INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-31 18:37 UTC

Dutch Takedown of Asocks Exposes Residential Proxy Abuse at Scale: 17 Million Devices, Criminal Infrastructure, and What SOC Teams Should Watch

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0387
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Android devices (via LumiApps/Asocks proxyware), IoT devices, routers, smartphones, tablets, and computers, no specific vendor CVEs identified
Published	2026-05-31T08:22:12
Discovery Source	Rss

Executive Summary

Dutch law enforcement, working with the Netherlands NCSC, dismantled a criminal residential proxy botnet called Asocks that silently enslaved at least 17 million devices globally, including smartphones, tablets, computers, and IoT hardware, to relay malicious traffic through legitimate residential IP addresses. Affected devices were compromised via proxyware SDKs embedded in mobile applications, with infected connections monetized as anonymous exit nodes for fraud, credential stuffing, and ad fraud operations. Enterprise security teams face elevated risk because attack traffic originating from this infrastructure appears to come from trusted consumer ISP ranges - specifically residential IP blocks rather than datacenter addresses - bypassing IP-reputation-based controls.

Technical Analysis

The Asocks botnet operated as a commercial residential proxy service, routing criminal traffic through devices infected with proxyware, primarily via the LumiApps SDK distributed inside mobile applications. The botnet reached at least 17 million devices globally across Android smartphones, tablets, routers, and IoT hardware. Dutch law enforcement seized over 200 Netherlands-based backend servers after directing the hosting provider to act; attribution of the operators remains unconfirmed.

No CVE has been assigned. Relevant CWEs: CWE-287 (Improper Authentication, enabling device compromise), CWE-1188 (Insecure Default Initialization, misconfigured devices recruited as nodes), CWE-494 (Download of Code Without Integrity Check, proxyware deployed via SDK without verification).

MITRE ATT&CK techniques observed: T1105 (Ingress Tool Transfer), T1090.002 (External Proxy), T1583.008 (Botnet infrastructure acquisition), T1496 (Resource Hijacking), T1110.004 (Credential Stuffing), T1059.004 (Unix Shell), T1078 (Valid Accounts), T1071.001 (Web Protocols for C2), T1036 (Masquerading).

The core detection challenge: exit node traffic originates from residential and consumer ISP IP ranges with no prior malicious reputation. Standard IP blocklists and geolocation-based controls are ineffective against this traffic pattern. The LumiApps SDK connection indicates proxyware may persist on devices where implicated applications remain installed.

Action Checklist

1. Containment, Audit mobile device management (MDM) policies for applications embedding the LumiApps SDK or other proxyware SDKs. Isolate or quarantine devices running implicated applications until review is complete. Block known Asocks infrastructure IPs at the perimeter if your threat intelligence feed has published indicators (verify against current feeds, do not rely on static lists). Reference NIST AC-17 (Remote Access) to enforce policy controls on mobile and remote devices.
2. Detection, Search proxy, firewall, and web gateway logs for anomalous outbound traffic patterns: high-volume connections to rotating residential IPs, unusual egress on ports 80/443 from endpoints that do not normally generate web traffic, and beaconing intervals inconsistent with user activity. Query endpoint logs for LumiApps SDK processes or associated application package names. Apply CIS 8.2 (Collect Audit Logs), confirm logging is active on all endpoint and network egress points. For SIEM, build detections around T1090.002 (External Proxy) behavioral patterns: unusual user-agent strings, high request rates from single endpoints to diverse destination IPs.
3. Eradication, Remove any applications confirmed to embed the LumiApps or Asocks proxyware SDK from managed devices via MDM. For unmanaged or BYOD devices with corporate access, require re-enrollment with a clean device profile before restoring access. Apply CWE-494 mitigations: enforce application allow-listing (CIS 2.3, Address Unauthorized Software) so only verified, integrity-checked applications can execute. Reference NIST CM-7 (Least Functionality) to disable unnecessary services on IoT and network devices that may have been recruited as proxy nodes.
4. Recovery, After removing implicated applications, monitor previously affected endpoints for 14 days for resumed outbound proxy traffic patterns. Rotate credentials for any accounts accessed from devices confirmed to have hosted proxyware, the botnet's documented use for credential stuffing (T1110.004) means compromised exit nodes may also have observed authentication traffic. Confirm that NIST AU-6 (Audit Record Review) processes are capturing egress anomalies post-remediation. Verify MDM enrollment status for all mobile devices with corporate access.
5. Post-Incident, This campaign exposed three control gaps: (1) insufficient vetting of third-party SDK supply chains in approved mobile applications, remediate with a software composition analysis process aligned to CIS 2.1 (Software Inventory); (2) over-reliance on IP reputation for malicious traffic detection, residential proxy abuse bypasses this entirely; supplement with behavioral analytics and D3-UAP (User Account Permissions) controls that restrict what compromised endpoints can reach; (3) absent or inconsistent MDM enforcement for BYOD, remediate with formal NIST AC-19 (Access Control for Mobile Devices) policy. Document lessons learned in a post-incident review and update threat hunting playbooks

