ANDROID BANKING MALWARE: SOPHISTICATED TROJANS VS. FAKE BANKING APPS

ENJOY SAFER TECHNOLOGY™

CONTENTS

Author: Lukáš Štefanko, ESET Malware Researcher
January 2019

INTRODUCTION

In this white paper, we will provide insight into the two most prevalent types of Android banking malware to date – sophisticated banking Trojans and fake banking apps – and compare their different approaches to achieving the same malicious goal.

At the same time, we will explore the impact of those approaches on potential victims.

Having identified the tactics of both categories, we will provide advice for users on how to stay safe from Android banking malware.

THE TWO TYPES OF ANDROID BANKING MALWARE

With our lives increasingly going mobile, banking apps are rapidly becoming the go-to method of managing finances. Malware authors motivated by financial gain have been quick to adapt their tools and techniques to profit from this shift. As a result, mobile banking malware – and especially that targeting the Android platform – has become a very real and potent, yet often underestimated, threat. Figure 1 shows the rising trend in Android banking malware detections as seen in ESET telemetry data.

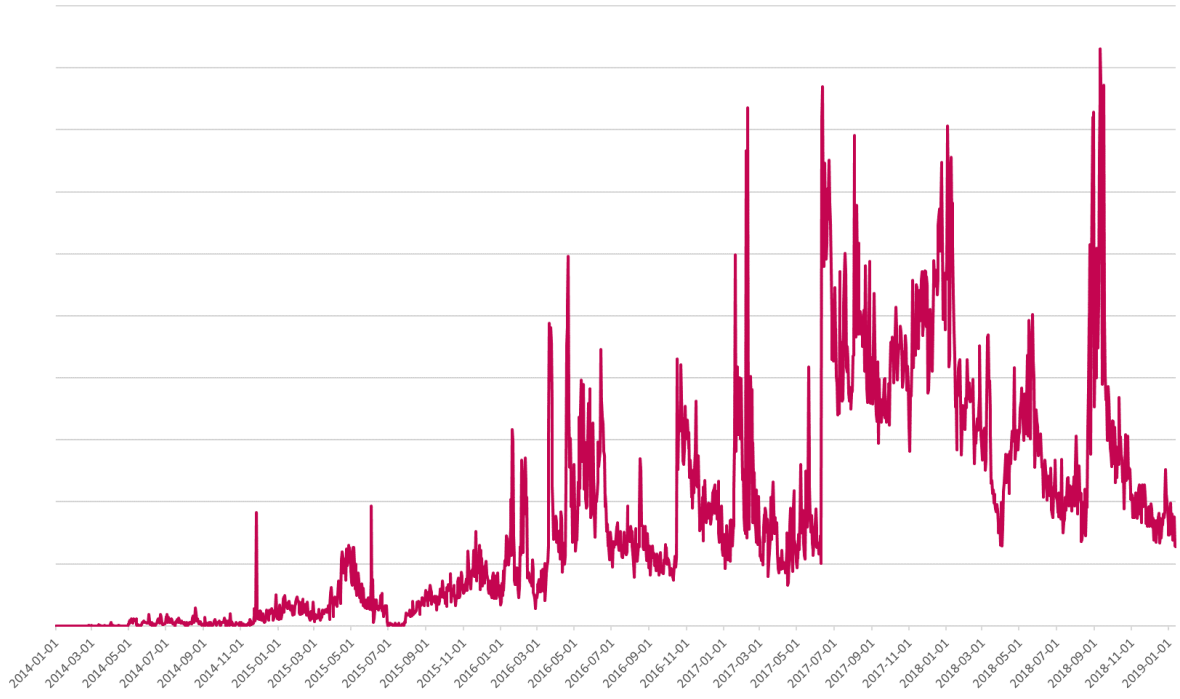

Figure 1 // Android banking malware trend according to ESET's telemetry

While the landscape of Android threats preying on sensitive financial information is undoubtedly complex and ever-evolving, the majority of current Android banking malware falls into one of the following, broad categories:

1. Sophisticated banking Trojans

2. Fake banking apps

Malware in both these categories is designed to achieve the same goal: steal credentials for, or money from, their victims' bank accounts. To achieve that, both sophisticated banking Trojans and fake banking apps need to elicit sensitive banking information from their victims and, if direct theft is the aim,

typically also need to gain access to SMS messages received on the compromised devices[1]. To lure the valuable information from potential victims, both types of malware make use of phishing and bogus login forms.

However, despite the similarities in their objectives, sophisticated banking Trojans and fake banking apps differ significantly in their strategy for deceiving victims. The following section will explore that difference and offer a more detailed look into the modus operandi of each distinct malware type.

Sophisticated banking Trojans

Malware in this category is typically complex in architecture, and advanced in functionality and detection evasion. MazarBot, BankBot, Anubis and Exobot are some of the most notorious examples of this type of Android threat.

An important point in the evolution of sophisticated Android banking Trojans was the publication of *BankBot's source code* on an underground forum in December 2016. The released code led to the creation of numerous new, hybrid-like, variants, and was likely one of the reasons behind the overall surge in Android banking Trojans observed throughout 2017.

Key features and strategy

The key tactic of Android banking Trojans is the **overlay attack** – a technique in which the malware overlays the targeted application with a phishing screen whenever that application is launched on the compromised device.

On the one hand, such phishing screens are very easy to craft nowadays, can be virtually indistinguishable from the impersonated layouts, and can be dynamically adapted to "fit" individual victims. On the other hand, drawing over other applications without the victims' knowledge gets more difficult with each Android version, due to measures taken against exactly this type of threat.

If we were to describe the strategy of Android banking Trojans in one word, it would be **stealth**: the presence of malware on the device and its connection to banking apps is meant to remain hidden for as long as possible, ideally keeping the victims in the dark until it is too late.

