INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-08 18:53 UTC

NSO Group Defies Court Order: WhatsApp Disrupts Active Pegasus-Linked Spear-Phishing Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0429
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	WhatsApp (Meta), iOS and Android mobile platforms; high-value individual targets
Published	2026-06-08T14:40:53
Discovery Source	Rss

Executive Summary

WhatsApp detected and disrupted an active spear-phishing campaign linked to NSO Group's Pegasus spyware, targeting high-value individuals on iOS and Android devices. The campaign used malicious redirect links and fake accounts to stage spyware delivery, and reportedly continues despite a 2025 U.S. federal permanent injunction against NSO Group. Organizations protecting journalists, executives, lawyers, activists, or government officials face elevated mobile threat exposure; technical mitigations are available at the infrastructure layer (DNS/proxy blocking, MDM controls) but on-device detection of Pegasus is difficult due to the spyware's stealth characteristics.

Technical Analysis

NSO Group's Pegasus infrastructure was observed conducting spear-phishing operations via WhatsApp, leveraging CWE-601 (URL Redirection to Untrusted Site) through malicious redirect links and CWE-451 (UI Misrepresentation of Critical Information) in social engineering lure delivery. Fake test accounts were used to stage or deliver spyware payloads. MITRE techniques observed include T1598.003 (Spearphishing Link), T1566.002 (Spearphishing via Service), T1204.001 (Malicious Link), T1071.001 (Web Protocols for C2), T1584.001 (Compromise Infrastructure: Domains), and T1585.001 (Establish Accounts). Three IOC domains were published by WhatsApp; no CVE is assigned to this campaign. CVSS does not apply to this campaign; severity is rated qualitatively as high based on attack scope and target criticality. This is a social-engineering-driven campaign, not a software vulnerability exploitation event. Confidence in the injunction-violation nexus is rated medium pending independent technical verification. Primary reporting source:

BleepingComputer (Tier 3).

Action Checklist

1. Step 1: Containment, Block the three IOC domains published by WhatsApp at DNS and web proxy layers for all enterprise mobile devices and MDM-managed endpoints. Restrict outbound mobile traffic to known-good infrastructure where MDM policy permits. Notify high-value individuals (executives, legal counsel, government liaisons) to treat unsolicited WhatsApp links as hostile until further notice.
2. Step 2: Detection, Query DNS resolver logs and web proxy logs for resolution or connection attempts to the three published IOC domains. Review mobile endpoint logs via MDM console for WhatsApp activity involving outbound redirects to unknown domains. Look for behavioral indicators mapped to T1598.003 and T1566.002: unsolicited WhatsApp messages containing URLs from unknown or newly registered accounts. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence.
3. Step 3: Eradication, No software patch applies. Eradication requires removing threat access vectors: revoke and rotate credentials for any accounts that interacted with IOC domains (NIST AC-2, Account Management; D3-CRO Credential Rotation). Remove or quarantine mobile devices showing confirmed IOC contact for forensic review. Enforce app allowlisting on managed devices to limit unauthorized communication channels per NIST CM controls.
4. Step 4: Recovery, Validate IOC domain blocks are enforced across all DNS and proxy tiers. Confirm no further outbound connections to IOC domains appear in MDM or proxy logs for a minimum 72-hour window. Re-provision devices confirmed to have received Pegasus payloads via full wipe and restore from clean backup created *before the suspected compromise date.* If backup date cannot be confirmed as pre-compromise, wipe without restore and provision as new device from factory image. Monitor for renewed campaign infrastructure using fresh domains not yet published.
5. Step 5: Post-Incident, Conduct a mobile threat posture review for high-value individual protection programs. Assess gaps in NIST AC-19 (Access Control for Mobile Devices) and CIS 6.3 (Require MFA for Externally-Exposed Applications). Evaluate whether current MDM policy enforces sufficient application controls and network traffic inspection. Establish a recurring process to ingest WhatsApp and NSO Group IOC feeds into DNS blocklists. Document and table findings for the next GRC review cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to executive leadership, legal counsel, and (if applicable) law enforcement immediately if any device belonging to a journalist, attorney, government official, or C-suite executive shows confirmed MVT-positive Pegasus indicators, as this may trigger breach notification obligations, attorney-client privilege concerns, or national security reporting requirements depending on jurisdiction.