to include proxyware behavioral indicators.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal and privacy counsel if forensic analysis confirms that Asocks relay traffic passing through corporate-owned or MDM-enrolled devices included authentication credentials, PII, or PHI — the relay-position exposure combined with T1110.004 credential stuffing use creates potential breach notification obligations under GDPR, CCPA, or HIPAA depending on jurisdiction and data types observed.
Recovery Notes	After eradication, maintain elevated egress monitoring on previously affected device IPs for a minimum of 14 days, with specific detection thresholds tuned to the residential proxy relay behavioral signature (>30 unique destination IPs per hour from a single endpoint outside business hours). Any authentication anomalies — particularly successful logins from residential proxy IP ranges to corporate SaaS or VPN — during this window should be treated as potential credential stuffing follow-on from the Asocks campaign and investigated under T1110.004. Do not reduce monitoring to baseline until two consecutive clean weeks of egress telemetry have been confirmed and all BYOD devices have completed MDM re-enrollment with verified clean application profiles.
Forensic Artifacts	Android logcat captures from implicated devices containing LumiApps SDK runtime logs, outbound socket initialization events, and proxy relay session identifiers — extracted via 'adb logcat -d' before application removal, tied directly to the SDK's background service execution model | Firewall and web gateway session logs showing sustained outbound TCP connections on ports 80/443 from enrolled mobile device IPs to high-diversity residential IP destination sets during off-hours — the primary network artifact of Asocks relay node operation distinct from normal user browsing | DNS query logs from the internal resolver for Asocks node registration and coordination domains, which devices would query during botnet enrollment and periodic check-in — cross-referenceable against NCSC-NL published Asocks infrastructure indicators | Preserved APK binaries of implicated applications extracted from affected devices before uninstall, containing the embedded LumiApps SDK code and configuration — essential for supply chain attribution and for generating YARA signatures to scan other applications in the MDM catalog | Identity provider authentication logs (Azure AD Event ID 4624, Okta system log sign-in events) filtered for source IPs within residential ISP ASN ranges during the campaign window — evidence of whether credentials relayed through Asocks nodes were subsequently replayed in credential stuffing attempts under T1110.004

Per-Action IR Details

Containment — Audit mobile device management (MDM) policies for applications embedding the LumiApps SDK or other proxyware SDKs. Suspend or quarantine devices running implicated applications until review is complete. Block known Asocks infrastructure IPs at the perimeter if your threat intelligence feed has published indicators (verify against current feeds — do not rely on static lists). Reference NIST AC-17 (Remote Access) to enforce policy controls on mobile and remote devices.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected assets to prevent continued proxy relay activity while preserving evidence of SDK-initiated outbound connections.

Controls: NIST AC-17 (Remote Access) — enforce MDM policy restrictions on mobile devices enrolled with corporate credentials that may host LumiApps SDK-bearing applications, NIST AC-19 (Access Control for Mobile Devices) —

restrict or suspend corporate resource access for devices not meeting clean application profile requirements, NIST CM-7 (Least Functionality) — disable or block proxy relay capability on IoT and mobile devices that should not be generating outbound relay traffic, CIS 4.4 (Implement and Manage a Firewall on Servers) — enforce egress filtering rules at the perimeter to block Asocks C2 and proxy relay destination IPs published by NCSC-NL and Dutch law enforcement advisories

