INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-29 06:52 UTC

Vidar Fills the Infostealer Vacuum: What the Post-Lumma Ecosystem Means for Enterprise Credential Security

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0237
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Enterprise endpoints broadly; credential stores, browsers, VPN clients, and authentication token repositories across Windows environments
Published	2026-04-28T15:07:16
Discovery Source	Rss

Executive Summary

Following law enforcement disruptions of Lumma and Rhadamanthys infostealer operations in 2025, Vidar has consolidated displaced affiliate networks and emerged as the dominant infostealer-as-a-service platform targeting enterprise credentials. The disruptions did not reduce threat volume, they reorganized it, with Vidar now operating at expanded capacity across browser credential stores, session tokens, and VPN authentication data on Windows endpoints. Organizations that reduced infostealer detection rules, EDR tuning, or threat hunting cadence after the 2025 takedowns face elevated risk of credential theft leading to account takeover, unauthorized access to enterprise systems, and downstream data breaches.

Technical Analysis

Vidar is a Windows-targeting infostealer operating under a malware-as-a-service model, currently absorbing affiliate operators displaced by the 2025 Lumma and Rhadamanthys disruptions. Primary collection targets include browser-stored credentials, session tokens, VPN client credential stores, and authentication tokens, frequently stored in cleartext or weakly protected formats (CWE-522: Insufficiently Protected Credentials; CWE-312: Cleartext Storage of Sensitive Information; CWE-319: Cleartext Transmission of Sensitive Information). Distribution relies on malvertising (T1189), spearphishing links (T1566), and malicious file execution (T1204.002). Post-infection, Vidar harvests credentials from browser stores (T1555.003) and other credential repositories (T1555), captures keylogger input (T1056.001), steals web session cookies (T1539), and exfiltrates via web services (T1567) or C2 channels (T1041), using legitimate web infrastructure to blend

exfiltration traffic (T1102). No CVE is assigned to this campaign; the threat exploits credential storage weaknesses rather than software vulnerabilities. Source: Microsoft Security Blog, February 2026 (T1 source).

Action Checklist

1. Containment: Audit and revoke active browser-stored credentials and session tokens across enterprise endpoints, prioritizing accounts with access to VPN, SSO, and privileged systems. Force re-authentication on all active sessions for high-value accounts.
2. Detection: Query EDR telemetry and endpoint logs for Vidar behavioral indicators: unexpected processes reading browser profile directories (e.g., Chrome's 'Login Data', 'Cookies' SQLite files), outbound connections to Telegram infrastructure or uncommon CDN endpoints used for C2 (T1102), and bulk file access to credential store paths. Cross-reference network logs for large outbound transfers to uncategorized or newly registered domains.
3. Eradication: Remove identified Vidar samples from affected endpoints and reimage where infection is confirmed. Purge browser-stored credentials organization-wide and enforce policy preventing credential storage in browsers via Group Policy or endpoint management tooling. Disable or restrict browser credential sync features.
4. Recovery: After remediation, validate that credential stores are cleared and that re-authentication events reflect expected user behavior in SIEM. Monitor for anomalous login attempts from new geolocations or devices for 30 days post-incident. Confirm VPN and SSO session token issuance logs show no unauthorized active sessions.
5. Post-Incident: Review and close the detection gap that widened after the 2025 takedowns. Evaluate whether infostealer-specific detection rules were deprioritized or tuned down. Implement phishing-resistant MFA (e.g., FIDO2) to reduce value of stolen credentials. Map control gaps to NIST CSF Detect and Respond functions and update infostealer playbooks to reflect Vidar's current affiliate-driven distribution methods.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately if evidence of successful credential exfiltration is confirmed (outbound transfer artifacts present, C2 beacon observed, or stolen credentials used for unauthorized VPN or SSO access), if affected accounts include executives or system administrators with privileged access, or if the organization is subject to breach notification obligations under state privacy law, HIPAA, or PCI DSS and PII or cardholder data was accessible in exfiltrated credential stores.
Recovery Notes	After eradication, enforce a universal browser credential purge and password reset for all accounts accessible from affected endpoints before restoring normal operations — Vidar exfiltrates credential stores wholesale, so partial resets leave residual risk wherever the stealer had file read access. Monitor IdP authentication logs, VPN gateway logs, and privileged account activity daily for a minimum of 30 days, specifically watching for logins from new device fingerprints, impossible travel events, or MFA bypass attempts that would indicate stolen credentials are being used externally. Validate that browser credential storage policy (GPO or MDM enforcement) and sync disablement are confirmed active on all endpoints before closing the incident.

