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

ClickFix Variant Uses WebDAV LOLBin Chain and Trojanized Electron App to Evade Microsoft Defender for Endpoint

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0021
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Defender for Endpoint, WorkFlowy desktop client v1.4.1050 (signed by FunRoutine Inc.), Windows (net use / WebDAV), Electron framework
Published	2026-03-14

Executive Summary

An evolved ClickFix campaign variant is actively delivering a trojanized desktop application signed with a legitimate-appearing code certificate, allowing it to bypass automated detection in Microsoft Defender for Endpoint. The malware impersonates WorkFlowy (v1.4.1050), a legitimate workplace productivity tool, and uses Windows-native file-sharing commands to load malicious code without triggering standard antivirus signatures. Organizations relying solely on automated endpoint detection are exposed; this campaign was only identified through manual threat hunting, meaning undetected infections may already exist in affected environments.

Technical Analysis

Atos researchers documented a ClickFix variant that replaces the traditional PowerShell/MSHTA execution chain with a 'net use' WebDAV drive-mapping LOLBin chain (T1218 - System Binary Proxy Execution; T1021.002). The trojanized Electron application, WorkFlowy desktop client v1.4.1050, carries a valid code signature from 'FunRoutine Inc.' (T1553.002 - Subvert Trust Controls: Code Signing), enabling it to pass Defender for Endpoint automated inspection. Malicious logic is embedded in the application's ASAR archive (CWE-506 - Embedded Malicious Code; CWE-494 - Download of Code Without Integrity Check; CWE-693 - Protection Mechanism Failure). Delivery mechanism is unconfirmed but phishing is suspected (T1566). The C2 registrant is listed as Hong Kong via OnlineNIC; final payload identity is not fully characterized. No CVE is assigned. Persistence mechanisms (T1547) are notably absent in the observed sample. The campaign evaded automated tooling entirely; detection was achieved exclusively via RunMRU registry telemetry analysis during

targeted threat hunting. A Sigma rule has been developed for this TTP cluster. Microsoft's security blog (published 2026-03-03, see sources) documents the same technique pattern of signed malware impersonating workplace applications to deploy RMM backdoors, confirming this is not an isolated variant but part of an active, evolving threat campaign.

Action Checklist

1. Step 1 (Immediate): Block execution of applications signed by 'FunRoutine Inc.' via application control policy or Defender for Endpoint custom indicators; treat this certificate as untrusted across all endpoints.
2. Step 2 (Immediate): Hunt RunMRU registry key telemetry (HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU) for 'net use' commands referencing WebDAV paths, particularly those mapping drives to external hosts; flag and isolate any matches for investigation.
3. Step 3 (Detection): Develop or source a Sigma rule covering T1218, T1553.002, and T1021.002 detection; consult Atos threat research for the published rule if available, otherwise adapt detection logic to your SIEM query language and validate coverage against this TTP cluster.
4. Step 4 (Assessment): Inventory all Electron-based applications in the environment; flag any instance of WorkFlowy v1.4.1050 or any application signed by 'FunRoutine Inc.' for immediate removal and forensic review.
5. Step 5 (Communication): Notify SOC leads and endpoint security owners that automated MDE detection is insufficient for this variant; escalate to threat hunting or MDR capability if in-house hunting bandwidth is limited.
6. Step 6 (Long-term): Review reliance on automated detection as a sole control for signed application threats; establish a recurring hunt cadence for LOLBin-based WebDAV activity and anomalous code-signing certificate usage.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal within 4 hours if any FunRoutine-signed malware is confirmed on production systems; escalate to forensic services if more than 10 endpoints are affected or if data exfiltration indicators (DNS/HTTP beaconing to external C2) are detected.
Recovery Notes	Post-eradication: Perform full system patching (prioritize Windows Update for code-signing validation improvements), re-image any compromised endpoints from verified clean backups, and restore from backups only after confirming malware signatures are absent from backup media. Conduct user awareness training on trojanized application risks and implement a software release approval process (e.g., require IT approval before installation of unfamiliar desktop apps). Restore business continuity for affected WorkFlowy users by provisioning a legitimate cloud-based alternative (e.g., Notion, Asana) and migrating user data.