Compensating: For teams without enterprise MDM: use Android Debug Bridge (ADB) to enumerate installed packages on corporate-owned Android devices — run 'adb shell pm list packages' and cross-reference against known LumiApps-affiliated app package names (e.g., com.lumiapps.* namespace or app titles flagged in NCSC-NL advisory). Block Asocks infrastructure IPs and CIDR ranges at the perimeter firewall using pfSense or iptables rules sourced from the Dutch Police / NCSC-NL published IOC list. Use Pi-hole or a local DNS sinkhole to redirect known Asocks proxy relay domains to a logging listener so you capture device DNS queries without enterprise tooling.

Evidence: Before suspending or quarantining devices, capture: (1) Android logcat output ('adb logcat -d > device_logcat.txt') to preserve SDK runtime activity and outbound socket connection attempts initiated by the LumiApps SDK; (2) network flow records (NetFlow/IPFIX or firewall session tables) showing outbound TCP sessions from the device to non-corporate destinations on ports 80/443 during hours inconsistent with user activity; (3) MDM enrollment records and last-seen timestamps for all managed Android devices to establish which devices were active during the Asocks campaign window; (4) a full installed application list with APK hashes from affected devices before any uninstall action, to support supply chain attribution.

Detection — Search proxy, firewall, and web gateway logs for anomalous outbound traffic patterns: high-volume connections to rotating residential IPs, unusual egress on ports 80/443 from endpoints that do not normally generate web traffic, and beaconing intervals inconsistent with user activity. Query endpoint logs for LumiApps SDK processes or associated application package names. Apply CIS 8.2 (Collect Audit Logs) — confirm logging is active on all endpoint and network egress points. For SIEM, build detections around T1090.002 (External Proxy) behavioral patterns: unusual user-agent strings, high request rates from single endpoints to diverse destination IPs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate endpoint application telemetry with network egress anomalies to identify devices silently operating as Asocks residential proxy relay nodes.

Controls: NIST AU-2 (Event Logging) — confirm logging is enabled for outbound network connections and application execution events on Android and IoT endpoints, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — actively review firewall and web gateway egress logs for T1090.002 behavioral indicators specific to residential proxy relay traffic, NIST SI-4 (System Monitoring) — implement continuous monitoring of egress traffic for high-frequency outbound connections to diverse residential IP ranges characteristic of Asocks proxy chaining, CIS 8.2 (Collect Audit Logs) — verify audit logging is active on all network egress points, web proxies, and mobile device management platforms before declaring detection coverage complete, MITRE ATT&CK T1090.002 (External Proxy) — behavioral pattern baseline for SIEM detection rule construction targeting LumiApps SDK relay activity

Compensating: Without SIEM: run the following on your firewall or web proxy log export — 'awk '{print $dst_ip}' firewall.log | sort | uniq -c | sort -rn | head -50' to surface endpoints with the highest unique destination IP counts, which is the primary network signature of residential proxy relay behavior. Use Zeek (formerly Bro) on a network tap to generate conn.log and http.log files, then query for HTTP requests where the 'host' field resolves to a residential ISP ASN rather than a corporate or CDN destination. For endpoint detection on Android: use ADB to pull and search logcat for 'LumiApps', 'asocks', or 'proxy' strings — 'adb logcat -d | grep -iE "lumiapps|asocks|proxy"'. Write a Sigma rule targeting Windows/Linux endpoints for high-frequency outbound HTTP connections from non-browser processes to diverse /16 subnets.

Evidence: Capture before concluding detection analysis: (1) raw firewall session logs covering the 90 days prior to detection, with destination IP, port, bytes transferred, and session count per source endpoint — Asocks relay activity will show sustained multi-hour sessions to diverse residential IPs even outside business hours; (2) DNS query logs from the internal resolver for domains resolving to Asocks-affiliated infrastructure (cross-reference with NCSC-NL IOC feed); (3) web gateway or proxy logs with full user-agent strings — LumiApps SDK-generated requests may use atypical or headless user-agent strings not matching any known browser; (4) Android device battery and data usage statistics, which are preserved in device health telemetry and will show abnormal background data consumption from

the implicated application during off-hours.

