INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-26 18:35 UTC

MuddyWater Escalates Espionage Operations: Signed Security Binaries Weaponized Across Nine Countries in Q1 2026

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0367
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Fortemedia fmapp.exe (version unspecified), SentinelOne sentinelmemoryscanner.exe (version unspecified), Chromium-based browsers (ChromElevator component)
Published	2026-05-26T11:48:41
Discovery Source	Rss

Executive Summary

Iran-linked threat group MuddyWater (Seedworm) conducted targeted espionage operations against at least nine organizations across airport, government, and manufacturing sectors in Q1 2026. The campaign abuses legitimately signed security and audio software binaries, including a SentinelOne component, to load malicious code, bypassing standard signature-based defenses. Organizations running SentinelOne or Fortemedia software face an elevated detection gap; the broader risk is credential theft, covert reconnaissance, and persistent access to sensitive operational environments.

Technical Analysis

MuddyWater (MITRE G0069) exploited DLL sideloading (T1574.002 / CWE-427, CWE-426) via two legitimately signed binaries: Fortemedia fmapp.exe and SentinelOne sentinelmemoryscanner.exe. Both binaries load attacker-controlled DLLs from the same working directory, executing arbitrary code under a trusted signature context. ChromElevator, a Chromium browser elevation component, was leveraged for credential harvesting (T1003, T1003.002, T1056.001 / CWE-522), consistent with SAM database and keylogging techniques. Reconnaissance used Node.js-driven PowerShell scripts (T1059.001, T1059.007, T1083). Command-and-control used SOCKS5 tunneling (T1090.001) for traffic obfuscation. Exfiltration paths include cloud service abuse (T1567). Additional techniques include use of valid accounts (T1078), obfuscated files (T1027), screen capture (T1113), masquerading (T1036.001), and remote services (T1021). No CVE identifiers are associated with this campaign; CVSS scoring is not applicable. Qualitative severity (High) is assessed

based on attack scope, target criticality, and operational impact per intelligence editorial policy. Attribution to MuddyWater (MITRE G0069) is based on Symantec/Broadcom threat research corroborating TTPs (DLL sideloading, ChromElevator abuse, SOCKS5 tunneling) with known MuddyWater operations. No independent corroboration from a second tier-1 vendor or law enforcement agency is currently available (medium confidence). As of this writing, neither SentinelOne nor Fortemedia has published an official advisory or patch addressing this sideloading vector. Affected product versions remain unspecified in public reporting.

Action Checklist

1. Step 1: Containment, Identify all hosts running Fortemedia fmapp.exe and SentinelOne sentinelmemoryscanner.exe. Cross-reference process execution logs for DLL loads originating from the same working directory as these binaries. Isolate any host where unexpected DLLs are loaded alongside these processes. Restrict execution of both binaries via application control policy (NIST CM-7, CIS 2.3) until vendor response status is confirmed.
2. Step 2: Detection, Query EDR and SIEM for: (a) fmapp.exe or sentinelmemoryscanner.exe loading DLLs from non-standard paths; (b) ChromElevator.exe spawning child processes or accessing credential stores; (c) PowerShell or Node.js execution chains initiating outbound SOCKS5 connections; (d) SAM database access events (Windows Security Event ID 4661/4663) from unexpected processes. Correlate with NIST AU-6 audit review process and CIS 8.2 audit log collection. Reference MITRE T1574.002 and T1003.002 detection logic in your detection engineering platform.
3. Step 3: Eradication, No vendor patch is currently available for this sideloading vector. Mitigate by: enforcing DLL search order hardening on affected hosts (D3-CH); placing fmapp.exe and sentinelmemoryscanner.exe under application allowlisting with execution path restrictions (NIST CM-7, CIS 4.6); rotating credentials for any account active on a potentially compromised host (D3-CRO); removing or quarantining any identified malicious DLL files identified during Step 1 investigation.
4. Step 4: Recovery, After isolation and eradication, validate DLL load integrity on remediated hosts using file analysis (D3-SFA). Confirm no unauthorized local accounts were created (D3-LAM, NIST AC-2). Verify SOCKS5 or proxy tunnel indicators are absent from network flow data (NIST SC-7). Re-enable affected binaries only after path-restriction controls are confirmed active. Monitor high-value targets in airport, government, and manufacturing segments with heightened alert thresholds for 30 days post-remediation.
5. Step 5: Post-Incident, This campaign exposed three control gaps: (a) over-reliance on signature-based detection, compensate with behavior-based EDR rules aligned to NIST SI-4 and D3-SFA; (b) insufficient DLL path controls on trusted vendor binaries, implement and document DLL load path hardening per CIS 4.6; (c) credential exposure via ChromElevator, enforce MFA on all accounts with access to sensitive systems (CIS 6.3, CIS 6.5, D3-MFA) and restrict browser elevation components via application control.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal counsel if SAM database access events (Event ID 4661/4663) or unauthorized account creation (Event ID 4720) are confirmed on any host in airport, government, or manufacturing operational technology (OT) adjacent segments, or if credential theft scope extends to accounts with access to regulated data requiring breach notification under applicable sector-specific regulations.

