# Android Trojan steals money from PayPal accounts even with 2FA on

By Lukas Stefanko

Archived: 2026-04-05 21:46:14 UTC

There is a new Trojan preying on Android users, and it has some nasty tricks up its sleeve.

First detected by ESET in November 2018, the malware combines the capabilities of a remotely controlled banking Trojan with a novel misuse of Android Accessibility services, to target users of the official PayPal app.

At the time of writing, the malware is masquerading as a battery optimization tool, and is distributed via third-party app stores.

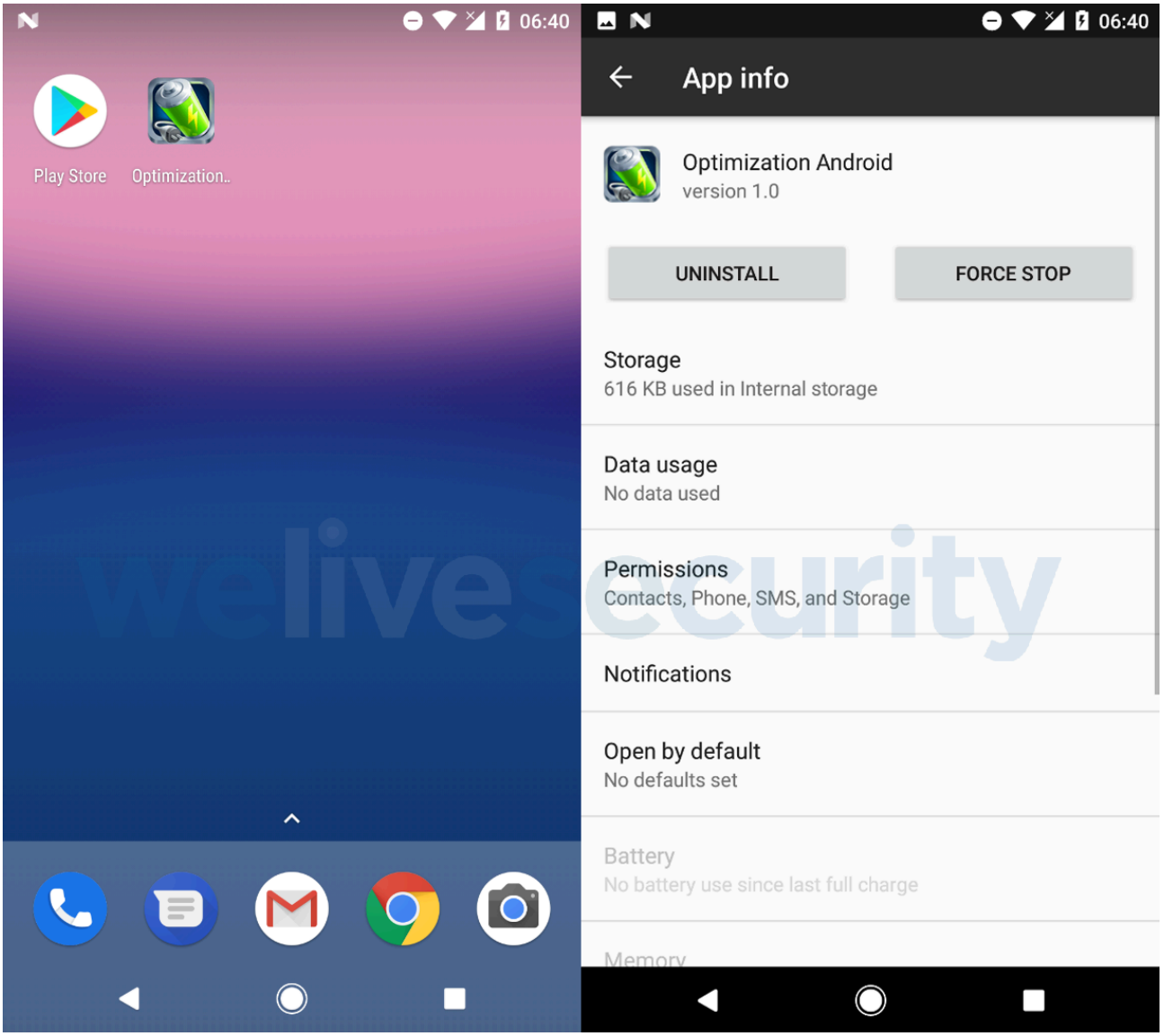

Figure 1 – The disguise used by the malware at the time of writing

## How does it operate?

After being launched, the malicious app terminates without offering any functionality and hides its icon. From then on, its functionality can be broken down into two main parts, as described in the following sections.

