INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:37 UTC

iOS Exploit Kits Coruna and DarkSword Targeting Unpatched iPhones via Watering Hole Attacks

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0058
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Apple iPhone and iPad running iOS 13, iOS 14, iOS 15 (below 15.8.7), iOS 16 (below 16.7.15), and any iOS version below current latest release
Published	2026-03-21

Executive Summary

Two iOS exploit kits, Coruna and DarkSword (names not independently verified against primary Apple advisories), are actively targeting iPhones and iPads running unpatched versions of iOS 13, 14, 15 (below 15.8.7), and 16 (below 16.7.15) through compromised websites. These kits are now deployed at scale across multiple countries. Organizations with unmanaged or BYOD mobile devices face immediate risk of device compromise and potential data exfiltration; emergency patches are available and should be deployed without delay.

Technical Analysis

Apple has released emergency updates addressing memory safety vulnerabilities exploited by unnamed iOS exploit kits (referred to in secondary reporting as 'Coruna' and 'DarkSword'; names not independently corroborated against primary Apple advisories as of this analysis) via watering hole attacks (MITRE T1189). Affected platforms: iOS/iPadOS 13 (all versions), 14 (all versions), 15 (below 15.8.7), and 16 (below 16.7.15). No CVE identifiers were assigned or disclosed in available source data. Exploit classes include use-after-free (CWE-416), out-of-bounds write (CWE-787), and buffer overflow/memory corruption (CWE-119). Exploitation chain likely involves watering hole infection via malicious or compromised web content (T1189, T1203), followed by local privilege escalation (T1404) to achieve persistent access. Post-exploitation activity may include data collection from device storage (T1005), camera or screenshot capture (T1512), location tracking (T1430), and C2 communication over HTTP/S (T1071.001). Remediation: iOS 15.8.7/iPadOS 15.8.7 (support.apple.com/en-us/126632) and iOS 16.7.15/iPadOS 16.7.15 (support.apple.com/en-us/126646). Devices that cannot receive these updates (e.g., iOS 13/14 hardware at end-of-support) have no

vendor-supplied patch and should be treated as persistently high-risk.

Action Checklist

1. Step 1, Patch immediately: Push iOS 15.8.7/iPadOS 15.8.7 or iOS 16.7.15/iPadOS 16.7.15 to all managed devices via MDM. Verify update status within 24 hours. Devices on iOS 13 or 14 cannot receive these patches and require escalated handling.
2. Step 2, Identify unmanaged and BYOD devices: Query your MDM (e.g., Jamf, Intune) for all enrolled iOS endpoints. Identify gaps where BYOD devices are accessing corporate email, VPN, or SaaS applications without enrollment. Flag devices below patch thresholds.
3. Step 3, Restrict access for unpatched devices: Apply conditional access policies to block or quarantine iOS devices below 15.8.7 or 16.7.15 from corporate resources until patched. For devices on iOS 13/14 with no patch path, initiate device replacement or hardware upgrade review.
4. Step 4, Review web proxy and DNS logs (if available) for watering hole indicators: If your organization deploys web proxy, DNS filtering, or mobile threat defense (MTD), review logs for anomalous web traffic from iOS devices to newly registered domains, domains with low reputation scores, or deviations from historical user browsing patterns. Organizations without these tools should focus on Step 3 (conditional access) and MDM inventory (Step 2) as primary detection mechanisms.
5. Step 5, Notify stakeholders and update mobile security policy: Brief security leadership on exposure scope from MDM inventory. Communicate patch urgency to employees with BYOD agreements. Review and update mobile device management policy to enforce minimum OS version requirements and automate non-compliant device quarantine going forward.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to security leadership and legal if more than 10% of managed iOS devices remain unpatched after 7 days, or if watering hole indicators are confirmed in proxy/DNS logs within your organization's network.
Recovery Notes	Post-containment, implement automated MDM compliance enforcement to prevent recurrence: set iOS 13/14 devices to automatic enrollment suspension, enforce quarterly patch audits, and integrate threat intelligence feeds into conditional access policies. Conduct post-incident review with mobile ops team to document response timelines, tool gaps, and personnel training needs. Engage with MDM vendor for native exploit detection/mitigation features (if available) to reduce detection lag on future zero-days.
Forensic Artifacts	MDM enrollment database (device OS versions, last check-in, compliance status, serial numbers, user assignments) | Web proxy access logs (iOS User-Agent, destination domain, timestamp, HTTP status, request/response size) | DNS resolver query logs (source iOS device IP, queried domain, response code, timestamp) | Mobile threat defense (MTD) alerts and blocked connection logs (threat name, source device, destination, timestamp) | Email gateway and VPN authentication logs (iOS device model/OS version from session metadata, login timestamp, source IP, success/failure status)

