INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-06 15:13 UTC

Veil#Drop Multi-Stage Malware Framework Abuses Google Blogspot to Deploy PureLog Stealer

THREAT CAMPAIGN | **HIGH** | CVSS 7.8

SCC Item ID	SCC-CAM-2026-0625
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.8
Affected Products	Windows endpoints targeted via phishing; no specific software product CVE identified
Published	2026-07-06
Discovery Source	Gemini

Executive Summary

Securonix researchers have documented Veil#Drop, a multi-stage malware framework that uses phishing lures and PowerShell loaders hosted on Google Blogspot to deploy PureLog Stealer entirely in memory on Windows endpoints. Because the attack abuses a trusted cloud platform and leaves minimal disk artifacts, conventional perimeter and file-based endpoint controls are largely ineffective. Organizations face credential theft, browser session compromise, and potential follow-on access by attackers who harvest credentials silently from employee workstations.

Technical Analysis

Veil#Drop is a fileless, multi-stage malware delivery framework documented by Securonix targeting Windows endpoints. The kill chain begins with a phishing or social engineering lure (T1566) that delivers an initial payload. That payload retrieves a PowerShell loader (T1059.001) hosted on a legitimate Google Blogger/Blogspot domain, abusing trusted cloud infrastructure to bypass reputation-based network controls (T1608.004, stage hosted on legitimate infrastructure). Subsequent stages leverage living-off-the-land binaries (LOLBins) for reflective or fileless code execution (T1218, system binary proxy execution; T1620, reflective code loading) and obfuscated payloads (T1027.011). The terminal payload is PureLog Stealer, executed entirely in memory, which harvests credentials from browsers and applications (T1555), active browser sessions/cookies (T1539), and exfiltrates data over standard channels (T1041). No CVE is associated with this campaign; exploitation does not depend on an unpatched software vulnerability. Relevant weaknesses include CWE-494 (download of code without integrity check), CWE-78 (OS command injection via LOLBin abuse), and CWE-601

(open redirect, consistent with Blogspot staging abuse). No vendor patch exists, mitigation is entirely detection- and configuration-based. Source: Securonix primary research, corroborated by The Hacker News, Infosecurity Magazine, and HivePro threat advisory.