Forensic Artifacts	Chrome 'Login Data' SQLite file (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data) and 'Cookies' file — Vidar reads these directly via SQLite API calls; presence of a non-browser process with file handle access to these paths is a primary indicator of credential harvesting activity. | Windows Sysmon Event ID 10 (ProcessAccess) logs showing cross-process memory access or file access from a non-browser process targeting browser profile directories — Vidar does not inject into browsers but reads credential files directly from disk, producing anomalous file open events by unsigned or recently-created processes. | DNS client query logs and network flow data for outbound connections to api.telegram.org and associated Telegram CDN IP ranges (149.154.160.0/20, 91.108.4.0/22) — Vidar uses Telegram channels as its C2 dead-drop resolver (MITRE T1102) to retrieve dynamic C2 addresses, making Telegram API calls a high-fidelity behavioral indicator. | HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce registry keys — Vidar affiliates frequently establish persistence via Run key entries pointing to the dropper or a renamed copy in %TEMP% or %APPDATA%\Roaming\; capture these via Reg export before reimaging. | Memory dump from the infected process (WinPmem or Magnet RAM Capture) — Vidar decrypts its configuration block (containing C2 channel identifier, exfiltration target list, and module tasking) entirely in memory using RC4; this configuration is not recoverable from disk artifacts alone and is critical for scoping what data categories were targeted by this specific affiliate's build.

Per-Action IR Details

Containment — Audit and revoke active browser-stored credentials and session tokens across enterprise endpoints, prioritizing accounts with access to VPN, SSO, and privileged systems. Force re-authentication on all active sessions for high-value accounts.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without enterprise IAM tooling, use PowerShell to enumerate active RDP and remote sessions: 'query session /server:' and 'Get-WmiObject Win32_LogonSession | Where-Object {$_.LogonType -eq 10}'. For browser credential revocation without MDM, push a GPO-enforced registry key: 'HKLM\SOFTWARE\Policies\Google\Chrome\PasswordManagerEnabled = 0' and run 'sqlite3 "%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data" "DELETE FROM logins;"' under a deployment script. Invalidate Okta/Azure AD sessions via CLI using 'az ad user revoke-signed-in-sessions --id ' or equivalent IdP admin console bulk revocation.

Evidence: Before revoking sessions, capture a snapshot of active SSO session tokens from your IdP audit logs (Okta System Log event type 'user.session.start', Azure AD Sign-in logs filtered to 'Interactive' logons in the last 72 hours). Export Chrome 'Login Data' and 'Cookies' SQLite files from affected endpoints — Vidar exfiltrates these verbatim, so their presence confirms what was accessible to the stealer. Preserve VPN authentication logs (e.g., Cisco AnyConnect event log at '%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\') to establish baseline session legitimacy before forced re-auth obscures the timeline.

Detection — Query EDR telemetry and endpoint logs for Vidar behavioral indicators: unexpected processes reading browser profile directories (e.g., Chrome's 'Login Data', 'Cookies' SQLite files), outbound connections to Telegram infrastructure or uncommon CDN endpoints used for C2 (T1102), and bulk file access to credential store paths. Cross-reference network logs for large outbound transfers to uncategorized or newly registered domains.

NIST Phase: Detection Analysis

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

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

Compensating: Without EDR, deploy Sysmon with SwiftOnSecurity config and hunt for Event ID 10 (ProcessAccess) where TargetImage contains 'chrome.exe' or 'Login Data' and SourceImage is not a browser or known credential manager process. Use Sysmon Event ID 3 (NetworkConnect) to flag outbound connections to Telegram IP ranges (149.154.160.0/20, 91.108.4.0/22) or domains matching newly registered TLD patterns. Run this osquery one-liner to identify non-browser processes accessing Chrome credential stores: 'SELECT p.name, p.pid, f.path FROM processes p JOIN process_open_files f ON p.pid = f.pid WHERE f.path LIKE "%Login Data%" AND p.name NOT IN ("chrome.exe","msedge.exe","brave.exe");'. Apply the public Sigma rule 'win_vidar_infostealer_file_access' (SigmaHQ repository) against Windows Security Event Log Event ID 4663 (object access auditing on credential file paths).

