INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-22 18:53 UTC

Infostealer Ecosystem and PaaS Platforms Drive 156% Surge in Identity-Based Attacks via Session Token Theft

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0351
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Broadly affects browsers, email clients, cloud services, financial portals, and cryptocurrency wallets; CrowdStrike Falcon Platform and Falcon Next-Gen Identity Security referenced as detection/response tooling
Discovery Source	Rss:T1 Threatintel

Executive Summary

Infostealer malware and Phishing-as-a-Service platforms have created an industrialized supply chain for stealing session tokens from authenticated users, allowing attackers to impersonate employees across cloud services, SaaS platforms, email, and financial portals without ever needing their passwords. Threat intelligence sources document significant year-over-year increase in identity-based attacks driven by this ecosystem. The business risk is direct account takeover of fully authenticated sessions, meaning existing password + second-factor MFA investments provide no protection against this attack class once initial authentication is complete; however, device-binding and phishing-resistant MFA (FIDO2) reduce exposure.

Technical Analysis

Infostealer families (Lumma Stealer, Raccoon Stealer) and Phishing-as-a-Service platforms (Tycoon 2FA, Acreed) harvest browser-stored session cookies, saved credentials, and autofill data from compromised endpoints via keylogging (T1056.001) and credential access from web browsers (T1555.003). Stolen session tokens are exfiltrated (T1041) and sold via underground markets or used directly to hijack authenticated sessions (T1539, T1185), bypassing MFA entirely because the attacker presents a valid post-authentication token rather than credentials. Valid accounts are then abused (T1078) and multi-factor authentication mechanisms are defeated (T1556.006). Phishing (T1566) and adversary-in-the-middle techniques (T1557, T1621) support initial access and token interception. Structurally relevant weaknesses: CWE-384 (Session

Fixation), CWE-613 (Insufficient Session Expiration), CWE-287 (Improper Authentication), CWE-522 (Insufficiently Protected Credentials). No CVE is assigned; this is a campaign-level threat pattern, not a discrete vulnerability. No vendor patch resolves this; the attack exploits design-level session management gaps and endpoint compromise.

