INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-01 13:28 UTC

Venom Stealer MaaS Platform Automates Continuous Credential Harvesting via ClickFix and Fake AV Sites

THREAT CAMPAIGN | **HIGH** | CVSS 7.8

SCC Item ID	SCC-CAM-2026-0134
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.8
Affected Products	Windows endpoints targeted by Venom Stealer MaaS; victims include users of browsers, crypto wallets, and credential stores
Discovery Source	Gemini

Executive Summary

Venom Stealer is a newly identified Malware-as-a-Service platform that automates continuous credential theft, cryptocurrency draining, and browser data exfiltration targeting Windows endpoints. Unlike conventional infostealers that perform a single data grab, Venom Stealer implements persistent harvesting, increasing the window of exposure and potential damage per compromised host. Organizations face elevated risk of credential-based account takeover, financial loss from crypto wallet draining, and downstream breaches if harvested credentials reach enterprise systems.

Technical Analysis

Venom Stealer is a MaaS-model infostealer targeting Windows endpoints via two primary delivery vectors: ClickFix-style social engineering (CWE-1021, CWE-601) and fraudulent Avast antivirus websites that simulate virus scan interfaces to trick users into executing malicious payloads (CWE-522, CWE-312). The platform abuses user execution (MITRE T1204.002) triggered through phishing lures (T1566) and fake browser error prompts that instruct victims to run PowerShell commands (T1059.001). Post-execution, the stealer targets browser-stored credentials (T1555.003), credential stores (T1555), crypto wallets, and email data (T1114). Input capture via keylogging (T1056) and cookie/session token theft (T1539) extend its reach beyond static credential stores. The masquerading technique (T1036.005) via fake AV branding facilitates initial trust. Exfiltration occurs over C2 channels (T1041), with attacker-controlled infrastructure provisioned in advance (T1583.001). The platform implements continuous or persistent harvesting rather than a single-pass grab, materially elevating dwell-time risk. No CVE is associated; exploitation is entirely behavior-dependent with no software vulnerability patching available as a primary mitigation. No confirmed threat actor attribution exists in current open sources.

Sources: Dark Reading, SecurityWeek, Infosecurity Magazine, Malwarebytes, Cybernews (all T3, March 2026).
Note: No verified IOCs were included in source data provided; IOC section reflects this.

