INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-17 06:48 UTC

Lumma Stealer + SectopRAT Combo Infections Signal Persistent MaaS Multi-Payload Strategy

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0181
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Windows endpoints; cryptocurrency wallets; 2FA browser extensions (Chrome, Edge, Firefox); browser-stored credentials targeted by infostealer harvesting
Published	2026-04-16T20:30:27
Discovery Source	Rss

Executive Summary

Attackers using the Lumma Stealer malware platform are deploying a secondary remote access trojan, SectopRAT, on already-infected Windows machines, turning what appears to be a credential theft incident into a persistent network intrusion. Any organization with Windows endpoints is a potential target; financial services, cryptocurrency operations, and businesses relying on browser-stored credentials face heightened exposure. Despite a May 2025 law enforcement disruption, Lumma's Malware-as-a-Service model has reconstituted rapidly, meaning the threat remains active and the business risk extends well beyond stolen passwords to full attacker persistence inside the network.

Technical Analysis

Lumma Stealer (LummaC2) is an infostealer sold on underground forums as a Malware-as-a-Service platform. It harvests browser credentials, session cookies, cryptocurrency wallet files, and 2FA browser extension data (Chrome, Edge, Firefox). In observed combo infections, Lumma's loader capability stages SectopRAT (also tracked as ArechClient2) as a secondary payload, giving attackers persistent remote access beyond the initial credential harvest. Relevant CWEs: CWE-502 (Deserialization of Untrusted Data), CWE-494 (Download of Code Without Integrity Check), CWE-506 (Embedded Malicious Code). No CVE is assigned to this campaign. MITRE ATT&CK coverage spans initial access via phishing (T1566, T1204.001, T1204.002), execution via scripting (T1059, T1059.001), credential access (T1555, T1555.003, T1539), keylogging (T1056, T1056.001), persistence via boot/logon autostart (T1547), obfuscation (T1027, T1140), code signing bypass (T1553), ingress tool transfer (T1105), C2 over HTTP/S (T1071.001), DLL hijacking (T1574.002), email collection (T1114), and data exfiltration (T1041, T1219). A Microsoft Digital Crimes Unit and Europol disruption operation in May 2025

seized Lumma infrastructure, but the platform reconstituted, consistent with distributed MaaS affiliate models. No vendor patch applies; mitigation is detection and response-based. Source quality for this item is moderate; treat specific IOCs with corresponding confidence.

Action Checklist

1. Step 1: Containment, Isolate any Windows endpoint generating Lumma or SectopRAT detections immediately. Block known Lumma C2 domains and IPs at the perimeter firewall and DNS layer. Disable browser-stored credential sync on affected machines until investigation concludes. Revoke active sessions for any accounts accessed from flagged endpoints.
2. Step 2: Detection, Query EDR telemetry for process injection, DLL side-loading (T1574.002), and suspicious PowerShell execution (T1059.001) on Windows hosts. Search SIEM for outbound connections to newly registered or low-reputation domains over HTTP/S from browser processes or unusual parent processes. Review endpoint logs for autorun/registry persistence entries (T1547) and unsigned or mismatched code-signing artifacts (T1553). Hunt for ArechClient2 process names and known SectopRAT behavioral patterns in EDR.
3. Step 3: Eradication, Remove malware artifacts identified during investigation: autorun registry keys, dropped binaries, and any DLLs placed in application directories for hijacking. Force password resets for all accounts whose credentials or session cookies may have been harvested. Revoke and reissue API keys, tokens, and certificates stored in affected browsers. Disable and re-enroll any 2FA browser extensions on compromised profiles.
4. Step 4: Recovery, Validate endpoint cleanliness via full EDR scan post-remediation before returning to production. Monitor previously affected accounts for anomalous access patterns for a minimum of 30 days. Confirm no SectopRAT persistence channels (scheduled tasks, registry run keys, remote access services) remain active. Revalidate cryptocurrency wallet integrity if any wallet software was present on affected hosts.
5. Step 5: Post-Incident, Audit browser credential storage policies and enforce password manager solutions that do not rely on browser-native stores. Evaluate phishing-resistant MFA (FIDO2/passkeys) to reduce 2FA extension exposure. Review MaaS threat model in your threat intelligence program; Lumma's reconstitution after law enforcement disruption confirms affiliate-distributed platforms require ongoing monitoring, not single-event response.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO, legal, and external IR retainer immediately if: SectopRAT C2 beaconing is confirmed (indicating the infection has progressed from credential theft to persistent remote access), any harvested credentials belong to privileged or service accounts, cryptocurrency wallet software was present on affected hosts (potential financial loss requiring executive notification), or if 10 or more endpoints show Lumma/SectopRAT indicators simultaneously (suggesting automated MaaS affiliate deployment at scale rather than targeted infection of a single host).

