

The Agent-Operated Android Trojan Hijacking Brazil's PIX Payments in Real Time

zimperium.com/blog/pixrevolution-the-agent-operated-android-trojan-hijacking-brazils-pix-payments-in-real-time
Aazim Yaswant March 11, 2026

 **Google play**



Expedia: viagem, hotel, voo
Expedia
Contém anúncios

4,9★
1,46 mi avaliações

50 mi+
Downloads

Livre
Classificação Livre

Instalar

[Compartilhar](#) [Adicionar à lista de desejos](#)

☐ Este app não está disponível para seu dispositivo



Executive Summary

In 2020, the Central Bank of Brazil implemented an instant payment system called PIX that significantly reformed the local payment landscape, with over 76% of the population utilizing it for immediate transfers via smartphones. The zLabs team has identified a novel Android banking trojan specifically targeting this system and implicitly targeting most Brazilian financial institutions.

This new strain of malware operates stealthily within the device until the moment the victim initiates a PIX transfer. The user inputs the desired amount, enters the payee's PIX key, and selects the send option. A familiar loading indicator, "*Aguarde...*" (please wait)," is displayed. Subsequently, the screen confirms the transfer's completion; however, the funds are not routed to the intended payee. Instead, they are diverted to a criminal entity that has been monitoring the victim's screen in real time.

This methodology characterizes the operation of **PixRevolution**. What distinguishes this threat from conventional banking trojans is its fundamental design: a human or AI agent operator is actively engaged on the remote end, observing the victim's phone screen instantaneously, poised to act at the precise moment of transaction.

Why PIX? Why Brazil?

Brazil's PIX system, launched by the Central Bank of Brazil in 2020, has fundamentally changed how money moves in the country. It processes more than **3 billion transactions per month**, operates 24/7, and settles payments in seconds. For consumers, it is fast and convenient. For criminals, those same properties create a near-perfect target: once a PIX transfer completes, it is **instant and irrevocable**. There is no chargeback window. There is no three-day hold. The money is simply gone.

PixRevolution is purpose-built to exploit this. Every technical decision in its architecture, from the real-time screen streaming to the operator-controlled injection model, is designed around one goal: intercepting a PIX transfer at the moment of confirmation and redirecting it before anyone notices.

How Victims Get Infected

The campaign uses a multi-layered distribution strategy built on impersonation and trust.

Attackers create **fake Google Play Store pages** hosted on domains they control. These pages are perfect replicas of legitimate Play Store listings, complete with app descriptions, ratings, and an "Install" button. The difference is that instead of directing users to the real Play Store, the button downloads a malicious APK.



Figure 1. Fake Google Play Store page used to distribute PixRevolution dropper APKs

Our analysis identified campaigns impersonating several well-known Brazilian entities. Analysis of 14 samples revealed the following brand disguises:

App Name	Brand Impersonated	Type
Expedia: viagem, hotel, voo	Expedia (travel booking)	Dropper
Sicredi X	Sicredi (banking cooperative)	RAT & Dropper

Correios	Brazilian Postal Service	RAT & Dropper
Reconhecimento XP	XP Investimentos	RAT
STJ	Superior Tribunal de Justiça (Supreme Court)	Dropper
Central Caçamba	Local waste collection services	RAT
PARANA CAÇAMBAS	Regional waste collection services	RAT & Dropper
Avg Antivirus	AVG Antivirus software	RAT & Dropper
PILATESEMCASA	Fitness/wellness app	RAT & Dropper

The choice of impersonation targets is deliberate. Expedia and Correios are apps that millions of Brazilians would plausibly install. The STJ – Brazil’s Superior Tribunal de Justiça – lends an air of government authority.

Some samples are **droppers**, their purpose is to silently install the actual RAT payload. The dropper carries the trojan as an embedded file (assets/update.apk) and uses Android’s PackageInstaller API to install it without requiring the user to navigate an installation dialog. The dropper even tracks its own progress internally, logging stages like `onInstallProgress(30)` through `onInstallFinished()`.