Per-Action IR Details

Step 1 — Patch immediately: Push iOS 15.8.7/iPadOS 15.8.7 or iOS 16.7.15/iPadOS 16.7.15 to all managed devices via MDM. Verify update status within 24 hours. Devices on iOS 13 or 14 cannot receive these patches and require escalated handling.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (Preparation phase: tools and resources)

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Information System Monitoring), CIS 3.10 (Address Unauthorized Software), CIS 1.2 (Inventory and Control of Hardware Assets)

Compensating: Without MDM: distribute patch via email with direct Apple ID instructions; create forced-update compliance checklist tracked in shared spreadsheet; audit compliance weekly via IT helpdesk support tickets. For iOS 13/14 devices, document ownership and initiate hardware replacement request process with finance and procurement.

Evidence: Before pushing updates: capture MDM enrollment roster with OS versions (export from Jamf/Intune as CSV); document current patch baseline via MDM reports; preserve pre-patch device inventory list with serial numbers and user assignments. Post-patch: retain MDM compliance reports showing update success/failure rates per device.

Step 2 — Identify unmanaged and BYOD devices: Query your MDM (e.g., Jamf, Intune) for all enrolled iOS endpoints. Identify gaps where BYOD devices are accessing corporate email, VPN, or SaaS applications without enrollment. Flag devices below patch thresholds.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Analysis: understanding the incident scope)

Controls: NIST CA-7 (Continuous Monitoring), NIST IA-4 (Identifier Management), CIS 1.1 (Inventory and Control of Hardware Assets), CIS 6.2 (Address Unauthorized Software)

Compensating: Without MDM: cross-reference corporate email access logs (via Exchange/Gmail audit logs) with VPN connection logs to identify unique iOS User-Agent strings and device IP addresses not matching known managed device baselines. Use conditional access logs in identity provider (Okta, Azure AD) to flag iOS sessions from unregistered devices. Manually survey BYOD agreements on file and contact users to self-report devices.

Evidence: Export MDM enrollment database with OS version, last check-in timestamp, and compliance status; pull VPN connection logs (auth and session records) for past 90 days filtered by iOS User-Agent; extract email access logs (login IP, user agent, device model from headers) for same period; capture identity provider conditional access logs showing blocked or prompted authentications from unmanaged iOS sources.

Step 3 — Restrict access for unpatched devices: Apply conditional access policies to block or quarantine iOS devices below 15.8.7 or 16.7.15 from corporate resources until patched. For devices on iOS 13/14 with no patch path, initiate device replacement or hardware upgrade review.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment phase: limiting scope and impact)

Controls: NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST SI-4 (Information System Monitoring), CIS 6.5 (Access Control Enforcement)

Compensating: Without conditional access: manually disable cloud app authentication tokens for unpatched iOS devices via identity provider (revoke Okta/Azure AD sessions by device OS version); configure VPN concentrator to deny connections from iOS 13/14/15/16 clients below specified version thresholds (check vendor ACL documentation for OS version filtering); block at email gateway by creating rule that rejects IMAP/ActiveSync from detected unpatched iOS User-Agents. Document each blocked user and device for tracking.

Evidence: Before restricting access: export list of all currently authenticated sessions from email, VPN, and cloud apps filtered by iOS device; capture baseline conditional access policy settings; document approved BYOD devices and their current OS versions. After restriction: retain access denial logs, quarantine event records, and notification logs sent to affected users.

Step 4 — Review web proxy and DNS logs for watering hole indicators: Check proxy, DNS, and mobile threat defense (MTD) logs for anomalous web traffic from iOS devices, particularly to newly registered domains, domains with low reputation scores, or domains not matching normal user browsing patterns in the days

preceding this advisory.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Analysis: indicators of compromise and artifact analysis)

Controls: NIST SI-4 (Information System Monitoring), NIST SI-12 (Information Handling and Retention), CIS 8.1 (Establish and Maintain Detailed Asset Inventory), CIS 13.6 (Collect and Analyze Network Traffic)

Compensating: Without MTD: query web proxy logs for iOS User-Agent traffic to domains registered in past 30 days (use WHOIS bulk query tools like whois.com API or domaintools; cross-reference against known malicious domain feeds from Abuse.ch, SURBL); search DNS resolver logs (if available from ISP or internal DNS appliance) for iOS client queries to low-reputation domains using threat intelligence feeds (AlienVault OTX, Shodan, VirusTotal). Manually correlate timeline: identify iOS devices accessing suspicious domains in 5-day window before advisory date. Use browser history exports from user interviews for non-centralized browsing.