Modus operandi

To reach their malicious goals, sophisticated Android banking Trojans typically take most or all of the following steps:

1. Trick the victim into unknowingly installing malware using various disguises (read more in **Distribution**)
2. Obtain needed permissions (read more in **Functionality and permissions** and **Stealth techniques and detection evasion**)
3. *Optional:* Ensure persistence on the device (read more in **Special permissions and persistence** and **Stealth techniques and detection evasion**)
4. Wait in the background until the targeted, legitimate app is launched or trick the victim into launching that app (read more in **Targeting**)
5. Overlay the legitimate app with a phishing screen requesting login credentials or credit/debit card details (read more in **Functionality and permissions**)
6. Harvest entered credentials or credit/debit card details and send them to the C&C server
7. Optional: Use SMS permissions to intercept one-time password (OTP)
8. Carry out fraudulent transactions using the victim's bank account and/or sell stolen credentials on the black market

1 Obtaining SMS permissions for illicit purposes will likely become more complicated due to *the recent change* to Google Play terms restricting the use of SMS and Call Log permission groups.

Impact on users compared to fake banking apps:

- The deciding part of this attack is getting to the point of overlaying the targeted, legitimate app without the user noticing, while obtaining intrusive permissions, which has a lower chance of succeeding than fake banking apps
- The malicious nature of the app is either revealed in the process of obtaining intrusive permissions, or when it is too late; the connection to the Trojanized app is not always obvious, so the apps may have a longer "lifespan" on Google Play than fake banking apps

Distribution

Android banking Trojans are spread through a variety of channels and under many different guises. They can be commonly found lurking in unofficial app stores, but from time to time, some also manage to sneak into the *official Google Play store*. Other common distribution methods include compromised websites and malicious download links disseminated through social media, emails or even SMS.

As their name suggests, *Trojans* hide behind a seemingly legitimate mask to gain users' trust – be it games, handy widgets, power boosters and battery managers, video or Flash players, or even horoscope-themed apps (see Figure 2). The apps used as disguise sometimes provide the advertised functionality – that is, work as expected – or provide no functionality other than the (hidden) malicious one. The disguises are frequently changed up, complicating manual spotting and removal of Trojans on compromised devices.

A recent example of a banking Trojan we discovered on Google Play is a *Trojanized QRecorder app* that targeted German, Polish and Czech banks and was installed more than 10,000 times before being reported by ESET and taken down from the store (see Figure 3).

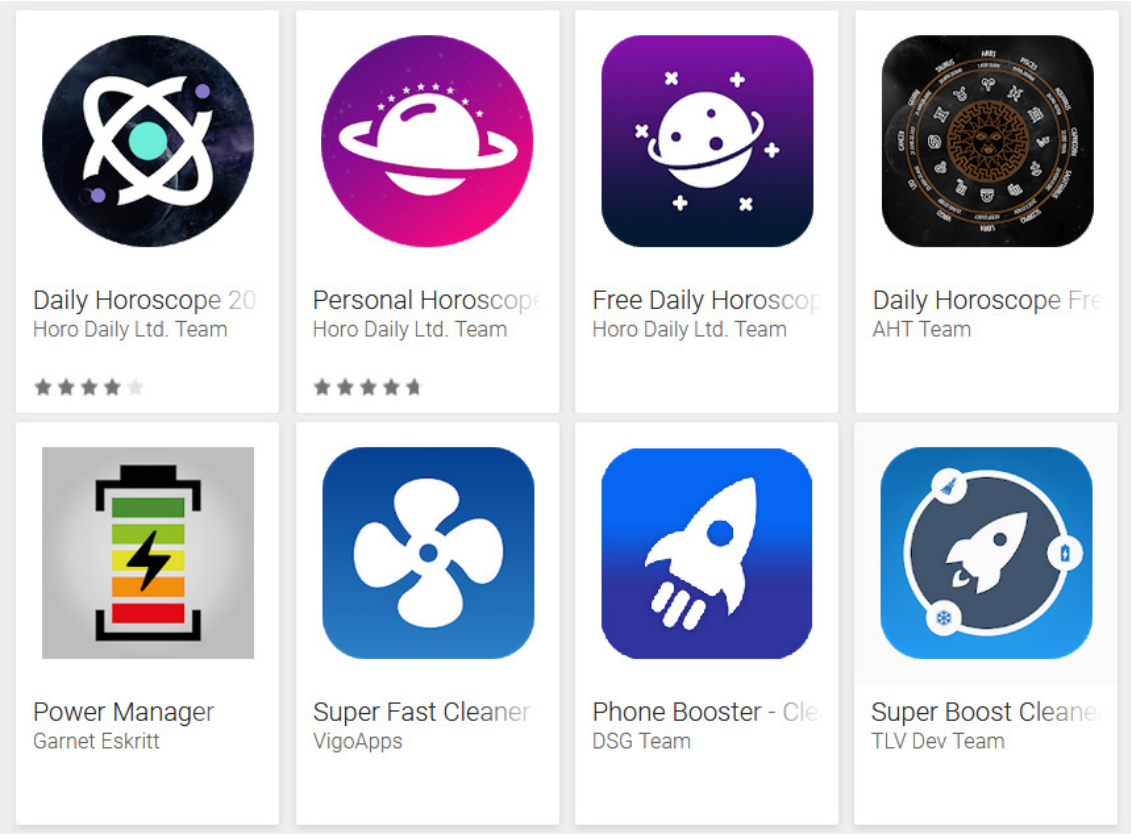

Figure 2 // Recent examples of banking Trojans found on Google Play

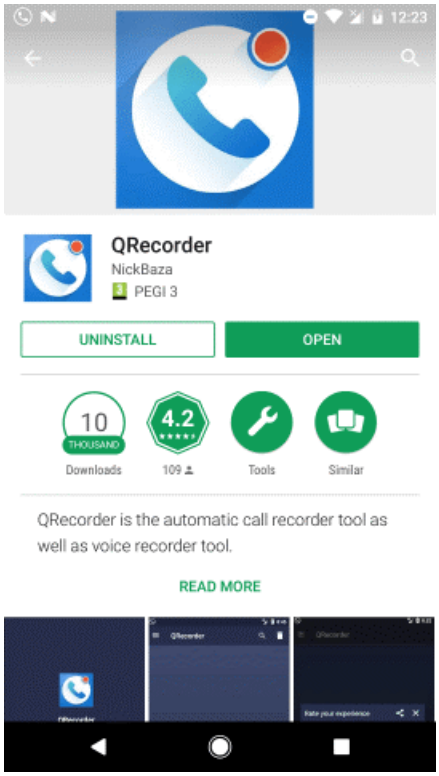

Figure 3 // The Trojanized QRecorder app on Google Play

Impact on users compared to fake banking apps:

- Malware disguised as legitimate apps have a potentially wider reach than fake banking apps

Targeting

The most usual target of Android banking Trojans are, unsurprisingly, banking apps (see Figure 4). However, it is also common for this type of malware to customize its overlay attacks for cryptocurrency wallets and exchanges as well as various non-banking apps like social media and messaging apps, booking apps, app stores, etc. In case of non-banking targets, the bogus overlay screens typically request credit/debit card details under some pretense (see Figure 5).

From the technical point of view, the scope of the overlay attacks can either depend on a hardcoded list of targeted applications, or be dynamically adjusted to impersonate any app of the attacker's choice. The latter is nowadays increasingly prevalent among Android banking Trojans.

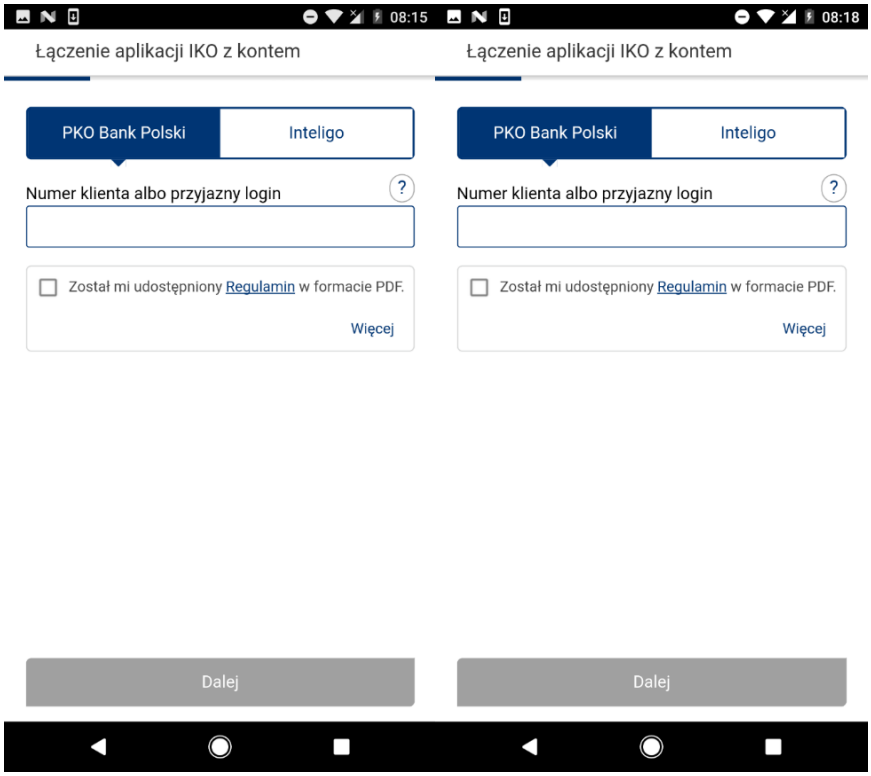

Figure 4 // Bogus overlay screen (left) indistinguishable from the legitimate banking app (right)

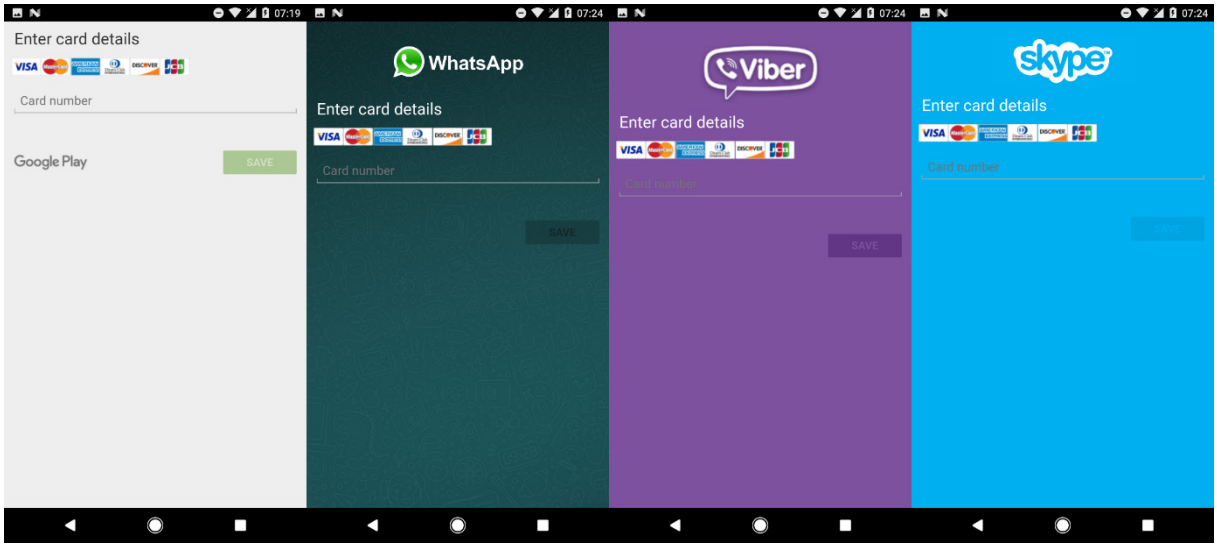

Figure 5 // Bogus overlay screens for various non-banking apps

Impact on users compared to fake banking apps:

- A potentially wider target group than fake banking apps

Functionality and permissions

The malicious functionality of Android banking Trojans typically includes the following capabilities:

- Remote control, using various communication methods with the C&C server
- Obtaining device information
- Downloading and executing additional apps
- Overlaying targeted, legitimate apps with phishing screens, using various techniques
- Harvesting credentials entered into the phishing forms and sending them to the C&C server
  - encrypted
  - unencrypted
- Intercepting, redirecting, sending and deleting SMS messages, to bypass SMS-based 2-factor authentication

Depending on permissions gained during and after installation, sophisticated banking Trojans targeting the Android platform are also commonly capable of:

- Displaying fake notifications to prompt victims to launch the targeted banking apps
- Obtaining the list of running applications
- Obtaining and editing the contact list
- Obtaining the phone call log, making and redirecting phone calls
- Accessing device storage
- Opening a browser and navigating to specific websites
- Accessing the camera
- Starting at device boot
- Remotely locking and unlocking the device by setting a lock screen password of the attackers' choice
- Displaying full-screen activity to cover malicious activity running in the background
- Recording a video of the screen
- Keylogging
- Running as a proxy to route network traffic through the compromised mobile device to fool banks' fraud detection mechanisms

Optionally, Android banking Trojans deliver the functionality advertised as part of their disguise – for example, provide the user with a real, functioning game. Offering legitimate functionality can help keep the malicious nature of the Trojan hidden for longer, both from affected users and Google's security mechanisms (read more in **Stealth techniques and detection evasion**).

On the other hand, the number of advanced techniques used and intrusive permissions requested by these Trojans can also work as triggers and thwart the operation before its malicious goals are realized.

Impact on users compared to fake banking apps:

- More powerful and potentially more damaging than fake banking apps but also more prone to detection due to advanced techniques acting as triggers for Google's security measures, researchers and users

Special permissions and persistence

To secure even greater control over the compromised device and ensure their malware cannot be uninstalled in one tap, cybercriminals are also interested in gaining elevated privileges and special permissions.

A very common way to gain a foothold in the system is obtaining **device administrator rights** for the malware – as long as an app is an active device administrator, it cannot be uninstalled. At the same time, device administrator rights come with some particularly intrusive permissions, such as changing the lock-screen password, locking the device, or wiping all its contents.

When requesting the activation of device administrator rights, Android banking Trojans either continue posing as whatever legitimate app they have been impersonating from the beginning, or employ the ruse of claiming to be a seemingly unrelated process (see Figure 6). Very often, we've seen malware impersonate Google or Adobe apps, or even the Android operating system itself.

Some Trojans take this persistence method a step further and employ measures to force the activation or prevent the deactivation of the device administrator, e.g. by having the request pop up in a loop until the user clicks „activate".

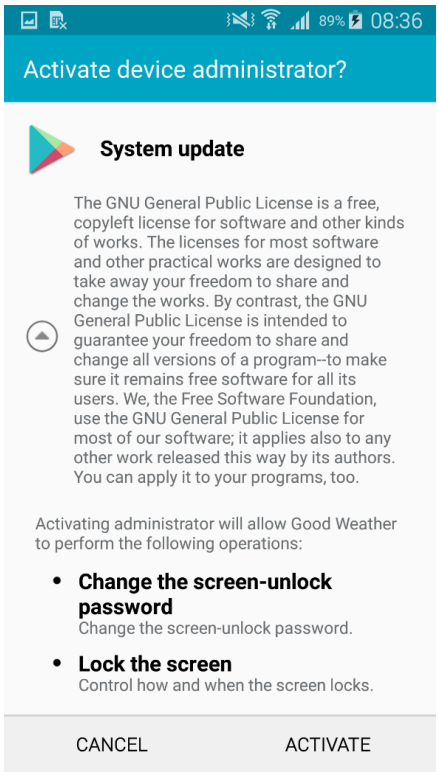

Figure 6 // A variant of BankBot posing as a "System update" with the Google Play icon to obtain device administrator rights

Another way to take over a device is through the misuse of the **Android Accessibility service**. Accessibility service functionality was created to assist users with disabilities in using Android devices by giving applications access to actions that would otherwise require physical interaction with the device. In practice, this means that an active Accessibility service with enabled accessibility permissions can, for example, mimic users' taps and swipes and thus navigate through screens on their behalf.

In the wrong hands, such capabilities can be incredibly dangerous, and enabling an Accessibility service belonging to a banking Trojan (or any other malware, for that matter) can have some nasty consequences.

As with device administrators, accessibility permissions are also often requested seemingly on behalf of a well-known, legitimate service rather than the actual banking Trojan app (see Figure 7).