Action Checklist

1. Step 1: Containment. Block known malicious domains associated with fake Avast sites at DNS and web proxy layers; enforce web filtering categories covering typosquatting and fake AV/security vendor impersonation. Restrict outbound PowerShell execution over the internet at the perimeter firewall. Identify any endpoints where users recently interacted with unsolicited browser error prompts or visited unofficial Avast-branded URLs.
2. Step 2: Detection. Query endpoint logs for PowerShell (T1059.001) executions spawned from browser processes (Chrome, Edge, Firefox parent PIDs). Search EDR telemetry for T1555 credential access patterns: access to browser credential stores (Login Data, Web Data SQLite files), DPAPI decryption calls, and wallet file enumeration. Review proxy/DNS logs for DNS queries to domains mimicking avast.com or avast-related brand names. Check for scheduled tasks, registry run keys, or service installations that could indicate persistence supporting continuous harvesting.
3. Step 3: Eradication. On confirmed compromised hosts: isolate immediately, revoke and rotate all credentials accessible from that endpoint (browser-saved passwords, SSO tokens, crypto wallet keys if recoverable). Remove any persistence mechanisms identified (scheduled tasks, registry autorun entries, dropped binaries). There is no vendor patch for this threat; eradication is host remediation and credential rotation. Reimage endpoints where full trust cannot be restored.
4. Step 4: Recovery. After reimage or confirmed clean state: force password resets for all accounts whose credentials may have been stored in affected browsers or credential managers. Revoke and reissue session tokens and API keys. Enable MFA on all accounts that did not have it, prioritizing email, financial, and administrative systems. Monitor those accounts for 30 days post-incident for anomalous login activity, particularly from new geolocations or devices.
5. Step 5: Post-Incident. Conduct user awareness training targeting ClickFix-style social engineering: specifically, the pattern of fake browser error prompts instructing users to run commands. Review and harden PowerShell execution policy (Constrained Language Mode, application allowlisting via WDAC or AppLocker). Assess whether browser credential storage is acceptable policy or whether a password manager with MFA provides a safer alternative. Map observed attacker techniques against MITRE ATT&CK T1204.002, T1566, T1059.001, T1555, T1539 to identify detection gaps in current SIEM/EDR rule sets.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership, legal counsel, and executive stakeholders immediately if more than one endpoint is confirmed compromised, if any harvested credentials are confirmed to include privileged/admin accounts or financial system credentials, if crypto wallet drains are confirmed (potential regulatory or fiduciary notification obligations), or if the organization lacks the internal capability to perform memory forensics and full credential scope assessment — engage a third-party DFIR retainer. Worth noting this touches active credential theft and potential financial loss — you may want to verify breach notification obligations with legal counsel, as state and federal notification timelines may be triggered depending on PII scope of the harvested browser credentials.
Recovery Notes	Recovery cannot be declared complete until all active session tokens and OAuth refresh tokens associated with compromised accounts have been revoked and reissued — Venom Stealer's persistent harvesting model means the endpoint reimage alone does not terminate attacker access if tokens remain valid. Monitor all accounts identified in scope for anomalous authentication events (new geolocation, new device fingerprint, impossible travel, off-hours access) for a minimum of 30 days post-credential rotation, given that harvested credentials may be held by the MaaS operator and sold or used on a delayed timeline. Verify endpoint integrity post-reimage by comparing the system's software inventory against a known-good baseline using CIS 2.1 (Establish and Maintain a Software Inventory) procedures before returning to production.
Forensic Artifacts	Browser SQLite credential stores — `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data`, `%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data`, `%APPDATA%\Mozilla\Firefox\Profiles\*.default\logins.json` — Venom Stealer directly reads and DPAPI-decrypts these files; file access timestamps and SQLite WAL journal entries will record the exact time of credential harvesting. | Windows Prefetch files at `%SystemRoot%\Prefetch\` — Venom Stealer dropper and stealer binary names will appear as `.pf` files with execution count and last-run timestamps; parse with PECmd (KAPE/EZTools, free) to reconstruct execution timeline without EDR. | Sysmon Event ID 1 (Process Creation) and Event ID 11 (FileCreate) logs — specifically entries showing `powershell.exe` spawned by `chrome.exe`/`msedge.exe`/`firefox.exe` (ClickFix execution chain) and FileCreate events targeting browser Login Data, MetaMask extension storage at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\nkbihfbeogaeaoehlefnkodbefgpgknn`, and any `.dat` wallet files under `%APPDATA%\Roaming\`. | Windows Registry autorun hives exported from `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SYSTEM\CurrentControlSet\Services`, and `HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved` — Venom Stealer's continuous harvesting persistence will manifest as a newly registered entry in one of these locations with a creation timestamp correlating to initial compromise. | DNS resolver cache and proxy access logs — run `ipconfig /displaydns` on live system before network isolation to capture any currently cached resolutions for fake Avast domains; correlate with web proxy logs for HTTP 200 responses to `avast`-typosquatted hostnames to establish initial access vector and identify other potentially exposed endpoints that resolved the same lure infrastructure.

Per-Action IR Details

Step 1: Containment — Block known malicious domains associated with fake Avast sites at DNS and web proxy layers; enforce web filtering categories covering typosquatting and fake AV/security vendor impersonation. Restrict outbound PowerShell execution over the internet at the perimeter firewall. Identify

any endpoints where users recently interacted with unsolicited browser error prompts or visited unofficial Avast-branded URLs.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST SI-3 (Malicious Code Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without a commercial DNS filtering solution, deploy Pi-hole or use Windows DNS Response Policy Zones (RPZ) to sink-hole Venom Stealer C2 and fake Avast domains. Block outbound PowerShell HTTPS (port 443) from non-admin workstations using Windows Firewall with Advanced Security via Group Policy: `netsh advfirewall firewall add rule name='Block PS Outbound' program='%SystemRoot%\System32\WindowsPowerShell\v1.0\powershell.exe' action=block dir=out`. Use ProxyInspector or manually review Squid/pfSense proxy logs for HTTP/S requests matching regex `avast[^.]*\.(?!avast\.com)` to surface typosquatted domains.