Recovery Notes	Before returning any remediated Windows endpoint to production, validate cleanliness with a YARA scan using current Lumma and SectopRAT signatures AND a full Autoruns diff against a known-good baseline — EDR scan alone is insufficient given Lumma's documented use of code-signing abuse (T1553) to evade signature detection. Monitor all accounts that were active on affected endpoints for a minimum of 30 days post-remediation, with specific alerting on impossible travel, new MFA device enrollment, OAuth application consent grants, and any access to cryptocurrency platforms or financial systems, as harvested session cookies may enable account takeover outside the remediation window. Given Lumma's demonstrated resilience through the May 2025 law enforcement disruption and its MaaS affiliate model, treat this as an ongoing threat requiring persistent IOC monitoring rather than a closed incident after remediation — re-run C2 domain blocklist updates weekly against current Lumma infrastructure feeds from abuse.ch and Feodo Tracker.
Forensic Artifacts	Chrome/Edge/Firefox credential and cookie stores: `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` (SQLite), `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies` (SQLite), and `%APPDATA%\Mozilla\Firefox\Profiles\*.default\logins.json` + `key4.db` — these are the primary Lumma stealer targets and will show last-accessed timestamps correlating to the harvesting event. | Sysmon Event ID 1 (Process Creation) and Event ID 10 (ProcessAccess) logs from `Microsoft-Windows-Sysmon/Operational` showing `ArechClient2.exe` process lineage and any browser process memory access, which documents both the SectopRAT deployment and Lumma's in-memory credential harvesting technique. | Registry persistence keys at `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`, `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`, and `HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce` — SectopRAT commonly writes autorun values in these locations; export full hive with timestamps before eradication. | Windows DNS Client cache and query logs (Event ID 3006/3010 in `Microsoft-Windows-DNS-Client/Operational`) and firewall logs showing outbound connection attempts from browser processes or `ArechClient2.exe` to low-reputation or newly registered domains — documents Lumma C2 communication pattern distinct from normal browser traffic. | Browser extension local storage directories at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\` indexed by extension ID — Lumma specifically targets 2FA extensions (e.g., Authenticator, Authy) and cryptocurrency wallet extensions (MetaMask); the presence and last-modified timestamps of these directories establish which extensions were present and accessible during the infection window.

Per-Action IR Details

Step 1: Containment — Isolate any Windows endpoint generating Lumma or SectopRAT detections immediately. Block known Lumma C2 domains and IPs at the perimeter firewall and DNS layer. Disable browser-stored credential sync on affected machines until investigation concludes. Revoke active sessions for any accounts accessed from flagged endpoints.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Network isolation: use Windows Firewall via GPO or `netsh advfirewall firewall add rule name='Block SectopRAT C2' dir=out action=block remoteip=` for known C2 IPs. For DNS blocking without enterprise tooling, push a null-route for known Lumma C2 domains via local hosts file (`C:\Windows\System32\drivers\etc\hosts`) or configure

your perimeter DNS resolver (e.g., pfSense DNS Resolver) to return NXDOMAIN for those domains. Revoke browser sync by disabling Chrome/Edge sync via local Group Policy (`Computer Configuration > Administrative Templates > Google Chrome > Sign-in > Disable synchronization of data with Google`). Session revocation: force sign-out via Azure AD portal (Revoke Sessions) or on-prem AD by disabling and re-enabling the account, invalidating Kerberos tickets.

Evidence: BEFORE isolating, capture: full RAM image using Magnet RAM Capture or WinPmem to preserve in-memory Lumma/SectopRAT process artifacts and injected code; browser profile directories (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\`, `%APPDATA%\Mozilla\Firefox\Profiles\`) to preserve harvested credential vaults, cookies (`Cookies`, `Login Data` SQLite files), and extension storage for 2FA apps; Windows Security Event Log Event ID 4624/4625 (logon/logon failure) to identify sessions that must be revoked; netstat output (`netstat -anob`) to capture live C2 connections before the endpoint is cut from the network; and a snapshot of `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` for SectopRAT persistence keys before they can be cleared by the attacker.