## Malicious Accessibility service targeting PayPal

The malware's first function, stealing money from its victims' PayPal accounts, requires the activation of a malicious Accessibility service. As seen in Figure 2, this request is presented to the user as being from the innocuous-sounding "Enable statistics" service.

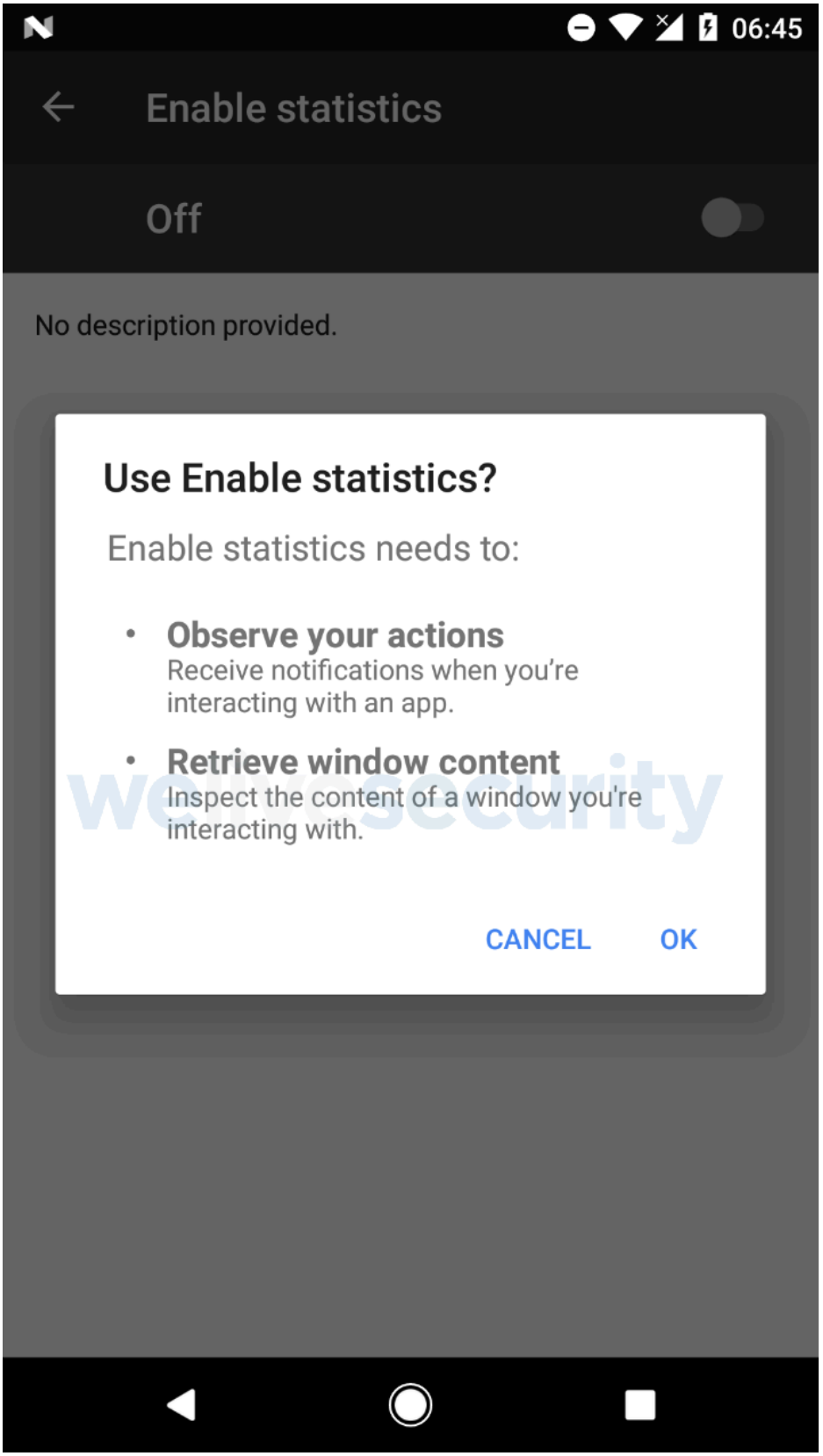


Figure 2 – Malware requesting the activation of its accessibility service, disguised as "Enable statistics"

If the official PayPal app is installed on the compromised device, the malware displays a notification alert prompting the user to launch it. Once the user opens the PayPal app and logs in, the malicious accessibility service

(if previously enabled by the user) steps in and mimics the user's clicks to send money to the attacker's PayPal address.