Evidence: BEFORE blocking, export DNS resolver logs (Windows DNS debug log at `%SystemRoot%\System32\dns\dns.log` or Sysmon Event ID 22 — DNSEvent) for queries resolving to avast-branded hostnames not matching `avast.com`, `avg.com`, or `avastbrowser.com`. Capture web proxy logs showing HTTP 200 responses to those domains from browser process user-agents (Chrome, Edge, Firefox). Preserve firewall flow logs showing outbound TCP 443 connections from `powershell.exe` or `cmd.exe` processes — these indicate the ClickFix payload has already executed and is staging or exfiltrating.

Step 2: Detection — Query endpoint logs for PowerShell (T1059.001) executions spawned from browser processes (Chrome, Edge, Firefox parent PIDs). Search EDR telemetry for T1555 credential access patterns: access to browser credential stores (Login Data, Web Data SQLite files), DPAPI decryption calls, and wallet file enumeration. Review proxy/DNS logs for DNS queries to domains mimicking avast.com or avast-related brand names. Check for scheduled tasks, registry run keys, or service installations that could indicate persistence supporting continuous harvesting.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config (minimum); enable Process Creation (Event ID 1) and Network Connection (Event ID 3) logging. Run this PowerShell query on each endpoint to surface browser-spawned PowerShell: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'powershell' -and $_.Message -match '(chrome|msedge|firefox)'}`. For DPAPI credential access without EDR, query Sysmon Event ID 10 (ProcessAccess) where `TargetImage` matches `lsass.exe` or `GrantedAccess` = `0x1fffff`. Hunt for wallet file enumeration using: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4663 -and $_.Message -match '(wallet\.dat|\.json|metamask|exodus)'}`. For persistence, run `schtasks /query /fo LIST /v | findstr /i 'Task To Run\|Status\|Run As'` and audit `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` manually. Use the Sigma rule `proc_creation_win_powershell_spawn_from_browser.yml` (SigmaHQ community ruleset) converted to Windows Event Log format.

Evidence: Collect Windows Security Event Log Event ID 4688 (Process Creation with command line auditing enabled) filtered for `powershell.exe` or `pwsh.exe` with parent process `chrome.exe`, `msedge.exe`, or `firefox.exe` — this is the direct forensic signature of ClickFix execution. Capture Sysmon Event ID 11 (FileCreate) entries for access to `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data`, `%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data`, and any path matching `wallet.dat` or `\AppData\Roaming\MetaMask`. Collect Registry hive exports from `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce`, and `HKLM\SYSTEM\CurrentControlSet\Services` for newly created keys with timestamps within the incident window. Export the Windows Task Scheduler operational log (`Microsoft-Windows-TaskScheduler/Operational`) for task registration events (Event ID 106) within the same

window.

Step 3: Eradication — On confirmed compromised hosts: isolate immediately, revoke and rotate all credentials accessible from that endpoint (browser-saved passwords, SSO tokens, crypto wallet keys if recoverable). Remove any persistence mechanisms identified (scheduled tasks, registry autorun entries, dropped binaries). There is no vendor patch for this threat; eradication is host remediation and credential rotation. Reimage endpoints where full trust cannot be restored.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AC-2 (Account Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Without EDR-assisted isolation, use Windows Firewall to immediately quarantine the host: `netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound` then allow only RDP from your jump host IP for continued investigation. For binary removal, generate a SHA-256 hash of any dropped executables found in `%TEMP%`, `%APPDATA%\Roaming`, or `%LOCALAPPDATA%` and scan against VirusTotal via its free API before deletion. Remove scheduled tasks with `schtasks /delete /tn '' /f` and prune registry run keys with `reg delete 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /v '' /f`. Use Autoruns (Sysinternals, free) to enumerate and disable all persistence mechanisms in a single view, filtering by VirusTotal hits. For crypto wallet compromise, document wallet addresses for potential chain analysis; recovery of drained funds is generally not possible but addresses may support law enforcement referral.