Eradication — Remove any applications confirmed to embed the LumiApps or Asocks proxyware SDK from managed devices via MDM. For unmanaged or BYOD devices with corporate access, require re-enrollment with a clean device profile before restoring access. Apply CWE-494 mitigations: enforce application allow-listing (CIS 2.3, Address Unauthorized Software) so only verified, integrity-checked applications can execute. Reference NIST CM-7 (Least Functionality) to disable unnecessary services on IoT and network devices that may have been recruited as proxy nodes.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the LumiApps/Asocks proxyware SDK from all confirmed devices and close the recruitment vector by enforcing application allow-listing to prevent reinfection via other SDK-embedded applications in the same supply chain.

Controls: NIST CM-7 (Least Functionality) — disable background data services, developer options, and sideloading capabilities on managed Android and IoT devices post-eradication to eliminate re-recruitment surface, NIST CM-11 (User-Installed Software) — enforce policy prohibiting installation of applications outside MDM-approved catalog to close the LumiApps SDK supply chain vector, NIST SI-2 (Flaw Remediation) — treat removal of SDK-bearing applications as a remediation action requiring verification and documentation equivalent to a patch deployment, CIS 2.3 (Address Unauthorized Software) — flag all applications not present in the approved software inventory; require removal or documented exception before device is returned to service, CIS 2.2 (Ensure Authorized Software is Currently Supported) — verify that any application previously hosting the LumiApps SDK has been replaced with a vendor-confirmed clean version or removed from the approved catalog entirely

Compensating: Without enterprise MDM for BYOD: issue a written device access policy requiring users to demonstrate removal of flagged applications (screenshot of installed app list post-removal) before VPN or corporate Wi-Fi credentials are reissued. For IoT devices (routers, smart devices) confirmed to have been recruited as Asocks nodes: perform a factory reset and reflash firmware from the manufacturer's verified download rather than attempting application-level removal, since proxyware on IoT may persist in non-volatile storage outside the normal application layer. Use ClamAV with a custom signature for LumiApps SDK file hashes (if published by NCSC-NL) to scan any Android APK files in your software distribution repository before redistribution.

Evidence: Before executing eradication: (1) extract and preserve the full APK file of each implicated application from affected devices using 'adb pull $(adb shell pm path com.example.app | cut -d: -f2)' — this preserves the SDK-embedded binary for supply chain forensics and potential law enforcement referral; (2) document all network connections active at the time of eradication using 'adb shell netstat -an' or equivalent, capturing any live Asocks relay sessions in progress; (3) for IoT devices, capture the running process list and open port state ('netstat -tulpn' on Linux-based IoT firmware) before reset to document which services the proxyware had activated; (4) preserve the device's application data directory if forensically accessible, as LumiApps SDK may store configuration data including assigned Asocks node ID, relay targets, and session keys in local storage.

Recovery — After removing implicated applications, monitor previously affected endpoints for 14 days for resumed outbound proxy traffic patterns. Rotate credentials for any accounts accessed from devices confirmed to have hosted proxyware — the botnet's documented use for credential stuffing (T1110.004) means compromised exit nodes may also have observed authentication traffic. Validate that NIST AU-6 (Audit Record Review) processes are capturing egress anomalies post-remediation. Confirm MDM enrollment status for all mobile devices with corporate access.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore devices to verified clean state, enforce credential rotation for accounts exposed through Asocks relay nodes, and confirm monitoring continuity to detect any reinfection or credential-based follow-on attacks.

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — activate enhanced egress log review for previously affected endpoints for a minimum 14-day post-remediation window targeting resumed T1090.002 relay behavior, NIST IA-5 (Authenticator Management) — mandate immediate credential rotation for all accounts authenticated from devices confirmed to have hosted the LumiApps/Asocks SDK, prioritizing privileged and

externally-exposed accounts, NIST AC-2 (Account Management) — audit and suspend any accounts showing authentication activity from Asocks exit node IPs during the campaign window, as those sessions may have been observed or relayed by the botnet, NIST IR-4 (Incident Handling) — document recovery actions and re-verify device integrity against a known-good MDM baseline before returning devices to production access, CIS 5.2 (Use Unique Passwords) — enforce unique password rotation across all corporate services for accounts accessed from implicated devices, not only the primary corporate SSO

