INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:40 UTC

Laundry Bear Deploys Browser-as-Backdoor: DRILLAPP Abuses Headless Edge and Chrome DevTools Protocol Against Ukrainian Targets

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0027
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Edge (headless mode), Chromium-based browsers, Windows (LNK and Control Panel module infection vectors)
Published	2026-03-16

Executive Summary

A Russian state-linked threat actor, Laundry Bear (also tracked as UAC-0190 and Void Blizzard), conducted a targeted espionage campaign against Ukrainian government entities in [February 2025], deploying a JavaScript backdoor called DRILLAPP. The malware runs inside Microsoft Edge in headless mode, a trusted and commonly allowlisted process, enabling covert access to cameras, microphones, screens, and the file system without triggering standard endpoint alerts. Organizations with remote workers, diplomatic missions, or operational ties to Ukraine face elevated risk of silent credential and data exfiltration through this technique.

Technical Analysis

DRILLAPP is a JavaScript backdoor that executes entirely within Microsoft Edge running in headless mode (--headless flag), abusing the Chrome DevTools Protocol (CDP) to bypass JavaScript's native file access restrictions. CDP provides low-level browser control typically used for testing and automation; DRILLAPP repurposes it to access the camera (T1125), microphone (T1123), screen (T1113), and file system (T1083) without user interaction. Initial access is achieved via malicious LNK files (T1566) and Windows Control Panel module (.cpl) abuse (T1218), consistent with prior Laundry Bear tradecraft. Persistence is established via Registry Run keys (T1547.001). The malware uses obfuscation (T1027), JavaScript execution (T1059.007), and web services for C2 communication (T1102.001, T1071.001). Because Edge is a signed Microsoft binary and headless operation is a legitimate enterprise use case, process-based allowlisting and many behavioral detection rules do not fire. No CVE is assigned to this campaign; the attack exploits legitimate browser

functionality rather than a patched vulnerability. Relevant CWEs: CWE-693 (Protection Mechanism Failure), CWE-73 (External Control of File Name or Path), CWE-276 (Incorrect Default Permissions). MITRE ATT&CK techniques mapped include T1566, T1564.003, T1083, T1071, T1056.001, T1113, T1547.001, T1027, T1125, T1059.007, T1218, T1105, T1547, T1102.001, T1071.001, T1123. No patch addresses this technique; mitigation requires configuration and detection controls.

Action Checklist

1. Step 1 (Immediate): Audit Group Policy and endpoint configurations to determine whether headless browser execution (msedge.exe --headless or chrome.exe --headless) is permitted or blocked; restrict headless mode via application control policy or GPO where not operationally required.
2. Step 2 (Detection): Search EDR and process logs for msedge.exe or chrome.exe launched with --headless, --remote-debugging-port, or --disable-gpu flags from unusual parent processes (e.g., explorer.exe, rundll32.exe, control.exe); alert on CDP port activity (default 9222) originating from browser processes outside sanctioned automation pipelines.
3. Step 3 (Detection): Hunt for LNK files created in user-writeable directories (Downloads, Temp, AppData) with unusual targets or arguments; monitor for Control Panel module (.cpl) execution via rundll32.exe or shell32.dll outside expected administrative workflows (T1218).
4. Step 4 (Assessment): Inventory systems with Microsoft Edge installed; identify any endpoints where Edge or Chromium-based browsers are allowlisted at the process level in EDR or application control tools without behavioral sub-controls; prioritize endpoints belonging to users with access to sensitive government, diplomatic, or Ukraine-related operational data.
5. Step 5 (Communication): Notify SOC and threat intelligence teams of active Laundry Bear / UAC-0190 / Void Blizzard targeting; if your organization has ties to Ukrainian government entities or operates in relevant sectors and CISA has published a related advisory, escalate to leadership and consider sharing indicators with your sector-specific ISAC.
6. Step 6 (Long-term): Update detection engineering rules to cover headless browser abuse as a persistent technique class, not just this campaign; review allowlisting policies to ensure signed Microsoft binaries are subject to behavioral controls, not blanket trust; incorporate T1218 (System Binary Proxy Execution) and T1564.003 (Hidden Window) into red team scope for the next assessment cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal immediately if any endpoints belonging to users with Ukraine-related operational access are confirmed compromised; engage external DFIR firm if more than five endpoints show evidence of DRILLAPP deployment or successful credential theft.
Recovery Notes	Post-containment: disconnect affected endpoints from network, image hard drives before remediation, analyze captured artifacts for lateral movement or data exfiltration indicators. Rebuild compromised systems from known-good media after forensic analysis completes. Reset credentials for all users who accessed sensitive systems from affected endpoints within 90 days prior to detection. Implement continuous behavioral monitoring on restored endpoints for 60 days to catch any re-infection.