The Social Engineering Trap

Once the app is installed, the victim sees a polished onboarding screen. It is built with modern web technologies and it asks the user to enable an accessibility service called “**Revolution.**”

The page provides manufacturer-specific instructions: step-by-step guidance for Samsung, Xiaomi, and Motorola devices (since instructions vary slightly among them). It reassures the user with the message: *“This permission is only used to enable app features. No personal information is collected.”*



Figure 2. Social engineering onboarding screen requesting the victim to enable the “Revolution” accessibility service, with manufacturer-specific instructions

This is, of course, entirely false. But the presentation is convincing enough that many users comply.

Once the accessibility service is enabled, the page redirects to the legitimate Banco do Brasil website, reinforcing the illusion that nothing is amiss. Behind the scenes, the trojan has just been granted the keys to the kingdom.

Inside the Attack: A Five-Act Heist

What happens next is best understood as an orchestrated sequence, with the malware and its operator working in concert.

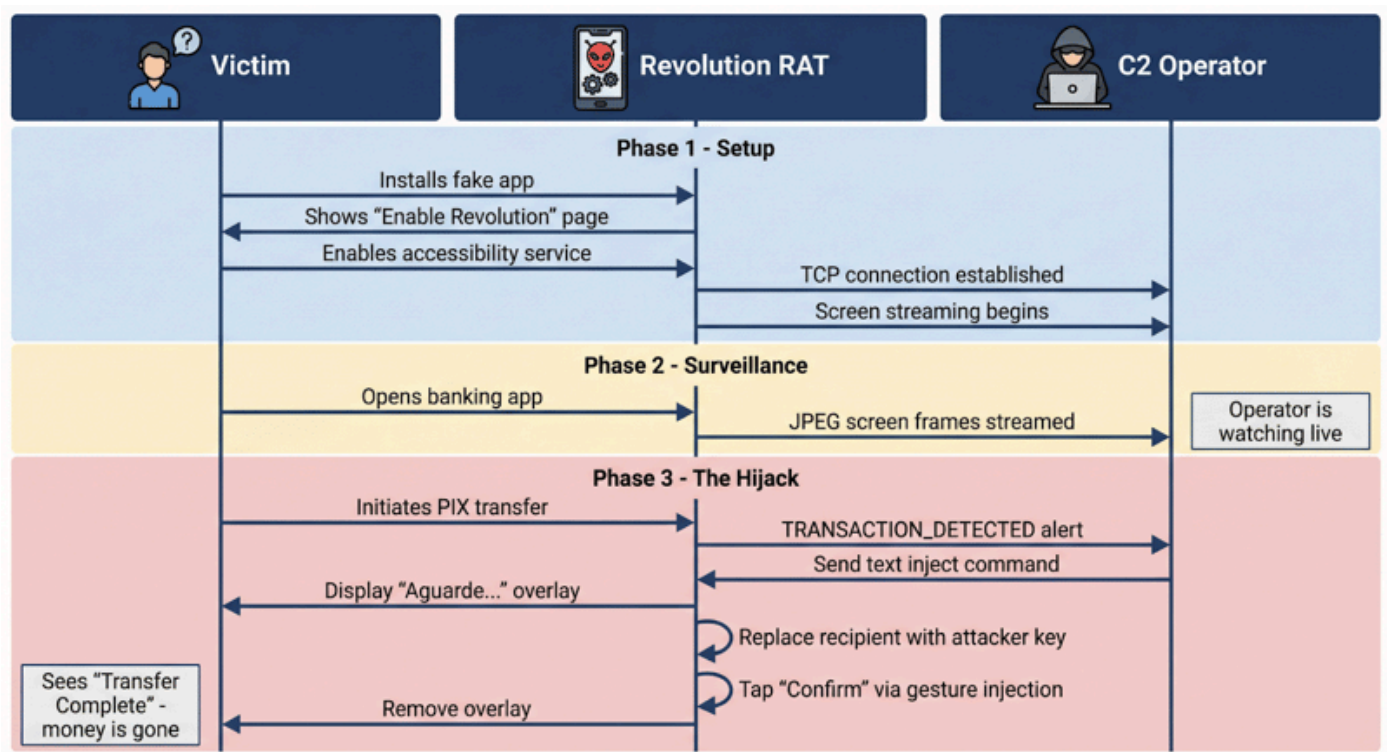


Figure 3. PixRevolution attack flow: from initial infection through real-time screen streaming to PIX transaction hijacking

Act 1: The Trojan Wakes Up

The moment the accessibility service is enabled, PixRevolution begins listening to **every event on the device**. Its accessibility configuration requests typeAllMask, meaning it receives notifications about every UI change in every application. It can read all text visible on screen. It can perform taps and swipes. It has full visibility into every app the user opens.

In code, this translates to a configuration like:

```
// Accessibility service configuration
eventTypes = "typeAllMask" // Listen to everything
canRetrieveWindowContent = true // Read all screen text
canPerformGestures = true // Inject taps and swipes
```

This is not limited to banking apps. The trojan can see messaging apps, email, social media – everything. But its interest lies in one thing: financial transactions.

Act 2: The Operator Connects

The trojan establishes a persistent TCP connection to a C2 (command & control) server on port 9000. It keeps this connection alive with periodic heartbeat messages that include the device ID, battery level, and network type. A secondary HTTP endpoint on port 3030 provides additional telemetry.

Critically, the trojan also activates **real-time screen capture** using Android’s MediaProjection API. It creates a virtual display that mirrors the device screen, captures each frame as a bitmap, compresses it to JPEG, and streams it to the C2 server. The operator on the other end sees exactly what the victim sees, in near real-time.