Step 2: Detection — Query EDR telemetry for process injection, DLL side-loading (T1574.002), and suspicious PowerShell execution (T1059.001) on Windows hosts. Search SIEM for outbound connections to newly registered or low-reputation domains over HTTP/S from browser processes or unusual parent processes. Review endpoint logs for autorun/registry persistence entries (T1547) and unsigned or mismatched code-signing artifacts (T1553). Hunt for ArechClient2 process names and known SectopRAT behavioral patterns in EDR.

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), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without EDR/SIEM, deploy Sysmon with SwiftOnSecurity config (minimum: Event ID 1 process creation, Event ID 7 image load, Event ID 10 process access, Event ID 3 network connection). Hunt for Lumma using: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match 'ArechClient2|lumma'}`. For DLL side-loading (T1574.002), query Sysmon Event ID 7 for unsigned DLLs loaded by legitimate executables: `Where-Object {$_.Message -match 'Signed: false'}`. Detect SectopRAT RAT activity via Sysmon Event ID 3 filtering on outbound connections from `ArechClient2.exe` or from browsers (`chrome.exe`, `firefox.exe`) to IPs with PTR mismatches. Use Sigma rule `proc_creation_win_powershell_encoded_param.yml` applied against Sysmon logs via `sigmac` + PowerShell. For unsigned binary detection without EDR, run `sigcheck -u -e C:\Users\%USERNAME%\AppData\` (Sysinternals sigcheck) to find unsigned executables in user-writable paths where Lumma typically drops.

Evidence: Sysmon Event ID 1 logs showing `ArechClient2.exe` spawning or being spawned by browser processes; Sysmon Event ID 10 (ProcessAccess) entries where Lumma's loader accesses `lsass.exe` or browser process memory for credential harvesting; Windows Security Event Log Event ID 4688 (Process Creation) for PowerShell with Base64-encoded `-EncodedCommand` arguments, which Lumma loaders commonly use for second-stage SectopRAT deployment; Sysmon Event ID 7 (ImageLoaded) entries for DLLs loaded from `%APPDATA%` or `%TEMP%` paths into legitimate signed executables (DLL side-loading indicator specific to this campaign's T1574.002 use); browser extension storage files at `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Local Extension Settings\` for 2FA extension data that Lumma targets; Windows DNS Client Event Log (Event ID 3006/3010) or DNS query logs showing resolution requests for newly registered domains contacted by browser or PowerShell processes.

Step 3: Eradication — Remove malware artifacts identified during investigation: autorun registry keys, dropped binaries, and any DLLs placed in application directories for hijacking. Force password resets for all accounts whose credentials or session cookies may have been harvested. Revoke and reissue API keys, tokens, and certificates stored in affected browsers. Disable and re-enroll any 2FA browser extensions on compromised profiles.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 2.3 (Address Unauthorized Software), CIS 5.2 (Use Unique Passwords), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Registry eradication: use `reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v /f` and equivalent HKLM path after confirming key names from the forensic capture. For binary removal, use Sysinternals Autoruns (`autorunsc -a * -user * -c > autoruns_baseline.csv`) to enumerate all persistence points, then cross-reference against known-good baseline; delete identified unsigned binaries from `%APPDATA%`, `%TEMP%`, and application subdirectories. For DLL side-loading cleanup, run sigcheck against application directories (`sigcheck -u -e C:\Program Files\\`) and remove DLLs not matching vendor signatures. For credential revocation without a PAM tool: enumerate browser-stored credentials using `sqlite3 '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data' 'SELECT origin_url, username_value FROM logins;'` to produce a complete reset list before wiping. Re-enrollment of 2FA extensions should use hardware security keys (FIDO2) rather than re-installing browser extensions targeted by Lumma.

Evidence: Before eradication, preserve: a copy of the full registry hive (`reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run hkcu_run_before_eradication.reg`) documenting SectopRAT persistence keys; SHA-256 hashes and file metadata (creation time, modified time) of all dropped binaries and DLLs identified in `%APPDATA%\Roaming`, `%TEMP%`, and any application directory used for DLL hijacking — timestamps document attacker dwell time; a full export of the Chrome `Login Data` and `Cookies` SQLite databases and Firefox `logins.json`/`key4.db` to document the scope of credential harvesting before wiping; a list of all browser extensions installed on compromised profiles (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\`) to identify which 2FA extensions were present and potentially exfiltrated; and scheduled task XML exports (`schtasks /query /fo LIST /v > schtasks_before_eradication.txt`) to document any SectopRAT-created persistence tasks before removal.

