iVerify.

# Mass-Scale Mobile Exploitation and the Enterprise Detection Gap

## What DarkSword & Coruna Reveal About Enterprise Mobile Security Gaps

The DarkSword iOS exploit kit, disclosed by iVerify researchers in conjunction with Google Threat Intelligence Group, and Coruna demonstrate that mobile attacks have evolved into fully industrialized operations. Exploits now combine high sophistication with broad reach, enabling attackers to compromise hundreds of millions of devices while bypassing standard security controls, even at an enterprise level.

Mobile devices play a central role in enterprise authentication, communication, and system access, making them a high-value target for exploitation. At the same time, limited telemetry and OS-level constraints leave them opaque to traditional monitoring and detection approaches.

This results in a structural mobile blind spot across the enterprise. Closing this gap requires treating mobile devices as primary enterprise endpoints, with visibility and detection at the process and memory level, implemented through a mobile-specific security approach.

### Key Characteristics of Exploitation

Both Coruna and DarkSword demonstrate deliberate efforts to minimize forensic artifacts and maximize invisibility:

- Injection into trusted processes instead of launching new ones.
- In-memory execution to avoid filesystem indicators.
- Cleanup of crash logs and temporary files.
- Use of legitimate system services for communication.

### Limited Visibility

Mobile endpoints operate with constrained visibility by design, leaving SOCs unable to detect in-memory or process-level exploit activity.

### Exploitation in Legitimate Contexts

Both DarkSword and Coruna execute within system processes or transient memory, making attacks difficult to detect and forensic analysis complex and costly.

### MDM Gaps

Mobile Device Management solutions enforce policy but do not provide runtime telemetry or exploit detection. Relying solely on MDM creates a coverage blind spot the size of your mobile fleet.

### Scalable Threats

Modern exploit kits are modular and automated, enabling opportunistic attacks at massive scale without manual targeting.

## The iVerify Solution: Delivering Operating System-Level Visibility on Mobile Devices

iVerify is designed to deliver device-level visibility, whether iOS- or Android-based, across your entire mobile fleet at the same execution layer where modern mobile exploits operate. By combining on-device analysis with continuously updated threat intelligence, iVerify detects behavioral signals, process anomalies, and system integrity violations left behind by exploit chains, even when traditional indicators are absent. This approach makes mobile activity observable, measurable, and actionable within enterprise security workflows.

The result is endpoint-level visibility for mobile devices, closing the structural blind spot and enabling organizations to detect and respond to threats targeting identity, communication, and access.

## Technical Coverage Overview

| iVerify Capability | Technical Overview | Why It Matters for Enterprise Security |
|---|---|---|
| **Advanced Exploit Detection** | Detects zero-click and N-day exploitation using real-time device behavioral signals | Provides the ability to see and respond to hidden threats operating below the application layer, securing mobile fleets before compromise occurs. |
| **Active Threat Identification** | Identifies anomalies across system processes and communications that indicate active threats. | Directly counters the technique of injecting capabilities into trusted system processes, enabling the distinction between malicious and normal system activity. |
| **Continuous Integrity Assessment** | Continuously assesses device integrity, not just configuration or compliance state. | Moves detection beyond policy enforcement, which MDM handles, to provide visibility into device integrity and behavioral changes. |
| **SmishGuard** *(available Q2 2026)* | Uses on-device NLP and ML models to analyze sender reputation, message body, and links for targeted smishing/vishing attacks while ensuring user privacy. | Protects employees from SMS and voice-based social engineering, safeguarding against corporate credential theft, data loss, and unauthorized transactions. |
| **SIM-Swap Detection** | Identifies anomalies that indicate a potentially unauthorized transfer of an employee's mobile number. | Prevents attackers from bypassing MFA via SIM-swap to gain access to corporate accounts. |
| **NowSecure Integration** | Enables automatic risk assessment of apps installed on corporate devices. | Provides continuous application security posture management by identifying and flagging risky or vulnerable apps on employee devices. |