Act 3: Waiting for the Right Moment

PixRevolution does not blindly attack. It waits.

The trojan contains a list of over **80 Portuguese-language phrases** related to financial transactions, all encoded in base64 to evade basic string scanning. When decoded, these phrases reveal the breadth of financial activity the malware monitors:

Category	Example Phrases (translated from Portuguese)
PIX transactions	“pix payment made,” “pix sent,” “pix confirmed,” “pix transfer completed”
Bank transfers	“transfer completed,” “transfer confirmed,” “bank transfer made”
Balance information	“available balance,” “current balance,” “insufficient balance”
Invoice payments	“invoice paid,” “invoice processed successfully”
Investments	“investment completed,” “investment confirmed”
General	“transaction completed successfully,” “payment confirmed,” “amount debited”

Every time text appears on the victim’s screen, the trojan scans it against this keyword list. When a match is found, it fires a structured alert to the C2 server:

TRANSACTION_DETECTED | keyword=pix enviado | raw=<full screen text> | frame=YES

The frame=YES flag indicates whether a screenshot was captured alongside the alert. This gives the operator both the contextual keyword that triggered the detection and a visual snapshot of exactly what the victim’s screen looks like at that moment.

Act 4: The Hijack

The operator, watching the victim's screen in real time, sees them navigate to a PIX transfer screen. They see the victim type in a recipient's PIX key. At precisely the right moment, the operator sends a command:

```
{"type": "text", "value": "<attacker_pix_key>"}
```

The trojan receives this command and executes a precise sequence:

1. **Show an overlay.** A full-screen “*Aguarde...*” (Wait...) spinner appears, blocking the victim's view. This is a locally stored HTML page loaded in a WebView.
2. **Find the active input field.** The malware calls `findFocus(INPUT_FOCUS)` to locate whichever text field the victim was just typing in, and verifies it is editable with `isEditable()`.
3. **Replace the text.** Using `performAction(ACTION_SET_TEXT)`, the trojan overwrites the contents of the focused field with the attacker's PIX key. The victim's intended recipient vanishes. The attacker's account takes its place.
4. **Confirm the transaction.** The trojan uses `dispatchGesture()` to simulate a tap on the confirmation button. It does not use hardcoded screen coordinates. Instead, it dynamically locates the button by querying the UI tree, retrieving its bounds with `getBoundsInScreen()`, and calculating the center point. This makes the attack resilient across different screen sizes and banking app layouts.
5. **Remove the overlay.** The spinner disappears. The victim sees a “transfer complete” confirmation screen and assumes everything went as planned.

