INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:33 UTC

Nation-State iOS Exploit Kits Go Commodity: Coruna and DarkSword Target Unpatched iPhones at Scale

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0113
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Apple iOS 13.0-17.2.1 (Coruna), Apple iOS 18.4-18.7 (DarkSword), iPadOS (multiple versions)
Published	2026-03-27
Discovery Source	Rss

Executive Summary

Apple issued on-device lock screen alerts warning that two active exploit kits, Coruna and DarkSword, are targeting unpatched iPhones and iPads via web-based delivery. Coruna is assessed as a commoditized evolution of the Operation Triangulation nation-state exploit chain, now accessible to criminal and espionage actors beyond its original developers; DarkSword targets devices running iOS 18.4 through 18.7. Any organization with unmanaged or unpatched Apple mobile devices faces elevated risk of device compromise, data exfiltration, and persistent surveillance without user interaction.

Technical Analysis

Two exploit kits are actively targeting Apple iOS and iPadOS devices via web-based vectors, requiring minimal or no user interaction beyond visiting a malicious or compromised site (T1189, Drive-by Compromise). Coruna targets iOS 13.0 through 17.2.1 and is assessed as a direct evolution of the Operation Triangulation exploit chain (low-to-medium confidence, based on secondary reporting pending primary source confirmation), a sophisticated multi-stage framework previously attributed to APT actors. Its commoditization indicates tooling has migrated to secondary markets accessible to lower-sophistication actors (T1587.004, Exploits). DarkSword targets iOS 18.4 through 18.7; actor attribution is low confidence pending additional technical reporting. Both kits exploit memory corruption vulnerability classes: use-after-free (CWE-416), out-of-bounds write (CWE-787), and improper restriction of operations within memory bounds (CWE-119). These patterns are consistent with browser-level or kernel-level exploit chains. Post-exploitation behavior maps to MITRE ATT&CK techniques

including exploitation for client execution (T1203), drive-by compromise (T1189), location tracking (T1430), standard application layer protocol for C2 (T1071.001), video capture (T1512), and exploitation of OS privilege escalation (T1404). No CVE identifiers are currently assigned. No EPSS data is available. CISA KEV status is negative as of 2026-03-04. CVSS base is assessed at 9.5 by the source pipeline; no vendor-confirmed CVSS vector is available. All source URLs are T3 (secondary/media) and require human validation before operational use.