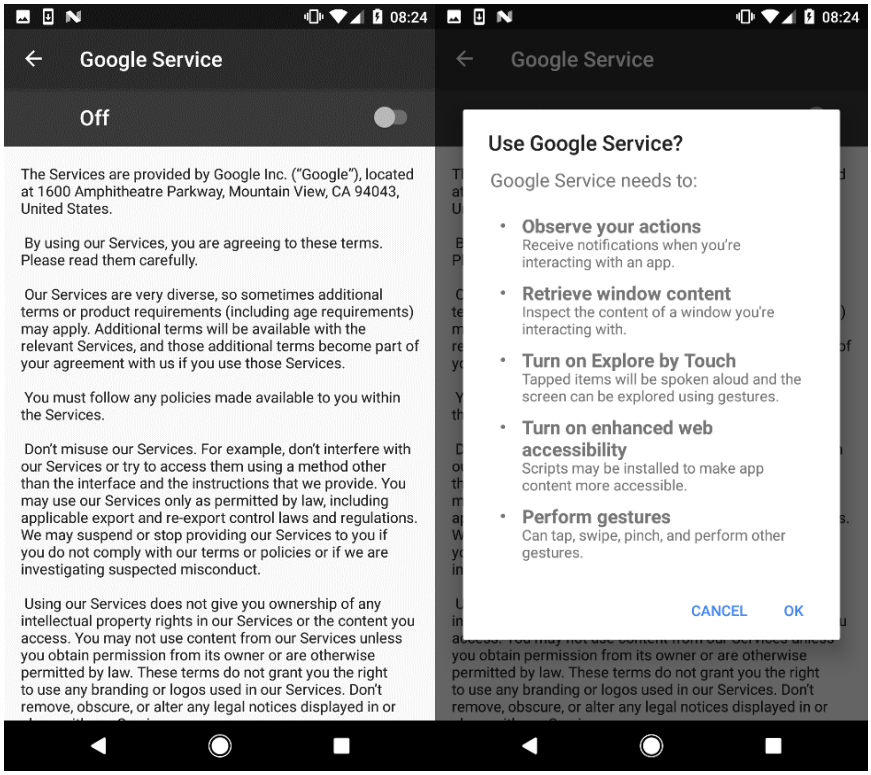

Figure 7 // A variant of BankBot requesting the activation of its malicious Accessibility service disguised as "Google service", and using a description taken from Google's original Terms of Service

In the past few years, we have observed malware abuse Accessibility services mainly to secure further intrusive permissions without having to rely on victims' consent.

In November 2018, we discovered a *novel Accessibility-abusing technique* in which the permission to perform clicks on behalf of the user is misused for direct theft with the malware navigating through targeted financial apps and transferring funds to its operators. For the technique to work, malware authors first need to reverse engineer the targeted, legitimate apps and identify relevant areas of activity, such as buttons and text boxes.

Besides legitimate permissions and rights that end up being misused by criminals, there are also special permissions that have been introduced to the Android platform specifically to counter malware attacks. From Android 6.0, apps that want to overlay the screen while another app is running need to obtain the permission to **Display over other apps**. As overlaying other apps with screen activity of their choosing is precisely what Android banking Trojans do, they need to either trick users into granting the permission, or circumvent it. That could mean using a different technique to display screens on top of others, or trying their luck with a malicious Accessibility service, which, when active, can carry out almost any action on the device.

Impact on users compared to fake banking apps:

- Potentially more damaging and more difficult to remove than fake banking apps but also more prone to detection due to advanced techniques acting as triggers for Google's security measures, security researchers and users
- Failure to gain intrusive permissions may disrupt their whole operation

Stealth techniques and detection evasion

As previously mentioned, banking Trojans are all about stealth – be it to remain unnoticed by defenders, or to keep their intentions hidden from potential victims.

Over the years, malware authors have been using increasingly advanced techniques to prevent their code from being detected and analyzed. Among the most commonly used detection evasion and anti-analysis measures are code obfuscation, packing, encryption and multi-stage malware architecture, as well as emulator and sandbox checks. More recently, timers scheduling the onset of malicious activity have been adopted by some sophisticated banking Trojans, with the aim of confusing both detection engines and affected users.

Using actual, complex apps built from open source code with added malicious functionality can have a similar effect in fooling both security measures and unsuspecting users – something that many Android banking Trojans take advantage of.

Deceiving users is of particular importance for criminals in the Android malware business – even the most sophisticated detection evasion measures are no use if a potential victim is alarmed by suspicious app behavior before the attack takes place. After installation, for example, Trojans often present users with fake error messages claiming the app has been uninstalled (see Figure 8), which is followed by the app's icon being hidden. To obtain intrusive permissions, banking Trojans commonly impersonate well-known, legitimate services. To cover malicious activity running in the background, sophisticated banking Trojans sometimes display full-screen activity that users cannot remove (see Figure 9).

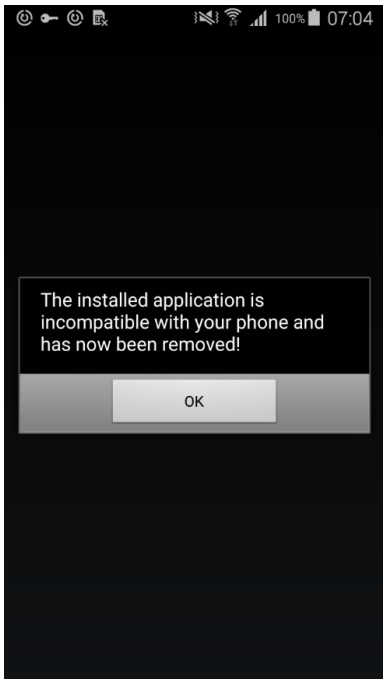

Figure 8 // Fake error message displayed by a banking Trojan found on Google Play

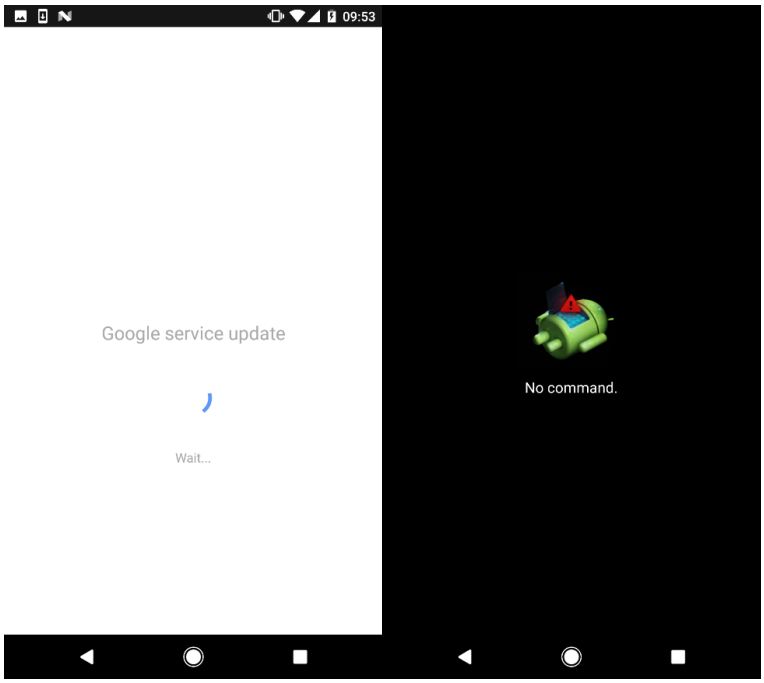

Figure 9 // Full screen activity covering malicious activity in the background, displayed by a variant of BankBot and Android/Charger.B