The entire sequence – from overlay to confirmation – takes seconds.

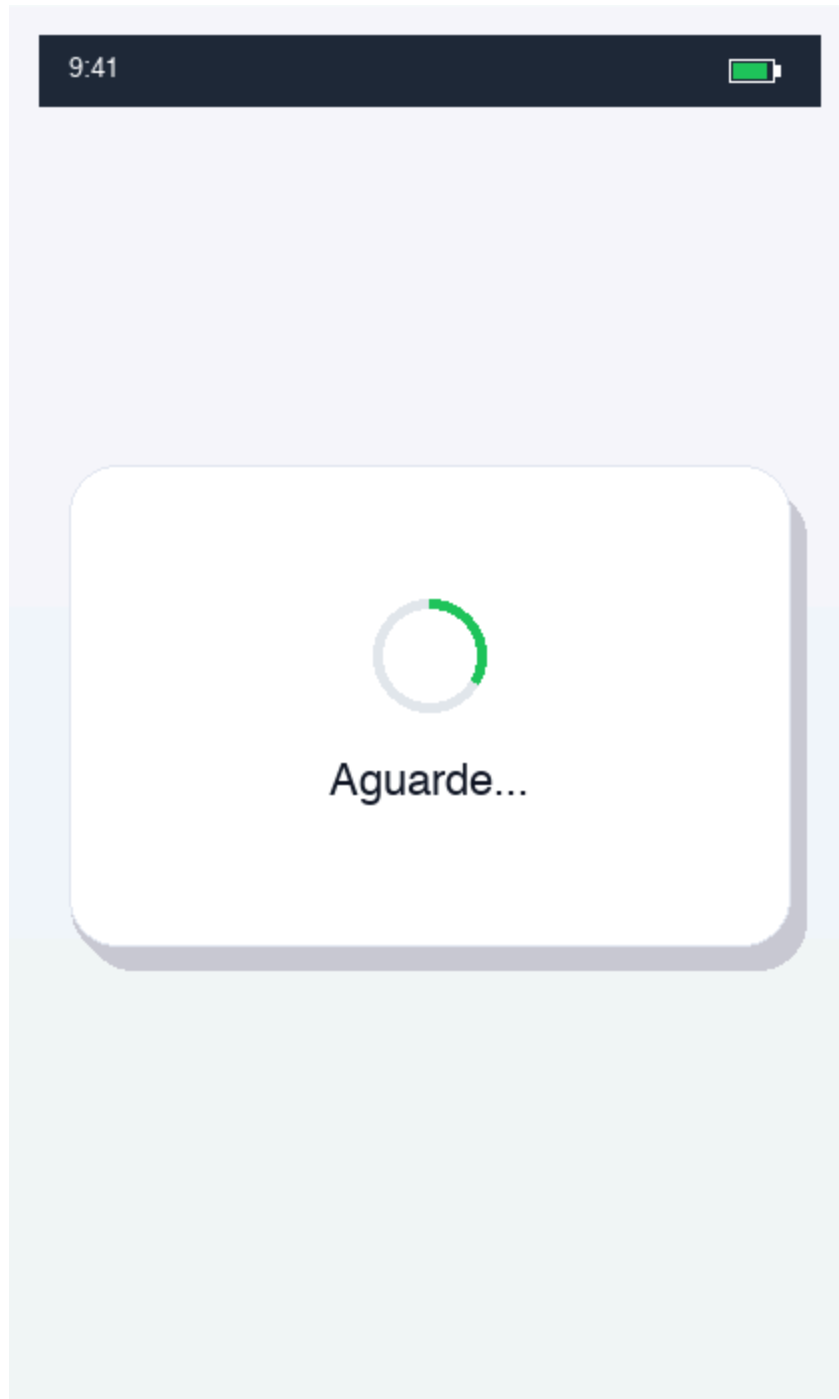


Figure 4. The “Aguarde...” (Wait...) overlay displayed to the victim while the trojan replaces the PIX recipient behind the scenes

Act 5: The Vanishing Act

From the victim’s perspective, nothing unusual happened. The app briefly showed a loading indicator, something that occurs routinely during legitimate banking operations. The transfer was confirmed successfully. The amount they intended to send was deducted from their account.

It is only later, sometimes much later, that the victim discovers the money went to the wrong account. And because PIX transfers are instant and final, recovery is extraordinarily difficult.

What Makes PixRevolution Different

The mobile banking trojan landscape is not new. But PixRevolution introduces several architectural choices that distinguish it from its predecessors.

The Agent-in-the-Loop Model

Most banking trojans operate on automation: they detect a target app, display a phishing overlay, capture credentials, and replay them. PixRevolution takes a fundamentally different approach. It requires an active operator in the loop: someone who watches the victim’s screen live and decides precisely when and how to act. This could be a human operator or an AI agent with access to the UI elements (similar to the recently released [OpenClaw<](#)). The malware sidesteps the biggest challenge in banking trojan development: **keeping up with UI changes across dozens of banking apps**.

Automated trojans break when a bank updates its interface. PixRevolution does not care what the interface looks like, because an agent is reading it in real time.

Bank-Agnostic by Design

There is no hardcoded list of target banking applications in PixRevolution’s code. It does not need one. The accessibility service monitors every app on the device, and the keyword detection system looks for transaction-related phrases regardless of which app is displaying them. This means the malware is effective against **any Brazilian financial app that uses PIX**, not just a pre-selected list.