Action Checklist

1. Step 1: Containment, Immediately identify all managed iOS and iPadOS devices in your environment. Flag any device running iOS 13.0-17.2.1 (Coruna exposure) or iOS 18.4-18.7 (DarkSword exposure) as high priority. If MDM is deployed, query enrolled device OS versions now. For unmanaged BYOD devices with corporate access, issue an emergency user notification requiring update confirmation before continued access. Restrict MDM-managed devices from accessing corporate resources until patch status is confirmed.
2. Step 2: Detection, No confirmed IOCs are available from verified sources as of 2026-03-04; treat IOC fields as unverified pending human source validation. For behavioral detection, review mobile threat defense (MTD) logs for anomalous process spawning, unexpected network connections from Safari or WebKit processes, or device jailbreak indicators. Query MDM telemetry for device integrity failures. If MTD is not deployed, check network perimeter logs for outbound connections from mobile device IP ranges to uncategorized or newly registered domains. Apple's on-device lock screen notification is itself an indicator, document any user-reported alerts immediately.
3. Step 3: Eradication, Apply the latest available Apple security update. As of 2026-03-04, Apple has issued updates addressing these exploit chains; confirm the specific patch version via Apple's Security Releases page at https://support.apple.com/en-us/100100 (human validation required, verify this URL resolves correctly before operational use). For devices that cannot be updated immediately, consider restricting Safari and disabling JavaScript in Safari settings as a partial mitigation for web-based delivery vectors. This does not eliminate risk but reduces the drive-by attack surface.
4. Step 4: Recovery, After patching, verify OS version compliance across all managed devices via MDM compliance reports. For any device that received an Apple lock screen warning or shows MTD anomaly indicators, treat as potentially compromised: perform a full device wipe and restore from a known-clean backup predating the suspected exposure window, or issue a replacement device. Monitor post-patch for residual C2 activity from previously compromised devices. Confirm no unauthorized MDM profiles or configuration changes were installed.
5. Step 5: Post-Incident, This campaign exposes three control gaps worth addressing regardless of whether active compromise is confirmed. First, mobile device patch lag: establish a policy requiring iOS updates within 72 hours of Apple security releases, enforced via MDM compliance gates. Second, mobile threat defense coverage: if MTD is absent, evaluate deployment, web-based zero-click and one-click vectors are not visible to traditional endpoint controls. Third, BYOD governance: the commoditization of nation-state tooling increases risk from personal devices with corporate access; review whether current BYOD policy reflects this elevated threat environment.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if any device that received an Apple on-device lock screen alert is confirmed to have accessed, stored, or transmitted PII, PHI, or regulated financial data during the Coruna or DarkSword exposure window, as this may trigger breach notification obligations under HIPAA, state data breach statutes, or PCI DSS Incident Response requirements; also escalate if any compromised device belongs to an executive, privileged IT administrator, or user with access to M&A, legal, or national security-adjacent data, given the nation-state lineage of Coruna.
Recovery Notes	Devices that received Apple's on-device lock screen warning must be treated as confirmed-compromised for recovery purposes — wipe and restore from a backup predating the exposure window, or replace the device, before returning to service; do not rely on patching alone for these devices given the documented persistence capabilities of the Operation Triangulation exploit chain from which Coruna descends. Post-recovery, monitor all previously exposed devices' network activity for a minimum of 30 days using perimeter firewall or DNS logs scoped to mobile device IP ranges, specifically watching for low-and-slow C2 beaconing patterns (periodic outbound connections to single IPs or domains on non-standard ports) that would indicate an implant survived the restore. Validate MDM re-enrollment integrity for all wiped devices by confirming the MDM profile is issued solely by your organization and that no secondary MDM or supervision certificate is present in `Settings > General > VPN & Device Management` before returning devices to production.
Forensic Artifacts	iOS crash logs from `/var/mobile/Library/Logs/CrashReporter/` on suspect devices — Coruna's WebKit-based delivery chain, consistent with its Operation Triangulation lineage, would produce crash reports from exploited com.apple.WebKit or MobileSafari processes with memory corruption signatures (EXC_BAD_ACCESS, SIGSEGV) at the time of initial exploitation, providing a timestamped exploitation event. | Safari browsing history and WebKit cache from `/var/mobile/Library/Safari/History.db` and `/var/mobile/Library/WebKit/` — these SQLite databases would contain the exploit kit delivery URL visited by the victim, which is the primary network indicator for both Coruna and DarkSword web-based delivery; extract with iMazing before any wipe. | MDM device compliance and integrity attestation logs showing `DeviceIntegrityStatus`, `IsSupervised`, `IsActivationLockEnabled`, and `ProfileList` fields — unauthorized MDM profiles or supervision certificates installed by an implant (a documented Operation Triangulation persistence technique) would appear as anomalies against your organization's known profile inventory. | Perimeter DNS and proxy logs filtered to mobile device IP ranges for the 90-day window preceding detection, queried for connections to domains with registration age under 30 days or to IP ranges in ASNs not consistent with legitimate CDN or SaaS traffic — exploit kit C2 infrastructure typically uses freshly registered domains to evade reputation-based blocking, making new-domain DNS queries the most reliable network-layer indicator available without MTD. | Apple lock screen alert user reports with device UDID, exact alert timestamp, and iOS version — Apple's on-device notification is a first-party attestation that the device was targeted; correlating the alert timestamp against iOS syslog entries and network perimeter logs from the same device at the same time provides a multi-source chain of custody record for the exploitation event.

