INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-01 18:41 UTC

Venom Stealer MaaS Platform Puts ClickFix Campaigns Within Reach of Low-Skill Threat Actors

THREAT CAMPAIGN | HIGH | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0137
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Not specified, ClickFix-based attacks target end users across browser and OS environments; no single product CVE identified
Published	2026-04-01T10:54:23
Discovery Source	Rss

Executive Summary

Venom Stealer is a Malware-as-a-Service platform that packages ClickFix social engineering attacks into a point-and-deploy toolkit, enabling low-skill attackers to run credential-theft campaigns at scale. The platform lowers the barrier to entry significantly: buyers do not need technical expertise to steal employee credentials, browser-stored passwords, or session tokens. Organizations face elevated risk of account compromise, data exfiltration, and downstream access abuse, particularly where phishing awareness training and endpoint controls are underdeveloped.

Technical Analysis

Venom Stealer automates ClickFix-based lure delivery, a social engineering technique that presents users with fake CAPTCHA or error dialogs and instructs them to manually paste and execute a PowerShell or shell command. The clipboard is pre-loaded with a malicious payload via JavaScript; the user completes execution themselves, bypassing many automated endpoint controls (CWE-693: Protection Mechanism Bypass). Once executed, the payload installs an information stealer targeting browser-stored credentials and cookies (CWE-522: Insufficiently Protected Credentials; T1555.003, T1539), with keylogging capability (T1056.001) and persistence via run-key or startup modification (T1547). Payload delivery uses PowerShell (T1059.001), phishing lures including spearphishing links (T1566.002), and ingress tool transfer (T1105). Lure infrastructure may exploit open redirects to increase link credibility (CWE-601; T1583.006). No CVE is associated with this campaign-class threat. No CISA KEV entry exists as of the configuration date. Threat actor attribution is

unknown; the MaaS model means buyer profiles are broad and uncharacterized. Primary source is Dark Reading (T3/secondary tier). No CISA, NVD, or MITRE ATT&CK advisory for Venom Stealer exists as of 2026-03-04. All technical details are derived from secondary reporting and should be treated as directionally accurate pending primary-source confirmation or independent threat intelligence corroboration.

Action Checklist

1. Containment: Block PowerShell execution initiated from browser processes (chrome.exe, msedge.exe, firefox.exe) using application control or EDR policy. Disable clipboard-to-execution pathways where feasible via Group Policy or endpoint agent rules. Flag and quarantine endpoints where unexpected PowerShell parent-child process chains are observed.
2. Detection: Hunt for PowerShell execution where parent process is a browser or document viewer (T1059.001, T1204.002). Search EDR/SIEM logs for: encoded PowerShell commands (-EncodedCommand, -enc), IEX or Invoke-Expression in command-line arguments, and unusual child processes spawned from browser executables. Review proxy and DNS logs for connections to newly registered or low-reputation domains following user web activity. Check for new persistence entries in HKCU\Software\Microsoft\Windows\CurrentVersion\Run or Startup folder modifications (T1547).
3. Eradication: Remove identified stealer payloads and persistence artifacts. Rotate all credentials that may have been exposed on affected endpoints, prioritizing browser-stored passwords, SSO session tokens, and VPN credentials. Revoke active sessions for affected user accounts across SaaS and identity platforms. Re-image endpoints where stealer execution is confirmed rather than attempting manual remediation.
4. Recovery: Verify credential rotation is complete and no residual persistence entries remain. Monitor authentication logs for anomalous access attempts using previously valid credentials for 30 days post-incident. Confirm endpoint agent telemetry is intact and not tampered with before returning systems to production.
5. Post-Incident: Ensure phishing awareness training includes ClickFix-style lures (fake CAPTCHA/error dialogs with copy-paste command instructions), which differ from traditional hyperlink phishing and require specific detection and reporting guidance. Review browser policy configurations to restrict clipboard API abuse and disable execution of clipboard-pasted commands where operationally feasible. Evaluate whether PowerShell Constrained Language Mode or WDAC/AppLocker policies would reduce exposure for non-developer user populations. Document the detection gap and update SOC playbooks to include ClickFix social engineering as a distinct attack pattern.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if credential exfiltration is confirmed for accounts with access to PII, PHI, or financial data — triggering breach notification obligations under HIPAA, state data breach laws, or PCI DSS §12.10.4 — or if stolen SSO/VPN credentials show evidence of successful reuse against downstream enterprise systems indicating active lateral movement beyond the initial endpoint.