Recovery Notes	Recovery for confirmed Pegasus-compromised devices is limited to full factory wipe and re-provisioning from a pre-compromise clean backup, as Pegasus employs kernel-level persistence on both iOS and Android that survives app removal and standard MDM wipe-and-enroll cycles. Monitor re-provisioned devices with daily MVT scans for a minimum of 14 days post-reissue to detect any re-infection from undetected secondary staging infrastructure not yet included in published IOC sets. Given NSO Group's documented practice of rapidly rotating domains and delivery infrastructure in response to disclosure, treat the three published IOC domains as a floor, not a ceiling, and maintain active threat hunting for newly registered domains exhibiting similar registrar, hosting, and TTL patterns.
Forensic Artifacts	iOS DataUsage.sqlite and Cache.db files: Pegasus process injection leaves anomalous per-process network usage records for implant processes masquerading as legitimate system daemons — recoverable via MVT from an encrypted iTunes backup taken before device wipe. | DNS resolver query logs (Pi-hole query.log or BIND queries.log): Contains the exact timestamp and source device IP of resolution attempts against the three NSO-linked redirect domains used as Pegasus staging infrastructure in this campaign. | Web proxy access logs (Squid access.log or equivalent): Preserves the full HTTP 301/302 redirect chain from the WhatsApp spear-phishing link through the multi-hop Pegasus delivery redirect sequence to the final exploit server — critical for reconstructing the delivery timeline. | Android /data/tombstones/ crash logs and ADB bugreport: WhatsApp exploitation for Pegasus delivery on Android has historically produced process crash tombstones from the initial memory corruption or logic flaw exploit — these are overwritten on reboot and must be captured immediately via ADB before quarantine. | MDM console device communication and app network activity logs for com.whatsapp: Documents the WhatsApp process initiating outbound connections to unknown or newly registered domains consistent with T1566.002 spear-phishing link delivery, providing device-level attribution for IOC contact before MDM block policies were enforced.

Per-Action IR Details

Step 1: Containment — Block the three IOC domains published by WhatsApp at DNS and web proxy layers for all enterprise mobile devices and MDM-managed endpoints. Restrict outbound mobile traffic to known-good infrastructure where MDM policy permits. Notify high-value individuals (executives, legal counsel, government liaisons) to treat unsolicited WhatsApp links as hostile until further notice.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Push a Pi-hole or BIND RPZ blocklist update with the three NSO-linked redirect domains to all DNS resolvers serving mobile device traffic. On Android MDM (e.g., open-source Headwind MDM), deploy a firewall profile blocking outbound HTTPS to the IOC FQDNs. For iOS without MDM, distribute the domains via Apple Configurator 2 as a DNS proxy content filter profile. Confirm blocks with a manual curl or nslookup from a test device: 'nslookup '.

Evidence: Before pushing blocks, capture a point-in-time DNS resolver query log snapshot (e.g., /var/log/named/queries.log or Pi-hole query log export) to preserve any pre-block resolution history for the IOC domains. Export MDM device communication logs showing WhatsApp process outbound connections. This preserves evidence of which managed devices may have already resolved Pegasus staging infrastructure prior to containment.

Step 2: Detection — Query DNS resolver logs and web proxy logs for resolution or connection attempts to the three published IOC domains. Review mobile endpoint logs via MDM console for WhatsApp activity involving outbound redirects to unknown domains. Look for behavioral indicators mapped to T1598.003 and T1566.002: unsolicited WhatsApp messages containing URLs from unknown or newly registered accounts. Reference

NIST AU-6 (Audit Record Review, Analysis, and Reporting) for log review cadence.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Run the following grep against Pi-hole or BIND query logs to identify any device that resolved the IOC domains: 'grep -E "||" /var/log/named/queries.log'. For web proxy (Squid), run: 'awk \'$7 ~ /ioc-domain/{print $1,$3,$7}\' /var/log/squid/access.log'. On managed iOS/Android, export MDM network activity reports and filter for WhatsApp (com.whatsapp) as the initiating process with outbound connections to domains registered within the past 30 days — cross-reference against WHOIS for newly registered domains consistent with NSO infrastructure TTPs. Use the free Sigma rule 'proc_creation_win_susp_redirect' as a template adapted for mobile proxy log format.

