INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-02 14:02 UTC

DriveSurge IAB Operates Mass Drive-By Campaign Using ClickFix and FakeUpdates Across Thousands of Hijacked Sites

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0394
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	All major browsers (Chrome, Firefox, Edge, Safari, Opera, Brave, Yandex, Vivaldi, Samsung Internet, UC Browser) on Windows and macOS endpoints; thousands of compromised legitimate websites used as delivery infrastructure
Published	2026-06-01T18:14:19
Discovery Source	Rss

Executive Summary

A threat actor called DriveSurge has compromised thousands of legitimate, high-reputation websites and is using them to redirect visitors toward malware delivery pages. Any employee browsing the web from a corporate device is a potential victim, regardless of whether the site they visit appears trustworthy. Because DriveSurge sells access to infected machines to other criminal groups, the downstream malware is unpredictable and may include ransomware, data stealers, or remote access tools.

Technical Analysis

DriveSurge operates as an initial access broker (IAB) running a mass drive-by delivery campaign across thousands of compromised legitimate websites. The campaign uses two social engineering lure frameworks: ClickFix, which prompts users to run malicious PowerShell or clipboard-injected commands under the pretext of fixing a browser or application error, and FakeUpdates (SocGholish-style), which serves fake browser update prompts. Traffic routing and victim fingerprinting are handled by zTDS, an open-source traffic distribution system that selects the contextually appropriate lure per visitor profile. Because DriveSurge is a pay-per-install IAB, there is no fixed second-stage payload, downstream malware varies by purchasing threat actor and may include information stealers, ransomware loaders, RATs, or commodity malware. All major browsers on Windows and macOS are affected delivery surfaces. Relevant MITRE ATT&CK techniques include T1189 (Drive-by Compromise), T1566 (Phishing), T1059.001 (PowerShell), T1204.002 (Malicious File execution), T1608.004

(Stage Capabilities: Drive-by Target), T1583.008 (Acquire Infrastructure: Malvertising), T1090.002 (External Proxy), T1105 (Ingress Tool Transfer), T1027 (Obfuscated Files or Information), and T1071.001 (Application Layer Protocol: Web Protocols). Applicable CWEs: CWE-20 (Improper Input Validation), CWE-116 (Improper Encoding/Escaping of Output), CWE-494 (Download of Code Without Integrity Check). No CVE is assigned; this is a campaign-level threat, not a product vulnerability. Primary research attributed to Silent Push (silentpush.com/blog/drivesurge).