Recovery Notes	Credential rotation alone is insufficient for Venom Stealer incidents — all browser-stored passwords and SSO session tokens accessible at time of stealer execution must be treated as fully compromised and rotated, not just accounts with confirmed exfiltration evidence, because the stealer harvests credential stores en masse. Monitor identity provider and VPN authentication logs for 30 days specifically for the previously valid credentials, as Venom Stealer operators running MaaS campaigns may sell stolen credential sets to secondary buyers who attempt replay attacks days or weeks after initial theft. Before returning any affected endpoint to production, verify PowerShell Constrained Language Mode or WDAC policy is active and confirm Sysmon telemetry is reporting cleanly, as returning an inadequately hardened endpoint creates immediate re-infection risk from the same ClickFix delivery mechanism.
Forensic Artifacts	PowerShell Script Block Logging (Microsoft-Windows-PowerShell/Operational Event ID 4104): captures the fully decoded Venom Stealer dropper payload pasted from clipboard via the ClickFix lure, even when the command was delivered base64-encoded via -EncodedCommand — primary artifact for IOC extraction | Browser credential store databases: Chrome Login Data (C:\Users\\AppData\Local\Google\Chrome\User Data\Default\Login Data), Edge equivalent, and Firefox logins.json + key4.db — these SQLite/JSON files record which stored passwords were accessible to the stealer process at execution time and establish breach notification scope | Windows Clipboard History store (C:\Users\\AppData\Local\Microsoft\Windows\Clipboard*): may preserve the exact ClickFix lure command the user was socially engineered to paste, providing the full kill-chain entry point artifact if clipboard history was enabled on the endpoint | HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry hive and C:\Users\\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\ directory: Venom Stealer MaaS payloads typically write persistence to per-user Run keys or Startup folders to survive reboot without requiring elevated privileges, consistent with low-skill operator deployment | Network proxy and DNS resolver logs filtered for outbound POST requests to newly registered domains (WHOIS age under 30 days) occurring within 60 seconds of PowerShell execution: Venom Stealer exfiltrates harvested credentials and session tokens over HTTPS to attacker-controlled C2 infrastructure, and the timing correlation to the ClickFix execution event is the primary network-layer indicator

Per-Action IR Details

Containment — Block PowerShell execution initiated from browser processes (chrome.exe, msedge.exe, firefox.exe) using application control or EDR policy. Disable clipboard-to-execution pathways where feasible via Group Policy or endpoint agent rules. Flag and quarantine endpoints where unexpected PowerShell parent-child process chains are observed.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and prevent further spread while preserving evidence

Controls: NIST IR-4 (Incident Handling), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality) — restrict browser processes from spawning interpreted execution environments, CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 2.3 (Address Unauthorized Software)

Compensating: Without EDR, deploy Sysmon with SwiftOnSecurity config and enable Event ID 1 (Process Create) filtering for powershell.exe or pwsh.exe where ParentImage contains chrome.exe, msedge.exe, or firefox.exe. Use the following PowerShell one-liner to audit current process-parent relationships in real time: Get-WmiObject Win32_Process | Where-Object { $_.Name -eq 'powershell.exe' } | Select-Object ProcessId, ParentProcessId, CommandLine. Block clipboard-to-execution via GPO: Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell — enable 'Turn on PowerShell Script Block Logging' and separately push a

Software Restriction Policy or WDAC deny rule for powershell.exe launched by browser process tokens.