Evidence: Preserve raw DNS resolver query logs with full timestamps and source IP (device identifier) before log rotation occurs — Pegasus delivery is a single-click event and the DNS resolution window may be seconds wide. Capture WhatsApp message metadata logs from MDM (not message content) showing sender account age, account creation date, and message link domain. Retain web proxy access logs showing HTTP 301/302 redirect chains from the IOC domains, which reflect the Pegasus multi-hop redirect staging mechanism used in this campaign.

Step 3: Eradication — No software patch applies. Eradication requires removing threat access vectors: revoke and rotate credentials for any accounts that interacted with IOC domains (NIST AC-2, Account Management; D3-CRO Credential Rotation). Remove or quarantine mobile devices showing confirmed IOC contact for forensic review. Enforce app allowlisting on managed devices to limit unauthorized communication channels per NIST CM controls.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Use the free Amnesty International Mobile Verification Toolkit (MVT) — 'mvt-ios check-backup --iocs ' or 'mvt-android check-adb --iocs ' — to confirm Pegasus indicators on devices that contacted the IOC domains before quarantining them. MVT checks for Pegasus-specific filesystem artifacts, process names, and network connections documented in Amnesty's forensic methodology. Credential rotation for accounts active on affected devices should be performed from a clean, uncompromised workstation — not the quarantined mobile device.

Evidence: Before wiping or quarantining devices, capture a full encrypted iTunes backup (iOS) or ADB backup (Android) for MVT analysis. On iOS, collect the DataUsage.sqlite file at '/private/var/mobile/Library/application Support/com.apple.CommCenter/Cache.db' and the DataUsage.sqlite at '/private/var/mobile/Library/application support/com.apple.networkd/' — Pegasus process injection leaves anomalous per-process network usage entries. On Android, capture 'adb bugreport' output and '/data/tombstones/' crash logs, as Pegasus exploitation of WhatsApp may leave process crash artifacts from the initial exploit delivery.

Step 4: Recovery — Validate IOC domain blocks are enforced across all DNS and proxy tiers. Confirm no further outbound connections to IOC domains appear in MDM or proxy logs for a minimum 72-hour window. Re-provision devices confirmed to have received Pegasus payloads — full wipe and restore from clean backup is the only reliable recovery path given Pegasus's persistence mechanisms. Monitor for renewed campaign infrastructure using fresh domains not yet published.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-19 (Access Control For Mobile Devices), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For re-provisioned iOS devices, restore only from an iCloud or iTunes backup predating the earliest confirmed IOC domain contact timestamp — do not restore from a backup taken after first contact, as Pegasus persistence survives backup and restore cycles on some iOS versions. Validate clean re-provisioned devices by

running MVT against the new device's first backup within 24 hours of restore. Subscribe to the free Abuse.ch URLhaus feed and DomainTools' free WHOIS history alerts for NSO Group-associated registrar patterns (historically Domains By Proxy and similar privacy registrars) to detect fresh campaign infrastructure.

Evidence: Before re-provisioning, confirm the full forensic backup (captured in the eradication step) is archived and hash-verified (SHA-256) to preserve chain of custody — this is relevant given the active U.S. federal injunction against NSO Group and potential future litigation or regulatory inquiry. Document the exact timestamp of last IOC domain contact per device from DNS and proxy logs to establish the contamination window for any post-incident disclosure assessment.

Step 5: Post-Incident — Conduct a mobile threat posture review for high-value individual protection programs. Assess gaps in NIST AC-19 (Access Control for Mobile Devices) and CIS 6.3 (Require MFA for Externally-Exposed Applications). Evaluate whether current MDM policy enforces sufficient application controls and network traffic inspection. Establish a recurring process to ingest WhatsApp and NSO Group IOC feeds into DNS blocklists. Document and table findings for the next GRC review cycle.