During our analysis, the app attempted to transfer 1000 euros, however, the currency used depends on the user's location. The whole process takes about 5 seconds, and for an unsuspecting user, there is no feasible way to intervene in time.

Because the malware does not rely on stealing PayPal login credentials and instead waits for users to log into the official PayPal app themselves, it also bypasses PayPal's two-factor authentication (2FA). Users with 2FA enabled simply complete one extra step as part of logging in, – as they normally would – but end up being just as vulnerable to this Trojan's attack as those not using 2FA.

The video below demonstrates this process in practice.


The attackers fail only if the user has insufficient PayPal balance and no payment card connected to the account. The malicious Accessibility service is activated every time the PayPal app is launched, meaning the attack could take place multiple times.

We have notified PayPal of the malicious technique used by this Trojan and the PayPal account used by the attacker to receive stolen funds.

## Banking Trojan relying on overlay attacks

The malware's second function utilizes phishing screens covertly displayed over targeted, legitimate apps.

By default, the malware downloads HTML-based overlay screens for five apps – Google Play, WhatsApp, Skype, Viber, and Gmail – but this initial list can be dynamically updated at any moment.

Four of the five overlay screens phish for credit card details (Figure 3); the one targeting Gmail is after Gmail login credentials (Figure 4). We suspect this is connected to the PayPal-targeting functionality, as PayPal sends

email notifications for each completed transaction. With access to the victim's Gmail account, the attackers could delete such emails to remain unnoticed longer.

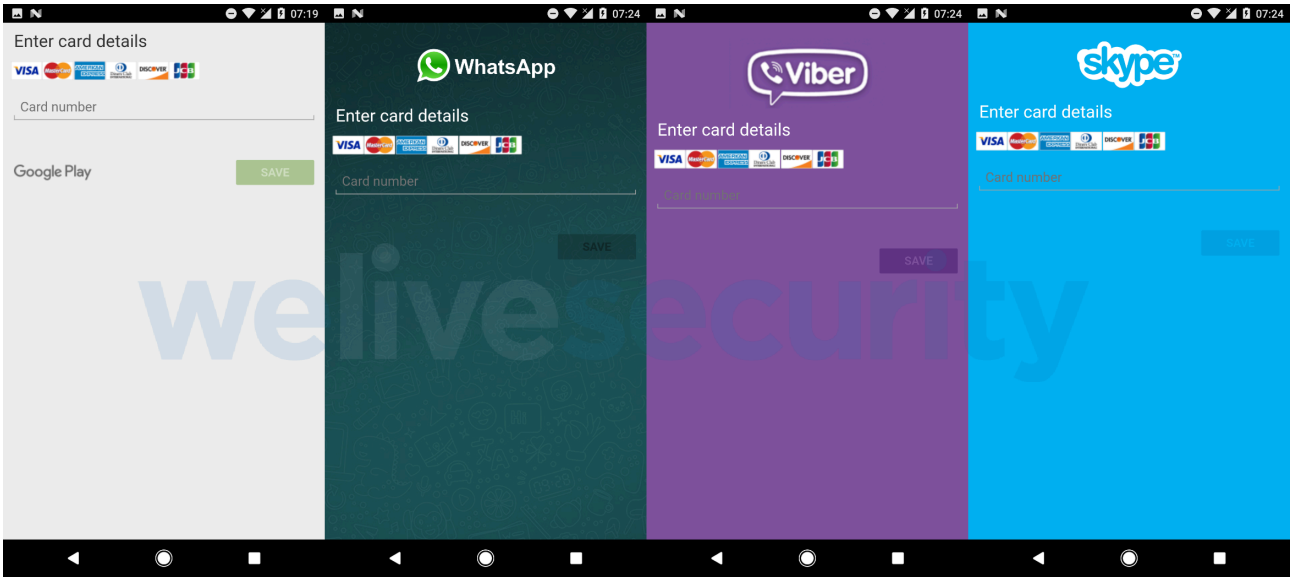


Figure 3 – Malicious overlay screens for Google Play, WhatsApp, Viber and Skype, requesting credit card details