Action Checklist

1. Step 1: Containment. Audit all active cloud and SaaS sessions for anomalous geographic or device-context mismatches; force-terminate suspicious sessions immediately. Enable Conditional Access policies that bind sessions to device compliance state and IP reputation. Apply NIST AC-12 (Session Termination) by configuring maximum session lifetimes of 8 hours or less across Microsoft 365, Google Workspace, Okta, and critical SaaS platforms. Disable persistent 'remember me' tokens on all externally exposed applications per CIS Benchmarks v8 6.3.
2. Step 2: Detection. Query endpoint detection telemetry for processes reading browser cookie stores across all platforms (Windows: AppData\Local\Google\Chrome\User Data\Default\Cookies; macOS: ~/Library/Application Support/Google/Chrome/Default/Cookies; Linux: ~/.config/google-chrome/Default/Cookies). Alert on credential-access tool signatures associated with Lumma Stealer and Raccoon Stealer. In identity logs, detect session token reuse from new device fingerprints or geolocations inconsistent with user baseline. Monitor for T1539 (Steal Web Session Cookie) and T1185 (Browser Session Hijacking) behavioral patterns. Apply AU-6 (Audit Record Review) per NIST SP 800-53 to identity provider logs daily. NIST CSF Protect controls (D3-LAM Local Account Monitoring and D3-SFA System File Analysis) apply directly.
3. Step 3: Eradication. Deploy endpoint detection and response coverage to all user workstations; ensure browser-stored credential and cookie access generates alerts. Enforce CIS Benchmarks v8 5.4 (Restrict Administrator Privileges) to limit blast radius. Implement device-binding for session tokens via Conditional Access or equivalent identity platform controls so tokens are cryptographically tied to a registered device. Rotate credentials for any account flagged in anomalous session reviews per NIST CSF Protect (D3-CRO Credential Rotation). Apply NIST CSF Protect (D3-CH Credential Hardening) across identity stores.
4. Step 4: Recovery. Validate that session lifetime limits are enforced end-to-end across all identity providers and application layers. Confirm device-compliance checks are active on all Conditional Access policies before re-enabling flagged accounts. Monitor affected accounts for 30 days post-incident using continuous session integrity checks. Apply AU-11 (Audit Record Retention) per NIST SP 800-53 to preserve identity logs for forensic review. Verify MFA enrollment is current on all accounts per CIS Benchmarks v8 6.3, 6.4, 6.5.
5. Step 5: Post-Incident. Conduct a session management architecture review against CWE-613 (Insufficient Session Expiration) and CWE-384 (Session Fixation) for all customer-facing and internal applications. Document control gaps in MFA-bypass resilience and update the risk register. Evaluate deployment of phishing-resistant MFA (FIDO2/passkeys) to reduce reliance on session-cookie-only controls. Map findings to NIST IR-4 (Incident Handling) and update playbooks for session-hijacking scenarios. Review underground marketplace monitoring capability to detect organizational credentials appearing for sale.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to legal, privacy counsel, and executive leadership immediately if identity provider logs confirm the compromised session accessed systems containing PII, PHI, PCI-scoped data, or financial records — the 156% YoY surge in this attack pattern and the sessionless (password-free) nature of token-replay attacks mean breach notification timelines under GDPR Article 33 (72 hours) and state breach notification laws may already be running from the first confirmed anomalous token use.
Recovery Notes	Before re-enabling any account flagged in this investigation, confirm three controls are independently verified and not merely assumed: session lifetime caps are enforced at the IdP layer (not just the application layer, which infostealer-replayed tokens bypass), device-compliance Conditional Access is blocking non-registered devices in enforcement mode (not report-only), and MFA re-enrollment used a new authenticator that was not present on the compromised endpoint. Monitor affected accounts for a full 30-day window using daily IdP log review, because stolen token batches are frequently sold to multiple buyers on PaaS platforms and replay attempts may occur days or weeks after the initial compromise is contained. Pay particular attention to OAuth application consent grants made during the compromised session window — attackers frequently use stolen sessions to silently authorize persistent OAuth apps that survive password rotation and session revocation.
Forensic Artifacts	Browser SQLite cookie stores on compromised endpoints — specifically `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies`, `%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Cookies`, and Firefox `cookies.sqlite` under the active profile — parse with sqlite3 to identify session cookies for M365, Google Workspace, Okta, Salesforce, and financial portals that were present at time of infostealer execution; last-accessed timestamps establish the exact exfiltration window. | Windows DPAPI master key blobs at `%APPDATA%\Microsoft\Protect\\` and the associated NTUSER.DAT hive — Lumma Stealer and Raccoon Stealer both target DPAPI-encrypted credential stores; these artifacts confirm scope of credential exposure beyond session cookies and are required for offline decryption during forensic analysis. | Identity provider authentication logs showing the first token-replay event — specifically Entra ID SigninLogs or Okta System Log entries where IsInteractive=false, TokenIssuerType=AzureAD, and the device fingerprint or IP differs from the user's 30-day baseline; the delta between cookie exfiltration timestamp (from endpoint) and first replay event (from IdP) establishes time-to-exploit for this specific campaign. | Sysmon Event ID 10 (ProcessAccess) logs capturing any process invoking ReadProcessMemory against Chrome, Edge, or Firefox browser processes — Lumma Stealer's in-memory extraction technique leaves this artifact in Sysmon telemetry and directly maps to MITRE ATT&CK T1539 (Steal Web Session Cookie); this is often the only host-based indicator before the token reaches the attacker's infrastructure. | Outbound network flow records or proxy logs showing DNS resolution and HTTPS connections to known Lumma Stealer or Raccoon Stealer C2 domains or IP ranges during the compromise window — these establish the exfiltration channel, confirm which stolen credential packages were transmitted, and support threat intelligence sharing under NIST 800-61r3 §4 post-incident reporting recommendations.

Per-Action IR Details

Step 1: Containment — Audit all active cloud and SaaS sessions for anomalous geographic or device-context mismatches; force-terminate suspicious sessions immediately. Enable Conditional Access policies that bind sessions to device compliance state and IP reputation. Apply NIST AC-12 (Session Termination) by configuring maximum session lifetimes of 8 hours or less across Microsoft 365, Google Workspace, Okta, and critical SaaS platforms. Disable persistent 'remember me' tokens on all externally exposed applications per

CIS 6.3.