Forensic Artifacts	Windows Event Log 4688 (Process Creation) — filtered for net.exe, msiexec.exe, regsvcs.exe, and Electron child processes with WebDAV-related commandline arguments | Registry HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU and HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths — for WebDAV drive mapping history | File Metadata and Code Signing Certificates — signtool output for all binaries signed by FunRoutine Inc., including timestamp, certificate chain, and revocation status | Network Traffic Logs (firewall, proxy, DNS) — all outbound connections to WebDAV servers (HTTP PROPFIND/MKCOL methods), C2 beaconing domains, and data exfiltration indicators | Process Monitor and Memory Dumps — for any running FunRoutine or WorkFlowy processes, including DLL injection chains, registry modifications, and inter-process communication

Per-Action IR Details

Step 1 (Immediate): Block execution of applications signed by 'FunRoutine Inc.' via application control policy or Defender for Endpoint custom indicators; treat this certificate as untrusted across all endpoints.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment Strategies)

Controls: NIST 800-53 SI-7 (Software, Firmware, and Information Integrity), NIST 800-53 AC-6 (Least Privilege), CIS Controls 6.1 (Establish and maintain application allow-lists)

Compensating: On endpoints without MDE, use Windows AppLocker in audit mode first to identify all FunRoutine-signed binaries: Get-AppLockerPolicy -Effective | Export-Xml. Once validated, deploy block rules via Group Policy (Computer Configuration > Windows Settings > Security Settings > Application Control Policies > AppLocker > Executable Rules). Manually review Process Monitor logs (filtered by Image Path and Signer) on at-risk systems weekly if no centralized monitoring exists.

Evidence: Capture code-signing certificate metadata before blocking: signtool verify /pa /v outputs full certificate chain. Export certificate from infected binary and hash it (SHA-256) for IOC distribution. Preserve Windows Event Log 4688 (Process Creation) and 4697 (Service Installed) for 30 days pre-block to baseline legitimate FunRoutine use. If MDE is active, export Device Timeline for all FunRoutine.exe execution events.

Step 2 (Immediate): Hunt RunMRU registry key telemetry (HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU) for 'net use' commands referencing WebDAV paths, particularly those mapping drives to external hosts; flag and isolate any matches for investigation.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.2 (Detection and Analysis) and §3.2.1 (Preparation — Baseline and Profile Networks)

Controls: NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), NIST 800-53 SI-4 (Information System Monitoring), CIS Controls 3.13 (Log all access and changes to application data)

Compensating: On systems without EDR/SIEM, manually export RunMRU from each endpoint: reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU RunMRU.reg. Parse the .reg file and search for 'net use' + 'http://', 'https://', or known external domains. Cross-reference against firewall logs for WebDAV traffic (port 80/443 with WebDAV-specific HTTP methods: PROPFIND, MKCOL, MOVE). For batch hunting: PowerShell Get-ItemProperty -Path 'HKCU:\Software\Microsoft\Windows\CurrentVersion\Explorer' -Name RunMRU on each machine and grep for 'net use' + external IPs.

Evidence: Before isolation: Capture live registry export (reg save HKCU RunMRU_live.hive), Windows Event Log 4688 (all net.exe execution with arguments), network captures (netsh trace start scenario=NetConnection tracefile=c:\temp\nettrace.etl) for 1 hour post-detection, and Process Monitor logs filtered by Parent Image = explorer.exe and Image = net.exe. Preserve %APPDATA%\Microsoft\Windows\Recent to check for MRU shortcuts to WebDAV drives.

Step 3 (Detection): Develop or source a Sigma rule covering T1218, T1553.002, and T1021.002 detection; consult Atos threat research for the published rule if available, otherwise adapt detection logic to your SIEM query language and validate coverage against this TTP cluster.

NIST Phase: Preparation

Reference: NIST 800-61r3 §3.1 (Preparation) and NIST 800-53 SI-4 (Information System Monitoring)

Controls: NIST 800-53 SI-4(1) (System Monitoring — Automated Tools), NIST 800-53 IR-4 (Incident Handling), CIS Controls 8.1 (Create a unified log collection target)

Compensating: Without SIEM: Create a scheduled task on a central Windows server to collect 4688 logs (Process Creation) from all endpoints via WEF (Windows Event Forwarding) and grep for: net use + WebDAV paths, Electron child processes + unsigned DLLs, and unusual code-signing certificates. Use Splunk Free, ELK Stack (open-source), or Graylog Community Edition to index and correlate. Manually author Sigma rule in YAML targeting Event ID 4688 with CommandLine containing 'net use' AND Image ending in 'net.exe' AND ParentImage matching '*Electron*' OR '*WorkFlowy*'.

Evidence: Validate rule against a lab environment replicating the attack: execute 'net use z: \\' and capture 4688 log entry. Confirm rule fires without false positives against normal 'net use' activity (e.g., domain-joined file shares). Export sample logs from endpoints with suspected activity and test rule against them. Document baseline false positive rate before deployment.