Per-Action IR Details

Step 1: Containment — Immediately identify all managed iOS and iPadOS devices in your environment. Flag any device running iOS 13.0-17.2.1 (Coruna exposure) or iOS 18.4-18.7 (DarkSword exposure) as high priority. If MDM is deployed, query enrolled device OS versions now. For unmanaged BYOD devices with corporate access, issue an emergency user notification requiring update confirmation before continued access. Restrict MDM-managed devices from accessing corporate resources until patch status is confirmed.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-8 (System Component Inventory), NIST AC-17 (Remote Access), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without MDM: run `curl -s https://your-mdm-api` is unavailable — instead, query Active Directory or Entra ID for mobile device registrations using `Get-MgDevice -Filter "operatingSystem eq 'iOS'" | Select-Object DisplayName,OperatingSystemVersion` (Microsoft Graph PowerShell). Cross-reference against any VPN or Wi-Fi RADIUS authentication logs to enumerate devices by IP range. For BYOD, send a forced acknowledgment email with a deadline; revoke VPN certificates or disable Wi-Fi 802.1X credentials for non-responders using your RADIUS server or firewall ACL.

Evidence: Before restricting access, capture MDM enrollment reports showing each device's current iOS version, last check-in timestamp, and assigned user — this establishes the exposure window for Coruna (iOS 13.0–17.2.1) and DarkSword (iOS 18.4–18.7) scope. Export network perimeter DHCP lease logs and NAC records mapping mobile device MAC addresses to IP assignments during the suspected exposure window. Preserve any MDM compliance violation alerts generated before containment, as these establish pre-action device state.

Step 2: Detection — No confirmed IOCs are available from verified sources as of 2026-03-04; treat IOC fields as unverified pending human source validation. For behavioral detection, review mobile threat defense (MTD) logs for anomalous process spawning, unexpected network connections from Safari or WebKit processes, or device jailbreak indicators. Query MDM telemetry for device integrity failures. If MTD is not deployed, check network perimeter logs for outbound connections from mobile device IP ranges to uncategorized or newly registered domains. Apple's on-device lock screen notification is itself an indicator — document any user-reported alerts immediately.

NIST Phase: Detection Analysis

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

Controls: NIST IR-5 (Incident Monitoring), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without MTD: configure your perimeter DNS resolver (Pi-hole, BIND, or Infoblox) to log all queries from the mobile device VLAN/subnet and pipe output to a text file for grep-based analysis — `grep -E '(newly-registered|uncategorized)' /var/log/dns-queries.log` won't work directly, but querying your ISP's or firewall's threat-categorization API against your DNS log is achievable with a short Python script. For jailbreak behavioral signals, use iMazing (free tier) on a macOS workstation to pull iOS syslog from a physically connected suspect device and search for entries referencing `libraryvalidation` failures, `amfid` denials, or `com.apple.WebKit` network activity to unexpected external IPs. Document every user-reported Apple lock screen warning with screenshot, timestamp, device identifier, and user account — this is your primary detection corpus in the absence of MTD.

Evidence: Capture iOS syslog from suspect devices via iMazing or Apple Configurator 2 before any update or wipe — Coruna, as a WebKit-delivered exploit chain descended from Operation Triangulation, would leave traces in `/var/mobile/Library/Logs/CrashReporter/` (crash logs from exploited WebKit/Safari processes), `/var/mobile/Library/Safari/` (browsing history showing the delivery URL), and syslog entries showing anomalous `com.apple.WebKit.Networking` process behavior. For network evidence, extract perimeter firewall or proxy logs filtered to mobile device IP ranges showing connections to domains registered within the past 30 days (DomainAge > 0, DomainAge < 30 in your proxy categorization data), which is consistent with web-based exploit kit infrastructure. Preserve screenshots or photos of any Apple lock screen alert as primary user-reported indicators and log the exact device, time, and user for correlation.

