INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-15 06:52 UTC

# Google Disrupts AI-Assisted Zero-Day Exploit Campaign Targeting Windows Credential Theft

**THREAT CAMPAIGN** | **HIGH** | CVSS 8.1

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0316 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 8.1 |
| **Affected Products** | Windows systems (specific versions unconfirmed in available source data) |
| **Published** | 2026-05-13 |
| **Discovery Source** | Gemini |

## Executive Summary

Google's threat intelligence team identified and disrupted a campaign using a zero-day exploit, assessed to have been developed with AI assistance, targeting Windows endpoints to steal credentials. No CVE has been assigned; specific affected Windows versions are unconfirmed in available source data. Organizations relying on Windows for authentication and identity workflows face elevated risk: successful credential theft enables account takeover, lateral movement, and potential business-wide access loss. Confidence in specific technical details is medium, as direct source verification of the Google finding was not possible from available URLs.

## Technical Analysis

This campaign involved exploitation of an unpatched Windows zero-day, with threat intelligence indicating AI tooling may have assisted in exploit development or weaponization. The attack chain maps to credential access via T1555 (Credentials from Password Stores), valid account abuse (T1078), and exploitation of authentication mechanisms (T1212). Delivery likely involved phishing (T1566), and exploit tooling was acquired from external sources or developed by the threat actor (T1588.005). Associated CWEs include CWE-693 (Protection Mechanism Failure), CWE-522 (Insufficiently Protected Credentials), and CWE-294 (Authentication Bypass by Capture-replay). Adjacent reporting confirms active Windows NTLM credential theft activity and exploitation of a Windows Shell zero-day (The Hacker News, 2026-04). No CVE identifier has been assigned to this specific campaign. No patch ID is confirmed at this time. Source quality score is 0.712; primary source (Microsoft blog, 2026-05-12) covers adjacent intrusion activity, not this specific finding. Technical details should be treated as medium-confidence pending direct Google publication. Note: CVSS 8.1 and EPSS values are system-assigned estimates; no vendor score is confirmed.

## Action Checklist

1. Step 1: Containment, Audit Windows endpoints for unauthorized credential access activity. Enforce least-privilege access on accounts with administrative rights. Restrict NTLM authentication where feasible using Group Policy (Network Security: Restrict NTLM settings). Identify and isolate systems with unusual authentication events pending further investigation.
2. Step 2: Detection, Query Windows Security Event Logs for Event IDs 4624 (successful logon), 4625 (failed logon), 4776 (NTLM authentication), and 4648 (explicit credential use). Correlate with process creation events (Event ID 4688) for credential-dumping tool signatures (e.g., lsass.exe access patterns). Monitor for anomalous use of stored credentials from password managers or browser credential stores (T1555). No confirmed IOCs are available for this specific campaign at this time.
3. Step 3: Eradication, No specific patch ID is confirmed for this zero-day at publication time. Apply all outstanding Windows cumulative updates immediately, prioritizing April and May 2026 security rollups. Rotate credentials for any accounts showing anomalous authentication patterns. Remove or rotate cached credentials on compromised endpoints. Restrict and audit service accounts.
4. Step 4: Recovery, Validate that Windows Update has applied current cumulative patches across all endpoints. Confirm no persistence mechanisms (scheduled tasks, new local accounts, registry run keys) were introduced during the window of exposure. Monitor authentication logs for 30 days post-remediation for residual access attempts using stolen credentials. Re-verify privileged account integrity.
5. Step 5: Post-Incident, This campaign highlights two control gaps: insufficient monitoring of credential stores (CWE-522) and reliance on NTLM authentication (CWE-294). Evaluate phased NTLM deprecation per Microsoft guidance. Assess whether endpoint detection coverage includes lsass access monitoring and credential-dumping behavioral signatures. Review AI-assisted threat development as an emerging capability gap in detection engineering timelines.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to CISO, legal, and external IR retainer immediately if Event ID 4648 (explicit credential use) or 4776 (NTLM authentication) anomalies are detected on privileged accounts, service accounts with broad domain access, or any system storing PII/PHI/PCI data — as successful credential theft in this campaign enables lateral movement and account takeover with potential breach notification obligations under HIPAA, PCI DSS, and applicable state data breach laws. |
| **Recovery Notes** | After eradication, re-admit systems to production only after confirming the April–May 2026 Windows cumulative rollup is applied, all flagged account passwords are rotated (including service accounts and cached credentials), and no new scheduled tasks, local accounts, or Run key entries exist outside the pre-incident baseline. Monitor Windows Security Event IDs 4624, 4648, and 4776 on all Domain Controllers and previously affected endpoints for a minimum of 30 days, filtering on the UPNs and workstation names identified during the investigation, as stolen credentials may be used from attacker infrastructure not yet blocked. Given that no CVE has been confirmed, treat any new Microsoft security advisory referencing Windows credential handling or NTLM issued after 2026-03-04 as potentially relevant to this campaign and re-evaluate patch applicability. |

