



SECIRON USE CASES

The device your customer trusts most is the one you can least control

Three real attack scenarios from Seciron deployments: HTTPS hijacking at a bank, months of silent reconnaissance, and 2,616 staff faking their GPS.



WHY THIS IS HAPPENING NOW

Mobile fraud has moved off the server and onto the device and the numbers show it accelerating

Banking, telecom and enterprise apps now run on hardware, operating systems and networks the business does not own. Independent threat research from 2025–2026 shows this shift isn't gradual it's compounding, and it follows the same pattern across every industry below. Attack tooling is also getting faster to weaponize: techniques that once took specialist skill to execute are now packaged, automated and shared, shrinking the gap between a new vulnerability and its exploitation in the wild.

271%

year-over-year rise in unique mobile banking trojan packages

67%

Increase in malware-driven fraudulent transactions year-over-year

60%

of mobile banking apps lack SSL pinning or equivalent controls, exposed to HTTPS interception

1 in 20

verification attempts to online financial services is now estimated to be fraudulent

Three components behind the shift

- 1 On-device fraud, not just credential theft.** Modern banking trojans like ROKAROLLA, Mamont and Anatsa no longer stop at stealing passwords — they use overlay screens, accessibility abuse and remote control to initiate transactions directly from the victim's own device, making the activity indistinguishable from a genuine session.
- 2 The app store is no longer a reliable gate.** Attackers routinely publish clean-looking utility apps that only activate malicious payloads weeks later — Anatsa reached 90,000 downloads on Google Play disguised as a document viewer before removal.
- 3 Location and identity signals are now trivially faked.** GPS spoofing tools, once niche, are widely available and can simultaneously fake latitude, longitude, altitude and speed — undermining any workflow, from KYC to attendance, that trusts a device's reported location.

The three components above don't stay confined to one industry. They show up as concrete, costly incidents wherever a mobile app handles money, identity or trust. The following three use cases, drawn from SecIron's own deployments, show each component in action: what it looked like on a real device, and how it was caught.

Sources: Kaspersky Securelist Mobile Statistics Q1–Q2 2026; RiskInMind, "Mobile Banking Risk" (2026); Bitsight Threat Intelligence.

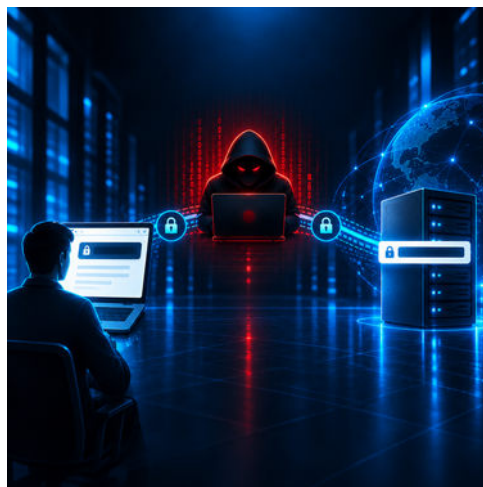


Use Case 1: HTTPS hijacking against a large bank

Attackers used HTTPS hijacking to bypass the bank's identity verification and steal customers' sensitive data — a technique that requires no server breach, only a compromised device.

The risk

Rooted devices, emulators, dynamic debugging and developer mode all create the conditions for traffic interception — invisible to defenses that only watch the server side.



How SecIron solved it

Detect: HTTPS hijacking and related attack indicators, root, emulator, dynamic debugging, developer mode and more. These are flagged in real time.

Respond: Once HTTPS hijacking is confirmed, the attack is blocked immediately and a real-time alert is sent to the server side.

Professional Service: Where deeper interpretation is needed, SecIron's security consultants review monitoring data and deliver an inspection and prediction analysis report.

2.5M

devices monitored

30,000

high-risk offensive devices
identified

130,000+

attacks detected in a day,
99.67% HTTPS hijacking

Consultant analysis blacklisted high-risk devices, flagged a rising pattern of hook and dynamic-injection risk, and prioritized abnormal root certificates and HTTPS hijacking as ongoing monitoring items.

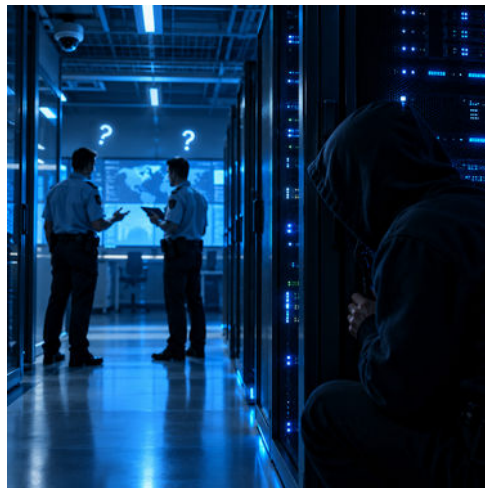


Use Case 2: Unknown penetration attacks against a Bank

The bank had no mobile app security analysis capability, no way to see hidden vulnerabilities, and no early warning before an attack landed.

The risk

Reconnaissance against a mobile app is invisible without device-level telemetry — attackers can map an app's weaknesses for months before striking.



