Targeted activity against critical sectors—including finance, legal, and government—correlates with global economic instability and the growing role of cyber mercenaries. As nation-states continue to develop offensive cyber programs, advanced tradecraft is cascading into the criminal underground via Malware-as-a-Service ecosystems.

In this environment, organisations must move beyond technical controls and incorporate geopolitical risk into cyber defence strategies. Understanding adversary motivations, regional affiliations, and evolving tactics is essential for informed investment in threat detection, incident response, and supply chain resilience.

References

Indicators of Compromise (IOCs)

HASHES (SHA256)

7bd39678ac3452bf55359b44c5192b79412ce61a82cd72eef88f91aba5792ee6	6b1621bded06b082f83c731319c9deb2fdf751a4cec1d1b2b00ab9e75f4c29ca
e67790b394f5238908fcc326a9db940b200d9b50cbb45f0bfa94038db50beeae	693cace37b4b6fed2ca67906c7a4b1c11273110561a207a222aa4e62fb4a184a
04c0a4f3b5f787a0c9fa8f6d8ef19e01097185dd1f2ba40ae4bbbeca9c3a1c72	67173036149718a3a06847d20d0f30616e5b9d6796e050dc520259a15588ddc8
7b399ccced1048d15198aeb67d6bcc49ebd88c7ac484811a7000b9e79a5aac90	6cfbffa4e0327969aeb955921333f5a635a9b2103e05989b80bb690f376e4404
b2b5c6a6a3e050dfe2aa13db6f9b02ce578dd224926f270ea0a433195ac1ba26	d75d545269b0393bed9fd28340ff42cc51d5a1bd7d5d43694dac28f6ca61df03
9218c8607323d7667f69ef26faea57cb861f9b3888a457ed9093c1b65eefa42b	b8f1341ade1fe50c4936b8f7bec7a8e47ad753465f716a1ec2f8220a18bf34a5
35dca05612aede9c1db55a868b1cd314b5d05bac00bed577fd0d437103c2a4a4	08f1ca6071cb206f53c2e81568b73d4bee7ac6a019d93d3ceaac7637b6dc891a
B480fec95b84980e88e0e5958873b7194029ffbaa78369cfe5c0e4d64849fb32	

URLs

- hxxps://www.4sync[.]com/web/directDownload/KFtZysVO/4jBKM7R0.baa89a7b43a7b73227f22ae561718f7f
- hxxps://geupdate-service[.]bond/img/3344379399.png

Public Intelligence:

- https://cyberpress.org/shelby-malware-uses-github-for-c2/?amp=1
- https://www.elastic.co/security-labs/the-shelby-strategy
- https://thehackernews.com/2025/04/new-malware-loaders-use-call-stack.html
- https://securitybrief.com.au/story/how-new-malware-shelby-targets-telecom-via-phishing
- https://malpedia.caad.fkie.fraunhofer.de/details/win.hijackloader