| | |
|---|---|
| **Forensic Artifacts** | Windows Security Event Log (Security.evtx) on Domain Controllers — specifically Event IDs 4624, 4625, 4648, and 4776 — which record the NTLM authentication chains and explicit credential use patterns this credential-theft campaign would produce during the access phase \| Sysmon EventID 10 (ProcessAccess) log entries targeting lsass.exe — the primary memory-access artifact produced by credential-dumping tools (Mimikatz, ProcDump, comsvcs.dll MiniDump) used to extract NTLM hashes and Kerberos tickets from Windows endpoint memory \| Browser credential store SQLite databases with last-accessed filesystem metadata: Chrome/Edge `%LOCALAPPDATA%\\User Data\Default\Login Data` and Firefox `%APPDATA%\Mozilla\Firefox\Profiles\\logins.json` — access by non-browser processes is a direct indicator of T1555.003 (Credentials from Web Browsers) exploitation \| Windows Credential Manager vault (`%APPDATA%\Microsoft\Credentials\` and `%LOCALAPPDATA%\Microsoft\Credentials\`) file access timestamps — this campaign's credential-theft mechanism would interact with these files if targeting stored Windows credentials beyond browser stores \| NTLM Operational Event Log (`Applications and Services Logs\Microsoft\Windows\NTLM\Operational`, Event ID 8004) on Domain Controllers — records the source workstation and account name for every NTLM authentication, providing a ground-truth timeline for lateral movement using stolen NTLM hashes from this campaign |

### Per-Action IR Details

**Step 1: Containment — Audit Windows endpoints for unauthorized credential access activity. Enforce least-privilege access on accounts with administrative rights. Restrict NTLM authentication where feasible using Group Policy (Network Security: Restrict NTLM settings). Identify and isolate systems with unusual authentication events pending further investigation.**

**NIST Phase:** Containment

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

**Controls:** NIST IR-4 (Incident Handling), NIST AC-6 (Least Privilege), NIST SI-4 (System Monitoring), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 4.4 (Implement and Manage a Firewall on Servers)

**Compensating:** Deploy Sysmon with SwiftOnSecurity config to capture lsass.exe access attempts (EventID 10, TargetImage: lsass.exe). Run the following PowerShell to enumerate accounts with AdminCount=1 and flag anomalous last-logon deltas: `Get-ADUser -Filter {AdminCount -eq 1} -Properties LastLogonDate | Where-Object {$_.LastLogonDate -gt (Get-Date).AddHours(-24)}`. Use Group Policy Management Console to set Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options: 'Network Security: Restrict NTLM: Incoming NTLM Traffic' to 'Deny All Accounts' on non-legacy systems. Isolate flagged hosts by disabling their switch port or applying a host-based firewall block via `netsh advfirewall set allprofiles state on`.

**Evidence:** Before isolating any endpoint, preserve: Windows Security Event Log (export with `wevtutil epl Security C:\IR\Security.evtx`), LSASS process memory using ProcDump (`procdump.exe -ma lsass.exe lsass.dmp`) if active compromise is suspected, NTLM authentication logs from Domain Controllers (Event ID 4776 with Workstation Name and Source IP), and a full list of currently active sessions (`qwinsta /server:` and `net session`). Capture registry hive `HKLM\SYSTEM\CurrentControlSet\Control\Lsa` to document current NTLM restriction settings before policy changes overwrite baseline state.

**Step 2: Detection — Query Windows Security Event Logs for Event IDs 4624 (successful logon), 4625 (failed logon), 4776 (NTLM authentication), and 4648 (explicit credential use). Correlate with process creation events (Event ID 4688) for credential-dumping tool signatures (e.g., lsass.exe access patterns). Monitor for anomalous use of stored credentials from password managers or browser credential stores (T1555). No confirmed IOCs are available for this specific campaign at this time.**

**NIST Phase:** Detection Analysis

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

**Controls:** NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), 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)

**Compensating:** Without SIEM, run this PowerShell query on each DC and affected endpoint to surface NTLM anomalies and credential-dumping indicators: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4648,4776,4688)} | Select-Object TimeCreated,Id,Message | Export-Csv C:\IR\auth_events.csv`. For lsass access detection without EDR, deploy Sysmon EventID 10 (ProcessAccess) filtering TargetImage='C:\Windows\System32\lsass.exe' and flag any SourceImage not matching known system processes (services.exe, wininit.exe). For browser credential store access (T1555.003), query Sysmon EventID 11 (FileCreate) and EventID 10 for access to `%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data` and equivalent Firefox/Edge paths. Apply the public Sigma rule `win_lsass_memory_dump_file_creation` (SigmaHQ GitHub) with Sysmon-compatible log source for no-SIEM coverage.