The bank logos found in the code are not detection triggers. They are **thematic assets**. The operator sends a bank code (like “NU” for Nubank or “I” for Itau) and the malware selects the corresponding logo to make the overlay more convincing. It is a detail that speaks to operational polish.

Targeted Financial Institutions

The malware contains hardcoded logo URLs for 10 major Brazilian financial institutions:

Bank	Code
Nubank	NU
Itaú Unibanco	I
Banco do Brasil	B

Caixa Econômica Federal	C
Santander Brasil	S
PicPay	P
PagSeguro	PG
Sicredi	SI
XP Investimentos	X



Figure 5. Hardcoded bank logos found in PixRevolution samples, used to theme the overlay for each targeted financial institution

This list represents the breadth of institutions the threat actors are prepared to impersonate, from traditional banks to digital-first fintechs to investment platforms.

Scale and Impact

The numbers paint a concerning picture. PIX is not a niche payment method, it is the dominant way Brazilians move money. With over 150 million registered users and billions of monthly transactions, even a small success rate for an operation like this translates to significant financial losses.

The infrastructure we observed is not the work of a lone hobbyist. Dedicated distribution domains with fake app store pages, multi-stage dropper chains, polished social engineering assets, a persistent TCP-based C2 protocol with heartbeat and screen streaming. This is organized, professional mobile fraud.

The instant, irrevocable nature of PIX transactions makes this class of attack particularly damaging. Unlike credit card fraud, where transactions can be disputed and reversed, a hijacked PIX transfer is final by the time the victim realizes something has happened.

Zimperium vs. PixRevolution

PixRevolution represents an evolution in mobile financial fraud. By combining real-time screen surveillance with a human or AI agent as an operator who decides when to strike, this malware family sidesteps the traditional arms race between automated trojans and banking app defenses. It does not need to reverse-engineer each bank's UI. It does not need to maintain a list of target applications. It does not need to guess when a transaction is happening. It simply watches and then acts.