Step 3: Eradication — Apply the latest available Apple security update. As of 2026-03-04, Apple has issued updates addressing these exploit chains; confirm the specific patch version via Apple's Security Releases page at https://support.apple.com/en-us/100100 (human validation required — verify this URL resolves correctly before operational use). For devices that cannot be updated immediately, consider restricting Safari and disabling JavaScript in Safari settings as a partial mitigation for web-based delivery vectors. This does not eliminate risk but reduces the drive-by attack surface.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST CM-8 (System Component Inventory), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without automated MDM patch enforcement: create a supervised iOS configuration profile (via Apple Configurator 2, free) that sets `allowJavaScriptInSafari = false` and deploys it to unpatched devices as an emergency restriction — this directly degrades the web-based drive-by delivery mechanism used by both Coruna and DarkSword without requiring a patch. Simultaneously, push a managed app restriction blocking Safari entirely if your MDM supports it, and direct users to a patched alternative browser as a stopgap. Track patch completion manually in a shared spreadsheet with device ID, UDID, iOS version before and after, and timestamp — this becomes your eradication evidence record for post-incident review.

Evidence: Before deploying the patch, capture the current iOS build version string from each device via MDM (`CurrentBuildVersion` field in MDM device inventory) and preserve it — this documents the vulnerable state for your incident record. For devices flagged as potentially compromised, extract a full iOS backup via iMazing to a write-protected destination before patching, preserving the file system state for later forensic analysis if compromise is confirmed. Check for unauthorized MDM configuration profiles installed on the device (`Settings > General > VPN & Device Management`) and screenshot or record any profiles not issued by your organization, as Coruna-class implants in the Operation Triangulation lineage have been documented installing persistence via configuration profiles.

Step 4: Recovery — After patching, verify OS version compliance across all managed devices via MDM compliance reports. For any device that received an Apple lock screen warning or shows MTD anomaly indicators, treat as potentially compromised: perform a full device wipe and restore from a known-clean backup predating the suspected exposure window, or issue a replacement device. Monitor post-patch for residual C2 activity from previously compromised devices. Confirm no unauthorized MDM profiles or configuration changes were installed.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CP-10 (System Recovery and Reconstitution), NIST AU-11 (Audit Record Retention), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For teams without MTD post-recovery monitoring: configure a firewall or DNS-based watchlist for the mobile device subnet for a minimum 30-day observation window post-patch, alerting on any outbound connection to domains or IPs not seen in your baseline. Use Wireshark or tcpdump on your perimeter with a BPF filter scoped to mobile device IP ranges (`host 192.168.x.0/24 and not (port 80 or port 443 to known-good CDNs)`) for periodic spot-checks. Validate backup integrity before restoring by checking the iMazing backup manifest for modification timestamps that postdate the suspected compromise window — do not restore a backup whose modification time falls within the exposure window without forensic review first.

Evidence: After wiping and restoring a device flagged by Apple's lock screen alert, capture and retain: the MDM compliance report showing the pre-wipe OS version and compliance failure timestamp; the iMazing or iTunes backup manifest from the device's last backup before suspected compromise (to validate restore-point integrity); and network perimeter logs from the 30 days post-recovery filtered to that device's MAC/IP, which would reveal residual C2 beaconing if an implant survived a restore (a known capability of advanced persistence mechanisms in the Operation Triangulation lineage, where kernel-level implants have survived backups in prior documented cases). Preserve the full device wipe confirmation log from MDM as your eradication attestation record.

Step 5: Post-Incident — This campaign exposes three control gaps worth addressing regardless of whether active compromise is confirmed. First, mobile device patch lag: establish a policy requiring iOS updates within 72 hours of Apple security releases, enforced via MDM compliance gates. Second, mobile threat defense coverage: if MTD is absent, evaluate deployment — web-based zero-click and one-click vectors are not visible to traditional endpoint controls. Third, BYOD governance: the commoditization of nation-state

tooling increases risk from personal devices with corporate access; review whether current BYOD policy reflects this elevated threat environment.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: For teams without budget for commercial MTD: deploy iVerify Basic (free tier, available on App Store) to user devices as a user-reportable jailbreak and compromise detection tool — it provides behavioral integrity checks aligned to known iOS exploit patterns including those in the Triangulation lineage. Establish a free CISA alert subscription (`cisa.gov/uscert/mailing-lists-and-feeds`) and Apple Security Research Device Program notifications to reduce future patch-lag detection time. Draft a one-page BYOD attestation form requiring users to confirm iOS version compliance within 72 hours of any Apple security release as a policy backstop where MDM compliance gates are not enforceable on personal devices.