Step 4: Recovery — Validate endpoint cleanliness via full EDR scan post-remediation before returning to production. Monitor previously affected accounts for anomalous access patterns for a minimum of 30 days. Confirm no SectopRAT persistence channels (scheduled tasks, registry run keys, remote access services) remain active. Revalidate cryptocurrency wallet integrity if any wallet software was present on affected hosts.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-10 (System Recovery and Reconstitution), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Without EDR post-remediation scan capability, run ClamAV with updated signatures (`freshclam && clamscan -r --infected --remove C:\Users\%USERNAME%\AppData\`) supplemented by a YARA scan using published Lumma and SectopRAT YARA rules (available from Elastic Security and ANY.RUN threat intel repositories — search for 'LummaC2 YARA' and 'SectopRAT YARA' on GitHub). Validate persistence clearance by re-running Autoruns and diffing against the post-eradication baseline: `autorunsc -a * -user * -c > autoruns_post.csv` then `Compare-Object (Import-Csv autoruns_baseline.csv) (Import-Csv autoruns_post.csv)`. For cryptocurrency wallet integrity, verify wallet file hashes against backup hashes if available; for software wallets (Exodus, Electrum, MetaMask), check transaction history via the blockchain explorer for any unauthorized transfers since the infection window. Monitor account anomalies via Azure AD Sign-in logs or Windows Security Event ID 4624 filtered for logon type 3 (network) and type 10 (remote interactive) from previously compromised accounts for 30 days.

Evidence: Before returning to production, confirm preservation of: a final Autoruns export and Sysmon Event ID 1 baseline snapshot documenting the clean state for future comparison; Windows Security Event Log Event ID 7045 (New Service Installed) entries covering the infection window to verify no SectopRAT remote access service was installed and remains active; scheduled task XML exports post-remediation confirming removal of any tasks created by SectopRAT (compare creation timestamps in `C:\Windows\System32\Tasks\` against infection window); cryptocurrency wallet application logs and, where applicable, on-chain transaction records from the infection window to establish whether wallet keys were exfiltrated and used; and a network traffic baseline (30-minute Wireshark capture from the remediated host) confirming absence of outbound connections to Lumma or SectopRAT C2 infrastructure

before production return.

Step 5: Post-Incident — Audit browser credential storage policies and enforce password manager solutions that do not rely on browser-native stores. Evaluate phishing-resistant MFA (FIDO2/passkeys) to reduce 2FA extension exposure. Review MaaS threat model in your threat intelligence program — Lumma's reconstitution after law enforcement disruption confirms affiliate-distributed platforms require ongoing monitoring, not single-event response.

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 RA-3 (Risk Assessment), NIST IA-5 (Authenticator Management), CIS 5.2 (Use Unique Passwords), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Browser credential audit: run `sqlite3 '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data' 'SELECT COUNT(*) FROM logins;'` across the fleet using a PowerShell loop to quantify browser-stored credential exposure before enforcing migration to an offline or standalone password manager (Bitwarden self-hosted or KeePassXC are zero-cost options). FIDO2 rollout without enterprise budget: enroll hardware keys (YubiKey 5 Series, Google Titan) for privileged accounts first; for general users, enforce passkeys via Microsoft Entra ID or Google Workspace at no additional licensing cost. For ongoing Lumma/SectopRAT MaaS monitoring, subscribe to CISA Known Exploited Vulnerabilities feed and configure a free MISP instance or OpenCTI community edition to ingest Lumma-specific OSINT feeds (Feodo Tracker, abuse.ch URLhaus filtered for LummaC2 tags). Document this incident in your lessons-learned register and update the IR playbook to include ArechClient2 as a specific SectopRAT indicator requiring immediate escalation to full dual-payload response, not single-stealer triage.

Evidence: For lessons-learned documentation, assemble: a complete timeline reconstructed from Sysmon, Windows Security, and DNS logs covering initial Lumma infection through SectopRAT secondary deployment, documenting attacker dwell time between stages; a browser credential exposure inventory (counts and domains from `Login Data` SQLite export) to quantify business risk for executive reporting and potential breach notification assessment; MITRE ATT&CK Navigator layer export documenting confirmed techniques observed (T1574.002, T1059.001, T1547, T1553) to drive detection gap analysis; the full list of C2 domains and IPs contacted during the infection, enriched with WHOIS registration dates to support threat intelligence reporting and sharing via ISAC if applicable; and all pre/post Autoruns comparison CSVs and scheduled task exports as evidence of complete eradication, retained per your IR record retention policy (NIST AU-11 (Audit Record Retention) recommends alignment with organizational records retention policy, typically minimum 1 year for security incidents).