**Evidence:** Capture before tuning or clearing any logs: full Security Event Log exports from all Domain Controllers and any endpoints flagged in Step 1; Sysmon operational log (`wevtutil epl Microsoft-Windows-Sysmon/Operational C:\IR\Sysmon.evtx`); browser credential store file metadata (last-accessed timestamps) for Chrome `Login Data`, Edge `Login Data`, and Firefox `logins.json` under each user profile; Windows Credential Manager vault contents (`cmdkey /list` per user context); and Prefetch files (`C:\Windows\Prefetch\`) for credential-dumping tool execution artifacts (e.g., MIMIKATZ.EXE-*.pf, PROCDUMP.EXE-*.pf, RUNDLL32.EXE-*.pf with suspicious arguments).

**Step 3: Eradication — No specific patch ID is confirmed for this zero-day at publication time. Apply all outstanding Windows cumulative updates immediately, prioritizing April and May 2026 security rollups. Rotate credentials for any accounts showing anomalous authentication patterns. Remove or rotate cached credentials on compromised endpoints. Restrict and audit service accounts.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication

**Controls:** NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST CM-6 (Configuration Settings), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

**Compensating:** Until a confirmed CVE and patch KB are published, enumerate and apply all pending Windows security updates via: `Get-WindowsUpdate -Category 'Security Updates' | Install-WindowsUpdate -AcceptAll` (PSWindowsUpdate module) or WUSA with offline MSU packages from Microsoft Update Catalog for air-gapped hosts. For credential rotation without a PAM tool, use the Active Directory PowerShell module: `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString '' -AsPlainText -Force)` for each flagged account. Clear cached credentials on compromised endpoints with `klist purge` (Kerberos) and `cmdkey /delete:` per stored entry. For service accounts, enumerate SPNs to detect Kerberoastable accounts: `Get-ADUser -Filter {ServicePrincipalName -ne '$null'} -Properties ServicePrincipalName` and rotate passwords to 25+ character random strings. Note: because no CVE is confirmed, treat this as a credential-compromise eradication, not a patch-only event.

**Evidence:** Before rotating credentials or applying patches, snapshot: `reg save HKLM\SAM C:\IR\SAM.hive` and `reg save HKLM\SYSTEM C:\IR\SYSTEM.hive` (requires SYSTEM privileges) to preserve the local credential store state for forensic comparison; export all scheduled tasks on flagged hosts (`schtasks /query /fo CSV /v > C:\IR\schtasks.csv`) to detect persistence established during the credential-theft window; enumerate local accounts (`net localgroup administrators`) to identify backdoor accounts; and record all service account last-password-set dates (`Get-ADUser -Filter {ServicePrincipalName -ne '$null'} -Properties PasswordLastSet`) before rotation overwrites the timeline.

**Step 4: Recovery — Validate that Windows Update has applied current cumulative patches across all endpoints. Confirm no persistence mechanisms (scheduled tasks, new local accounts, registry run keys) were introduced during the window of exposure. Monitor authentication logs for 30 days post-remediation for residual access attempts using stolen credentials. Re-verify privileged account integrity.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), NIST CM-6 (Configuration Settings), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

**Compensating:** Validate patch state across endpoints without a management platform using: `Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object -First 10` and compare against the Microsoft Security Update Guide for April–May 2026 rollups. Audit registry Run keys for persistence using: `reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` and `reg query HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` on each remediated host. Audit new local accounts created in the exposure window: `Get-LocalUser | Select-Object Name,Enabled,LastLogon,PasswordLastSet | Where-Object {$_.PasswordLastSet -gt ''}`. For the 30-day authentication monitoring window without SIEM, configure a scheduled PowerShell task to export Event IDs 4624 and 4648 daily and email results to the SOC alias, filtering on previously compromised account UPNs.

**Evidence:** Before returning systems to production, document: current patch level (`systeminfo | findstr /B /C:'OS' /C:'Hotfix'`); a before/after diff of scheduled tasks, local accounts, and Run key entries against the pre-incident baseline captured in Step 3; Sysmon EventID 13 (RegistryValueSet) entries for Run/RunOnce keys created during the exposure window; and Windows Security Event ID 4720 (account created) and 4732 (member added to security-enabled local group) logs from DCs and local hosts to confirm no backdoor accounts survived eradication.