Recovery Notes	After containment and eradication, maintain elevated Sysmon Event ID 7 monitoring specifically for fmapp.exe, sentinelmemoryscanner.exe, and ChromElevator.exe DLL load paths for a minimum of 30 days, as MuddyWater campaigns historically demonstrate re-entry attempts after partial remediation. Validate that all rotated credentials have not been re-used on other systems by auditing Active Directory password change logs (Event ID 4723/4724) and confirming MFA enrollment for all rotated accounts before restoring full network access. Any re-emergence of SOCKS5 outbound connections from PowerShell or Node.js processes on remediated hosts within the 30-day monitoring window should be treated as a new incident, not a residual artifact.
Forensic Artifacts	Sysmon Event ID 7 (Image Loaded) logs for fmapp.exe and sentinelmemoryscanner.exe showing DLL loads from the binary's working directory rather than System32 or the legitimate vendor install path — this is the primary forensic signature of MuddyWater's T1574.002 DLL sideloading technique against these specific binaries. | Windows Security Event Log Event IDs 4661 and 4663 with ObjectName '\REGISTRY\MACHINE\SECURITY\SAM' from any process other than lsass.exe — evidence of T1003.002 SAM credential dumping, likely triggered after initial access via the sideloaded DLL in fmapp.exe or sentinelmemoryscanner.exe. | File system artifacts: unexpected DLL files co-located in the same working directory as fmapp.exe (Fortemedia install path) or sentinelmemoryscanner.exe (SentinelOne install path) — these DLLs will typically be named to match a legitimate Windows or vendor DLL that the signed binary attempts to load, exploiting the DLL search order (T1574.002); hash all co-located DLLs against VirusTotal or a known-good reference. | NetFlow or Windows Firewall connection logs showing outbound TCP connections on port 1080 or SOCKS5 protocol handshakes from powershell.exe or node.exe processes — MuddyWater's post-exploitation tunneling infrastructure specific to this Q1 2026 campaign, used to exfiltrate credentials and maintain persistent C2 access. | Windows Security Event Log Event IDs 4720 (local account created) and 4732 (account added to local administrators group) timestamped within the dwell window — MuddyWater espionage operations frequently establish local backdoor accounts on high-value targets in government and critical infrastructure sectors to maintain access after tool removal.

Per-Action IR Details

Step 1: Containment — Identify all hosts running Fortemedia fmapp.exe and SentinelOne sentinelmemoryscanner.exe. Cross-reference process execution logs for DLL loads originating from the same working directory as these binaries. Isolate any host where unexpected DLLs are loaded alongside these processes. Restrict execution of both binaries via application control policy (NIST CM-7, CIS 2.3) until the vendor advisory status is confirmed.

NIST Phase: Containment

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

Controls: NIST CM-7 (Least Functionality), NIST IR-4 (Incident Handling), CIS 2.3 (Address Unauthorized Software), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Without EDR, use Sysinternals Process Monitor (procmon) filtered on fmapp.exe and sentinelmemoryscanner.exe with the 'Load Image' event filter to capture all DLL loads and their full paths. Run: 'wmic process where name="fmapp.exe" get ProcessId,ExecutablePath' and 'wmic process where name="sentinelmemoryscanner.exe" get ProcessId,ExecutablePath' across endpoints via PSExec or a WMI one-liner script. For immediate network isolation without EDR, use Windows Firewall GPO to block outbound traffic from identified PIDs or push a blocking rule targeting the host's IP segment.

