BLACKSWAN CYBERSECURITY

# THREAT ADVISORY

## Venom Info Stealer MaaS

**April 1, 2026**

**Threat Level:** High (active MaaS with ongoing development and real-time credential theft capability)
**Target Platform:** Windows (primary payload); operators can manage from Windows or macOS

## Executive Summary

Venom Stealer is a newly emerged **Malware-as-a-Service (MaaS)** infostealer sold via Telegram under the handle "VenomStealer". It is licensed at $250 per month or $1,800 lifetime (including updates) and includes an affiliate program. Unlike traditional one-shot stealers, Venom Stealer emphasizes **persistence and automation**, most notably a background "session listener" that enables **continuous credential harvesting**—phoning home approximately twice daily with newly saved passwords and wallet activity. This defeats password-rotation defenses commonly used in incident response or corporate policies.

Additional advanced features include silent bypass of Chrome v10/v20 password encryption (no UAC prompt or forensic artifacts), server-side GPU-assisted cracking of stolen crypto wallets, and automated fund sweeping across multiple blockchain networks. Delivery relies on ClickFix-style social-engineering lures. The malware was first publicly detailed in late March 2026 updates.

## Key Capabilities

- **Credential & Data Theft**: Extracts saved passwords, session cookies, browsing history, autofill data, and browser extension inventories from all profiles in Chromium-based browsers (Chrome, Edge, Brave, Opera) and Firefox.
- **Crypto Wallet Theft**: Targets vaults from MetaMask, Phantom, Solflare, Trust Wallet, Atomic, Exodus, Electrum, Bitcoin Core, Monero, and Tonkeeper (newly added). Server-side GPU cracking recovers seed phrases/addresses; an auto-transfer engine then sweeps funds (ERC-20, SPL tokens, liquid staking, DeFi positions) across nine chains.
- **Continuous Harvesting**: Persistent session listener monitors browser activity in real time and exfiltrates new credentials/wallet data bi-daily.
- **System Profiling**: Captures full system fingerprint, desktop screenshot, and filesystem search for seed phrases.
- **Evasion & Exfiltration**: Immediate HTTP POST exfiltration with minimal local staging; silent privilege escalation; anti-VM/debugger checks; direct syscalls; process enumeration; sleep delays.

## Infection Vectors

- Sophisticated **ClickFix** social-engineering templates:
  - Fake Cloudflare CAPTCHA
  - Fake OS update / SSL certificate error
  - Fake font install page

- Victims are tricked into opening the Run dialog (Windows) or Terminal (macOS), pasting a command (e.g., PowerShell -w h or curl/bash), and pressing Enter.
- Payload installation is fully automated after command execution.
- Example campaign: Fake Avast virus-scan sites delivering Avast_system_cleaner.exe.

## Tactics, Techniques, and Procedures (TTPs)

**MITRE ATT&CK mappings (partial, based on observed behavior):**

- **Initial Access (TA0001)**: T1204.001 – User Execution (ClickFix social engineering)
- **Execution (TA0002)**: T1059.001 – PowerShell; T1059.004 – Unix Shell
- **Privilege Escalation (TA0004)**: T1548.002 – UAC Bypass (CMSTPLUA COM interface for silent Chrome decryption key extraction)
- **Credential Access (TA0006)**: T1555.003 – Web Browser (passwords/cookies/autofill); T1539 – Steal Web Session Cookie; T1552.001 – Credentials In Files
- **Collection (TA0009)**: T1005 – Data from Local System; desktop screenshots
- **Command and Control (TA0011)**: Custom Cloudflare domains; periodic heartbeat and upload
- **Exfiltration (TA0010)**: T1041 – Exfiltration Over C2 Channel (immediate HTTP POST, no staging)
- **Impact (TA0040)**: T1657 – Financial Theft (automated wallet cracking + sweeping)
- **Defense Evasion (TA0005)**: T1036 – Masquerading (e.g., v20svc.exe in Chrome Application folder); anti-analysis (VM detection, direct syscalls)

**Persistence**: Background session listener; masquerades as legitimate Chrome service (v20svc.exe --v20c flag). Marker files and session data stored in C:\Users\Public\NTUSER.dat and %APPDATA%\Microsoft\fd1cd7a3\sess.

## Indicators of Compromise (IOCs)

Specific IOCs are **not disclosed** in the primary research (payloads are compiled per-operator). The following are observed from related public reporting on an active fake-Avast campaign:

**File Hashes**

- SHA-256: ecbeaa13921dbad8028d29534c3878503f45a82a09cf27857fa4335bd1c9286d
- MD5: 0a32d6abea15f3bfe2a74763ba6c4ef5

**File Names / Paths**

- **Dropper**: Avast_system_cleaner.exe (example)
- **Payload**: v20svc.exe (dropped to C:\Program Files\Google\Chrome\Application\)
- **Screenshot**: %TEMP%\screenshot_*.jpg
- **Session marker**: %APPDATA%\Microsoft\fd1cd7a3\sess
- **Additional marker**: C:\Users\Public\NTUSER.dat

**Network / C2**

- **Domain**: app-metrics-cdn[.]com (Cloudflare-hosted; IP: 104.21.14.89)

- **C2 Endpoints**:
  - /api/upload
  - /api/upload-json
  - /api/upload-complete
  - /api/listener/heartbeat
- **MaaS-related panel/distribution (observed in ThreatFox)**: https://venom-stealer.com/m/7d8df27d95d9**Note**: Operators can configure their own custom Cloudflare domains, so C2 infrastructure varies.

## Detection & Mitigation Recommendations

1. **User Awareness**: Train employees to never paste commands from web prompts into Run/Terminal (ClickFix hallmark).
2. **Technical Controls**:
   - Restrict PowerShell execution for standard users.
   - Disable Run dialog (via Group Policy) for non-admin accounts where feasible.
   - Application allow-listing / WDAC to block unsigned executables in Chrome Application folder.
   - Monitor browser processes for anomalous access to Login Data files.
3. **Endpoint Detection**:
   - Look for creation of v20svc.exe, %TEMP%\screenshot_*.jpg, or fd1cd7a3\sess.
   - Detect UAC-bypass patterns (CMSTPLUA COM usage).
4. **Network Monitoring**:
   - Alert on HTTP POSTs to suspicious “analytics-like” domains or unknown Cloudflare subdomains with multipart/form-data.
   - Block known IOC domains/IPs and monitor for similar patterns.
5. **Credential Hygiene**:
   - Use password managers that do not store credentials locally in browser vaults when possible.
   - Enable 2FA / hardware keys; monitor accounts for post-breach activity (continuous harvesting means rotation alone may not suffice).
6. **Response**:
   - If infection suspected, isolate system immediately, reset all credentials, and scan for the listed file artifacts.

Venom Stealer represents a significant evolution in infostealer capabilities by shifting from opportunistic one-time theft to persistent, real-time credential and crypto drainage. Organizations should prioritize ClickFix awareness and browser-data-access monitoring.

**Contact Blackswan Cybersecurity at 855-BLK-SWAN or Contact@Blackswancybersecurity.com**