Detection Guidance

Primary detection signals: (1) EDR alerts for process hollowing, DLL hijacking, or unusual child processes spawned by browsers or document viewers. (2) DNS and proxy logs showing outbound connections to low-reputation or newly registered domains, particularly from browser or Office application processes; Lumma C2 communication uses HTTP/S (T1071.001). (3) PowerShell script block logging (Event ID 4104) capturing encoded or obfuscated commands consistent with T1059.001 and T1027. (4) Windows Event Log: look for new autorun entries (Registry: HKCU\Software\Microsoft\Windows\CurrentVersion\Run) and scheduled task creation (Event ID 4698). (5) File system monitoring for unexpected .exe or .dll drops in user-writable application directories, which may indicate DLL hijacking staging. (6) Network detection: SectopRAT (ArechClient2) communicates over remote access protocols; flag unexpected RDP, VNC, or custom TCP sessions originating from workstations. Behavioral indicator: Lumma specifically targets browser profile directories (e.g., Chrome User Data, Firefox profiles) and cryptocurrency wallet files; file access alerts on these paths from non-browser processes are high-confidence indicators. Note: Specific IOC hashes, domains, and IPs should be sourced from current threat intelligence feeds (e.g., VirusTotal, MISP community, vendor threat intel); the source data for this

item does not include confirmed IOC values at publication.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not available — no confirmed IOC values present in source data`	Lumma C2 infrastructure domains should be sourced from current threat intelligence feeds; infrastructure was partially disrupted in May 2025 and has since reconstituted with new domains	LOW
HASH	`Not available — no confirmed sample hashes present in source data`	SectopRAT/ArechClient2 and Lumma Stealer sample hashes available via Malpedia (https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma) and VirusTotal threat intelligence	LOW

Framework Mappings

MITRE-ATTACK

- **T1555** — Credentials from Password Stores
- **T1574.002** — DLL Side-Loading
- **T1056** — Input Capture
- **T1204.001** — Malicious Link
- **T1140** — Deobfuscate/Decode Files or Information
- **T1056.001** — Keylogging
- **T1027** — Obfuscated Files or Information
- **T1547** — Boot or Logon Autostart Execution
- **T1105** — Ingress Tool Transfer
- **T1059** — Command and Scripting Interpreter
- **T1204.002** — Malicious File
- **T1059.001** — PowerShell
- **T1539** — Steal Web Session Cookie
- **T1219** — Remote Access Tools
- **T1566** — Phishing
- **T1071.001** — Web Protocols
- **T1555.003** — Credentials from Web Browsers
- **T1114** — Email Collection
- **T1041** — Exfiltration Over C2 Channel
- **T1553** — Subvert Trust Controls

NIST-800-53R5

- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **SI-10** — Information Input Validation
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

SOC2-TSC

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

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1555	Credentials from Password Stores	Credential-Access
T1574.002	DLL Side-Loading	Persistence
T1056	Input Capture	Collection
T1204.001	Malicious Link	Execution
T1140	Deobfuscate/Decode Files or Information	Defense-Evasion
T1056.001	Keylogging	Collection

Technique ID	Technique Name	Tactic
T1027	Obfuscated Files or Information	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1105	Ingress Tool Transfer	Command-And-Control
T1059	Command and Scripting Interpreter	Execution
T1204.002	Malicious File	Execution
T1059.001	PowerShell	Execution
T1539	Steal Web Session Cookie	Credential-Access
T1219	Remote Access Tools	Command-And-Control
T1566	Phishing	Initial-Access
T1071.001	Web Protocols	Command-And-Control
T1555.003	Credentials from Web Browsers	Credential-Access
T1114	Email Collection	Collection
T1041	Exfiltration Over C2 Channel	Exfiltration
T1553	Subvert Trust Controls	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://malpedia.caad.fkie.fraunhofer.de/details/win.lumma	T3
New Password Stealer Bypasses 2FA—Chrome, Edge And Firefox ...	https://www.forbes.com/sites/daveywinder/2026/04/06/new-password-st...	T3
THREAT ADVISORY Venom Info Stealer MaaS April 1, 2026	https://blackswan-cybersecurity.com/threat-advisory-venom-info-stea...	T3
A Quiet "Storm": Infostealer Hijacks Sessions, Decrypts Server-Side	https://www.varonis.com/blog/storm-infostealer	T3

Source	URL	Tier
Storm is a Windows infostealer that steals encrypted browser data ...	https://www.facebook.com/SlashGear/posts/storm-is-a-windows-infoste...	T3

Generated 2026-04-17 06:48 UTC by TJS Security Command Center