NIST Phase: Containment

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

Controls: NIST AC-12 (Session Termination), NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), NIST IR-4 (Incident Handling)

Compensating: For teams without Okta or Azure AD Premium Conditional Access: use Microsoft 365 PowerShell to revoke all refresh tokens org-wide — `Get-AzureADUser | Revoke-AzureADUserAllRefreshToken`. For Google Workspace, use Admin SDK Directory API or the Admin Console under Security > Session Management to set session duration to 8 hours. For on-prem identity stores, deploy a Nginx or Apache reverse proxy rule to reject requests bearing cookies older than 8 hours based on cookie issuance timestamp. Document each terminated session with timestamp, account UPN, source IP, and user-agent string before termination for forensic chain of custody.

Evidence: Before terminating sessions, export the full active-session inventory from each IdP: Microsoft Entra ID sign-in logs (Log Analytics table: SigninLogs, filter on IsInteractive=false and TokenIssuerType=AzureAD), Google Workspace Admin Audit logs filtered for login events with device_type=unknown, and Okta System Log filtered for event_type=user.session.start where client.geographicalContext.country differs from user's registered country. Capture the raw cookie values or refresh token IDs if accessible — these are the stolen artifacts the infostealer exfiltrated, and having them enables you to confirm whether revocation was complete.

Step 2: Detection — Query endpoint detection telemetry for processes reading browser cookie stores (Chrome: AppData\Local\Google\Chrome\User Data\Default\Cookies; Firefox: places.sqlite). Alert on credential-access tool signatures associated with Lumma Stealer and Raccoon Stealer. In identity logs, detect session token reuse from new device fingerprints or geolocations inconsistent with user baseline. Monitor for T1539 (Steal Web Session Cookie) and T1185 (Browser Session Hijacking) behavioral patterns. Apply AU-6 (Audit Record Review) to identity provider logs daily. D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) countermeasures apply directly.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST SI-3 (Malicious Code Protection), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config and add a custom rule targeting FileAccess events on `*\Chrome\User Data\Default\Cookies`, `*\Firefox\Profiles\*.default*\cookies.sqlite`, and `*\Microsoft\Edge\User Data\Default\Cookies` — any process other than the browser binary itself reading these files is high-confidence T1539. Use the following PowerShell one-liner to hunt for recent anomalous reads: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 11 -and $_.Message -match 'Cookies'}`. For network-side detection, run Zeek or Wireshark and write a signature for HTTP requests where the Cookie header matches a valid session but the User-Agent or TLS JA3 fingerprint differs from the user's established baseline — this catches the token-replay step after exfiltration. Sigma rule `proc_access_win_browser_credential_stealing.yml` from the SigmaHQ repository covers Lumma and Raccoon Stealer process-injection patterns.

Evidence: Collect the following before any endpoint remediation: (1) Copy `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cookies` (SQLite file — do not open in place; copy first) and parse with `sqlite3` to identify recently accessed cookie rows for sessions matching your SaaS domains. (2) Check Windows Security Event Log for Event ID 4663 (Object Access) on the Cookies file path — requires Object Access auditing enabled on the file. (3) Retrieve Sysmon Event ID 10 (ProcessAccess) logs for any non-browser process accessing the browser process memory — Lumma Stealer uses in-memory cookie extraction via ReadProcessMemory. (4) Export identity provider authentication logs showing the first appearance of the stolen token from a new device fingerprint or IP — this timestamp anchors your compromise timeline. (5) Check Windows Prefetch or Shimcache for evidence of Lumma/Raccoon dropper execution artifacts at `C:\Users\\AppData\Roaming` or `C:\ProgramData`.