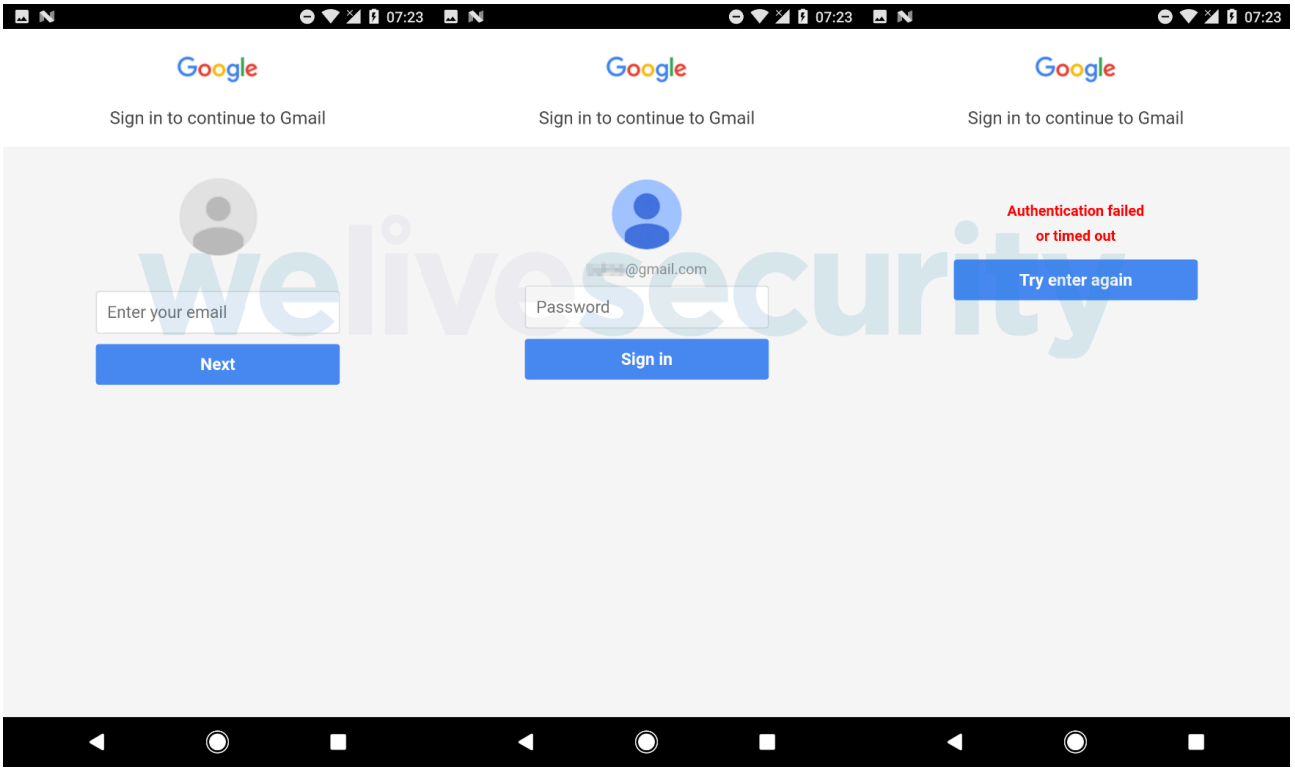


Figure 4 – Malicious overlay screens phishing for Gmail credentials

We've also seen overlay screens for legitimate banking apps requesting login credentials to victims' internet banking accounts (Figure 5).