Impact on users compared to fake banking apps:

- Sophisticated banking Trojans employing advanced detection evasion techniques might be more successful at bypassing Google's and AV security measures and thus potentially reach and affect more users
- Large, legitimate code base may help conceal malicious capabilities, or otherwise be less suspicious to heuristic detection methods

Fake banking apps

Contrary to the complex workings of sophisticated banking Trojans, fake banking apps operate in a more straightforward way, with functionality usually limited to displaying bogus login screens and harvesting entered data. This type of malware continued to increase in prevalence throughout 2018.

Note: *We refer to this category of malware as fake banking apps because legitimate banking apps are its most usual target. However, cryptocurrency exchanges and wallets, as well as other finance-oriented and payment services and/or apps, are also sometimes impersonated by malicious fakes operating similarly to the malware described below.*

Key features and strategy

Fake banking apps bet everything on the success of **impersonation** – their whole operation stands or falls on how believably they can imitate a legitimate banking application, or stand in for a non-existent one, from the very first moment a potential victim comes across them, up to the point when the victim enters sensitive information.

Their weapon of choice is therefore their presentation – from app name, through app description, to icon and preview images, the apps need to appear trustworthy to attract unsuspecting users.

Modus operandi

To reach their malicious goals, fake banking apps typically take the following steps:

1. Trick victims into installing malware by posing as a legitimate banking app (read more in Distribution)
2. Obtain needed permissions
3. Upon launch, display a phishing screen mimicking a legitimate banking app and requesting login credentials or credit/debit card details (read more in **Targeting**)
4. Harvest credentials or credit/debit card details entered into the bogus form
5. Display an error/thank-you message; offer no further functionality
6. Optional: Use SMS permissions to intercept one-time password (OTP)
7. Carry out fraudulent transactions using the victim's account or sell credentials on the black market

Impact on users compared to sophisticated banking Trojans:

- The deciding part of the operation is its beginning – successful impersonation leading to a potential victim's decision to install the fake banking app
- People who fall for the impersonation and install the app are likely to become victims as they install these apps believing they are installing legitimate banking apps, and thus expect to see a login screen after launching the app and are willing to enter their credentials
- The malicious nature of the app is revealed when it is too late, but in an obvious manner, which often motivates victims to take action against the app – as a result, the apps may have a shorter "lifespan" on Google Play than sophisticated banking Trojans

Distribution

Fake banking apps are usually spread through Google Play or unofficial app stores, where they pose as legitimate banking, or other finance, applications.

Attackers spreading these malicious fakes try to entice their victims by using legitimate-looking app names and icons, accompanied by sleek preview images and trustworthy descriptions. What can sometimes serve as an indicator of something fishy is a mismatched app category (e.g. an apparent banking app placed in the 'Books & Reference' category, as seen in Figure 10), or an unfamiliar developer name with no connection to the financial institution supposedly issuing the app.