Forensic Artifacts	Windows Event Log Security channel (4688 Process Creation, 4689 Process Terminated, 4657 Registry value modified) | NTFS $MFT (Master File Table) and $USN Journal for file creation/deletion timeline reconstruction | Windows Prefetch files (C:\Windows\Prefetch*.pf) for process execution history and command-line arguments | Windows Registry hives (NTUSER.DAT, SOFTWARE, SYSTEM) for browser policies, installed applications, and Run/RunOnce keys | Browser cache, cookies, and DevTools session artifacts (C:\Users*\AppData\Local\Microsoft\Edge\User Data\Default\Cache; C:\Users*\AppData\Local\Google\Chrome\User Data\Default\Cache)

Per-Action IR Details

Step 1 (Immediate): Audit Group Policy and endpoint configurations to determine whether headless browser execution (msedge.exe --headless or chrome.exe --headless) is permitted or blocked; restrict headless mode via application control policy or GPO where not operationally required.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and policies)

Controls: NIST 800-53 SI-7 (Software, firmware, and information integrity), NIST 800-53 AC-6 (Least privilege), CIS Controls v8 2.4 (Address unauthorized software)

Compensating: On each endpoint, run `Get-AppLockerPolicy -Effective | Export-Clixml` (PowerShell) to export current AppLocker rules; manually audit for headless exclusions. If AppLocker unavailable, create a GPO that denies execution of msedge.exe and chrome.exe with command-line arguments containing '--headless' using Image File Execution Options registry hive (HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options). Test with `tasklist /v | findstr headless` after policy deployment.

Evidence: Before restricting: capture Group Policy Report (`gpresult /h report.html`), current AppLocker effective policy export, and registry export of HKLM\Software\Policies\Microsoft\Windows\AppCompat. Document baseline allowed processes via `Get-Process | Export-Csv baseline.csv` to validate no production services rely on headless execution.

Step 2 (Detection): Search EDR and process logs for msedge.exe or chrome.exe launched with --headless, --remote-debugging-port, or --disable-gpu flags from unusual parent processes (e.g., explorer.exe, rundll32.exe, control.exe); alert on CDP port activity (default 9222) originating from browser processes outside sanctioned automation pipelines.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Detection and Analysis: anomaly detection)

Controls: NIST 800-53 SI-4 (Information system monitoring), NIST 800-53 AU-12 (Audit generation), CIS Controls v8 8.5 (Log all access and changes to sensitive data)

Compensating: Use Windows Event Log 4688 (Process Creation) with command-line auditing enabled via Group Policy (Computer Config > Policies > Admin Templates > System > Audit Process Creation). Query manually: `wevtutil qe Security /q:*[System[(EventID=4688)] and EventData[Data[@Name='CommandLine'] and (contains(., '--headless') or contains(., '--remote-debugging-port') or contains(., '--disable-gpu'))]]* /f:text`. For CDP port detection without EDR, enable NetFlow or configure Windows Firewall to log outbound connections to port 9222 via `netsh advfirewall firewall add rule name='Log CDP Port' dir=out action=allow protocol=tcp remoteport=9222 profile=any logonname=allow`; parse logs hourly with `wevtutil qe Security /q:*[System[(EventID=5156)]] | findstr 9222`.

Evidence: Capture all instances of Windows Event Log 4688 (Process Creation) for msedge.exe and chrome.exe for the past 30 days; Windows Event Log 4657 (Registry value modified) tracking HKLM\Software\Microsoft\EdgeUpdate and HKLM\Software\Google\Chrome; Windows Firewall logs (C:\Windows\System32\logfiles\Firewall\pfirewall.log) filtered for port 9222; network packet capture (tcpdump or Wireshark) from any network tap showing port 9222 connections; EDR process tree exports showing parent-child relationships.