Compensating: Without SIEM for 14-day monitoring: configure a cron job or scheduled PowerShell task to run daily firewall log exports and pipe them through the same high-unique-destination-count query used during detection ('sort | uniq -c | sort -rn') on previously affected device IPs, alerting if the count exceeds a defined threshold. For credential rotation on a small team: prioritize VPN, email, and any SaaS applications accessible via browser on the affected Android device — these are the credential targets most exposed to a relay-position adversary. Use Have I Been Pwned's API (free tier) to check corporate email addresses against breach databases as a secondary indicator that credentials observed through the relay were subsequently weaponized.

Evidence: During recovery monitoring, preserve: (1) authentication logs from identity providers (Azure AD sign-in logs, Okta system log, or on-prem Active Directory Security Event ID 4624/4625) filtered by source IPs matching Asocks-affiliated residential proxy ranges, to determine whether credentials observed through the relay have been replayed in credential stuffing attempts (T1110.004); (2) continued network flow captures from previously affected device IPs for the full 14-day monitoring window as a clean baseline comparison; (3) MDM compliance status reports exported at enrollment re-verification, documenting that re-enrolled devices passed application integrity checks before access was restored.

Post-Incident — This campaign exposed three control gaps: (1) insufficient vetting of third-party SDK supply chains in approved mobile applications — remediate with a software composition analysis process aligned to CIS 2.1 (Software Inventory); (2) over-reliance on IP reputation for malicious traffic detection — residential proxy abuse bypasses this entirely; supplement with behavioral analytics and D3-UAP (User Account Permissions) controls that restrict what compromised endpoints can reach; (3) absent or inconsistent MDM enforcement for BYOD — remediate with formal NIST AC-19 (Access Control for Mobile Devices) policy. Document lessons learned in a post-incident review and update threat hunting playbooks to include proxyware behavioral indicators.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review focused on the three specific control gaps exposed by the Asocks campaign and update detection playbooks with residential proxyware behavioral indicators to reduce dwell time in future campaigns.

Controls: NIST IR-4 (Incident Handling) — update the incident handling process to include SDK supply chain vetting as a mandatory step in the mobile application approval workflow, NIST SA-12 (Supply Chain Protection) — implement software composition analysis (SCA) tooling or manual review process to identify proxyware SDKs (LumiApps and equivalents) embedded in third-party mobile applications before enterprise approval, NIST SI-7 (Software, Firmware, and Information Integrity) — enforce APK integrity verification against vendor-published hashes as part of the MDM application distribution process to detect tampered or SDK-injected builds, NIST AC-19 (Access Control for Mobile Devices) — formalize BYOD access policy with mandatory MDM enrollment, application allow-listing, and periodic compliance attestation as direct remediation for the BYOD gap exposed by this campaign, CIS 2.1 (Establish and Maintain a Software Inventory) — extend software inventory to include third-party SDK components embedded in approved mobile applications, not only top-level application titles, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate proxyware SDK identification into the vulnerability management scope, treating SDK-embedded proxyware as a supply chain vulnerability class requiring remediation SLAs

Compensating: For a 2-person team without SCA budget: use the free MobSF (Mobile Security Framework) tool to statically analyze APK files of all MDM-approved applications for known proxyware SDK signatures — MobSF will identify LumiApps and similar SDK components in the application's decompiled manifest and code. Write a Sigma detection rule targeting the behavioral fingerprint of residential proxy relay: process making >50 unique external HTTP connections per hour with no corresponding user browser activity, and publish it to your threat hunting repository. Document the Asocks-specific IOCs (Asocks node registration domains, LumiApps SDK package identifiers, relay traffic behavioral thresholds) in a structured threat hunting playbook entry so a future analyst can operationalize them

without reconstructing context from scratch.

Evidence: For the post-incident review record, compile: (1) a timeline of the Asocks campaign dwell period on your network derived from firewall and DNS log analysis, establishing earliest-known compromise date versus detection date to quantify dwell time; (2) a complete inventory of all MDM-approved applications that were active during the campaign window, with SCA results for each, to determine whether LumiApps SDK exposure was isolated to confirmed applications or present in additional approved titles; (3) documentation of which detection controls (IP reputation, behavioral analytics, MDM compliance alerts) fired or failed to fire during the campaign, to support honest gap analysis; (4) a record of all credential rotation actions taken during recovery, with account types and access scope, to demonstrate regulatory due diligence if notification obligations arise from the credential stuffing exposure.