Evidence: Preserve Sysmon Event ID 1 (Process Creation) entries for any process with command-line arguments referencing '%APPDATA%\Microsoft\Windows\INetCookies', '%LOCALAPPDATA%\Google\Chrome\User Data\', or '%APPDATA%\Mozilla\Firefox\Profiles\'. Capture DNS query logs or Windows DNS Client event log (Event ID 3008/3020) for lookups to api.telegram.org and any CDN subdomain not previously seen in baseline (Vidar uses Telegram channels as dead-drop resolvers per MITRE T1102). Collect network flow data showing large (>1MB) outbound HTTPS POSTs to non-categorized destinations within 60 minutes of the suspicious process execution window.

Eradication — Remove identified Vidar samples from affected endpoints and reimage where infection is confirmed. Purge browser-stored credentials organization-wide and enforce policy preventing credential storage in browsers via Group Policy or endpoint management tooling. Disable or restrict browser credential sync features.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-6 (Configuration Settings), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For teams without enterprise endpoint management, create a YARA rule targeting Vidar's known string patterns (RC4 key schedule artifacts, SQLite library imports, and hardcoded Telegram API strings) and scan endpoints using 'yara64.exe vidar_hunt.yar C:\' from a USB-booted or network-deployed scanner. To enforce browser credential policy without MDM, deploy via GPO: set 'HKLM\SOFTWARE\Policies\Google\Chrome\PasswordManagerEnabled' = 0 (DWORD) and 'HKLM\SOFTWARE\Policies\Google\Chrome\SyncDisabled' = 1 to block Chrome sync. For Firefox, push a 'policies.json' file to '%ProgramFiles%\Mozilla Firefox\distribution\' with 'PasswordManagerEnabled: false'. Use ClamAV with the unofficial Vidar signature database (clamav-unofficial-sigs project) for a second-pass sweep on quarantined samples.

Evidence: Before reimaging, acquire a full memory dump using WinPmem or Magnet RAM Capture — Vidar injects into legitimate processes and decrypts its configuration (including C2 channel details and exfiltration target list) in memory, which will be lost on reimage. Preserve the Vidar dropper and any associated files from '%TEMP%', '%APPDATA%\Roaming\', and startup persistence locations (HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run) as forensic artifacts. Document the exact set of credential store files (SQLite databases, cookie files, autofill data) present at time of discovery to establish scope of potential exfiltration.

Recovery — After remediation, validate that credential stores are cleared and that re-authentication events reflect expected user behavior in SIEM. Monitor for anomalous login attempts from new geolocations or device fingerprints for 30 days post-incident. Confirm VPN and SSO session token issuance logs show no unauthorized active sessions.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Without a SIEM, implement a daily PowerShell script that queries Azure AD or on-prem AD audit logs for logon events (Event ID 4624, logon type 3 and 10) from IP addresses not seen in the prior 90 days and emails the delta to the security team. For VPN session validation without centralized tooling, pull the Cisco AnyConnect or GlobalProtect authentication logs and diff against a pre-incident baseline of known user-IP pairings. Use 'Get-ADUser -Filter * -Properties LastLogonDate,BadPwdCount | Where-Object {$_.BadPwdCount -gt 3}' to flag credential stuffing attempts against accounts that Vidar may have exfiltrated.

Evidence: Retain IdP sign-in logs covering the full 30-day monitoring window as evidence of recovery integrity — these establish whether stolen credentials were used post-eradication. Preserve VPN gateway authentication logs showing session establishment (source IP, device certificate, MFA factor used) to confirm no sessions are authenticating with pre-remediation credentials. Capture before-and-after snapshots of the Chrome 'Login Data' SQLite row count on remediated endpoints to confirm credential purge was effective.

Post-Incident — Review and close the detection gap that widened after the 2025 takedowns. Evaluate whether infostealer-specific detection rules were deprioritized or tuned down. Implement phishing-resistant MFA (e.g., FIDO2) to reduce value of stolen credentials. Map control gaps to NIST CSF Detect and Respond functions and update infostealer playbooks to reflect Vidar's current affiliate-driven distribution methods.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IA-5 (Authenticator Management), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a tabletop exercise specifically around Vidar's affiliate model: simulate a scenario where a phishing lure drops a new Vidar variant with no known hash, and validate whether behavioral detection (process accessing credential stores) would catch it independently of signature-based tools. Review SigmaHQ for current Vidar detection rules and re-enable or retune any that were suppressed post-Lumma takedown due to assumed reduced threat volume. For FIDO2 rollout without enterprise budget, deploy Windows Hello for Business using on-premises AD with Azure AD Hybrid Join — no third-party vendor required. Document the lesson that threat ecosystem disruptions (Lumma, Rhadamanthys takedowns) historically consolidate affiliate volume rather than reduce it, and add this as an explicit assumption to the infostealer threat model.