Evidence: Before quarantining the endpoint, capture: (1) Sysmon Event ID 1 logs showing powershell.exe with ParentImage path of chrome.exe/msedge.exe/firefox.exe and full CommandLine including any -EncodedCommand or IEX strings specific to the Venom Stealer dropper; (2) Windows Event Log Security Event ID 4688 (Process Creation with command-line auditing enabled) from the Microsoft-Windows-Security-Auditing provider; (3) Clipboard content snapshot if the endpoint has clipboard history enabled (C:\Users\\AppData\Local\Microsoft\Windows\Clipboard*) which may contain the ClickFix lure payload the user was instructed to paste; (4) Browser process memory dump (procdump.exe -ma chrome.exe) to recover injected or in-memory PowerShell stager strings before process termination.

Detection — Hunt for PowerShell execution where parent process is a browser or document viewer (T1059.001, T1204.002). Search EDR/SIEM logs for: encoded PowerShell commands (-EncodedCommand, -enc), IEX or Invoke-Expression in command-line arguments, and unusual child processes spawned from browser executables. Review proxy and DNS logs for connections to newly registered or low-reputation domains following user web activity. Check for new persistence entries in HKCU\Software\Microsoft\Windows\CurrentVersion\Run or Startup folder modifications (T1547).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across log sources to confirm adversary presence and scope of Venom Stealer deployment

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without SIEM, use Chainsaw (free, by WithSecure) against collected Windows Event Log .evtx files to run Sigma rule matches: chainsaw hunt C:\Windows\System32\winevt\Logs\ --sigma sigma_rules\ --mapping mappings\sigma-event-logs-all.yml targeting rules for T1059.001 and T1547.001. For DNS hunting without a SIEM, export DNS debug logs from the Windows DNS client (netsh trace start capture=yes) or query the local DNS cache with ipconfig /displaydns and grep for domains registered within the last 30 days using a free VirusTotal API lookup script. For registry persistence, run: reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run and compare output against a clean baseline using fc.exe or a PowerShell diff on exported .reg files.

Evidence: Collect before analysis is complete: (1) Full PowerShell Script Block Logging output from Microsoft-Windows-PowerShell/Operational (Event ID 4104) which will contain the decoded Venom Stealer payload commands even when -EncodedCommand was used at invocation; (2) Browser proxy or network logs filtered for POST requests to low-reputation or newly registered domains within 5 minutes of the ClickFix lure page visit — Venom Stealer exfiltrates credentials over HTTP/S to attacker-controlled C2 infrastructure; (3) Windows Prefetch files (C:\Windows\Prefetch\POWERSHELL.EXE-*.pf) recording execution timestamps for PowerShell correlating to the suspected lure event; (4) HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry hive export capturing any Run key persistence written by the stealer installer; (5) Browser credential database files (Chrome: C:\Users\\AppData\Local\Google\Chrome\User Data\Default\Login Data; Edge: equivalent path) to confirm whether the stealer accessed or copied these SQLite databases.

Eradication — Remove identified stealer payloads and persistence artifacts. Rotate all credentials that may have been exposed on affected endpoints, prioritizing browser-stored passwords, SSO session tokens, and VPN credentials. Revoke active sessions for affected user accounts across SaaS and identity platforms. Re-image endpoints where stealer execution is confirmed rather than attempting manual remediation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: eliminate all components of the Venom Stealer MaaS payload from affected systems and invalidate all credentials accessible to the stealer at time of execution

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management) — disable and re-provision compromised accounts, NIST IA-5 (Authenticator Management) — rotate all exposed authenticators, CIS 5.3 (Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without enterprise identity platforms, use Microsoft's free Entra ID (formerly AAD) sign-in logs via the Azure Portal to revoke all refresh tokens for affected users: Revoke-AzureADUserAllRefreshToken -ObjectId via AzureAD PowerShell module. For on-prem AD, force password reset and invalidate Kerberos TGTs with: Get-ADUser | Set-ADUser -ChangePasswordAtLogon $true followed by running nltest /SC_RESET to flush cached credentials. Use Autoruns (Sysinternals, free) to enumerate and remove persistence entries written to Run keys, Startup folders, scheduled tasks, and WMI subscriptions on affected hosts before re-imaging is confirmed. Retain a forensic disk image using FTK Imager (free) before wiping to preserve evidence chain.