Evidence: Before isolating hosts, capture: (1) full DLL load list from running fmapp.exe and sentinelmemoryscanner.exe processes using Sysinternals Listdlls: 'Listdlls.exe fmapp.exe' — preserve output and hash all loaded DLLs against known-good values; (2) the working directory contents of each binary's execution path,

specifically looking for DLLs co-located with the legitimate signed binary that do not belong to the vendor installation package; (3) Windows Prefetch files at C:\Windows\Prefetch\FMAPP.EXE-*.pf and SENTINELMEMORYSCANNER.EXE-*.pf to establish execution history and associated DLL loads; (4) snapshot of running process tree at time of containment showing parent-child relationships for both binaries.

Step 2: Detection — Query EDR and SIEM for: (a) fmapp.exe or sentinelmemoryscanner.exe loading DLLs from non-standard paths; (b) ChromElevator.exe spawning child processes or accessing credential stores; (c) PowerShell or Node.js execution chains initiating outbound SOCKS5 connections; (d) SAM database access events (Windows Security Event ID 4661/4663) from unexpected processes. Correlate with NIST AU-6 audit review process and CIS 8.2 audit log collection. Reference MITRE T1574.002 and T1003.002 detection logic in your detection engineering platform.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with a configuration that captures Event ID 7 (Image Loaded) and filter for ImageLoaded paths that are NOT under the expected vendor installation directory for fmapp.exe (typically under Program Files\Fortemedia) or sentinelmemoryscanner.exe (under SentinelOne's install path). Use the following Sigma rule pattern: detection on sysmon_image_loaded where ParentImage ends with 'fmapp.exe' or 'sentinelmemoryscanner.exe' and ImageLoaded does NOT start with the expected vendor path. For ChromElevator credential access, query Windows Security Event Log for Event ID 4661 and 4663 with ObjectName containing 'SAM' where SubjectProcessName includes 'ChromElevator.exe'. For SOCKS5 detection without SIEM, run Wireshark or tcpdump on a span port filtering for TCP port 1080 or SOCKS5 CONNECT handshakes from endpoint IPs. Use osquery: 'SELECT name, path, pid FROM processes WHERE name IN ("fmapp.exe","sentinelmemoryscanner.exe","ChromElevator.exe");'

Evidence: Collect before analysis: (1) Sysmon Event ID 7 (Image Loaded) logs specifically for fmapp.exe and sentinelmemoryscanner.exe showing full ImageLoaded paths — MuddyWater's DLL sideloading via T1574.002 will show a DLL loaded from the binary's working directory rather than System32 or the vendor's install path; (2) Windows Security Event Log Event ID 4688 (Process Creation) showing ChromElevator.exe spawning cmd.exe, powershell.exe, or node.exe as children — this is anomalous for a Chromium elevation component and indicative of T1574.002 abuse; (3) Windows Security Event Log Event IDs 4661 and 4663 with ObjectName 'SAM' or '\REGISTRY\MACHINE\SECURITY\SAM' from any process other than lsass.exe or expected system processes, indicating T1003.002 SAM credential dumping; (4) NetFlow or Windows Firewall logs showing outbound port 1080 or established SOCKS5 sessions originating from PowerShell or Node.js PIDs — MuddyWater is known to use SOCKS5 tunneling for C2.

Step 3: Eradication — No vendor-issued patch exists for this sideloading vector at this time. Mitigate by: enforcing DLL search order hardening on affected hosts (D3-CH); placing fmapp.exe and sentinelmemoryscanner.exe under application allowlisting with execution path restrictions (NIST CM-7, CIS 4.6); rotating credentials for any account active on a potentially compromised host (D3-CRO); removing or quarantining any identified malicious DLL files identified during Step 1 investigation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST CM-7 (Least Functionality), NIST AC-2 (Account Management), NIST IA-5 (Authenticator Management), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 5.2 (Use Unique Passwords)

Compensating: Without enterprise application control, use Windows Software Restriction Policies (SRP) or AppLocker (available on Windows Enterprise/Education) to create path rules that allow fmapp.exe and sentinelmemoryscanner.exe to execute ONLY from their verified installation directories. To harden DLL search order without patching: set the registry key 'HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\SafeDllSearchMode' to 1, and audit the working directory of both binaries to ensure no unexpected DLLs are present. For malicious DLL quarantine, move identified files to an isolated directory with restricted ACLs rather than

deleting, to preserve forensic evidence. Credential rotation for accounts on compromised hosts should include domain accounts, local accounts, and any service accounts associated with SentinelOne or Fortemedia services — use 'net user ' locally or AD PowerShell for domain accounts.