Step 4 (Assessment): Inventory all Electron-based applications in the environment; flag any instance of WorkFlowy v1.4.1050 or any application signed by 'FunRoutine Inc.' for immediate removal and forensic review.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Preparation — Tools and Resources) and §3.2.2 (Detection and Analysis)

Controls: NIST 800-53 CM-8 (Information System Component Inventory), NIST 800-53 SI-7 (Software, Firmware, and Information Integrity), CIS Controls 2.1 (Maintain an inventory of all software assets)

Compensating: Use PowerShell to enumerate Electron apps across all endpoints: Get-ChildItem -Path 'C:\Users*\AppData\Local\Programs\', 'C:\Program Files*' -Recurse -Filter '*Electron*' 2>/dev/null | Get-FileMetadata. Cross-reference against known-good Electron app hashes (Slack, VSCode, Discord) and flag unknowns. Export file signatures: signtool verify /pa /v >> electron_inventory.txt. For WorkFlowy specifically, search: Get-ChildItem -Recurse -Include '*workflowy*' or Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall* | Where {$_.DisplayName -match 'WorkFlowy'}.

Evidence: Before removal: Hash all flagged Electron binaries (SHA-256 via Get-FileHash), export file metadata (FileVersionInfo), capture code-signing certificate details (signtool), and preserve full installation directories to external USB or isolated drive. Document software inventory snapshot (HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall registry export). Take memory dumps of any running Electron processes: rundll32 c:\windows\system32\comsvcs.dll MiniDump c:\temp\minidump.dmp.

Step 5 (Communication): Notify SOC leads and endpoint security owners that automated MDE detection is insufficient for this variant; escalate to threat hunting or MDR capability if in-house hunting bandwidth is limited.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.3 (Post-Incident Activities — Lessons Learned) and §2.4.4.4 (Communication)

Controls: NIST 800-53 IR-6 (Incident Reporting), NIST 800-53 IR-2 (Incident Response Training), CIS Controls 17.1 (Designate personnel to fulfill incident response roles)

Compensating: If no MDR or internal hunting team exists: Schedule mandatory incident response briefing with SOC, security ops, and IT leadership within 24 hours. Document detection gaps in writing (e.g., 'MDE failed to flag FunRoutine.Inc certificates and WebDAV LOLBin chains'). Engage managed threat intelligence service (e.g., CISA AIS, Mandiant Intelligence) for 48-hour threat assessment. If budget-constrained, contract with a regional DFIR firm for 40-hour post-incident review ($8K–$15K typical) to identify gaps and retrain team.

Evidence: Prepare incident summary: list all detected compromise indicators (hashes, file paths, timestamps, affected users), MDE detection logs showing what was and was not flagged, and registry/network artifacts. Create communication timeline showing when alerts were received, analyzed, and acted upon. Preserve email threads and ticket records (ServiceNow, Jira, etc.) documenting detection-to-response latency.

Step 6 (Long-term): Review reliance on automated detection as a sole control for signed application threats; establish a recurring hunt cadence for LOLBin-based WebDAV activity and anomalous code-signing certificate usage.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.3 (Post-Incident Activities) and NIST 800-53 IR-3 (Incident Response Testing)

Controls: NIST 800-53 IR-3 (Incident Response Testing), NIST 800-53 SI-4 (Information System Monitoring), CIS Controls 14.6 (Establish a process to evaluate and update incident response procedures)

Compensating: Establish a monthly hunt calendar for resource-constrained teams: Week 1 — certificate reputation analysis (query all code-signed binaries against VirusTotal and Hybrid Analysis APIs via curl/PowerShell). Week 2 — LOLBin WebDAV detection (grep Windows Event Log 4688 for 'net use' + remote paths, 'msiexec /i http://', 'regsvcs http://'). Week 3 — Electron application baseline validation (compare current inventory to whitelist and flag new Electron apps). Week 4 — Root cause analysis on any positives. Use free tools: OSINT hunting (Shodan, URLhaus for FunRoutine certificate reuse), VirusTotal graph API, and regex-based log analysis. Automate via Python scripts if SIEM is unavailable.

Evidence: Document current state: audit all endpoints for code-signing certificates in use (export HKLM:\Software\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllCreateIndirectData). Establish baseline of legitimate signed applications per business unit. Create hunting playbook with runbooks for each TTP. Schedule quarterly review (NIST 800-61 §3.3.4) to measure hunting effectiveness and adjust detection rules.