Action Checklist

1. Step 1: Containment, Block outbound connections to Blogger/Blogspot domains (*.blogspot.com) at the proxy or DNS layer for managed endpoints where legitimate business use does not require it. Review and enforce proxy category policies to flag or block content-hosting platforms used as staging infrastructure. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices).
2. Step 2: Detection, Hunt for LOLBin-based PowerShell execution chains: query EDR and SIEM for PowerShell (T1059.001) invoked by unusual parent processes, PowerShell with encoded or download commands (-EncodedCommand, IEX, DownloadString, Invoke-Expression), and system binaries (e.g., mshta.exe, regsvr32.exe, rundll32.exe, certutil.exe) executing network calls or spawning PowerShell (T1218). Review proxy and DNS logs for outbound GET/POST requests to *.blogspot.com or *.blogger.com originating from endpoint processes rather than browsers. Check process memory and event logs for in-memory stealer indicators (T1620). Reference: NIST AU-2 (Event Logging), AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), D3-SFA (System File Analysis), D3-LAM (Local Account Monitoring).
3. Step 3: Eradication, There is no vendor patch; the attack does not exploit a software CVE. Eradication requires: (1) isolating any endpoint where Veil#Drop activity is confirmed; (2) revoking and rotating all credentials accessible from affected endpoints, including browser-saved passwords, application tokens, and session cookies (NIST AC-3, Access Enforcement); (3) applying PowerShell Constrained Language Mode or AppLocker/WDAC policies to restrict LOLBin abuse (NIST AC-3, Access Enforcement, AC-6, Least Privilege); (4) enforcing script block logging and module logging for PowerShell (NIST AU-12, Audit Record Generation). Reference: CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software).
4. Step 4: Recovery, After credential rotation and endpoint remediation: (1) validate that no persistent scheduled tasks, registry run keys, or WMI subscriptions were established during the infection (check NIST SI-4 equivalent via EDR persistence sweep); (2) confirm proxy/DNS blocks on Blogspot staging domains are active and logging; (3) monitor authentication logs for anomalous access using harvested credentials for at least 30 days post-incident (NIST AU-6, AU-11, Audit Record Retention); (4) verify MFA is enforced on all externally exposed applications and remote access (CIS 6.3, CIS 6.4, CIS 6.5, NIST IA-2, Multi-Factor Authentication).
5. Step 5: Post-Incident, This campaign exposed gaps in: (1) phishing resistance, review and strengthen end-user security awareness training covering social engineering lures; (2) LOLBin and fileless execution controls, assess maturity of application control policies (NIST AC-3, CIS 4.6); (3) credential storage hygiene, evaluate whether browser-saved credentials and session tokens represent an acceptable risk posture (NIST IA-4, Identifier Management); (4) network egress visibility, assess whether DNS and proxy logging provides sufficient fidelity to detect staging-domain abuse in future campaigns (NIST AU-2, CIS 8.2).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal/privacy counsel if forensic analysis confirms PureLog Stealer accessed browser credential stores or session tokens on endpoints with access to systems storing PII, PHI, or financial data, as credential exfiltration to an external actor may trigger breach notification obligations under GDPR, HIPAA, or applicable state data protection laws; also escalate if any rotated credentials show post-rotation successful authentication, indicating active attacker use before containment was complete.
Recovery Notes	After endpoint remediation and credential rotation, maintain a 30-day active watch on authentication logs (Windows Security Event IDs 4624, 4648, 4776) for all accounts that were accessible from affected endpoints, specifically flagging logons from new geolocations, unusual hours, or non-standard user agents that would indicate attacker use of harvested credentials or session cookies before they expired. Verify that proxy and DNS blocking of *.blogspot.com and *.blogger.com is enforced and logging at the process-attribution level before returning any remediated endpoint to production. Confirm that no WMI subscriptions, scheduled tasks, or registry run-key persistence artifacts survive the reimaged or remediated host by running Autoruns (autorunsc.exe) against the clean baseline and diffing against the pre-incident snapshot.
Forensic Artifacts	PowerShell Script Block Logging Event ID 4104 (Microsoft-Windows-PowerShell/Operational log) — will contain the decoded multi-stage Veil#Drop loader content including IEX calls, DownloadString URIs pointing to *.blogspot.com staging pages, and the base64-encoded PureLog Stealer payload prior to in-memory execution | Sysmon Event ID 3 (Network Connection) records — will show non-browser processes (e.g., powershell.exe, mshta.exe) making outbound TCP/443 connections to Google-hosted IP ranges (172.217.0.0/16, 142.250.0.0/15) used by Blogspot, with process GUID linking back to the parent LOLBin execution chain via Sysmon Event ID 1 | Full RAM acquisition (WinPmem/DumpIt output) — the only source for the PureLog Stealer PE image and its in-memory credential harvest buffers, since the payload is designed to leave no on-disk artifact; process memory of any injected or hollowed process will contain the unpacked stealer binary and harvested plaintext credential strings | Browser credential store files pre-rotation: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data (SQLite), %APPDATA%\Mozilla\Firefox\Profiles*.default-release\logins.json and key4.db — hash and preserve these before any remediation action to establish what credentials PureLog Stealer had access to during the infection window | Windows Prefetch files (C:\Windows\Prefetch\) for POWERSHELL.EXE-*.pf, MSHTA.EXE-*.pf, CERTUTIL.EXE-*.pf, REGSVR32.EXE-*.pf — provide execution timestamps and loaded DLL/file references that reconstruct the LOLBin execution chain and establish first-execution time even if Security Event Log has been partially cleared

Per-Action IR Details

Step 1: Containment — Block outbound connections to Blogger/Blogspot domains (*.blogspot.com) at the proxy or DNS layer for managed endpoints where legitimate business use does not require it. Review and enforce proxy category policies to flag or block content-hosting platforms used as staging infrastructure. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices).

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On endpoints without a managed proxy, use Windows Firewall with Advanced Security (netsh advfirewall) or a hosts-file redirect to block *.blogspot.com and *.blogger.com at the OS level. For DNS-layer blocking, configure a local RPZ (Response Policy Zone) on an internal BIND/Unbound resolver, or deploy Pi-hole with a custom blocklist entry for blogger.com and blogspot.com. Confirm blocking with: Resolve-DnsName blogspot.com from an affected endpoint and verify it returns the sinkhole address.