Evidence: Preserve full proxy logs for past 30 days filtered by iOS User-Agent (request from proxy vendor if archived); extract DNS query logs for same period; download current MTD/mobile security gateway reports showing blocked threats per device; document domain reputation scores and registration dates for all flagged destinations; capture user access timeline (timestamp, source IP, destination domain, HTTP response code) for devices flagged as accessing watering hole indicators.

Step 5 — Notify stakeholders and update mobile security policy: Brief security leadership on exposure scope from MDM inventory. Communicate patch urgency to employees with BYOD agreements. Review and update mobile device management policy to enforce minimum OS version requirements and automate non-compliant device quarantine going forward.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities: improving monitoring and response processes)

Controls: NIST CA-2 (Security Assessments), NIST PM-6 (Security Planning), NIST IR-2 (Incident Response Training and Testing), CIS 19.1 (Establish and Maintain a Cybersecurity Awareness Program)

Compensating: Without formal stakeholder communication channels: distribute incident summary via email to all department heads with executive summary of exposure (unpatched device count, affected user count, data at risk); post BYOD policy update notice to employee intranet/wiki with step-by-step patching instructions and deadline (recommend 14-day enforcement window); hold optional helpdesk office hours for BYOD users to ask questions. Create policy document in accessible format (PDF + plain text) detailing minimum OS version (15.8.7, 16.7.15), auto-quarantine triggers, and device replacement request process.

Evidence: Document all notifications sent (email headers, timestamp, recipient list); retain signed acknowledgments from employees confirming policy review; capture updated MDM policy rules showing OS version enforcement thresholds; log all device replacement/upgrade requests initiated post-advisory; preserve baseline compliance metric (% patched devices) at Day 0, Day 7, Day 14, Day 30 for post-incident report.

Detection Guidance

No specific IOCs (IPs, domains, hashes) were disclosed in available source material. Detection should focus on behavioral and telemetry signals. (1) MDM/UEM telemetry: Query enrolled device OS versions to identify all endpoints below iOS 15.8.7 or 16.7.15. Devices on iOS 13 or 14 have no patch path and should be flagged immediately. (2) Mobile Threat Defense (MTD): If deployed (e.g., Lookout, Zimperium, Microsoft Defender for Endpoint on iOS), review alerts for anomalous process execution, privilege escalation attempts, or unexpected network connections from iOS devices. (3) Web proxy and DNS logs: Look for iOS user-agent strings accessing domains with newly registered certificates, low Alexa/Tranco rank, or domains flagged by threat intel feeds. Watering hole delivery means the malicious site may appear legitimate; volume-based anomalies (e.g., many iOS devices hitting the same uncommon domain) are a higher-value signal than single-instance lookups. (4) Network egress: Post-exploitation C2 uses HTTP/S (T1071.001). Look for iOS devices establishing persistent or

repetitive outbound connections to non-categorized or low-reputation hosts, particularly outside business hours. (5) SIEM correlation: Combine MDM-reported unpatched device list with proxy logs to surface unpatched devices that recently accessed high-risk or uncategorized web content. Note: Without disclosed CVEs or specific IOCs, detection confidence is limited. Human verification against updated Apple advisories and threat intel feeds is recommended before concluding a device is compromised.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No IOCs disclosed in available source data`	Apple advisories and secondary reporting (The Hacker News, Forbes, March 2026) did not publish specific indicators of compromise for Coruna or DarkSword activity. Monitor vendor threat intelligence feeds and CISA advisories for updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1189** — Drive-by Compromise
- **T1005** — Data from Local System
- **T1404** — Exploitation for Privilege Escalation
- **T1512** — Video Capture
- **T1071.001** — Web Protocols
- **T1430** — Location Tracking
- **T1587.001** — Malware
- **T1203** — Exploitation for Client Execution

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

CIS-V8

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

OWASP-TOP10-2021

- **A03:2021** — Injection

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1189	Drive-by Compromise	Initial-Access
T1005	Data from Local System	Collection
T1404		
T1512		
T1071.001	Web Protocols	Command-And-Control
T1430		
T1587.001	Malware	Resource-Development
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/03/apple-warns-older-iphones-vulnera...	T3
About the security content of iOS 15.8.7 and iPadOS 15.8.7	https://support.apple.com/en-us/126632	T3
About the security content of iOS 16.7.15 and iPadOS 16.7.15	https://support.apple.com/en-us/126646	T3
Apple has issued an urgent warning urging iPhone users to update ...	https://www.facebook.com/androidioszone/posts/apple-has-issued-an-u...	T3
New iOS Update Warning—Check Your iPhone Now For ... - Forbes	https://www.forbes.com/sites/kateoflahertyuk/2026/03/12/new-ios-upd...	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 2026-03-29 18:37 UTC by TJS Security Command Center