NIST Phase: Post Incident

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

Controls: NIST AC-19 (Access Control For Mobile Devices), NIST AU-11 (Audit Record Retention), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For high-value individuals who cannot be placed under full MDM, implement Apple Lockdown Mode (iOS 16+) as a free hardening control — it restricts the WebKit JIT compiler and link previews that Pegasus historically exploits in WhatsApp and iMessage delivery chains. Document Lockdown Mode activation per device in the asset inventory. Integrate the Amnesty International IOC repository (GitHub: AmnestyTech/investigations) into Pi-hole or BIND RPZ via a free cron-driven sync script to ensure NSO infrastructure domains are blocked as new campaigns are disclosed. Schedule a quarterly MVT scan cadence for all devices used by identified high-value individuals.

Evidence: Retain all DNS resolver logs, proxy access logs, MDM activity exports, and MVT forensic outputs for a minimum of 12 months under NIST AU-11 (Audit Record Retention) — the active federal injunction against NSO Group means these artifacts may be subpoenaed or required for regulatory inquiries. Archive the WhatsApp-published IOC list with ingestion timestamps to document the organization's response timeline relative to public disclosure.

Detection Guidance

Primary detection surface is DNS and outbound web proxy telemetry. Query for resolution attempts against the three IOC domains published by WhatsApp; exact domain values should be sourced directly from WhatsApp's official disclosure or the BleepingComputer report (URL: https://www.bleepingcomputer.com/news/security/whatsapp-says-it-disrupted-new-nso-spyware-phishing-attacks/, Tier 3 source, recommend human validation). If domains are not yet published, check WhatsApp Security Center directly. In MDM consoles, filter for mobile devices that received WhatsApp messages containing outbound redirect URLs shortly before or after IOC domain contact. Behavioral indicators aligned to T1598.003 and T1566.002: unsolicited WhatsApp messages from unknown accounts containing shortened or redirect-chained URLs, especially targeting named high-value individuals. Pegasus infections produce minimal on-device indicators; behavioral network telemetry is more reliable than endpoint artifact scanning. Reference NIST AU-2 (Event Logging) and AU-6 (Audit Record Review) to confirm relevant log sources are enabled and retained per AU-11. Note: No SIEM query template is provided here; specific query syntax depends on your DNS/proxy platform. Construct queries against your verified IOC list.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`See WhatsApp official disclosure or BleepingComputer report for the three published IOC domains`	Three domains published by WhatsApp linked to Pegasus spear-phishing redirect infrastructure. Exact values not reproduced here — source directly from the primary report to avoid transcription error.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1598.003** — Spearphishing Link
- **T1204.001** — Malicious Link
- **T1071.001** — Web Protocols
- **T1584.001** — Domains
- **T1566.002** — Spearphishing Link
- **T1585.001** — Social Media Accounts

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1598.003	Spearphishing Link	Reconnaissance

Technique ID	Technique Name	Tactic
T1204.001	Malicious Link	Execution
T1071.001	Web Protocols	Command-And-Control
T1584.001	Domains	Resource-Development
T1566.002	Spearphishing Link	Initial-Access
T1585.001	Social Media Accounts	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/whatsapp-says-it-dis...	T3
WhatsApp has patched a security vulnerability that allowed ...	https://www.facebook.com/gleanerjamaica/posts/whatsapp-has-patched-...	T3
What the WhatsApp API Vulnerability Teaches Us About Rate ...	https://equixly.com/blog/2025/12/14/whats-app-api-vulnerability/	T3
Meta patches WhatsApp flaws, Google fixes Android RCE, Apple ...	https://www.linkedin.com/posts/techrepublic_itleaders-security-cybe...	T3
CVE-2025-55177: WhatsApp Authorization Bypass Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2025-55177/	T3

Generated 2026-06-08 18:53 UTC by TJS Security Command Center