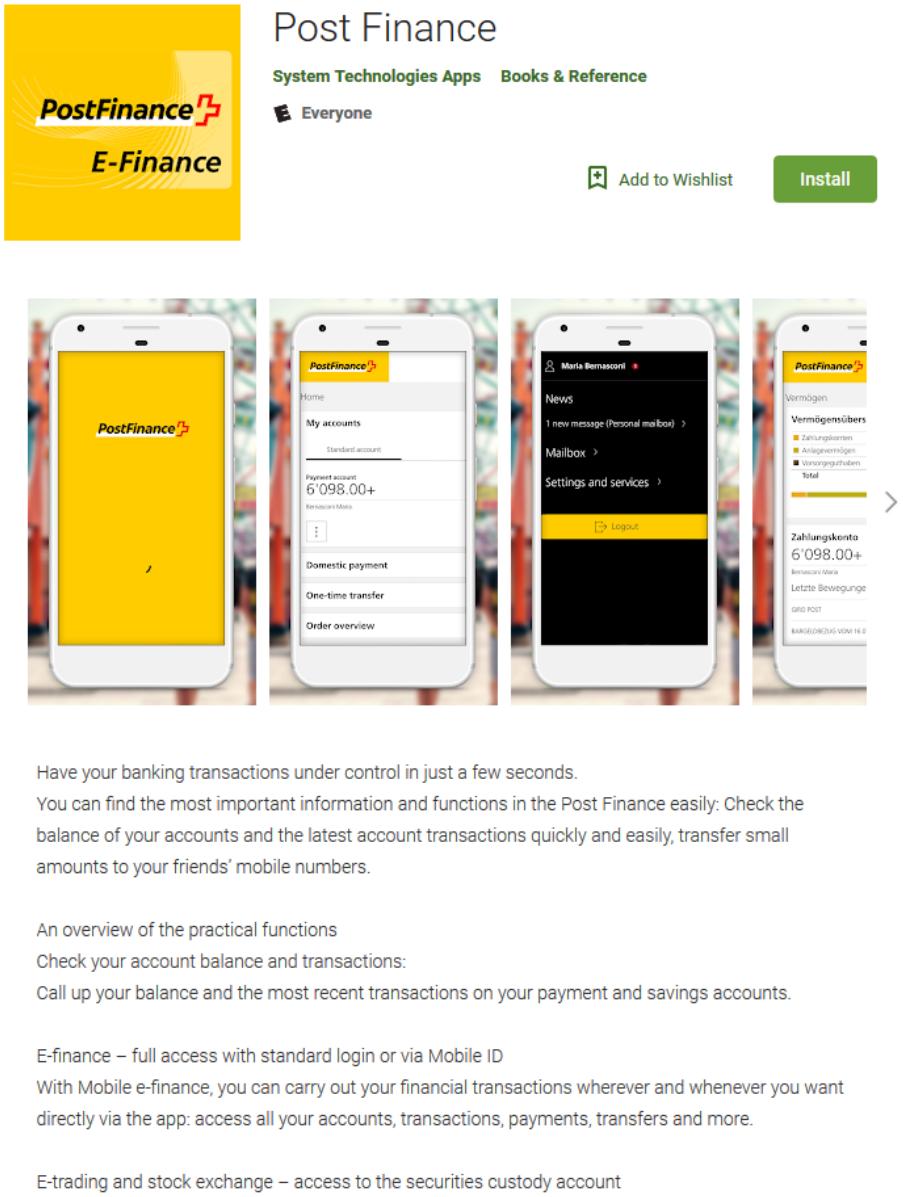

Figure 10 // Malicious app impersonating PostFinance, a Swiss financial institution, on Google Play

Impact on users compared to sophisticated banking Trojans:

- A more limited reach than banking Trojans disguised as various non-banking apps

Targeting

In contrast to banking Trojans, fake banking apps typically focus on targeting customers of just one financial institution or service – the one that they impersonate. An exception to this was a fake app claiming to be a universal banking tool for Polish users that *targeted customers of 19 Polish banks* with bogus login screens.

When choosing their target, some malware authors take advantage of *the absence of an official mobile app* for the targeted bank or service, while others attempt to fool users by impersonating existing official apps. Occasionally, the fakes pretend to offer additional, attractive functionality to existing legitimate apps, such as offering bank rewards, gifts or offering to *increase credit card limits* (**see Figure 11**).

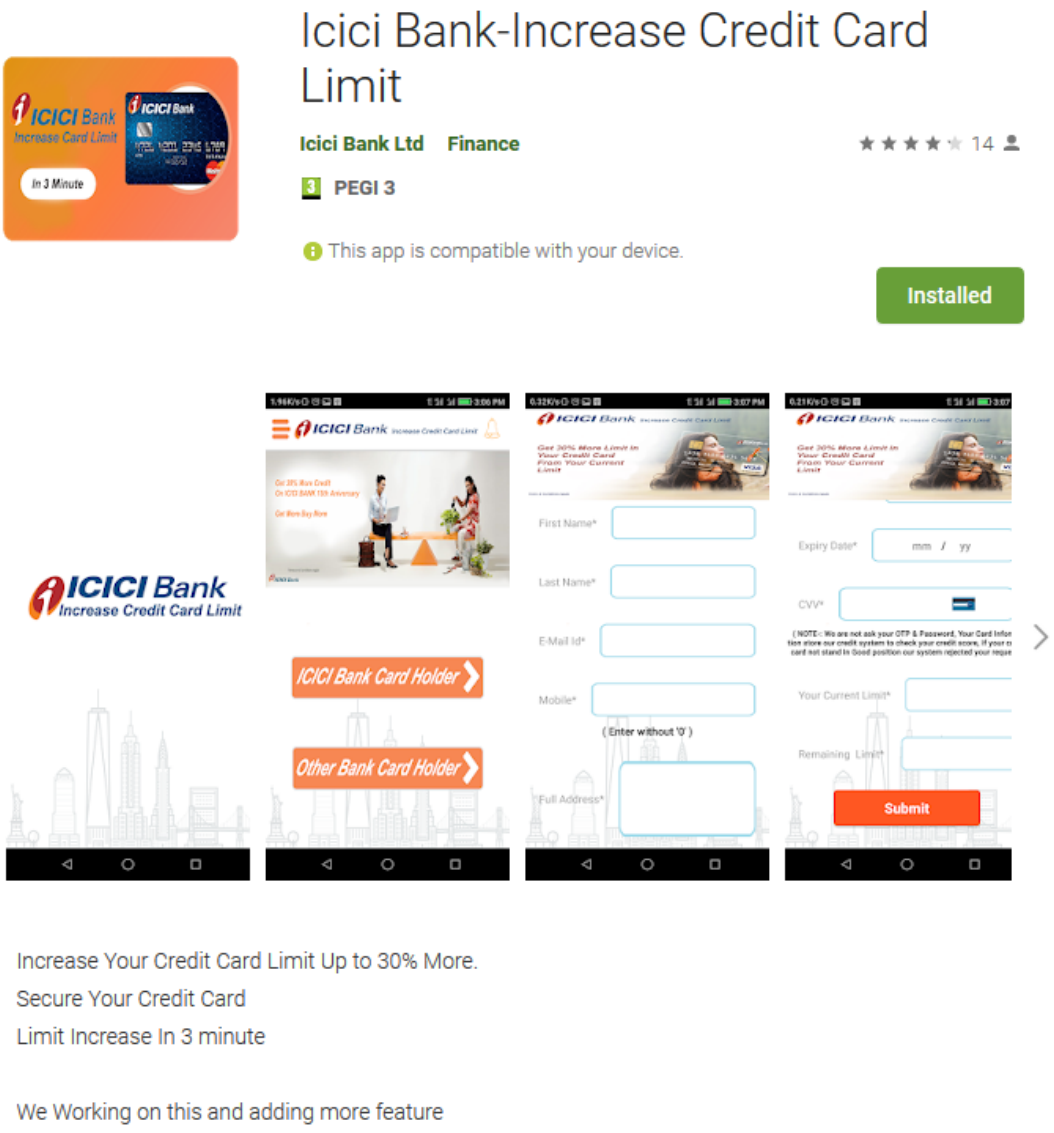

Figure 11 // Malicious app impersonating Indian Icici bank and claiming to increase credit card limit for its customers

Impact on users compared to sophisticated banking Trojans:

- A more limited target group than sophisticated banking Trojans (depending on the customer base of the targeted institution or service)

Functionality and permissions

As previously mentioned, these fake apps rely on deception through impersonation, thus their functionality comes down to displaying bogus login screens and harvesting credentials entered into the fake forms (see Figure 12).