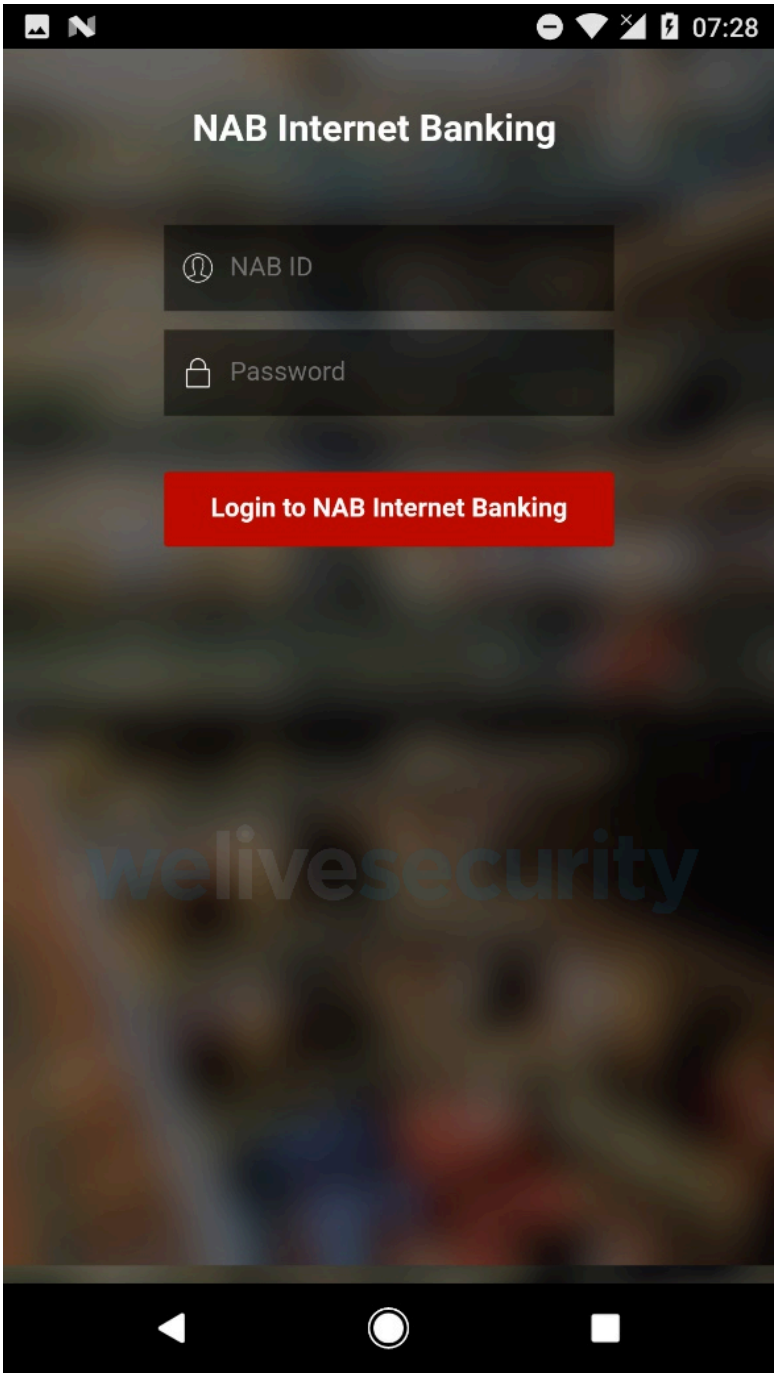


Figure 5 – Malicious overlay screen for the NAB (National Australia Bank) Mobile Banking app

Unlike overlays used by most Android banking Trojans, these are displayed in lock foreground screen – a technique also used by Android ransomware. This prevents the victims from removing the overlay by tapping the back button or the home button. The only way to get past this overlay screen is to fill out the bogus form, but fortunately, even random, invalid inputs make these screens disappear.

According to our analysis, the authors of this Trojan have been looking for further uses for this screen-overlaying mechanism. The malware's code contains strings claiming the victim's phone has been locked for displaying child pornography and can be unlocked by sending an email to a specified address. Such claims are reminiscent of early mobile ransomware attacks, where the victims were scared into believing their devices were locked due to reputed

police sanctions. It is unclear whether the attackers behind this Trojan are also planning to extort money from victims, or whether this functionality would merely be used as a cover for other malicious actions happening in the background.

Besides the two core functions described above, and depending on commands received from its C&C server, the malware can also:

- Intercept and send SMS messages; delete all SMS messages; change the default SMS app (to bypass SMS-based two-factor authentication)
- Obtain the contact list
- Make and forward calls
- Obtain the list of installed apps
- Install app, run installed app
- Start socket communication

## Accessibility Trojans also lurking on Google Play

We also spotted five malicious apps with similar capabilities in the Google Play store, targeting Brazilian users.

The apps, some of them also reported by Dr. Web and now removed from Google Play, posed as tools for tracking the location of other Android users.  In reality, the apps use a malicious Accessibility service to navigate inside legitimate applications of several Brazilian banks. Besides that, the Trojans phish for sensitive information by overlaying a number of applications with phishing websites. The targeted applications are listed in the IoCs section of this blogpost.