Evidence: BEFORE reimaging, acquire a full memory image using WinPmem (free, open-source) to capture any in-memory Venom Stealer components, decrypted credential buffers, or C2 connection state that will not survive reboot. Collect a forensic disk image or at minimum the following live artifacts: contents of `%TEMP%` and `%APPDATA%\Roaming` directories with file metadata (creation/modified timestamps using `dir /T:C /A`), the full contents of Chrome/Edge/Firefox `Login Data` SQLite files (to document scope of credential exposure), and a registry export of all Run/RunOnce/Services keys. Preserve the Windows Prefetch directory (`%SystemRoot%\Prefetch`) for evidence of Venom Stealer executable names and execution count using PECmd (KAPE toolset, free). Hash all collected binaries with `Get-FileHash -Algorithm SHA256` for chain-of-custody documentation per NIST 800-61r3 §3.4 evidence handling guidance.

Step 4: Recovery — After reimage or confirmed clean state: force password resets for all accounts whose credentials may have been stored in affected browsers or credential managers. Revoke and reissue session tokens and API keys. Enable MFA on all accounts that did not have it, prioritizing email, financial, and administrative systems. Monitor those accounts for 30 days post-incident for anomalous login activity, particularly from new geolocations or devices.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.2 (Use Unique Passwords)

Compensating: Without a SIEM for 30-day monitoring, configure Azure AD / Microsoft 365 Sign-In logs (free with any M365 license) to export to a Log Analytics workspace and create an alert rule for sign-ins from new countries or impossible travel (built-in Microsoft Entra ID Protection, free tier). For on-prem Active Directory, enable Account Logon auditing (Event ID 4768/4769 Kerberos ticket requests, 4624 logon success) and run a weekly PowerShell script: `Get-EventLog -LogName Security -InstanceId 4624 | Where-Object {$_.Message -match ''}` to surface unexpected logon sources. For crypto wallet recovery assessment: document all wallet addresses from the compromised host's `%APPDATA%\Roaming\` paths (Exodus, Electrum, MetaMask extension storage at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\`) and perform blockchain transaction lookups to quantify drained assets; this supports insurance claims and law enforcement referrals.

Evidence: BEFORE re-enabling accounts post-reimage, query Azure AD or on-prem AD for all active sessions and refresh tokens associated with the compromised user accounts — Venom Stealer's continuous harvesting model means tokens exfiltrated during the persistence window may still be valid and actively abused after the endpoint is clean. Export authentication logs from all SaaS platforms (documented in browser saved passwords scope) showing logins during the infection window. Capture current browser extension lists from the clean reimaged system as a baseline, and compare against any extension installation Event IDs logged during the compromise window (Chrome extension installs log to `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions` with timestamped directory creation).

Step 5: Post-Incident — Conduct user awareness training targeting ClickFix-style social engineering: specifically, the pattern of fake browser error prompts instructing users to run commands. Review and harden PowerShell execution policy (Constrained Language Mode, application allowlisting via WDAC or AppLocker). Assess whether browser credential storage is acceptable policy or whether a password manager with MFA provides a safer alternative. Map observed attacker techniques against MITRE ATT&CK T1204.002, T1566, T1059.001, T1555, T1539 to identify detection gaps in current SIEM/EDR rule sets.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-2 (Incident Response Training), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Enforce PowerShell Constrained Language Mode via Group Policy (registry key `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment` — set `__PSLockdownPolicy` = `4`) as a zero-cost hardening measure that directly neutralizes the ClickFix PowerShell download-and-execute pattern used by Venom Stealer. For ATT&CK gap analysis without a commercial platform, load the incident's observed technique IDs (T1204.002, T1059.001, T1555, T1539) into the free MITRE ATT&CK Navigator and overlay against your Sysmon + Windows Event Log detection coverage to visually identify blind spots. Deploy the SigmaHQ rule `proc_creation_win_powershell_download_cradle.yml` and convert to your SIEM or Windows Event Forwarding format using `sigma convert` (free CLI). For browser credential policy, deploy Bitwarden (free, open-source) as an organizational password manager and disable browser native password saving via Group Policy (`SOFTWARE\Policies\Google\Chrome\PasswordManagerEnabled` = `0`).

