Threat Intelligence

The Mobile Signal Your Threat Intelligence Program is Missing

iVerify Threat Intelligence provides high-signal mobile intelligence built from kernel-adjacent telemetry, exploit research, cellular signaling data, and forensic investigations.

The Mobile Intelligence Gap

Mobile users are actively targeted by opportunistic criminal attackers, nation-state actors, and commercial spyware operators. Without mobile intelligence, security teams lack the visibility to investigate, anticipate, and respond to attacks targeting their mobile workforce.

Five Evidence Streams. One Structured Intelligence Layer.

Kernel-Adjacent Telemetry
Behavioral and diagnostic telemetry collected across iOS and Android environments.

Exploit Research
Analysis of vulnerabilities, exploit chains, and post-exploitation activity observed in the wild.

Cellular Signaling
Carrier and signaling-derived insights that provide additional visibility into mobile attacks and global surveillance activity.

Mobile Operator Data
Extracts of global data from over 1000 mobile operators, providing unique insights into key network identifiers, IP addresses, vendor equipment, and international transit carriers used to exchange inter-operator signaling and service traffic.

Forensic Investigations
Artifacts recovered from real-world mobile compromise investigations and incident response engagements.

Intelligence Outcomes

Earlier Threat Identification
Identify emerging mobile malware and network campaigns, exploit activity, and adversary operations before they become widespread incidents.

Faster Triage & Investigation
Reduce analyst effort through contextual intelligence around malware behavior, attack surfaces, and adversary TTPs.

Improved Detection Coverage
Use intelligence derived from in the wild mobile telemetry and exploit research to inform detection engineering and threat hunting workflows.

Better Risk Prioritization
Focus remediation efforts on threats based on geography, severity, attacker sophistication, and organizational exposure.

Structured, High-Signal Intelligence
Not generic indicators. Not raw alerts. Actionable intelligence for security decision-making.

What Makes iVerify Different?

Traditional Threat Intelligence	iVerify Threat Intelligence
IOC-centric reporting	Behavior and TTP-centric intelligence
Network & endpoint visibility	Visibility across iOS, Android, cellular network, & network supply chain threats
Third-party reporting & shared feeds	Original exploit research and forensic investigations
Public indicators & malware samples	Kernel-adjacent telemetry, cellular signaling, & attack artifacts, in-the-wild attacks, & actor attribution
Threat activity after public disclosure	Early indicators from active mobile threat research with constantly updated telemetry
Generic threat prioritization	Prioritization based on attacker behavior, severity, global risk, geopolitical indicators, & organizational exposure
Limited visibility into mobile attack chains	Deep analysis of mobile-specific exploit chains, malware behavior, mobile operators & network infrastructure, adversary upstream connections, & C2 sources
Broad threat coverage	Specialized intelligence focused exclusively on multi-domain mobile threats

Why iVerify?

iVerify researchers disclosed DarkSword and Coruna before they became widespread enterprise incidents. The same research team powers iVerify Threat Intelligence, providing early indicators and actionable intelligence on emerging mobile threats.

- **Kernel-adjacent telemetry**
- **Mobile exploit research**
- **Real-world forensic investigations**
- **iOS & Android coverage**

Built For

Threat Intel Teams

Track emerging mobile threats & adversary activity

Threat Hunters

Access investigation artifacts & technical indicators

Incident Responders

Accelerate investigations with mobile-specific context

Detection Engineers

Build detections from observed TTPs & attack patterns

SOC Analysts

Prioritize alerts using threat intelligence & risk context

Close the Mobile Gap in Your Threat Intelligence Program

See how iVerify can transform your mobile security posture in just 15 minutes. Request a demo today.