Step 3 (Detection): Hunt for LNK files created in user-writeable directories (Downloads, Temp, AppData) with unusual targets or arguments; monitor for Control Panel module (.cpl) execution via rundll32.exe or

shell32.dll outside expected administrative workflows (T1218).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Deep investigation of malware artifacts)

Controls: NIST 800-53 SI-3 (Malware protection), NIST 800-53 CA-7 (Continuous monitoring), CIS Controls v8 2.1 (Inventory all software)

Compensating: Search all user-writeable directories for .lnk files created in the past 60 days: `forfiles /S /M *.lnk /D +60 /C "cmd /c @path >> lnk_inventory.txt"". Extract LNK target and arguments using a free tool like `lnk-parser` (GitHub: Matlog/lnk-parser) or WinHexEditor; parse each LNK header for TargetPath field. Monitor rundll32.exe execution: query Event Log 4688 for `rundll32.exe` with arguments matching `*.cpl` patterns: `wevtutil qe Security /q:*[System[(EventID=4688)] and EventData[Data[@Name='CommandLine'] and contains(., '.cpl')]]* | findstr rundll32`. Establish baseline of legitimate .cpl calls (e.g., from Control Panel processes) and alert on deviations.

Evidence: Export all .lnk file metadata from (%USERPROFILE%\Downloads, %TEMP%, %APPDATA%) including file creation/modification timestamps, target path, arguments, icon location, and hotkey fields; Windows Event Log 4688 for all rundll32.exe and shell32.dll executions with .cpl arguments for the past 30 days; NTFS $MFT (Master File Table) from forensic image to recover deleted .lnk files and establish creation timeline; Windows Prefetch files (C:\Windows\Prefetch\) for rundll32.exe and shell32.dll to identify execution frequency and parameters.

Step 4 (Assessment): Inventory systems with Microsoft Edge installed; identify any endpoints where Edge or Chromium-based browsers are allowlisted at the process level in EDR or application control tools without behavioral sub-controls; prioritize endpoints belonging to users with access to sensitive government, diplomatic, or Ukraine-related operational data.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: asset inventory and prioritization)

Controls: NIST 800-53 CM-8 (Information system component inventory), NIST 800-53 AC-2 (Account management and access control), CIS Controls v8 1.1 (Establish and maintain detailed asset inventory)

Compensating: Query Active Directory for all endpoints: `Get-ADComputer -Filter * -Properties Name,OperatingSystem | Export-Csv endpoints.csv`. On each endpoint, check for Edge/Chrome installation via registry query: `reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall" | findstr /I "edge chrome"` or via WMI: `Get-WmiObject -Class Win32_Product | Where-Object {$_.Name -match "Edge|Chrome"} | Export-Csv installed_browsers.csv`. Cross-reference sensitive user accounts (pulled from AD security groups for government/diplomatic roles) with endpoint inventory. Check EDR/AppLocker policies: export allow-lists and flag any entry with msedge.exe or chrome.exe lacking behavioral rules (e.g., command-line restrictions, memory limits, parent-process whitelisting).

Evidence: Export Active Directory user accounts and group memberships for sensitive roles; Windows Registry HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall for browser installation records; EDR policy exports showing browser allow-list entries and absence of behavioral sub-rules; DHCP logs correlating user accounts to endpoint IP addresses; VPN/remote access logs showing which sensitive users logged in from which endpoints; file share access logs (if centralized) showing which endpoints accessed sensitive Ukraine-related directories.

Step 5 (Communication): Notify SOC and threat intelligence teams of active Laundry Bear / UAC-0190 / Void Blizzard targeting; if your organization has ties to Ukrainian government entities or operates in relevant sectors and CISA has published a related advisory, escalate to leadership and consider sharing indicators with your sector-specific ISAC.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.5 (Notification and escalation)

Controls: NIST 800-53 IR-6 (Incident reporting), NIST 800-53 CA-7 (Continuous monitoring and incident coordination), CIS Controls v8 6.3 (Address unauthorized changes)

Compensating: Create a standardized incident communication template (one-pager) with: threat actor names (Laundry Bear, UAC-0190, Void Blizzard), campaign name (DRILLAPP), technical indicators (MITRE ATT&CK TTPs:

T1218, T1564.003), affected software (msedge.exe, chrome.exe in headless mode), and immediate detection queries. Distribute to SOC via email with severity level tagged. Contact your sector ISAC (e.g., Financial Services ISAC for banking, Government ISAC for public sector) via their standard submission form; include indicators (IP addresses, file hashes, domain IOCs) extracted from threat intelligence feeds (CISA, Mandiant, MITRE).

Evidence: Document all communication timestamps and recipients in an incident log; retain copies of initial advisory or threat intelligence report (CISA alert, vendor advisory) with extraction date; maintain list of IOCs shared with sector ISAC and any feedback received; track internal notifications to SOC, security leadership, and legal/compliance teams.