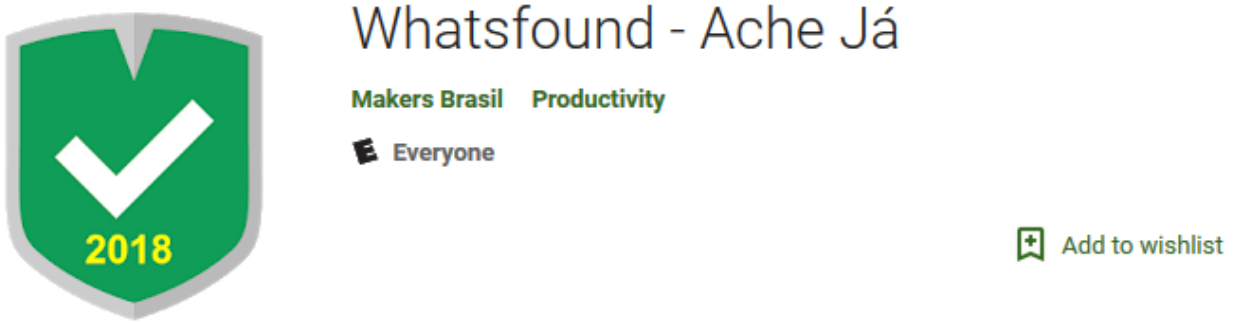


Figure 6 – One of the malicious apps on Google Play

Interestingly, these Trojans also use Accessibility to thwart uninstallation attempts by repeatedly clicking the “Back” button whenever a targeted antivirus app or app manager is launched, or when strings suggesting uninstallation are detected in the foreground.

## How to stay safe

Those who have installed these malicious apps will have likely already fallen victim to one of their malicious functions.

If you have installed the PayPal-targeting Trojan, we advise you to check your bank account for suspicious transactions and consider changing your internet banking password/PIN code, as well as Gmail password. In case of unauthorized PayPal transactions, you can report a problem in PayPal's Resolution Center.

For devices that are unusable due to a lock screen overlay displayed by this Trojan, we recommend using Android's Safe Mode, and proceed with uninstalling an app named "Optimization Android" under Settings > (General) > Application manager/Apps.

Uninstalling in Safe Mode is also recommended for Brazilian users who installed one of the Trojans from Google Play.

To stay safe from Android malware in the future, we advise you to:

- Stick to the official Google Play store when downloading apps
- Make sure to check the number of downloads, app ratings and the content of reviews before downloading apps from Google Play
- Pay attention to what permissions you grant to the apps you install
- Keep your Android device updated and use a reliable mobile security solution; ESET products detect these threats as Android/Spy.Banker.AJZ and Android/Spy.Banker.AKB

## Indicators of Compromise (IoCs)

### Android Trojan targeting PayPal users

| Package Name | Hash | ESET detection name |
|---|---|---|
| jhgfjhgfj.tjgyjgjgjy | 1C555B35914ECE5143960FD8935EA564 | Android/Spy.Banker.AJZ |

### Android banking Trojan targeting Brazilian users

| Package Name | Hash | ESET detection name |
|---|---|---|
| service.webview.kiszweb | FFACD0A770AA4FAA261C903F3D2993A2 | Android/Spy.Banker.AKB |
| service.webview.webkisz | D6EF4E16701B218F54A2A999AF47D1B4 | Android/Spy.Banker.AKB |
| com.web.webbrickd | 5E278AAC7DAA8C7061EE6A9BCA0518FE | Android/Spy.Banker.AKB |
| com.web.webbrickz | 2A07A8B5286C07271F346DC4965EA640 | Android/Spy.Banker.AKB |
| service.webview.strongwebview | 75F1117CABC55999E783A9FD370302F3 | Android/Spy.Banker.AKB |

### Targeted applications (phishing overlays)

- com.uber
- com.itaucard
- com.bradesco

- br.com.bb.android
- com.netflix
- gabba.Caixa
- com.itau
- Any app containing the string “twitter”

### Targeted applications (in-app navigation)

- com.bradesco
- gabba.Caixa
- com.itau
- br.com.bb
- Any app containing the string “santander”

### Targeted antivirus apps and app managers

- com.vtm.uninstall
- com.ddm.smartappunsintaller
- com.rhythm.hexise.uninst
- com.GoodTools.Uninstalle
- mobi.infolife.uninstaller
- om.utils.uninstalle
- com.jumobile.manager.systemapp
- com.vsrevogroup.revouninstallermobi
- oo.util.uninstall
- om.barto.uninstalle
- om.tohsoft.easyuninstalle
- vast.android.mobile
- om.android.cleane
- om.antiviru
- om.avira.andro
- om.kms.free

---