Coruna Exploit

Nation-State Grade ● Mass Exploitation Scale ● March 3, 2026

Threat	Coruna
Affected Devices	iPhones running iOS 13 to 17.2.1
Delivery	1-click exploit kit comprising 23 exploits across 5 complete attack chains
Attribution	Built by the United States, later leaked/stolen and resold on the secondary market
Objectives	Steal cryptocurrency and sensitive personal information

WHAT HAPPENED

On March 3, 2026, Google's Threat Intelligence Group disclosed Coruna, a sophisticated iOS 1-click exploit kit comprising 23 exploits across five complete attack chains targeting iPhones running iOS 13 through 17.2.1. iVerify researchers had been independently tracking the same kit for several weeks prior to this disclosure.

iVerify believes this highly sophisticated framework was almost certainly built by a nation-state, very likely the United States, leaked and/or stolen, and resold on the secondary market.

Coruna was used in two contexts. First, by Russian adversaries to surveil Ukrainians, and second, by Chinese e-criminal groups. In the Chinese e-criminal case, Coruna is delivered via a watering hole attack: a compromised or malicious website that silently executes an exploit chain the moment a vulnerable device loads the page. No user interaction beyond the page visit is required. The exploit achieves remote code execution in Safari, escalates to full device control, and deploys an implant, all within seconds and without any visible indication to the user.

The implant provides the attacker with persistent access to messages, photos, notes, credentials, and installed applications. It is designed to operate within legitimate iOS system processes to avoid detection, and maintain a backup command channel over SMS should primary infrastructure become unavailable. The primary goal of the implants were to steal cryptocurrency and sensitive personal information, which iVerify confirmed with in-the-wild testing.

WHY THIS MATTERS

Attacks against mobile operating systems have historically been rare and targeted. This attack marks a significant escalation in the mobile threat landscape as the first perpetrated by an e-criminal group for purely criminal purposes and the first time a nation-state developed tool has fallen into the hands of criminal groups. This is the "EternalBlue" moment for mobile security, as Andy Greenberg wrote in WIRED magazine.

Moreover, there are at any point in time a half dozen of iOS remote access toolkits in circulation on the secondary market at any point in time. The odds of copycat, follow-on attacks are high and the impact of falling victim severe. The highly modular nature of this framework makes it easy for criminal groups to write new implant modules that achieve other objectives, such as compromising payment accounts.

MITIGATIONS

There are two key points at which Coruna can be mitigated – the network and the endpoint. Coruna relies on watering holes and smishing techniques to distribute the malware, so solutions that block malicious links can offer a degree of protection.

At the endpoint level, iVerify has not observed Coruna running on iOS 26, so devices on the latest iOS patch should be protected. Devices on N-1 patching cadences may remain exposed. Finally, most enterprises rely on Mobile Device Management (MDM) tools or containerization (MAM) to manage their mobile fleets. It's important to remember that these tools can enforce patching policies, but otherwise offer no additional mitigations, as Coruna operates entirely within legitimate iPhone system processes.

- **MDM enforces policy.** It does not detect or stop attacks at the OS level. A device can be fully enrolled and managed, yet still be compromised.
- **Containerization does not protect the device.** Separating work apps into a container does not prevent the underlying operating system from being exploited. Once the OS is compromised, containers are easily breached and exploited

RECOMMENDED ACTIONS

Timeframe	Action
0-72 Hours	Update all managed iPhones to iOS 17.3 or later. Apple has patched the vulnerabilities Coruna exploits in subsequent releases.
0-72 Hours	Identify iPhones with access to corporate systems that fall outside MDM enrollment.
30 Days	Assess whether current mobile security tooling has visibility into OS-level activity, not just the application layer or network layer.
30 Days	Consider forensic review of high-risk individuals: executives, finance, legal, and IT administrators who used iPhones on vulnerable iOS versions.
90 Days	Review mobile security architecture against this class of threat and determine whether detection capabilities need to be extended to the system level.

ABOUT iVERIFY

iVerify is a leading Mobile Endpoint Detection and Response solution that directly addresses the structural detection gap exposed by the DarkSword incident. The purpose-built tool detects remote zero-click exploitation and sophisticated mobile threats that legacy Mobile Threat Detection (MTD) and Mobile Device Management (MDM) platforms fundamentally cannot see.

Key Features for Enterprise Detection and Protection

- **Unrivaled Mobile Visibility:** Provides continuous system-level telemetry collection on iOS and Android devices without requiring scanning, tethering, or user action.
- **Advanced Threat Detection:** Detects modern exploitation techniques such as remote zero-click spyware, nation-state campaigns, and credential theft, with proven success finding advanced threats like Coruna, Pegasus, and Predator.
- **Network-Level Protection:** Offers network-level detections to identify SIM swapping attempts and connections to malicious cellular infrastructure.
- **True BYOD Protection:** Enables security without MDM, collects zero PII, and deploys flexibly through zero-touch, on-prem, or cloud options, making it easier to roll out across a fleet.

Book a personalized demo today to protect your fleet from the next mass-scale attack.

Further Resources:

iVerify Mobile Threat Briefing - Coruna Mobile Exploit Framework

Coruna: Inside the Nation-State-Grade iOS Exploit Kit We've Been Tracking

Coruna iOS Exploit: How to Detect and Prevent Infection

Other Threat Intel:

DarkSword Technical Findings

DarkSword Threat Briefing