Step 6 (Long-term): Update detection engineering rules to cover headless browser abuse as a persistent technique class, not just this campaign; review allowlisting policies to ensure signed Microsoft binaries are subject to behavioral controls, not blanket trust; incorporate T1218 (System Binary Proxy Execution) and T1564.003 (Hidden Window) into red team scope for the next assessment cycle.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 (Post-Incident Activities: lessons learned and process improvement)

Controls: NIST 800-53 IR-2 (Incident response training and testing), NIST 800-53 CA-7 (Continuous monitoring), CIS Controls v8 6.2 (Address unauthorized software)

Compensating: Create detection rules using free/open-source SIEM rule templates (Sigma rules from SigmaHQ GitHub). Build a Sigma rule for headless browser execution: `detection: selection: EventID: 4688 CommandLine|contains: '--headless' ParentImage|endswith: ['explorer.exe', 'rundll32.exe', 'control.exe'] condition: selection`. Integrate into Splunk, ELK, or native Windows event log alerting. Document rule rationale, false-positive baseline, and tuning thresholds in a detection runbook. Schedule quarterly red team exercises targeting T1218 and T1564.003: simulate LNK-based execution chains and headless browser abuse; measure time-to-detect and response completeness.

Evidence: Maintain version-controlled detection rule repository with change history; document baseline tuning data (false positive rates, detection latency) from initial rule deployment; capture red team engagement reports showing attack paths tested and detection gaps identified; track post-incident process improvements and their implementation dates.

Detection Guidance

Primary behavioral indicators: msedge.exe or chrome.exe spawned with --headless and --remote-debugging-port arguments, particularly when the parent process is explorer.exe, rundll32.exe, control.exe, or an Office application. Secondary indicators: outbound network connections on TCP 9222 (default CDP port) or non-standard high ports from browser processes; browser processes accessing camera or microphone device interfaces without a visible UI window (check Windows device access audit logs under HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\CapabilityAccessManager). LNK-related indicators: LNK files in user profile directories pointing to cmd.exe, powershell.exe, or wscript.exe with encoded or obfuscated arguments; recent LNK creation timestamps not matching user activity patterns. Registry persistence: monitor for new entries under HKCU\Software\Microsoft\Windows\CurrentVersion\Run or HKLM equivalent referencing browser binaries or script runners (T1547.001). Network indicators: JavaScript-based C2 often uses web service APIs for blending (T1102.001); look for browser processes making periodic low-volume HTTPS requests to newly registered or low-reputation domains outside normal browsing hours. Log sources to prioritize: EDR process creation events, Windows Security Event ID 4688, Sysmon Event IDs 1 (process create) and 3 (network connection), and Windows device access audit logs. No confirmed public IOCs (IPs, domains, hashes) are available from the listed sources at the time this content was generated; monitor CERT-UA, CISA, and Microsoft MSTIC daily for indicator releases as the campaign evolves.

Indicators of Compromise

Type	Value	Context	Confidence
BEHAVIORAL	`msedge.exe --headless --remote-debugging-port=*`	DRILLAPP execution pattern — Edge launched in headless mode with CDP port exposed; flagged in process creation logs	HIGH
BEHAVIORAL	`control.exe executing .cpl file from user-writable path`	Initial access vector — Windows Control Panel module abuse used for DRILLAPP delivery (T1218)	HIGH
BEHAVIORAL	`LNK file in %APPDATA%, %TEMP%, or Downloads targeting cmd.exe or wscript.exe with encoded arguments`	Initial access vector, LNK files in user-writable directories (%APPDATA%, %TEMP%, Downloads) with encoded command-line arguments targeting cmd.exe or wscript.exe are suspicious because legitimate shortcuts rarely use obfuscated parameters; detect by monitoring LNK file creation/execution followed by cmd/wscript spawning with base64, hex, or PowerShell encoding in arguments, which differs from standard shortcut behavior and is consistent with Laundry Bear's macro-free delivery tradecraft (T1566).	HIGH
BEHAVIORAL	`Browser process establishing outbound TCP connection on port 9222`	CDP remote debugging port activity from browser process outside sanctioned automation pipeline	MEDIUM
REGISTRY	`HKCU\Software\Microsoft\Windows\CurrentVersion\Run — new entry referencing msedge.exe or script runner`	Persistence mechanism consistent with T1547.001; review for anomalous entries post-infection	MEDIUM
DOMAIN	`pastefy.app`	Legitimate pastebin-style service abused for C2 staging by DRILLAPP; outbound connections from workstations to this domain warrant investigation	MEDIUM
BEHAVIORAL	`msedge.exe --remote-debugging-port=9222 --headless`	Command-line pattern associated with DRILLAPP launching Edge in headless mode for CDP abuse	MEDIUM