Action Checklist

1. Step 1: Containment, Block known DriveSurge-associated domains and zTDS infrastructure at the web proxy and DNS layer immediately. Restrict PowerShell execution policy on endpoints to prevent clipboard-injected command execution (set to 'AllSigned' or 'Restricted' via Group Policy). Disable or alert on clipboard-based PowerShell invocation patterns at the endpoint. Reference: CIS Controls v8 4.4, CIS 4.5 (host-based firewall and filtering on endpoints and servers).
2. Step 2: Detection, Query endpoint detection logs for PowerShell processes spawned from browser parent processes (e.g., chrome.exe, firefox.exe, msedge.exe spawning powershell.exe or cmd.exe). Search DNS and proxy logs for connections to zTDS-associated redirect domains identified in Silent Push research. Hunt for CWE-494 indicators: unsigned or unverified executable downloads initiated from browser sessions. Review SIEM for T1204.002 (user-executed malicious files) and T1059.001 (PowerShell) correlated with web browsing activity. Relevant controls: NIST AU-6 (audit record review and analysis), NIST SI-4 (system monitoring).
3. Step 3: Eradication, On any endpoint where ClickFix or FakeUpdates lure execution is confirmed, isolate the host, capture a memory image for forensic review, and initiate full credential rotation for accounts active on that device (D3-CRO: Credential Rotation). Remove any dropped payloads identified during forensic triage. Block the execution of unsigned scripts enterprise-wide. Apply application allowlisting to prevent unauthorized executable downloads per CIS Controls v8 2.3 (Address Unauthorized Software).
4. Step 4: Recovery, Validate that PowerShell execution policy restrictions are enforced across all endpoints via Group Policy and confirm via compliance scan. Re-image any endpoint where second-stage malware execution is confirmed rather than attempting in-place remediation. Monitor reinstated endpoints for 30 days using enhanced behavioral telemetry. Verify no persistent mechanisms (scheduled tasks, registry run keys) were installed by the dropped payload. Reference: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring).
5. Step 5: Post-Incident, Conduct a user awareness review focused on ClickFix and FakeUpdates social engineering lures; users must be able to recognize fake browser update prompts and clipboard-paste command instructions as attack vectors. Evaluate whether web content filtering categorizes compromised-but-legitimate sites differently than known-malicious domains, this campaign demonstrates that reputation-based filtering alone is insufficient. Implement DNS-layer filtering (e.g., via a secure DNS resolver) to catch zTDS redirect chains before browser-level delivery. Reference: NIST AC-17 (Remote Access controls for browsing), CIS Controls v8 7.1 (Vulnerability Management Process), D3-UAP (User Account Permissions) to limit blast radius of any successful infection.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if forensic triage confirms execution of a second-stage payload (info-stealer, RAT, or ransomware precursor) on any endpoint with access to PII, PHI, PCI-scoped systems, or privileged credentials, as this triggers breach notification assessment obligations and may indicate DriveSurge has already sold access to a downstream ransomware operator.
Recovery Notes	Re-image all endpoints with confirmed second-stage execution — do not attempt in-place remediation given DriveSurge's IAB model means the downstream payload type is unknown and may include rootkit-capable malware. Reinstated endpoints must be monitored for a minimum of 30 days with Sysmon Event ID 1 alerting specifically on browser-to-shell parent-child process chains, as DriveSurge infrastructure has demonstrated the ability to re-compromise endpoints through repeat visits to still-compromised legitimate sites. Validate that DNS-layer blocking of zTDS infrastructure remains effective by reviewing DNS resolver logs weekly against updated Silent Push IOC exports for the duration of the 30-day monitoring window.
Forensic Artifacts	Sysmon Event ID 1 (Process Create) logs showing chrome.exe, firefox.exe, msedge.exe, brave.exe, or opera.exe as ParentImage with powershell.exe or cmd.exe as Image — the direct forensic signature of a ClickFix clipboard-injected command execution on a DriveSurge-compromised site | Browser download history and %TEMP% / %APPDATA%\Local\Temp directory contents for executables with names mimicking browser updates (e.g., ChromeSetup.exe, FirefoxUpdate.exe, EdgeInstaller.exe) written during the suspect browsing session — FakeUpdates' characteristic payload delivery artifact | Windows DNS Client event log (Microsoft-Windows-DNS-Client/Operational) and proxy access logs showing rapid sequential resolution of multiple high-entropy or newly-registered domains within a single browsing session, consistent with the zTDS traffic distribution system redirect chain | Registry keys HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, and HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce exported at time of triage, plus output of 'schtasks /query /fo LIST /v' — persistence mechanisms commonly installed by second-stage RAT or stealer payloads acquired through DriveSurge's IAB marketplace | Browser extension directories (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\; Edge: %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Extensions\) inspected for recently-added or modified extensions with broad host permissions, as FakeUpdates delivery chains have historically included malicious browser extension installation as a persistence and credential-harvesting mechanism

Per-Action IR Details

Step 1: Containment — Block known DriveSurge-associated domains and zTDS infrastructure at the web proxy and DNS layer immediately. Restrict PowerShell execution policy on endpoints to prevent clipboard-injected command execution (set to 'AllSigned' or 'Restricted' via Group Policy). Disable or alert on clipboard-based PowerShell invocation patterns at the endpoint. Reference: CIS 4.4, CIS 4.5 (host-based firewall and filtering on endpoints and servers).

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CM-7 (Least Functionality), NIST AC-3 (Access Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 9.2 — Use DNS Filtering Services (IG2/IG3)

Compensating: For teams without a commercial proxy: deploy Pi-hole or BIND RPZ (Response Policy Zone) with DriveSurge/zTDS IOC feeds exported from Silent Push or URLhaus to block redirect domains at DNS. Enforce PowerShell policy via Group Policy Object (GPO): Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies, or run: 'Set-ExecutionPolicy AllSigned -Scope LocalMachine -Force' pushed via a startup script. Deploy Sysmon with SwiftOnSecurity config to log Event ID 1 (Process Create) and capture parent-child chains showing browsers spawning powershell.exe or cmd.exe.