Step 3: Eradication — Deploy endpoint detection and response coverage to all user workstations; ensure browser-stored credential and cookie access generates alerts. Enforce CIS 5.4 (Restrict Administrator

Privileges) to limit blast radius. Implement device-binding for session tokens via Conditional Access or equivalent identity platform controls so tokens are cryptographically tied to a registered device. Rotate credentials for any account flagged in anomalous session reviews per D3-CRO (Credential Rotation). Apply D3-CH (Credential Hardening) across identity stores.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST AC-6 (Least Privilege), NIST IA-5 (Authenticator Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 5.2 (Use Unique Passwords)

Compensating: For teams without enterprise EDR: deploy OSQuery with the `browser_plugins` and `file_events` tables configured to alert on new writes or reads to browser cookie store paths — run as a scheduled query every 15 minutes. For credential rotation without a PAM tool, use a scripted approach: generate randomized passwords with `openssl rand -base64 24` for each affected account and force immediate change via `Set-ADAccountPassword` (AD) or Google Admin SDK. To implement lightweight device-binding without Conditional Access Premium, configure your IdP to restrict login to known device IPs using named location policies (available in Entra ID Free for IP-based restrictions). Deploy ClamAV with the `SecuriteInfo` unofficial database signatures that include Lumma Stealer and Raccoon Stealer heuristics for endpoint scanning across affected workstations.

Evidence: Before reimaging or cleaning endpoints, preserve: (1) Full memory dump of the affected user session using WinPmem or `procdump -ma` targeting any suspicious process identified in Step 2 — Lumma Stealer operates in-memory and artifacts will be lost on reboot. (2) Copy the entire browser user-data directory (`%LOCALAPPDATA%\Google\Chrome\User Data\`) to forensic storage — this preserves the Login Data SQLite file containing saved credentials (encrypted with DPAPI) and the browsing history that may reveal phishing delivery vector. (3) Export Windows DPAPI master key blobs from `%APPDATA%\Microsoft\Protect\` — these are required to decrypt any DPAPI-protected credentials the stealer may have harvested and confirm the full scope of credential exposure. (4) Collect AmCache.hve and NTUSER.DAT hive snapshots to establish malware execution timeline before eradication begins.

Step 4: Recovery — Validate that session lifetime limits are enforced end-to-end across all identity providers and application layers. Confirm device-compliance checks are active on all Conditional Access policies before re-enabling flagged accounts. Monitor affected accounts for 30 days post-incident using continuous session integrity checks. Apply AU-11 (Audit Record Retention) to preserve identity logs for forensic review. Verify MFA enrollment is current on all accounts per CIS 6.3, 6.4, 6.5.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-11 (Audit Record Retention), 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)

Compensating: For teams without a SIEM to run 30-day continuous session monitoring: configure Microsoft 365 Audit Log Search (available in all M365 tiers) with a daily scheduled export of `UserLoggedIn` and `UserLoginFailed` events for the affected accounts, piped to a CSV and diffed against the previous day's baseline — flag any new device ID or IP block. For Google Workspace, use the Reports API with `applicationName=login` filtered to affected users and alert on `login_type=exchange` events (token-based logins) from unrecognized devices. Document the exact session lifetime values configured in each IdP after enforcement as evidence of control implementation — this matters if a regulatory notification obligation arises from identity compromise involving PII.

Evidence: Before re-enabling flagged accounts, collect and retain: (1) Screenshot or exported record of the Conditional Access policy configuration showing device-compliance requirement and session lifetime cap — this is the before/after control-state evidence. (2) Identity provider sign-in log export for each affected account covering the full incident window (from earliest anomalous token use to session revocation) — retain per AU-11 for a minimum of 3 years if any financial or regulated-data access occurred during the compromised session. (3) MFA enrollment audit export confirming re-enrollment on a new, verified authenticator device — not the same device that may have been compromised by the infostealer. (4) Network flow logs or proxy logs showing outbound connections from affected

endpoints to known Lumma/Raccoon C2 infrastructure during the compromise window, to determine what data was actually exfiltrated beyond session tokens.

Step 5: Post-Incident — Conduct a session management architecture review against CWE-613 (Insufficient Session Expiration) and CWE-384 (Session Fixation) for all customer-facing and internal applications. Document control gaps in MFA-bypass resilience and update the risk register. Evaluate deployment of phishing-resistant MFA (FIDO2/passkeys) to reduce reliance on session-cookie-only controls. Map findings to NIST IR-4 (Incident Handling) and update playbooks for session-hijacking scenarios. Review underground marketplace monitoring capability to detect organizational credentials appearing for sale.