Evidence: For the lessons-learned review, compile a complete timeline of the ClickFix social engineering lure delivery (web proxy logs showing the fake Avast site visit), the PowerShell execution trigger (Event ID 4688 parent-child chain), first Venom Stealer binary execution (Prefetch artifacts), first credential store access (Sysmon Event ID 11 on Login Data files), first C2 beacon (Sysmon Event ID 3 network connections from the stealer process), and first confirmed exfiltration (DNS/proxy logs). This timeline directly supports ATT&CK technique mapping and identifies the earliest detection opportunity missed — which is the actionable output for SIEM/EDR rule improvements. Retain all collected artifacts for a minimum of 12 months per NIST AU-11 (Audit Record Retention) to support any regulatory breach notification obligations or subsequent law enforcement referrals.

Detection Guidance

Primary behavioral indicators to hunt: (1) Browser process (chrome.exe, msedge.exe, firefox.exe) spawning PowerShell or cmd.exe child processes, high-fidelity indicator of ClickFix execution. (2) PowerShell accessing browser profile directories (AppData\Local\Google\Chrome\User Data\Default\Login Data, equivalent Edge/Firefox paths) outside of administrative context. (3) DPAPI CryptUnprotectData API calls from non-standard processes attempting to decrypt browser credential blobs. (4) File read or copy activity targeting wallet files (.wallet, wallet.dat, keystore directories for common crypto wallets). (5) Scheduled task or registry run key creation (HKCU\Software\Microsoft\Windows\CurrentVersion\Run) by PowerShell or a dropped binary, consistent with persistent harvesting mechanism. (6) Outbound HTTP/S POST requests to newly registered or

low-reputation domains, particularly in short bursts following the above activity (exfiltration pattern T1041). DNS monitoring: flag queries to domains that closely resemble avast.com (edit-distance typosquats, subdomain abuse). No confirmed IOCs (hashes, IPs, domains) were included in the provided source data. Treat any specific IOC values from third parties as requiring independent validation before blocklisting.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not confirmed — fake Avast-branded domains reported but specific values not available in provided source data]`	Fraudulent Avast antivirus sites used for payload delivery; exact domains not confirmed in available sources	LOW

Framework Mappings

MITRE-ATTACK

- **T1114** — Email Collection
- **T1204.002** — Malicious File
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1539** — Steal Web Session Cookie
- **T1555.003** — Credentials from Web Browsers
- **T1555** — Credentials from Password Stores
- **T1056** — Input Capture
- **T1583.001** — Domains
- **T1041** — Exfiltration Over C2 Channel
- **T1059.001** — PowerShell
- **T1566** — Phishing

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **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)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents

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
T1114	Email Collection	Collection
T1204.002	Malicious File	Execution
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1539	Steal Web Session Cookie	Credential-Access
T1555.003	Credentials from Web Browsers	Credential-Access
T1555	Credentials from Password Stores	Credential-Access
T1056	Input Capture	Collection
T1583.001	Domains	Resource-Development
T1041	Exfiltration Over C2 Channel	Exfiltration
T1059.001	PowerShell	Execution
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Venom Stealer MaaS Platform Commoditizes ClickFix Attacks	https://www.darkreading.com/endpoint-security/venom-stealer-maas-co...	T3
New Venom Stealer MaaS Platform Automates Continuous Data Theft	https://www.infosecurity-magazine.com/news/venom-stealer-maas-autom...	T3
Venom Stealer Raises Stakes With Continuous Credential Harvesting	https://www.securityweek.com/venom-stealer-raises-stakes-with-conti...	T3
Bogus Avast website fakes virus scan, installs Venom Stealer instead	https://www.malwarebytes.com/blog/threat-intel/2026/03/bogus-avast-...	T3
Venom Stealer turns ClickFix into Crypto Drainer - Cybernews	https://cybernews.com/security/venom-stealer-clickfix-crypto-theft/	T3

Generated 2026-04-01 13:28 UTC by TJS Security Command Center