How SecIron solved it

- **Participate:** the bank's environment fed into SecIron's platform data collection and analysis, rather than being assessed cold.
- **Investigate:** security experts manually analyzed the attacker's abnormal behavior to establish intent and capability.
- **Predict & advise:** findings were used to forecast likely future attacks, with concrete recommendations to close the gaps.

9 abnormal IPs

Discovered on day one of expert inspection

High-risk devices were running attack frameworks including **EdXposed** and **Frida**, and frequently rotating IP addresses. Correlation analysis tied all 9 IPs to a single hacker organization assessed as likely to attempt HTTPS hijacking or hook attacks next — with the affected IPs and devices recommended for blocking.

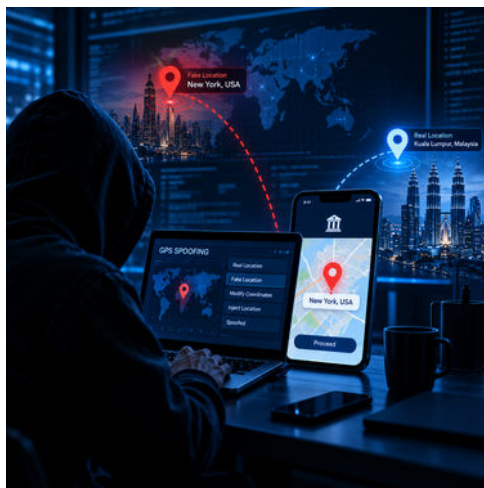


Use Case 3: Location fraud at a telco company

Outsourced staff used location-spoofing tools to "check in" without being physically present, letting the company pay subsidies for work that never happened.

The risk

Root access, emulators, dynamic debugging and developer mode make GPS spoofing straightforward and the business has no way to tell a real check-in from a simulated one.



How SecIron solved it

Detect: location fraud and related attack indicators — root, emulator, dynamic debugging, developer mode and more.

Respond: once GPS fraud is detected, the mobile app blocks the attack immediately and sends a real-time alert to the server side.

Professional Service: where security expertise is needed to interpret monitoring data or analyze hidden risk, SecIron provides consultant-led inspection and a security prediction analysis report.

2,616 outsourced staff caught using location fraud tools

SecIron traced the **specific tool used, its frequency, timing and the identity of each offending staff member and blacklisted the high-risk devices and emulators involved**, making location fraud a standing priority monitoring item.

TIP This visibility comes from IronSKY's core monitoring capabilities: security event count, risk device identification, vulnerable models, threat type breakdown, time trend analysis and geography. The same signals used to catch location fraud apply to any anomalous device behavior across the fleet.

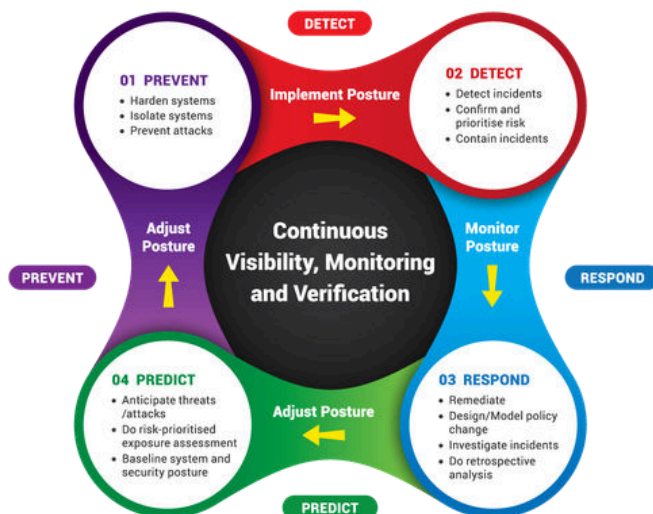


WHY SECIRON, NOT A WORKAROUND

Building this in-house, or patching it with point tools, doesn't hold

Seciron follows an Adaptive Security Architecture (ASA), where protection operates as a continuous cycle rather than a one-time control. This enables the platform to continuously adapt as attackers evolve their tactics and techniques.

The approach is built around four key objectives: Prevent, Detect, Respond and Predict. These are supported by continuous monitoring and threat intelligence, automation, integration, and risk-based decision-making.



The three products behind every use case above

IRONSCAN

Scans apps for vulnerabilities and exposed secrets before release.

IRONWALL

Codeless hardening applied to the built app — no source changes.

IRONSKY

Real-time monitoring and response, with every detection logged.

What sets the platform apart

Codeless integration

No source code changes, no friction for dev teams, no disruption to existing CI/CD pipelines.

End-to-end coverage

Prevent, detect, respond and predict across the full mobile app lifecycle — not one stage in isolation.

Low overhead

Enterprise-grade protection that doesn't compromise app performance or the user experience.



SEE IT ON YOUR OWN APP

Every use case above started with one question: What's actually happening on the devices running your app?

Get a clearer view of your mobile app's security posture. Speak with a Seciron expert about assessing potential vulnerabilities, risks and areas of exposure.

[Talk to Us](#)

✉ business@seciron.com

🌐 www.seciron.com

or book a 15-minute technical demo at seciron.com/contact-us