For the victim in our opening scenario, the entire theft was invisible. A brief loading spinner, a completed transfer, and money that will never return. The sophistication is not in complexity but in simplicity: the right permissions, a live video feed, and a well-timed text replacement.

As instant payment systems continue to expand globally, from PIX in Brazil to UPI in India to FedNow in the United States, the operational model pioneered by PixRevolution is unlikely to remain confined to a single market. The lesson for defenders is clear: when the attacker is an agent with a live feed of your screen, static detection is not enough. Protecting users requires real-time, on-device defense that can identify and block these behaviors the moment they occur.

PixRevolution's agent-in-the-loop design and abuse of legitimate Android APIs - Accessibility Services, MediaProjection, and standard TCP networking, allow it to evade conventional, signature-based defenses that rely on static indicators alone. The malware does not download secondary payloads from well-known malicious URLs, does not exploit known CVEs, and does not use traditional phishing overlays. Instead, it weaponizes permissions that the user voluntarily grants, making detection dependent on behavioral analysis rather than known-bad signatures.

[Zimperium's Mobile Threat Defense \(MTD\)](#) and [Mobile Runtime Protection \(zDefend\)](#) provide on-device, behavioral detection that identifies PixRevolution the moment it activates on a device. Zimperium's dynamic detection engine recognizes the combination of accessibility service abuse, unauthorized screen capture via MediaProjection, and persistent C2 communication as a composite threat signal, providing zero-day protection even as threat actors repackage samples under new brand disguises and operator IDs.

For enterprises, PixRevolution poses a direct risk to any organization whose employees access financial services, corporate banking, or payment workflows from mobile devices. A compromised device can silently redirect funds during legitimate transactions, and the instant, irrevocable nature of PIX transfers means losses are realized before detection is possible through traditional monitoring. In BYOD environments where personal banking apps coexist with corporate resources, an infection like PixRevolution can result in direct financial loss, operational disruption, and erosion of trust in mobile channels - making on-device, behavior-based protection a critical control.

MITRE ATT&CK Techniques

Tactic	ID	Name	Description
Initial Access	T1476	Deliver Malicious App via Other Means	Fake Google Play Store pages hosted on attacker-controlled domains distribute malicious APKs directly to victims.
Initial Access	T1660	Phishing	Attacker-controlled domains impersonate trusted Brazilian brands (Expedia, Correios, STJ) to lure users into installing malicious apps.
Persistence	T1541	Foreground Persistence	Starts a foreground service for MediaProjection screen capture to maintain persistent access and survive background process termination.
Defense Evasion	T1655.001	Masquerading: Match Legitimate Name or Location	Dropper APKs impersonate well-known brands (Expedia, Correios, AVG Antivirus) and use convincing app icons and descriptions.
Defense Evasion	T1628.001	Hide Artifacts: Suppress Application Icon	Dropper component conceals itself after silently installing the RAT payload via PackageInstaller API.
Discovery	T1426	System Information Discovery	Heartbeat messages to C2 include device ID, battery level, and network type to profile victim devices.
Collection	T1513	Screen Capture	Uses Android MediaProjection API to create a virtual display, capture screen frames as bitmaps, compress to JPEG, and stream to C2 in real time.
Collection	T1417	Input Capture	Accessibility service with typeAllMask configuration reads all text visible on screen across every application.
Command and Control	T1437	Application Layer Protocol	Persistent TCP connection to C2 on port 9000 with heartbeat keepalives; secondary HTTP endpoint on port 3030 for telemetry.

