One-pager

Device Takeover Fraud: Fraud that hides in plain sight

DTO is now one of the biggest blind spots in mobile fraud detection.

It gives attackers real-time control of your customer's device, letting them access banking apps, intercept codes, and move money, without raising a single alert.

There's no credential breach. No Account Takeover. Just fraud happening inside a trusted session, using a known device, and passing all your existing checks.

Starting much earlier than most teams are watching

DTO doesn't begin with a login or transaction, it begins when malware is installed.

That might happen via a malicious app. But increasingly, it's coming from inside the software supply chain.

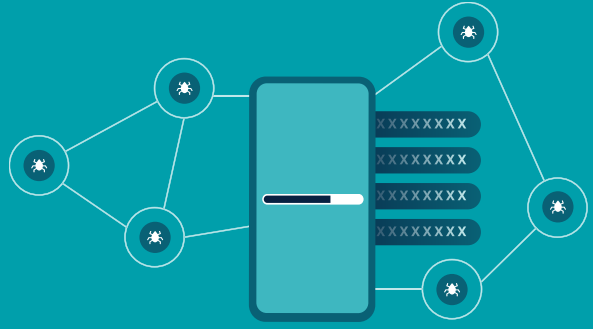
In one case, a telecoms provider unknowingly shipped malware in a routine app update via a compromised SDK. Millions downloaded it. The code had access to screen content, SMS, and app permissions. Just like that, attackers had a clear path to banking apps.

Users didn't click anything suspicious. The brand was legitimate. And the compromise went undetected by fraud controls.

The blind spot: malware embedded in 'trusted' apps

Anti-fraud tools are designed to spot unusual logins, locations, or payment patterns. DTO bypasses all of that because it happens on the customer's device.

By the time a session starts, the attacker is already in control. They're clicking, swiping, and entering PINs using malware to act like the customer. Fraud teams get clean session data. Risk engines see nothing strange.



One compromise upstream, full compromise downstream

Supply chain attacks aren't just about back-end infrastructure anymore; they now extend to mobile SDKs, third-party apps, and even telecom providers.

Telecom apps have become an ideal attack vector: trusted, pre-installed, and widely used. **Supply chain attacks remain a top cyber threat.**

Europol, 2024 Internet Organised Crime Threat Assessment (IOCTA)

25%

Increase in supply chain attacks on mobile SDKs (YoY)

Source Cyble

63%

Targeted IT, telecom, and tech apps (Cyble 2025)

Source Cyble

60%

SDKs are opaque binaries, no transparency, no SBOMs

Source 2025 Global Mobile Threat Report

Your customers may already be infected. You just can't see it.

Cleafy gives you visibility where others can't

Cleafy operates within your web and mobile applications, detecting fraud as it happens, before money moves and before fraud teams are blindsided.

We see what others miss:

- Malware overlays and fake login screens
- Remote control activity (e.g., AnyDesk, VNC-like input patterns)
- Abuse of Accessibility Services and screen-sharing permissions
- Zero-day and known strains like TeaBot, SharkBot, SuperCard X
- Supply chain attacks embedding malicious code in legitimate apps
- Session behaviour anomalies, e.g., robotic input speed, motion mismatches

What this means for your team

01.

Fraud Ops

Spot device control fraud before money moves. Less time chasing noise, more time resolving real cases.

02.

Security

Bridge the gap between infection and financial loss. Get telemetry from inside the device, not just the network edge.

03.

Compliance

Show active detection of live threats inside your app. Without adding friction or damaging UX.

DTO is live in your customers' sessions. Are you watching?

Let us show you what your current tools are missing.

Learn more today

To learn more about how we can help you

- **Visit cleafy.com**
- **Email us at info@cleafy.com**

Trusted by leading European and LATAM banks, boasting a 4.2 score on Gartner Peer Reviews.

Gartner peerinsights™