Evidence: Before activating proxy/DNS blocks, capture all outbound HTTP/HTTPS connections in progress from endpoint processes: run 'netstat -ano' or 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}' and cross-reference PIDs against running process list ('Get-Process'). Export proxy access logs showing GET/POST requests to *.blogspot.com or *.blogger.com, preserving originating process name, source IP, timestamp, and full URI — these URLs contain the encoded PowerShell payload paths specific to Veil#Drop staging. Capture DNS query logs from the resolver showing which endpoints resolved blogger.com/blogspot.com and at what times before the block is applied.

Step 2: Detection — Hunt for LOLBin-based PowerShell execution chains: query EDR and SIEM for PowerShell (T1059.001) invoked by unusual parent processes, PowerShell with encoded or download commands (-EncodedCommand, IEX, DownloadString, Invoke-Expression), and system binaries (e.g., mshta.exe, regsvr32.exe, rundll32.exe, certutil.exe) executing network calls or spawning PowerShell (T1218). Review proxy and DNS logs for outbound GET/POST requests to *.blogspot.com or *.blogger.com originating from endpoint processes rather than browsers. Check process memory and event logs for in-memory stealer indicators (T1620). Reference: NIST AU-2 (Event Logging), AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), D3-SFA (System File Analysis), D3-LAM (Local Account Monitoring).

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity or Olaf Hartong's modular config to capture Event ID 1 (Process Create), Event ID 3 (Network Connection), and Event ID 10 (Process Access — for memory injection indicators). Hunt with: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Message -match "EncodedCommand|DownloadString|IEX|Invoke-Expression"}'. Enable PowerShell Script Block Logging (HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging, EnableScriptBlockLogging=1) and review Event ID 4104 in the Microsoft-Windows-PowerShell/Operational log for decoded payload content. Use Sigma rule 'proc_creation_win_powershell_encoded_param.yml' (SigmaHQ) against collected Sysmon logs with chainsaw or sigmac.

Evidence: This is a detection/analysis step that reads live state rather than altering it, but volatile memory must be preserved if a suspect process is found: before any process termination, acquire a full RAM image using WinPmem or DumpIt to recover the PureLog Stealer payload executing entirely in memory, which will leave no on-disk PE artifact. Collect: Windows Security Event Log Event ID 4688 (Process Creation with command line auditing enabled) filtering for powershell.exe, mshta.exe, regsvr32.exe, rundll32.exe, or certutil.exe spawned by atypical parents (e.g., winword.exe, outlook.exe, explorer.exe); PowerShell Script Block Logging Event ID 4104 entries containing decoded IEX or DownloadString calls to blogspot.com URLs; Sysmon Event ID 3 (Network Connection) records from non-browser processes connecting to 172.217.0.0/16 or 142.250.0.0/15 (Google-hosted Blogspot IP ranges); and browser credential store paths (%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data, %APPDATA%\Mozilla\Firefox\Profiles*.default\logins.json) for baseline integrity hashing before any credential sweep.

Step 3: Eradication — There is no vendor patch; the attack does not exploit a software CVE. Eradication requires: (1) isolating any endpoint where Veil#Drop activity is confirmed; (2) revoking and rotating all credentials accessible from affected endpoints, including browser-saved passwords, application tokens, and session cookies (D3-CRO — Credential Rotation); (3) applying PowerShell Constrained Language Mode or AppLocker/WDAC policies to restrict LOLBin abuse (NIST AC-3 — Access Enforcement, AC-6 — Least Privilege); (4) enforcing script block logging and module logging for PowerShell (NIST AU-12 — Audit Record Generation). Reference: CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 4.7 (Manage Default

Accounts on Enterprise Assets and Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-2 (Event Logging), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: For teams without enterprise MDM to push AppLocker/WDAC policies: set PowerShell Constrained Language Mode via registry ('HKLM:\SYSTEM\CurrentControlSet\Control\Session Manager\Environment', add REG_SZ __PSLockdownPolicy = 4) and validate with '$ExecutionContext.SessionState.LanguageMode' returning 'ConstrainedLanguage'. Block mshta.exe, regsvr32.exe, and certutil.exe from making outbound network calls using Windows Firewall rules scoped to those executable paths. Revoke browser-stored credentials manually: clear Chrome Login Data (sqlite3 'Login Data' 'DELETE FROM logins;') and Firefox logins.json, then force password resets for all accounts whose credentials were stored on the affected host.