Detection Guidance

Primary behavioral indicators for Asocks/residential proxy botnet activity in your environment:

1. Anomalous outbound proxy traffic: Endpoints initiating high volumes of outbound HTTP/HTTPS connections to diverse, rotating destination IPs, particularly outside normal business hours or inconsistent with the user's role. Look for connections where the destination IPs resolve to residential ISP ranges (not datacenter ASNs).

2. LumiApps SDK process signatures: Search EDR telemetry and MDM application inventories for package names or process names associated with LumiApps or applications known to embed it. Check application stores and sideloaded APK sources.

3. SIEM detection logic (behavioral, not IP-based, IP lists age quickly):

- Rule: Endpoint generates >500 outbound connections/hour to unique destination IPs with no corresponding inbound session, flag for analyst review. (Adjust threshold upward in environments with legitimate proxy or VPN traffic to reduce false positives.)

- Rule: Mobile device on corporate network establishes persistent low-bandwidth sessions to IPs outside established cloud service ASNs.

- Rule: User-agent strings inconsistent with installed browser versions on the same endpoint.

4. DNS telemetry: Look for DNS queries to domains associated with Asocks infrastructure. Check current threat intelligence feeds (e.g., CISA, commercial TI platforms) for published Asocks-related domains, this report does not include confirmed domain IOCs.

5. Resource consumption anomaly: Devices showing unexplained sustained network I/O without corresponding user activity, consistent with T1496 (Resource Hijacking) behavior.

NIST SI-4 (System Monitoring) and AU-6 (Audit Record Review) should govern the frequency and scope of this log review. MITRE D3FEND countermeasures applicable: D3-LAM (Local Account Monitoring) for detecting unauthorized processes, D3-SFA (System File Analysis) for proxyware installation artifacts.

Note: Because exit traffic originates from residential IP space, IP reputation-based detection will not catch this. Behavioral and process-based detection is the effective path.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`asocks.com`	Primary domain of the Asocks commercial residential proxy service — the criminal infrastructure dismantled in this operation	HIGH
URL	`https://lumiapps.io`	LumiApps SDK distribution site — proxyware SDK linked to Asocks botnet recruitment via mobile applications. Verify against current threat intelligence before blocking; legitimate SDK may have dual-use distribution.	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1105** — Ingress Tool Transfer
- **T1090.002** — External Proxy
- **T1583.008** — Malvertising
- **T1496** — Resource Hijacking
- **T1110.004** — Credential Stuffing
- **T1059.004** — Unix Shell
- **T1078** — Valid Accounts
- **T1071.001** — Web Protocols
- **T1036** — Masquerading

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **AT-2** — Literacy Training and Awareness
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **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

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

NIST-CSF-2

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1105	Ingress Tool Transfer	Command-And-Control
T1090.002	External Proxy	Command-And-Control
T1583.008	Malvertising	Resource-Development
T1496	Resource Hijacking	Impact
T1110.004	Credential Stuffing	Credential-Access
T1059.004	Unix Shell	Execution
T1078	Valid Accounts	Defense-Evasion

Technique ID	Technique Name	Tactic
T1071.001	Web Protocols	Command-And-Control
T1036	Masquerading	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/05/dutch-authorities-dismantle-botne...	T3
Dutch National Cyber Security Center actions and 17 million devices	https://beeble.com/en/blog/dutch-national-cyber-security-center-act...	T3
Top 7 Mobile Security Threats - Kaspersky	https://usa.kaspersky.com/resource-center/threats/top-seven-mobile-...	T3
The vulnerability is reportedly still available even on devices running ...	https://www.facebook.com/NoypiGeeks/posts/the-vulnerability-is-repo...	T3
Botnet of more than 17 million devices dismantled - Ars Technica	https://arstechnica.com/security/2026/05/botnet-of-more-than-17-mil...	T2

Generated 2026-05-31 18:37 UTC by TJS Security Command Center