Evidence: Before hardening the GPO, capture the current PowerShell execution policy baseline across endpoints using: 'Invoke-Command -ComputerName -ScriptBlock {Get-ExecutionPolicy -List}' — document any endpoints already set to Unrestricted or Bypass, as these are highest-risk hosts. Export current DNS resolver cache on endpoints ('Get-DnsClientCache | Export-Csv dns_cache_baseline.csv') to preserve pre-containment resolution history showing any zTDS redirect chain lookups before blocking takes effect.

Step 2: Detection — Query endpoint detection logs for PowerShell processes spawned from browser parent processes (e.g., chrome.exe, firefox.exe, msedge.exe spawning powershell.exe or cmd.exe). Search DNS and proxy logs for connections to zTDS-associated redirect domains identified in Silent Push research. Hunt for CWE-494 indicators: unsigned or unverified executable downloads initiated from browser sessions. Review SIEM for T1204.002 (user-executed malicious files) and T1059.001 (PowerShell) correlated with web browsing activity. Relevant controls: NIST AU-6 (audit record review and analysis), NIST SI-4 (system 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), NIST SI-4 (System Monitoring), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), MITRE ATT&CK T1204.002 — User Execution: Malicious File, MITRE ATT&CK T1059.001 — Command and Scripting Interpreter: PowerShell, MITRE ATT&CK T1566.002 — Phishing: Spearphishing Link (drive-by delivery variant)

Compensating: Without a SIEM, run the following PowerShell query across endpoints to detect browser-spawned shells from Sysmon Event ID 1 logs: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Id -eq 1} | Where-Object {$_.Message -match "powershell|cmd.exe" -and $_.Message -match "chrome|firefox|msedge|brave|opera"} | Select-Object TimeCreated, Message | Export-Csv browser_shell_hunt.csv'. For DNS hunting without a commercial tool, export Windows DNS debug log or router syslog and grep for known zTDS TLD patterns (e.g., domains with high-entropy subdomains resolving to bulletproof hosting ASNs). Use Sigma rule 'proc_creation_win_powershell_parent_process_suspicious' against Sysmon logs via sigmac converted to PowerShell or Splunk.

Evidence: Collect Sysmon Event ID 1 (Process Create) entries where ParentImage matches any browser executable and Image matches powershell.exe, cmd.exe, wscript.exe, or mshta.exe — this is the precise execution chain produced when a ClickFix lure instructs the victim to paste a clipboard-injected command. Capture Sysmon Event ID 7 (Image Load) for unsigned DLLs loaded by browser processes, and Event ID 11 (File Create) for executables written to %TEMP%, %APPDATA%, or %PUBLIC% directories immediately following the browser session. Pull Windows DNS Client event log (Microsoft-Windows-DNS-Client/Operational, Event ID 3008 for failed queries) alongside successful resolutions from proxy access logs filtered on the timeframe of the browser session — zTDS redirect chains typically produce a sequence of rapid successive DNS lookups across multiple domains before delivering the payload.

Step 3: Eradication — On any endpoint where ClickFix or FakeUpdates lure execution is confirmed, isolate the host, capture a memory image for forensic review, and initiate full credential rotation for accounts active on that device (D3-CRO: Credential Rotation). Remove any dropped payloads identified during forensic triage. Block the execution of unsigned scripts enterprise-wide. Apply application allowlisting to prevent unauthorized executable downloads per CIS 2.3 (Address Unauthorized Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST AC-2 (Account Management), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 5.3

(Disable Dormant Accounts), CIS 6.2 (Establish an Access Revoking Process), MITRE ATT&CK T1059.001 — PowerShell, MITRE ATT&CK T1547.001 — Boot or Logon Autostart Execution: Registry Run Keys

Compensating: Use WinPmem (free, open-source) or DumpIt for memory acquisition before isolation to preserve in-memory indicators of second-stage payloads delivered via DriveSurge's IAB infrastructure (e.g., in-memory RATs or stealers that never touch disk). After isolation, run ClamAV with the latest signaturedatabase against %TEMP%, %APPDATA%\Roaming, %APPDATA%\Local\Temp, and browser download directories to identify FakeUpdates-themed executable drops (commonly named as browser_update.exe, ChromeSetup.exe, or similar). For credential rotation scoping without a SIEM, run 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624} | Where-Object {$_.TimeCreated -gt [datetime]""}' to enumerate all accounts that authenticated on the compromised host during the suspect window.