Evidence: For lessons-learned documentation, compile: a timeline mapping Apple's security release date to your organization's last-device-patched date for this incident (quantifies patch lag for the after-action report); MTD or DNS log data showing whether any mobile device successfully contacted known exploit kit delivery infrastructure during the exposure window (establishes whether exposure translated to delivery attempts); and a count of BYOD versus MDM-managed devices in the affected iOS version ranges (quantifies the unmanaged device governance gap for leadership reporting). This data directly supports the three control gap findings identified in this step and provides measurable baselines for the policy improvements recommended.

Detection Guidance

No verified IOCs are available from confirmed primary sources as of 2026-03-04. All source URLs are T3 (media/secondary) and require human validation before use in detection rules or threat intel platforms. Do not ingest unverified IOCs into production detection infrastructure. Behavioral indicators to prioritize: (1) MDM-reported devices running iOS 13.0-17.2.1 or iOS 18.4-18.7 with no recent update activity; (2) MTD alerts for WebKit or Safari process anomalies, unexpected kernel-level activity, or jailbreak detection; (3) user-reported Apple lock screen warning notifications, log these as a soft indicator and treat the device as suspect; (4) network logs showing outbound traffic from mobile device subnets to newly registered domains, domains with low Alexa/Tranco ranking, or domains using fast-flux DNS, consistent with T1071.001 (Application Layer Protocol: Web Protocols) for C2; (5) DNS queries for domains not previously seen in your environment, initiated from mobile device IP ranges. For hunting: if your SIEM ingests MDM or MTD data, build a query for devices in the affected OS version ranges that have not checked in for a patch update in the last 14 days. Flag those devices for manual review.

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No IOCs available`	No verified IOCs have been confirmed from primary or validated secondary sources as of 2026-03-04. All discovery sources are T3 (media). Do not fabricate or ingest unverified indicators. Monitor Google Cloud Threat Intelligence, iVerify, and Apple Security Releases for updated IOC releases as technical reporting matures. Human validation of all source URLs is required before use.	LOW

Framework Mappings

MITRE-ATTACK

- **T1203** — Exploitation for Client Execution
- **T1430** — Location Tracking
- **T1189** — Drive-by Compromise
- **T1071.001** — Web Protocols
- **T1584** — Compromise Infrastructure
- **T1404** — Exploitation for Privilege Escalation
- **T1624** — Event Triggered Execution
- **T1512** — Video Capture
- **T1587.004** — Exploits

NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10**
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1203	Exploitation for Client Execution	Execution
T1430	Location Tracking	Collection
T1189	Drive-by Compromise	Initial-Access
T1071.001	Web Protocols	Command-And-Control
T1584	Compromise Infrastructure	Resource-Development
T1404	Exploitation for Privilege Escalation	Privilege-Escalation
T1624	Event Triggered Execution	Persistence
T1512	Video Capture	Collection
T1587.004	Exploits	Resource-Development

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/apple-sends-lock-screen-alerts-to...	T3
iOS Exploit Chain Adopted by Multiple Threat Actors - Google Cloud	https://cloud.google.com/blog/topics/threat-intelligence/darksword-...	T3
New 'DarkSword' Hack Targets Older iOS 18 Versions | PCMag	https://www.pcmag.com/news/update-your-iphone-now-new-darksword-hac...	T3
Inside DarkSword: A New iOS Exploit Kit Delivered Via ... - iVerify	https://iverify.io/blog/darksword-ios-exploit-kit-explained	T3
Apple urges iPhone users to update as Coruna and DarkSword ...	https://securityaffairs.com/189716/security/apple-urges-iphone-user...	T3

DISCLAIMER

Generated 2026-03-29 18:33 UTC by TJS Security Command Center