Evidence: Before re-imaging, preserve: (1) Full disk image or at minimum a forensic copy of C:\Users\\AppData\Local\Google\Chrome\User Data\Default\Login Data and equivalent paths for Edge and Firefox (logins.json, key4.db) to document which credential stores were accessible to the stealer at time of execution; (2) Windows Security Event ID 4624 (Logon) and 4648 (Explicit Credential Use) logs from the affected endpoint covering the 24 hours post-execution showing any lateral movement attempts using stolen credentials; (3) Memory dump of any running PowerShell or cmd.exe child processes spawned by the browser before termination — Venom Stealer stages may reside entirely in memory; (4) Network capture (Wireshark) of outbound traffic at time of execution to document C2 destination IPs and exfiltration endpoints used by this specific Venom Stealer campaign instance.

Recovery — Verify credential rotation is complete and no residual persistence entries remain. Monitor authentication logs for anomalous access attempts using previously valid credentials for 30 days post-incident. Confirm endpoint agent telemetry is intact and not tampered with before returning systems to production.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operation only after confirming eradication is complete and implementing monitoring for reuse of stolen credentials

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-9 (Protection of Audit Information) — verify telemetry integrity was not tampered with by stealer, NIST SI-7 (Software, Firmware, and Information Integrity), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

Compensating: Without enterprise SIEM for 30-day credential monitoring, configure Windows Event Forwarding (WEF, free, built-in) to centralize Security Event ID 4625 (Failed Logon) and 4648 (Explicit Credential Logon) from all domain controllers to a Windows Event Collector server, then use a scheduled PowerShell script to alert on accounts flagged during the incident attempting logons from new source IPs or outside business hours. Verify Autoruns output on rebuilt endpoints matches a known-good baseline captured from a clean reference image. For telemetry integrity, use Sysmon Event ID 255 (error) monitoring to detect agent tampering and confirm Sysmon service status with: Get-Service -Name Sysmon64.

Evidence: Before returning to production, document: (1) Autoruns export from the recovered endpoint confirming no residual Run key, scheduled task, or WMI subscription entries matching Venom Stealer persistence patterns (compare against pre-incident baseline if available); (2) Entra ID or AD audit logs confirming successful password resets and session revocations for all affected accounts, with timestamps; (3) Authentication logs from VPN gateway and SaaS identity provider showing no successful logins using the previously compromised credentials after rotation, confirming stolen tokens are not being replayed by the attacker against external services.

Post-Incident — Assess phishing awareness training coverage for ClickFix-style lures, which differ from traditional link-click phishing and require specific user education. Review browser policy configurations to restrict clipboard API abuse and disable execution of clipboard-pasted commands where operationally feasible. Evaluate whether PowerShell Constrained Language Mode or WDAC/AppLocker policies would reduce exposure for non-developer user populations. Document the detection gap and update SOC playbooks to include ClickFix social engineering as a distinct attack pattern.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review specific to ClickFix delivery mechanism and update detection, training, and hardening controls to prevent Venom Stealer MaaS reuse

Controls: NIST IR-4 (Incident Handling) — update capability based on lessons learned, NIST IR-2 (Incident Response Training) — add ClickFix-specific social engineering scenarios, NIST IR-8 (Incident Response Plan) — revise playbook to include ClickFix as distinct pattern, NIST SI-2 (Flaw Remediation) — address configuration gaps in browser and PowerShell policy, CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without a security awareness platform, develop a targeted 5-minute internal briefing specifically demonstrating the ClickFix lure pattern (fake CAPTCHA or browser error page instructing users to open Run dialog and paste a command) — this is mechanically distinct from link-click phishing and existing training materials almost certainly do not cover it. Enforce PowerShell Constrained Language Mode via GPO for all non-developer OUs at no cost: set __PSLockdownPolicy registry value to 4 under HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment. Publish free Sigma rules for ClickFix browser-spawned PowerShell patterns to your Chainsaw or Hayabusa local hunting workflow so the SOC can detect recurrence without a SIEM.