Evidence: Before eradication actions, preserve: (1) Full memory image capturing any injected shellcode or in-memory stealer payloads (DriveSurge downstream malware commonly includes info-stealers operating entirely in memory); (2) a forensic copy of browser profile directories (Chrome: %LOCALAPPDATA%\Google\Chrome\User Data\Default\; Edge: %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\) which may contain injected extensions or modified preferences used as persistence by FakeUpdates payloads; (3) Windows Prefetch files from C:\Windows\Prefetch\ for any executables with names matching fake browser update patterns to establish first-execution timestamps; (4) Registry export of HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM\Software\Microsoft\Windows\CurrentVersion\Run to capture any autostart persistence installed by the dropped second-stage payload.

Step 4: Recovery — Validate that PowerShell execution policy restrictions are enforced across all endpoints via Group Policy and confirm via compliance scan. Re-image any endpoint where second-stage malware execution is confirmed rather than attempting in-place remediation. Monitor reinstated endpoints for 30 days using enhanced behavioral telemetry. Verify no persistent mechanisms (scheduled tasks, registry run keys) were installed by the dropped payload. Reference: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST CM-6 (Configuration Settings), NIST SI-2 (Flaw Remediation), NIST CP-10 (System Recovery and Reconstitution), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Without an enterprise compliance scanner, validate PowerShell policy enforcement using: 'Invoke-Command -ComputerName -ScriptBlock {Get-ExecutionPolicy -List | Where-Object {$_.ExecutionPolicy -notin @("AllSigned","Restricted")}} | Export-Csv policy_audit.csv' — any result returned indicates a non-compliant endpoint. For scheduled task persistence verification on re-imaged or suspect hosts, run: 'schtasks /query /fo LIST /v > scheduled_tasks_full.txt' and filter for tasks with actions referencing PowerShell, cmd.exe, wscript.exe, or paths under %TEMP% or %APPDATA%. Use Sysmon Event ID 1 with enhanced logging on reinstated endpoints for 30 days, specifically alerting on any browser process spawning a child process — the behavioral signature that triggered this incident.

Evidence: Before returning an endpoint to production, collect and retain: the post-reimaging GPO compliance report confirming AllSigned/Restricted policy is applied; a scheduled task export ('schtasks /query /fo CSV /v > baseline_tasks.csv') and registry run key export from the clean build to establish a verified baseline for the 30-day monitoring period; and a Sysmon operational log snapshot from the first 48 hours of reinstated endpoint activity, which serves as forensic confirmation that no dormant persistence mechanisms survived the reimaging process or were reintroduced via a shared network drive or user profile roaming.

Step 5: Post-Incident — Conduct a user awareness review focused on ClickFix and FakeUpdates social engineering lures; users must be able to recognize fake browser update prompts and clipboard-paste command instructions as attack vectors. Evaluate whether web content filtering categorizes compromised-but-legitimate sites differently than known-malicious domains — this campaign demonstrates

that reputation-based filtering alone is insufficient. Implement DNS-layer filtering (e.g., via a secure DNS resolver) to catch zTDS redirect chains before browser-level delivery. Reference: NIST AC-17 (Remote Access controls for browsing), CIS 7.1 (Vulnerability Management Process), D3-UAP (User Account Permissions) to limit blast radius of any successful infection.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST AT-2 (Literacy Training and Awareness), NIST AT-3 (Role-Based Training), NIST SI-4 (System Monitoring), NIST AC-17 (Remote Access), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For DNS-layer filtering without a commercial resolver contract, configure Cloudflare Gateway (free tier) or Quad9 (free, malware-blocking) as the enterprise DNS resolver — both block known malicious domains including active threat actor infrastructure and can intercept zTDS redirect chains before the browser receives the redirect response. To measure user susceptibility to ClickFix lures specifically, run a targeted phishing simulation using GoPhish (free, open-source) with a scenario replicating the fake browser update modal and clipboard-paste instruction — this directly tests the social engineering vector DriveSurge exploits rather than a generic email phishing scenario.