Detection Guidance

Primary detection signal: RunMRU registry telemetry showing 'net use' commands mapping drives to WebDAV endpoints. Query HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU for entries containing 'net use' combined with UNC paths using HTTP/HTTPS (e.g., \\@\). Secondary signal: process execution of net.exe or net1.exe with 'use' arguments spawned from user-interactive context rather than scripted administrative tasks. Tertiary signal: Electron application processes (e.g., electron.exe or app-named wrappers) making outbound connections to non-CDN infrastructure shortly after launch. Code-signing check: flag any application signed by 'FunRoutine Inc.' as a high-confidence malicious indicator. ASAR inspection: if WorkFlowy v1.4.1050 is found on a host, extract and inspect the ASAR archive for injected scripts or unexpected Node.js modules; legitimate WorkFlowy builds will not contain unauthorized additions. C2 pivot: the registrant is listed as Hong Kong via OnlineNIC; treat any DNS or network connections to recently registered domains matching this registrar profile as medium-confidence indicators pending further analysis. Automated MDE detection alone is insufficient for this variant; hunting is required.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not characterized`	Trojanized WorkFlowy v1.4.1050 Electron application — hash not publicly released in available sources; extract from forensic sample for local IOC matching	LOW
DOMAIN	`not characterized`	C2 infrastructure — registrant listed as Hong Kong via OnlineNIC; specific domain not disclosed in available sources	LOW
URL	`not characterized`	WebDAV delivery path used in 'net use' LOLBin chain — specific URL not disclosed in available sources; pattern is \\@\ UNC format over HTTP	LOW
CERT_SUBJECT	`FunRoutine Inc.`	Code-signing certificate subject used to sign the trojanized WorkFlowy application; treat as malicious indicator across all signed binaries	HIGH
REGISTRY_KEY	`HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU`	Threat hunting target, entries containing 'net use' or UNC paths indicate potential Run dialog abuse consistent with this campaign technique	MEDIUM
FILE	`WorkFlowy Desktop v1.4.1050 ASAR archive (app.asar)`	Tampered ASAR archive used to inject malicious JavaScript into legitimate Electron application process; verify hash integrity against vendor distribution	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1218** — System Binary Proxy Execution
- **T1059** — Command and Scripting Interpreter
- **T1132** — Data Encoding
- **T1553.002** — Code Signing
- **T1553.002** — Code Signing
- **T1059.001** — PowerShell
- **T1027** — Obfuscated Files or Information
- **T1204.002** — Malicious File
- **T1071.001** — Web Protocols
- **T1036.001** — Invalid Code Signature
- **T1105** — Ingress Tool Transfer
- **T1105** — Ingress Tool Transfer

- **T1112** — Modify Registry
- **T1566** — Phishing
- **T1021.002** — SMB/Windows Admin Shares
- **T1218** — System Binary Proxy Execution
- **T1082** — System Information Discovery
- **T1547** — Boot or Logon Autostart Execution

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

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

CIS-V8

- **2.5**
- **2.6**
- **8.2** — Collect Audit Logs

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
T1059	Command and Scripting Interpreter	Execution
T1132	Data Encoding	Command-And-Control
T1553.002	Code Signing	Defense-Evasion
T1059.001	PowerShell	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1204.002	Malicious File	Execution
T1071.001	Web Protocols	Command-And-Control

Technique ID	Technique Name	Tactic
T1036.001	Invalid Code Signature	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1112	Modify Registry	Defense-Evasion
T1566	Phishing	Initial-Access
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1082	System Information Discovery	Discovery
T1547	Boot or Logon Autostart Execution	Persistence

Sources

Source	URL	Tier
Security News	https://staging.techjacksolutions.com/news/security-news/investigat...	T3
Microsoft Defender Antivirus event IDs and error codes	https://learn.microsoft.com/en-us/defender-endpoint/troubleshoot-mi...	T1
Signed malware impersonating workplace apps deploys RMM ...	https://www.microsoft.com/en-us/security/blog/2026/03/03/signed-mal...	T1
Electron-based app flagged as Potentially Unwanted Software by ...	https://stackoverflow.com/questions/77748400/electron-based-app-fla...	T3
Exclusions overview - Microsoft Defender for Endpoint	https://learn.microsoft.com/en-us/defender-endpoint/navigate-defend...	T1
Security News	https://thehackernews.com/2026/03/investigating-new-click-fix-varia...	T3
Behavior:Win32/RegRun MRU.SA threat description - Microsoft	https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-d...	T1
Detection: Windows RunMRU Command Execution - Splunk Research	https://research.splunk.com/endpoint/a15aa1ab-2b79-467f-8201-65e0f3...	T3

Source	URL	Tier
Potentially Suspicious Command Executed Via Run Dialog Box	https://detection.fyi/sigmahq/sigma/windows/registry/registry_set/r...	T3

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