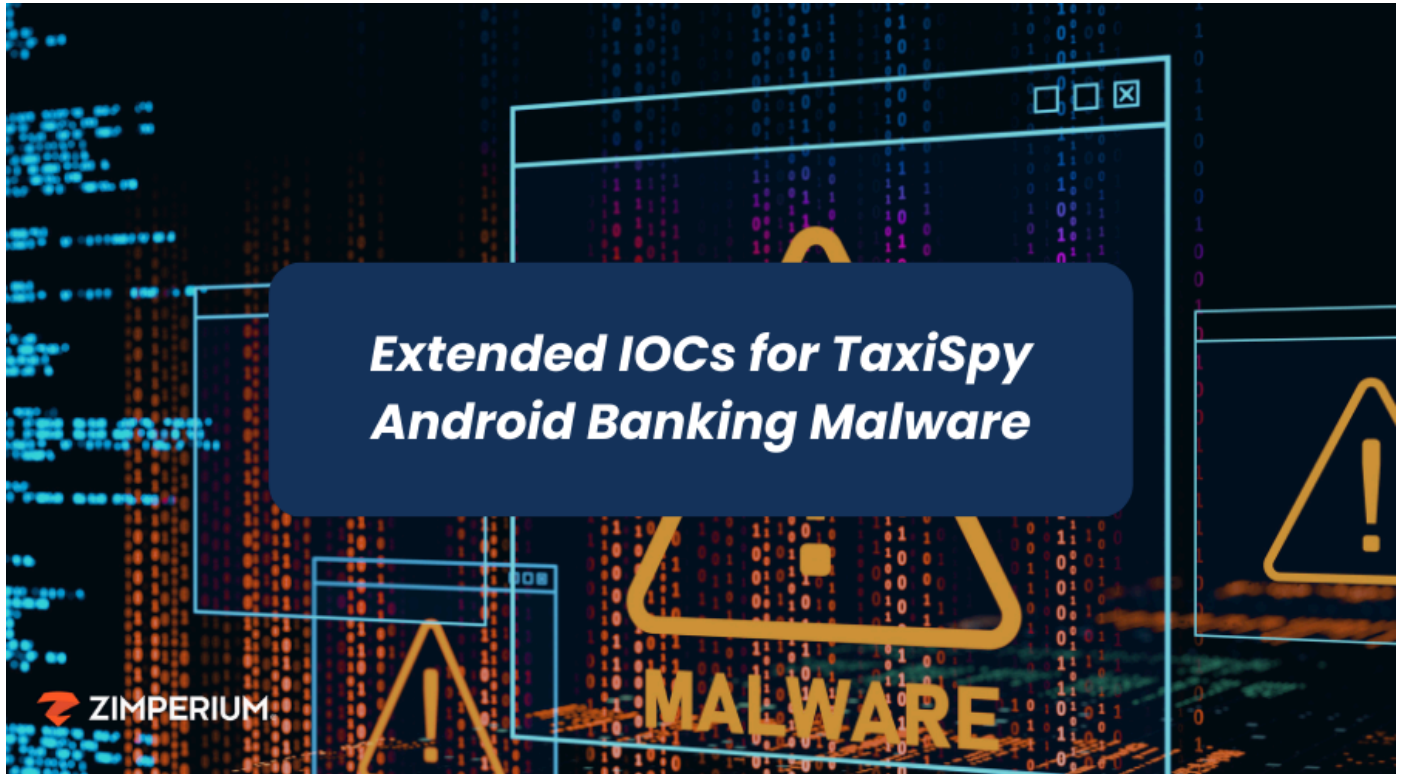
Impact	T1516	Input Injection	Uses performAction(ACTION_SET_TEXT) to replace PIX recipient and dispatchGesture() to simulate confirmation tap, hijacking transactions behind a full-screen overlay.
--------	-----------------------	-----------------	---

Indicators of Compromise

The IOCs for this campaign can be found in this [Github repository](#).

[zLabs](#)

[Threat Intelligence](#)



[Mar 09, 2026](#)

[Extended IOCs for TaxiSpy Android Banking Malware](#)



Mar 04, 2026

Coruna iOS Exploit Kit Highlights the Need for Multi-Layer Mobile Defense