Evidence: For the post-incident review, compile: (1) Timeline of the ClickFix lure delivery — browser history (C:\Users\\AppData\Local\Google\Chrome\User Data\Default\History SQLite database) identifying the specific URL that served the fake CAPTCHA or error page used in this campaign; (2) PowerShell Script Block Log (Event ID 4104) entries showing the exact clipboard-pasted command executed by the victim, preserving the full decoded Venom Stealer dropper command for IOC extraction and Sigma rule development; (3) Any network proxy or DNS logs showing the C2 domains contacted by this specific campaign instance, to be submitted to CISA's AIS program or shared via ISAC if your sector participates.

Detection Guidance

Primary behavioral indicator: PowerShell or cmd.exe spawned as a child of a browser process, or with encoded/obfuscated command-line arguments containing IEX, Invoke-Expression, DownloadString, or -EncodedCommand. Secondary indicator: clipboard content containing PowerShell syntax immediately before a Run dialog or terminal open event. SIEM query focus areas: (1) process creation events where ParentImage matches browser executables and ChildImage is powershell.exe or cmd.exe; (2) command-line telemetry containing Base64 strings longer than 100 characters passed to PowerShell; (3) new autorun registry keys or scheduled tasks created within minutes of a browser session. Network indicators: outbound connections to newly registered domains or domains with low Alexa/popularity rank shortly after user web activity; DNS queries for domains using dynamic DNS providers. No confirmed IOCs for Venom Stealer infrastructure were available from primary sources as of the configuration date. Organizations without access to Venom-specific IOCs should focus on behavioral hunting: monitor for browser-to-PowerShell process chains, clipboard API abuse, and newly registered domain callbacks during user web sessions. Consider subscribing to dark web intelligence feeds or managed threat intelligence services that track MaaS platform infrastructure for updated IOCs. Source for detection logic: MITRE ATT&CK T1059.001, T1204.002, T1547, T1105.

Indicators of Compromise

Type	Value	Context	Confidence
TECHNIQUE	`PowerShell child of browser process`	ClickFix execution chain — user pastes clipboard payload into Run dialog or terminal; browser spawns PowerShell (T1059.001, T1204.002)	HIGH

Type	Value	Context	Confidence
TECHNIQUE	`Encoded PowerShell command-line arguments`	Stealer payload delivery commonly uses Base64-encoded commands to evade signature detection	HIGH
TECHNIQUE	`New HKCU Run key or Startup folder entry post-infection`	Persistence mechanism (T1547) — look for entries created within the session window of suspicious PowerShell execution	MEDIUM
TECHNIQUE	`Outbound connection to low-reputation domain following browser activity`	C2 or payload staging (T1105, T1583.006) — correlate with proxy/DNS logs near time of clipboard execution	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1555** — Credentials from Password Stores
- **T1539** — Steal Web Session Cookie
- **T1056.001** — Keylogging
- **T1059.001** — PowerShell
- **T1566** — Phishing
- **T1547** — Boot or Logon Autostart Execution
- **T1583.006** — Web Services
- **T1204.002** — Malicious File
- **T1105** — Ingress Tool Transfer
- **T1555.003** — Credentials from Web Browsers
- **T1566.002** — Spearphishing Link

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **IA-5** — Authenticator Management

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1555	Credentials from Password Stores	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1056.001	Keylogging	Collection
T1059.001	PowerShell	Execution
T1566	Phishing	Initial-Access
T1547	Boot or Logon Autostart Execution	Persistence
T1583.006	Web Services	Resource-Development
T1204.002	Malicious File	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1555.003	Credentials from Web Browsers	Credential-Access
T1566.002	Spearphishing Link	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/endpoint-security/venom-stealer-maas-co...	T3
K24823443: Apache Commons Text vulnerability CVE-2022-42889	https://my.f5.com/manage/s/article/K24823443	T3
The vulnerability CVE 2022-42889 older commons-text- jar files ...	https://knowledge.informatica.com/s/article/000206280?language=en_US	T3
Security Notice: Apache commons-text vulnerability (CVE-2022 ...	https://support.xmatters.com/hc/en-us/articles/13843436346139-Secur...	T3
Critical vulnerability surfaces in Apache Commons Text library	https://www.cybersecuritydive.com/news/critical-vulnerability-apach...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-01 18:41 UTC by TJS Security Command Center