Evidence: BEFORE isolating the endpoint or revoking credentials, capture in strict order of volatility: (1) full RAM image (WinPmem/DumpIt) to recover the in-memory PureLog Stealer PE and any harvested credential buffers it holds in process heap space; (2) 'Get-NetTCPConnection' and 'netstat -ano' output to document active C2 or exfiltration sessions; (3) running process list with command lines ('Get-Process | Select-Object Id,ProcessName,Path,StartTime' plus 'wmic process get processid,commandline'); (4) Prefetch files from C:\Windows\Prefetch\ for mshta.exe, regsvr32.exe, rundll32.exe, certutil.exe, and powershell.exe to establish execution history and timestamps; (5) export Windows Security Event Log Event ID 4648 (Explicit Credential Use) and 4624/4625 (Logon Success/Failure) to identify credential reuse attempts already in flight before rotation. Only after all volatile evidence is preserved should endpoint isolation and credential revocation proceed.

Step 4: Recovery — After credential rotation and endpoint remediation: (1) validate that no persistent scheduled tasks, registry run keys, or WMI subscriptions were established during the infection (check NIST SI-4 equivalent via EDR persistence sweep); (2) confirm proxy/DNS blocks on Blogspot staging domains are active and logging; (3) monitor authentication logs for anomalous access using harvested credentials for at least 30 days post-incident (NIST AU-6, AU-11 — Audit Record Retention); (4) verify MFA is enforced on all externally exposed applications and remote access (CIS 6.3, CIS 6.4, CIS 6.5, D3-MFA).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), 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: Sweep persistence without EDR using: 'schtasks /query /fo LIST /v | findstr /i "Task To Run\|Status\|Run As"' for scheduled tasks; 'reg query HKCU\Software\Microsoft\Windows\CurrentVersion\Run' and the HKLM equivalent for run keys; and 'Get-WMIObject -Namespace root\subscription -Class __EventFilter' plus '__EventConsumer' and '__FilterToConsumerBinding' for WMI subscriptions. Use Autoruns (Sysinternals) with 'autorunsc.exe -a * -c -h -v -vt' to enumerate and hash all persistence locations, then submit unknown hashes to VirusTotal via its CLI API. For authentication monitoring without SIEM, configure Windows Event Forwarding (WEF) to a central collector and alert on Event ID 4648 and 4776 (NTLM credential validation) for any account that was rotated.

Evidence: This step occurs after containment and eradication; primary volatile evidence should already be captured. However, before restoring the endpoint to production, document the post-remediation baseline: export the full registry hive (reg export HKLM hklm_post_remediation.reg) and scheduled task XML exports ('schtasks /query /xml') to confirm no Veil#Drop persistence artifacts remain. Retain proxy and DNS logs showing the timeline of *.blogspot.com and *.blogger.com resolution events across all endpoints — this establishes the blast-radius boundary (which hosts beaconed to staging infrastructure) and is needed to scope the 30-day credential-monitoring watchlist.

Step 5: Post-Incident — This campaign exposed gaps in: (1) phishing resistance — review and strengthen end-user security awareness training covering social engineering lures; (2) LOLBin and fileless execution controls — assess maturity of application control policies (NIST AC-3, CIS 4.6); (3) credential storage hygiene

— evaluate whether browser-saved credentials and session tokens represent an acceptable risk posture (D3-CH — Credential Hardening, D3-UAP — User Account Permissions); (4) network egress visibility — assess whether DNS and proxy logging provides sufficient fidelity to detect staging-domain abuse in future campaigns (NIST AU-2, CIS 8.2).

NIST Phase: Post Incident

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

Controls: NIST AC-3 (Access Enforcement), NIST AU-2 (Event Logging), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 8.2 (Collect Audit Logs)

Compensating: Conduct a structured lessons-learned session within 5 business days using the NIST 800-61r3 §4 question set. Produce a gap assessment specifically covering: (a) whether PowerShell Script Block Logging (Event ID 4104) and process command-line auditing (Event ID 4688) were enabled on all endpoints before the incident; (b) whether proxy logs captured process-level attribution (i.e., which executable made the request, not just source IP); (c) whether browser credential stores were protected by enterprise policy (e.g., Chrome managed profile blocking local password save via GPO 'PasswordManagerEnabled'=false). Document findings in a risk register entry referencing the Veil#Drop campaign and assign remediation owners with 30/60/90-day target dates.