Type	Value	Context	Confidence
BEHAVIORAL	`mshta.exe executing HTA from remote or user-writable path`	mshta.exe executing HTA files from remote (http/https/UNC paths) or user-writable directories (AppData, Temp, Downloads) is suspicious because it bypasses code signing and execution policies - legitimate mshta.exe usage loads HTAs from protected system directories or trusted application paths, whereas this pattern indicates T1218.005 Living off the Land Binary abuse used for malware delivery; detect this by alerting on mshta.exe child processes with command-line arguments containing remote URLs or non-admin-writable paths, especially when spawned by Office applications, script interpreters, or Windows Management Instrumentation processes.	MEDIUM
BEHAVIORAL	`rundll32.exe or control.exe loading CPL from non-system path`	rundll32.exe or control.exe loading Control Panel files (.cpl) from non-system directories (outside %SystemRoot%\System32) is suspicious because legitimate Windows Control Panel modules are always digitally signed and restricted to protected system paths; attackers exploit this trusted execution path to sideload malicious CPL files that bypass application whitelisting. In EDR/logs, detect rundll32.exe or control.exe with command-line arguments referencing .cpl files outside System32, especially when followed by child process creation (cmd.exe, powershell.exe), network connections to external IPs, or registry modifications within seconds of execution - legitimate Control Panel access typically loads only signed system CPLs without subsequent suspicious activity.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1564.003** — Hidden Window
- **T1083** — File and Directory Discovery
- **T1071** — Application Layer Protocol

- **T1056.001** — Keylogging
- **T1113** — Screen Capture
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1027** — Obfuscated Files or Information
- **T1125** — Video Capture
- **T1059.007** — JavaScript
- **T1218** — System Binary Proxy Execution
- **T1105** — Ingress Tool Transfer
- **T1547** — Boot or Logon Autostart Execution
- **T1102.001** — Dead Drop Resolver
- **T1071.001** — Web Protocols
- **T1123** — Audio Capture

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

CIS-V8

- **8.2** — Collect Audit Logs

NIST-CSF-2

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

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1564.003	Hidden Window	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1071	Application Layer Protocol	Command-And-Control
T1056.001	Keylogging	Collection

Technique ID	Technique Name	Tactic
T1113	Screen Capture	Collection
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1027	Obfuscated Files or Information	Defense-Evasion
T1125	Video Capture	Collection
T1059.007	JavaScript	Execution
T1218	System Binary Proxy Execution	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1547	Boot or Logon Autostart Execution	Persistence
T1102.001	Dead Drop Resolver	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1123	Audio Capture	Collection

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/drillapp-backdoor-targets-ukraine...	T3
Microsoft Silently Patches Windows LNK Flaw After Years of Active ...	https://thehackernews.com/2025/12/microsoft-silently-patches-window...	T3
Release notes for Microsoft Edge Security Updates	https://learn.microsoft.com/en-us/deployedge/microsoft-edge-relnote...	T1
Multiple Vulnerabilities in Microsoft Edge (Chromium-based) Could ...	https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-mic...	T3
Microsoft Edge Vulnerability: Key Security Insights - BitNinja	https://bitninja.com/blog/microsoft-edge-vulnerability-key-security...	T3
Microsoft Edge (Chromium) < 144.0.3719.162 Multiple Vulnerabilities	https://www.tenable.com/plugins/nessus/301411	T3

Source	URL	Tier
Microsoft Edge CVE-2025-59251 Remote Code Execution ...	https://zeropath.com/blog/cve-2025-59251-microsoft-edge-rce-summary	T3
Opened Website Seemingly Flagged as Malicious due to Process ...	https://learn.microsoft.com/en-us/answers/questions/4117248/opened-...	T1
Microsoft Edge (Chromium) < 145.0.3800.97 Multiple ...	https://www.tenable.com/plugins/nessus/301410	T3
CVE-2020-17048: Microsoft Edge Buffer Overflow ...	https://www.sentinelone.com/vulnerability-database/cve-2020-17048/	T3

Generated 2026-03-29 18:40 UTC by TJS Security Command Center