Evidence: Preserve the full incident timeline and detection gap analysis as a lessons-learned artifact per NIST 800-61r3 §4 — specifically document the date range during which infostealer detection rules were tuned down or deprioritized relative to when Vidar affiliate volume increased post-2025 takedowns. Retain all IOCs (Vidar C2 Telegram channel identifiers, file hashes, registry persistence keys, CDN domains used for payload staging) in your threat intelligence platform or a structured CSV for integration into updated detection rules. Archive the pre- and post-incident versions of browser credential policy GPOs to demonstrate the control improvement for audit and compliance purposes.

Detection Guidance

Detection focus areas, mapped to MITRE ATT&CK: (1) Credential access, monitor for process access to browser SQLite credential files ('Login Data', 'Web Data', 'Cookies') by non-browser processes; flag access from scripting engines (powershell.exe, wscript.exe, mshta.exe) or unknown executables. (2) C2 via legitimate services (T1102), alert on outbound connections to Telegram API endpoints (api.telegram.org) or Discord CDN from non-user-initiated processes. (3) Exfiltration, detect large POST requests to uncategorized or newly

registered domains, particularly from processes not associated with normal user activity. (4) Initial access, correlate malvertising and phishing lure delivery: look for browser-spawned child processes, downloads of archive files (.zip, .rar) followed immediately by execution of contained binaries (T1204.002). (5) Session token theft (T1539), alert on bulk cookie file reads or copies outside of browser update processes. EDR solutions with behavioral analytics should be tuned for credential store access patterns. SIEM correlation rules should link credential access events to subsequent anomalous authentication in identity provider logs.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`api.telegram.org`	Vidar and related infostealers commonly use Telegram Bot API for C2 communications and credential exfiltration (T1102); outbound connections from non-browser, non-messaging processes to this domain warrant investigation	MEDIUM
URL	`https://www.microsoft.com/en-us/security/blog/2026/02/02/infostealers-without-borders-macos-python-stealers-and-platform-abuse/`	Microsoft T1 source documenting current infostealer ecosystem including Vidar activity; reference for detection patterns and behavioral indicators	HIGH

Framework Mappings

MITRE-ATTACK

- **T1539** — Steal Web Session Cookie
- **T1189** — Drive-by Compromise
- **T1204** — User Execution
- **T1566** — Phishing
- **T1102** — Web Service
- **T1555** — Credentials from Password Stores
- **T1555.003** — Credentials from Web Browsers
- **T1056.001** — Keylogging
- **T1567** — Exfiltration Over Web Service
- **T1041** — Exfiltration Over C2 Channel
- **T1204.002** — Malicious File

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring

- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **SC-8** — Transmission Confidentiality and Integrity
- **IA-5** — Authenticator Management

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **3.10** — Encrypt Sensitive Data in Transit
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(e)(1)** — Transmission 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.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1539	Steal Web Session Cookie	Credential-Access
T1189	Drive-by Compromise	Initial-Access
T1204	User Execution	Execution
T1566	Phishing	Initial-Access
T1102	Web Service	Command-And-Control

Technique ID	Technique Name	Tactic
T1555	Credentials from Password Stores	Credential-Access
T1555.003	Credentials from Web Browsers	Credential-Access
T1056.001	Keylogging	Collection
T1567	Exfiltration Over Web Service	Exfiltration
T1041	Exfiltration Over C2 Channel	Exfiltration
T1204.002	Malicious File	Execution

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/vulnerabilities-threats/vidar-top-chaot...	T3
Infostealers without borders: macOS, Python stealers, and platform ...	https://www.microsoft.com/en-us/security/blog/2026/02/02/infosteale...	T1
Infostealer Malware | How It Works & How to Stay Protected - DeXpose	https://www.dexpose.io/infostealer-malware/	T3
Infostealer Malware Targeting Third-Party Vendors | Bitsight	https://www.bitsight.com/blog/infostealer-malware-targeting-third-p...	T3
2026 State of Enterprise Infostealer Identity Exposure - Flare	https://flare.io/learn/resources/2026-enterprise-infostealer-identi...	T3

Generated 2026-04-29 06:52 UTC by TJS Security Command Center