Evidence: Preserve before eradication: (1) full disk image or at minimum a forensic copy of the directory containing fmapp.exe or sentinelmemoryscanner.exe and any co-located DLLs — hash all files with SHA-256 before removal; (2) registry export of 'HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs' and 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs' to confirm whether the malicious DLL established persistence via KnownDLLs hijacking or AppInit; (3) Volume Shadow Copy inventory ('vssadmin list shadows') to determine if the attacker deleted VSS copies as part of covering tracks; (4) LSASS memory dump (if legally and operationally authorized) from suspected compromised hosts to assess credential exposure scope before rotating — use ProcDump: 'procdump.exe -ma lsass.exe lsass.dmp'.

Step 4: Recovery — After isolation and eradication, validate DLL load integrity on remediated hosts using file analysis (D3-SFA). Confirm no unauthorized local accounts were created (D3-LAM, NIST AC-2). Verify SOCKS5 or proxy tunnel indicators are absent from network flow data (NIST SC-7). Re-enable affected binaries only after path-restriction controls are confirmed active. Monitor high-value targets in airport, government, and manufacturing segments with heightened alert thresholds for 30 days post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST SC-7 (Boundary Protection), NIST SI-2 (Flaw Remediation), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Validate DLL integrity on recovered hosts by running 'Get-FileHash' (PowerShell) against all DLLs in fmapp.exe and sentinelmemoryscanner.exe working directories and comparing SHA-256 hashes against a known-good reference extracted from an uncompromised installation or vendor-provided hash manifest. For unauthorized account verification, run: 'net localgroup administrators' and 'wmic useraccount list full' on each recovered host and compare against your baseline account inventory. For SOCKS5 tunnel verification without SIEM, capture 5 minutes of traffic on recovered hosts with Wireshark filtering for 'tcp.port == 1080 or socks' and inspect for CONNECT method handshakes. Re-enable fmapp.exe or sentinelmemoryscanner.exe in production ONLY after confirming the working directory contains no DLLs that were not present in a clean installation.

Evidence: Before returning hosts to production: (1) re-run Sysmon Event ID 7 (Image Loaded) monitoring for a 24-hour validation window after re-enabling affected binaries — any recurrence of DLL loads from non-vendor paths indicates incomplete eradication or re-infection; (2) pull Windows Security Event Log for Event ID 4720 (user account created) and 4732 (user added to security-enabled local group) for the incident timeframe to identify any backdoor accounts MuddyWater may have created during the access window; (3) review NetFlow data for any resumed SOCKS5 sessions to the same external IPs identified during Step 2 detection — MuddyWater operations have shown persistence and re-entry attempts after partial remediation; (4) verify Windows Firewall logs confirm no outbound connections from node.exe or powershell.exe to external IPs on non-standard ports.

Step 5: Post-Incident — This campaign exposed three control gaps: (a) over-reliance on signature-based detection — compensate with behavior-based EDR rules aligned to NIST SI-4 and D3-SFA; (b) insufficient DLL path controls on trusted vendor binaries — implement and document DLL load path hardening per CIS 4.6; (c) credential exposure via ChromElevator — enforce MFA on all accounts with access to sensitive systems (CIS 6.3, CIS 6.5, D3-MFA) and restrict browser elevation components via application control.

NIST Phase: Post Incident

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

Controls: NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), NIST RA-3 (Risk Assessment), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For behavior-based detection without enterprise EDR, create Sigma rules targeting: (1) T1574.002 — any signed binary loading a DLL from its own working directory where the DLL is not in the Windows KnownDLLs list; deploy via Chainsaw or Hayabusa against collected Windows Event Logs. (2) T1003.002 — Security Event ID 4663 on

SAM object access from non-LSASS processes; alert via a scheduled PowerShell script that queries the event log and emails on match. For MFA enforcement without enterprise IAM, enable Windows Hello for Business or configure RADIUS-based MFA on VPN and RDP gateways using a free FreeRADIUS + Google Authenticator stack. Document all ChromElevator.exe execution restrictions in AppLocker and conduct a quarterly review to ensure the rule persists across Chromium updates.