**Step 5: Post-Incident — This campaign highlights two control gaps: insufficient monitoring of credential stores (CWE-522) and reliance on NTLM authentication (CWE-294). Evaluate phased NTLM deprecation per Microsoft guidance. Assess whether endpoint detection coverage includes lsass access monitoring and credential-dumping behavioral signatures. Review AI-assisted threat development as an emerging capability gap in detection engineering timelines.**

**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-2 (Flaw Remediation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** To address the CWE-522 (insufficiently protected credentials) gap without commercial DLP: deploy YARA rules targeting credential-store file access patterns and browser SQLite database reads from non-browser processes (public rules available in the Neo23x0/signature-base repository). For NTLM deprecation planning, audit current NTLM dependency using the Microsoft `NTLM Auditing` Group Policy: enable 'Network Security: Restrict NTLM: Audit Incoming NTLM Traffic' and review Event ID 8004 in the Applications and Services > Microsoft > Windows > NTLM > Operational log before blocking. For detection engineering against AI-accelerated zero-days (where IOC lead time may be hours, not days), prioritize behavioral Sigma rules over IOC-hash rules — specifically the SigmaHQ `credential_access` category covering lsass access, credential manager reads, and browser store access. Submit lessons-learned findings to CISA's Voluntary Reporting portal to contribute to national-level threat intelligence on AI-assisted exploit campaigns.

**Evidence:** For the lessons-learned review, assemble: the full authentication anomaly timeline reconstructed from Event IDs 4624, 4625, 4648, and 4776 exports; Sysmon EventID 10 logs showing lsass access events with source process lineage; a comparison of detection rule coverage before and after the incident (document which Sigma or Sysmon rules would have fired on the observed TTPs — specifically MITRE T1003.001 for lsass memory and T1555.003 for browser credential access); and a gap analysis of NTLM usage from the NTLM Operational log Event ID 8004 audit data collected during the recovery phase.

## Detection Guidance

Focus detection on credential access and lateral movement indicators across Windows environments. Key log sources: Windows Security Event Log (Event IDs 4624, 4625, 4648, 4776, 4688), Sysmon (Event IDs 1, 10 for lsass access, 3 for unexpected outbound connections). Behavioral indicators: unexpected access to lsass.exe;

processes reading from credential stores (Credential Manager, browser stores); NTLM authentication to external or unusual destinations; phishing delivery artifacts (suspicious Office or script execution chains per T1566). No confirmed IOCs (hashes, IPs, domains) are publicly available for this specific campaign at time of publication. Detection rules should be built on behavioral patterns aligned to MITRE T1555, T1078, T1212, and T1566 rather than static indicators. Cross-reference with Microsoft's May 2026 third-party compromise blog for adjacent TTPs. Treat any matches as medium-confidence pending confirmed IOC release.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| DOMAIN | `[none confirmed]` | No IOCs have been publicly released for this specific campaign at time of publication. Monitor threat intelligence feeds for Google Threat Intelligence Group releases. | LOW |

## Framework Mappings

### MITRE-ATTACK

- **T1555** — Credentials from Password Stores
- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1588.005** — Exploits
- **T1212** — Exploitation for Credential Access

### NIST-800-53R5

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

### 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
- **15.1** — Establish and Maintain an Inventory of Service Providers

### HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

### SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

### ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

### NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1555 | Credentials from Password Stores | Credential-Access |
| T1078 | Valid Accounts | Defense-Evasion |
| T1566 | Phishing | Initial-Access |
| T1588.005 | Exploits | Resource-Development |
| T1212 | Exploitation for Credential Access | Credential-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Undermining the trust boundary: Investigating a stealthy intrusion ...** | https://www.microsoft.com/en-us/security/blog/2026/05/12/underminin... | T1 |

| Source | URL | Tier |
|---|---|---|
| **From Stealers to Systems: The New Model of Credential Theft** | https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-di... | T3 |
| **Windows Zero■Day Vulnerability Enables NTLM Credential Theft** | https://petri.com/windows-zero-day-ntlm-credential-theft/ | T3 |
| **Microsoft Confirms Active Exploitation of Windows Shell CVE-2026 ...** | https://thehackernews.com/2026/04/microsoft-confirms-active-exploit... | T3 |
| **Windows vulnerability exploited despite patch - LinkedIn** | https://www.linkedin.com/posts/erickimminau_multiple-attackers-are-... | T3 |



Generated 2026-05-15 06:52 UTC by TJS Security Command Center