Evidence: Assemble the post-incident evidence package for the lessons-learned review: the full timeline reconstructed from Sysmon Event ID 1/3 logs, PowerShell Script Block Event ID 4104 decoded payload content, proxy logs showing the initial Blogspot staging domain fetch, memory forensics output confirming PureLog Stealer execution scope (which credential stores were accessed in-process), and the credential-rotation log showing which accounts were revoked and when. This package establishes the dwell-time window, confirms whether any harvested credentials were used before rotation, and provides the IOC set (Blogspot staging URLs, PowerShell payload hashes, injected process names) needed to update detection rules for future Veil#Drop-family campaigns.

Detection Guidance

Primary detection surface is process execution telemetry and proxy/DNS logs. Key behavioral indicators based on the documented Veil#Drop kill chain: (1) PowerShell spawned by unusual parent processes (Office applications, script hosts, LOLBins such as mshta.exe, regsvr32.exe, rundll32.exe, certutil.exe), map to T1218 and T1059.001; (2) PowerShell command lines containing IEX, Invoke-Expression, DownloadString, or -EncodedCommand strings alongside outbound network calls; (3) Outbound DNS queries or HTTP/HTTPS connections to *.blogspot.com or *.blogger.com from processes other than user browsers, particularly from PowerShell or LOLBin processes, map to T1608.004; (4) Reflective loading indicators: in-memory .NET assembly loading, PowerShell runspace creation outside expected tooling, map to T1620; (5) Credential access patterns: access to browser credential stores (e.g., Login Data SQLite files in Chromium-based browsers), DPAPI calls from unexpected processes, map to T1555 and T1539; (6) Anomalous data transfer from endpoints to external IPs, particularly following a LOLBin execution chain, map to T1041. Relevant log sources: EDR process telemetry, Windows Event Log (PowerShell script block logging, Event IDs 4104, 4103; process creation, Event ID 4688 with command-line auditing enabled), proxy/web gateway logs, DNS query logs. Reference: NIST AU-2 (Event Logging), AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`*.blogspot.com`	Reported staging domain pattern used to host Veil#Drop PowerShell loaders; legitimate domain abused as infrastructure — block/alert on non-browser process connections only	MEDIUM
DOMAIN	`*.blogger.com`	Associated Google platform domain; reported as part of the same staging infrastructure abuse pattern	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1218** — System Binary Proxy Execution
- **T1608.004** — Drive-by Target
- **T1041** — Exfiltration Over C2 Channel
- **T1620** — Reflective Code Loading
- **T1027.011** — Fileless Storage
- **T1059.001** — PowerShell
- **T1555** — Credentials from Password Stores
- **T1566** — Phishing
- **T1539** — Steal Web Session Cookie

NIST-800-53R5

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

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A03:2021** — Injection

CIS-V8

- **2.5** — Allowlist Authorized Software

- **2.6** — Allowlist Authorized Libraries
- **16.10** — Apply Secure Design Principles in Application Architectures
- **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(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
- **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
T1218	System Binary Proxy Execution	Defense-Evasion
T1608.004	Drive-by Target	Resource-Development
T1041	Exfiltration Over C2 Channel	Exfiltration
T1620	Reflective Code Loading	Defense-Evasion
T1027.011	Fileless Storage	Defense-Evasion
T1059.001	PowerShell	Execution
T1555	Credentials from Password Stores	Credential-Access
T1566	Phishing	Initial-Access
T1539	Steal Web Session Cookie	Credential-Access

Sources

Source	URL	Tier
VEIL#DROP: Blogspot-Hosted PowerShell Loader	https://www.securonix.com/blog/veildrop-blogspot-hosted-powershell-...	T3
VEIL#DROP Malware Chain Uses Blogger Platform to ...	https://thehackernews.com/2026/07/veildrop-malware-chain-uses-blogg...	T2
Veil#Drop Uses Google Blogspot to Deploy PureLog Stealer	https://www.infosecurity-magazine.com/news/veil-drop-blogspot-purel...	T2
Veil#Drop Abuses Google Blogspot to Deliver Fileless ...	https://www.hivepro.com/threat-advisory/veil-drop-abuses-google-blo...	T3
VEIL#DROP Uses Blogspot and LOLBins to Deploy PureLogs ...	https://www.mallory.ai/stories/019f1f17-7fe6-724c-ae24-cf3ead658b7c	T3

Generated 2026-07-06 15:13 UTC by TJS Security Command Center