Evidence: For lessons-learned documentation: (1) compile the full timeline of MuddyWater DLL sideloading activity from Sysmon Event ID 7 logs across all affected hosts to quantify dwell time — this is critical for determining the credential exposure window for breach notification assessments; (2) extract all external IP addresses contacted via SOCKS5 tunnels and submit to CISA's automated indicator sharing (AIS) program and your sector ISAC (aviation, government, or manufacturing as applicable) to contribute to collective defense against this active MuddyWater campaign; (3) document which fmapp.exe and sentinelmemoryscanner.exe versions were deployed across the environment at time of incident — this forms the basis for a formal vendor disclosure to Fortemedia and SentinelOne requesting signed binary hardening or updated guidance.

Detection Guidance

Primary detection surface is process-DLL relationship anomalies and outbound tunnel traffic. Query for: (1) fmapp.exe or sentinelmemoryscanner.exe loading DLLs from directories outside their expected install path, flag any DLL load where the DLL directory matches the binary's working directory but is not a vendor-designated library path; (2) ChromElevator.exe accessing LSASS, SAM, or credential manager APIs, correlate Windows Security Event IDs 4656, 4661, 4663 for SAM access attempts; (3) PowerShell (T1059.001) or Node.js (T1059.007) spawned by or associated with the above processes, especially with encoded command arguments (T1027), Sysmon Event ID 1 (process creation) and Event ID 7 (image load) are high-value sources; (4) outbound SOCKS5 tunnel traffic on non-standard ports (T1090.001), look for long-lived TCP sessions with proxy-protocol handshakes to external IPs, particularly from endpoints where the above binaries execute; (5) exfiltration indicators: large outbound transfers to cloud storage or web services (T1567) from systems not normally generating such traffic. Behavioral IOCs should be prioritized over static signatures given the trusted binary abuse vector. D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) should be applied to hosts identified as high-risk. File hashes, malicious DLL names, and C2 IP/domain indicators are not available in public reporting as of this writing. Behavioral IOCs (DLL sideloading patterns, SOCKS5 tunnel signatures) are more reliable than static indicators for this campaign.

Framework Mappings

MITRE-ATTACK

- **T1090.001** — Internal Proxy
- **T1021** — Remote Services
- **T1003.002** — Security Account Manager
- **T1003** — OS Credential Dumping
- **T1078** — Valid Accounts
- **T1083** — File and Directory Discovery
- **T1027** — Obfuscated Files or Information
- **T1056.001** — Keylogging
- **T1059.001** — PowerShell

- **T1574.002** — DLL Side-Loading
- **T1113** — Screen Capture
- **T1059.007** — JavaScript
- **T1036.001** — Invalid Code Signature
- **T1567** — Exfiltration Over Web Service

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **IA-2** — Identification and Authentication (Organizational Users)
- **AC-6** — Least Privilege
- **IA-5** — Authenticator Management
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **SI-3** — Malicious Code Protection
- **SI-7** — Software, Firmware, and Information Integrity

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

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

SOC2-TSC

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

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1090.001	Internal Proxy	Command-And-Control
T1021	Remote Services	Lateral-Movement
T1003.002	Security Account Manager	Credential-Access
T1003	OS Credential Dumping	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1083	File and Directory Discovery	Discovery
T1027	Obfuscated Files or Information	Defense-Evasion
T1056.001	Keylogging	Collection
T1059.001	PowerShell	Execution
T1574.002	DLL Side-Loading	Persistence
T1113	Screen Capture	Collection
T1059.007	JavaScript	Execution
T1036.001	Invalid Code Signature	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/muddywater-uses-dll-side-loading-...	T3
Symantec uncovers Iran-linked Seedworm espionage campaign ...	https://industrialcyber.co/threats-attacks/symantec-uncovers-iran-l...	T3
CVE-2023-2033: Google Chrome Vulnerability - SentinelOne	https://www.sentinelone.com/blog/google-chrome-cve-2023-2033/	T3
CVE-2025-0441: Google Chrome Information Disclosure Flaw	https://www.sentinelone.com/vulnerability-database/cve-2025-0441/	T3
Stealth & Automation: Seedworm's 2026 Global Campaign Hijacks ...	https://securityonline.info/seedworm-espionage-campaign-2026-sentin...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-05-26 18:35 UTC by TJS Security Command Center