Evidence: For the post-incident lessons learned review, compile: proxy and DNS logs showing the full population of employees who visited any DriveSurge-compromised site during the campaign window (not just confirmed victims) to establish the true exposure scope; a categorization audit from your web filter showing how the compromised legitimate sites were classified at time of visit (expected result: 'Business/News/Reference' — trusted categories) versus how known DriveSurge delivery domains were classified, documenting the gap that reputation-based filtering could not close; and incident timeline reconstruction showing first zTDS redirect observed in logs versus when containment blocks were applied, to quantify detection-to-containment dwell time for the lessons learned report per NIST 800-61r3 §4.

Detection Guidance

Primary detection focus: browser-to-shell process chains and unsigned payload downloads. (1) EDR/endpoint logs, alert on powershell.exe or cmd.exe with a parent process of any major browser (chrome.exe, firefox.exe, msedge.exe, brave.exe, vivaldi.exe). This is the canonical ClickFix execution signature. (2) DNS and proxy logs, query for resolution of domains associated with zTDS traffic distribution infrastructure. Silent Push's research (silentpush.com/blog/drivesurge) contains domain and IP indicators; import these into your threat intelligence platform and run historical lookups against DNS/proxy logs for the past 90 days. (3) Endpoint file system, look for unsigned executable files downloaded to %TEMP% or %APPDATA% directories from browser processes, consistent with CWE-494 (Download of Code Without Integrity Check). (4) SIEM correlation rule, correlate T1189 (Drive-by Compromise) browser download events with T1059.001 (PowerShell) execution within a 5-minute window on the same host. (5) Clipboard abuse, some ClickFix variants instruct users to paste commands into Run dialogs; monitor for Win+R followed by clipboard paste patterns where clipboard content contains encoded PowerShell. (6) Network, inspect for HTTP traffic matching FakeUpdates delivery patterns: JavaScript-heavy redirects from legitimate domains that serve .js dropper files. Relevant controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review), NIST SI-4 (System Monitoring), CIS Controls v8 8.2 (Collect Audit Logs).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	See Silent Push research at silentpush.com/blog/drivesurge for zTDS-associated domains	DriveSurge zTDS traffic distribution and redirect infrastructure — specific IOC list maintained by Silent Push	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1189** — Drive-by Compromise
- **T1608.004** — Drive-by Target
- **T1059.001** — PowerShell
- **T1583.008** — Malvertising
- **T1090.002** — External Proxy
- **T1105** — Ingress Tool Transfer
- **T1027** — Obfuscated Files or Information
- **T1204.002** — Malicious File
- **T1071.001** — Web Protocols

NIST-800-53R5

- **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
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **SI-10** — Information Input Validation
- **CP-9** — System Backup
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

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
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1189	Drive-by Compromise	Initial-Access
T1608.004	Drive-by Target	Resource-Development
T1059.001	PowerShell	Execution
T1583.008	Malvertising	Resource-Development
T1090.002	External Proxy	Command-And-Control
T1105	Ingress Tool Transfer	Command-And-Control
T1027	Obfuscated Files or Information	Defense-Evasion
T1204.002	Malicious File	Execution
T1071.001	Web Protocols	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/hackers-hijack-thous...	T3
Chrome, Brave, Edge, Vivaldi Updates Fix 151 Security ... - YouTube	https://www.youtube.com/watch?v=oDD6i9322kE	T3
One of the internet's most popular browsers has a security flaw, and ...	https://www.facebook.com/kimkomando/posts/one-of-the-internets-most...	T3
Meet DriveSurge: A New Threat Actor Using ClickFix and Fake ...	https://www.silentpush.com/blog/drivesurge/	T3
Firefox, Chrome each fix more than a dozen vulnerabilities - Intego	https://www.intego.com/mac-security-blog/firefox-chrome-each-fix-mo...	T3

Generated 2026-06-02 14:02 UTC by TJS Security Command Center