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 RA-3 (Risk Assessment), NIST SA-11 (Developer Testing and Evaluation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For FIDO2 evaluation without budget for hardware keys: Google and Microsoft both offer free passkey support for Workspace and Entra ID respectively — begin a pilot with privileged accounts at zero hardware cost using platform authenticators (Windows Hello, Touch ID). For underground marketplace monitoring without a commercial threat intel subscription, configure free monitoring via HaveIBeenPwned API (free tier for domain-level breach alerts) and set up Google Alerts for your organization's domain name combined with terms like 'logs', 'stealer', and 'combolist'. For the CWE-613/CWE-384 session audit, use OWASP ZAP in authenticated-scan mode against your internal applications to automatically flag session tokens that persist beyond logout or do not rotate on privilege change — free and scriptable for CI/CD integration.

Evidence: Post-incident documentation must capture: (1) The full session token lifecycle for the compromised accounts — from issuance timestamp to first anomalous use to revocation — reconstructed from IdP logs, to quantify the dwell time window that infostealer-stolen tokens remained valid. (2) Evidence of which specific PaaS infostealer platform delivered the malware (Lumma Stealer subscription, Raccoon Stealer affiliate panel, etc.) if determinable from C2 infrastructure analysis or underground forum intelligence — this attribution informs whether the organization is a targeted victim or opportunistic collateral. (3) A mapping of every SaaS application accessed during the compromised session window, drawn from identity provider and OAuth consent logs — this defines the true blast radius and drives breach notification scoping decisions. (4) Risk register entry documenting the gap between existing TOTP/SMS MFA controls and phishing-resistant FIDO2 MFA, with this incident as the evidence record supporting upgrade prioritization.

Detection Guidance

Primary detection surfaces are endpoint telemetry and identity provider logs. On endpoints: alert on any process accessing browser cookie databases outside of the browser process itself (Chrome Cookies SQLite file, Firefox cookies.sqlite). Flag execution of known infostealer process names and hashes associated with Lumma Stealer and Raccoon Stealer families; current signatures are maintained in threat intelligence feeds and vendor EDR rulesets. In identity provider logs (Entra ID, Okta, Google Workspace): query for session token reuse events where the device fingerprint, user-agent string, or source IP differs from the authenticating session baseline. Specifically hunt for T1539 (Steal Web Session Cookie) and T1185 (Browser Session Hijacking) ATT&CK technique indicators. SIEM correlation rule: flag any authenticated session where the source IP ASN or country changes mid-session without a corresponding re-authentication event. Apply NIST CSF Protect (D3-LAM Local Account Monitoring) for local account anomalies and NIST CSF Protect (D3-SFA System File Analysis) for unauthorized access to browser credential stores. NIST AU-6 (Audit Record Review) per SP 800-53 requires regular analysis of these logs; increase review frequency to daily for high-privilege accounts during elevated threat periods.

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1555.003** — Credentials from Web Browsers
- **T1566** — Phishing
- **T1056.001** — Keylogging
- **T1621** — Multi-Factor Authentication Request Generation
- **T1078** — Valid Accounts
- **T1556.006** — Multi-Factor Authentication
- **T1539** — Steal Web Session Cookie
- **T1557** — Adversary-in-the-Middle
- **T1185** — Browser Session Hijacking

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)

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
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

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** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1555.003	Credentials from Web Browsers	Credential-Access
T1566	Phishing	Initial-Access
T1056.001	Keylogging	Collection
T1621	Multi-Factor Authentication Request Generation	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1556.006	Multi-Factor Authentication	Credential-Access
T1539	Steal Web Session Cookie	Credential-Access
T1557	Adversary-in-the-Middle	Credential-Access
T1185	Browser Session Hijacking	Collection

Sources

Source	URL	Tier
Blog	https://www.crowdstrike.com/en-us/blog/how-to-protect-identities-an...	T3
	https://thehackernews.com/expert-insights/2026/04/session-cookie-th...	T3
	https://hackread.com/infostealers-as-a-service-identity-hacks-recor...	T3
	https://www.crowdstrike.com/en-us/blog/reasons-why-nonprofits-are-t...	T3

Source	URL	Tier
CrowdStrike Falcon® Next-Gen Identity Security	https://www.crowdstrike.com/en-us/platform/next-gen-identity-security/	T3

Generated 2026-05-22 18:53 UTC by TJS Security Command Center