After the credentials are stolen, some apps display generic messages with a promise to get back to the victim, as a cover for not offering any real functionality (see Figure 13). Optionally, depending on permissions gained during and after installation, fake banking apps can also intercept and redirect SMS messages to bypass SMS-based 2-factor authentication. As users install these apps believing they are installing real banking applications, they are likely to grant the apps SMS permissions without thinking twice about it.

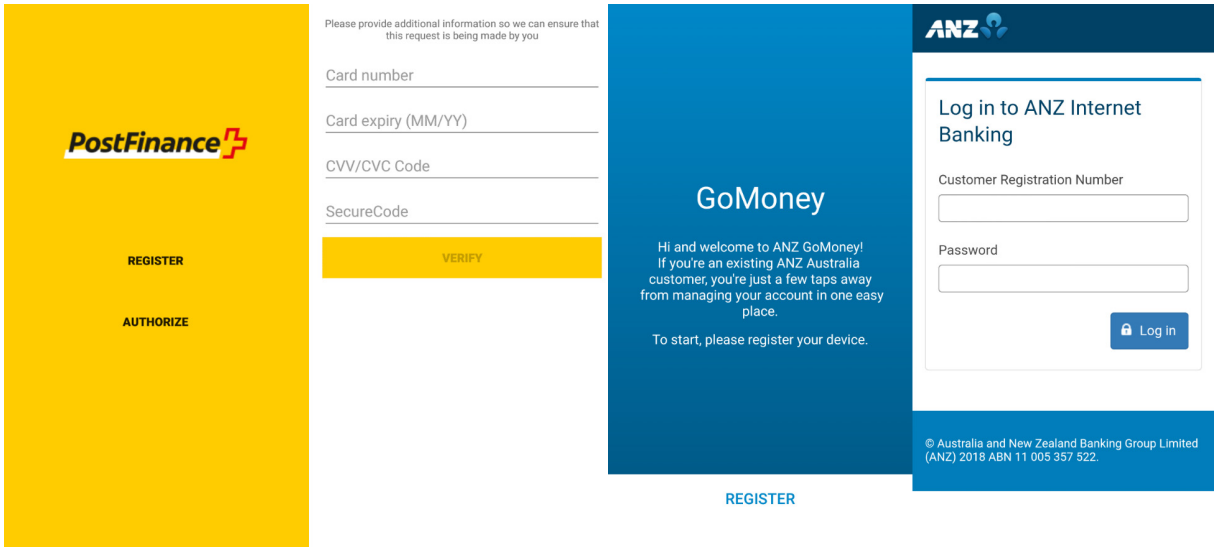

Figure 12 // Bogus login screens displayed by fake banking apps found on Google Play

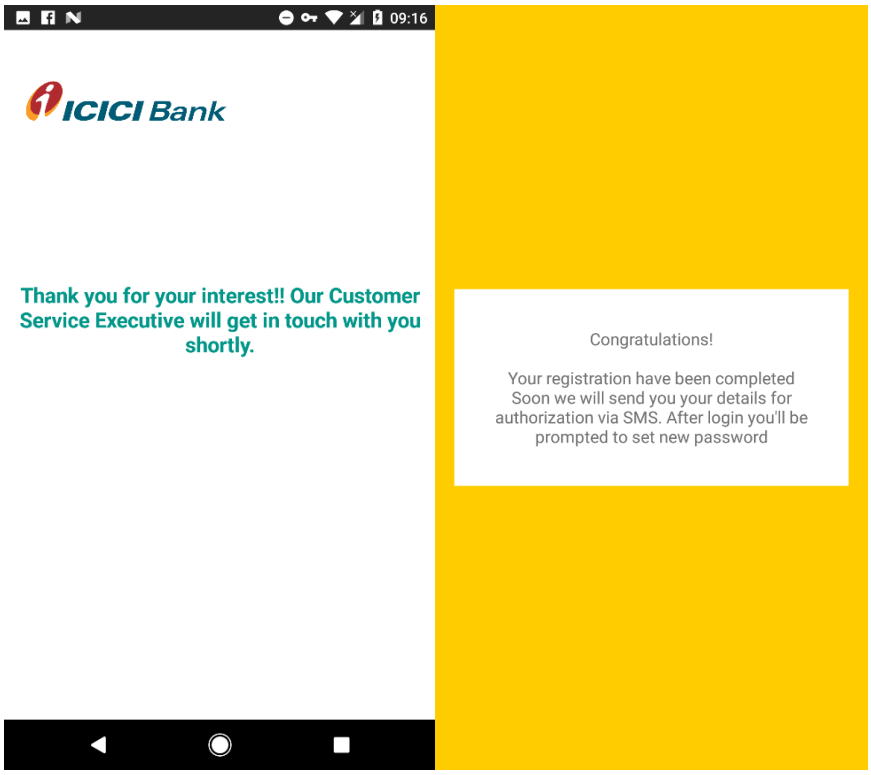

Figure 13 // Messages displayed by fake banking apps to distract victims from the absence of real functionality

Impact on users compared to sophisticated banking Trojans:

- Less powerful than sophisticated banking Trojans but also less prone to early detection due to a lack of advanced techniques acting as triggers for Google's security measures, researchers and users

Special permissions and persistence

If the operation of fake banking apps goes according to plan, they reach their goal almost immediately after being installed and launched by a victim. For this reason, the fraudulent apps typically do not attempt to obtain extensive permissions on the affected device and can thus be considered less invasive than sophisticated banking Trojans. Then again, the absence of intrusive techniques may help them fly under the radar for longer periods of time.

Impact on users compared to sophisticated banking Trojans:

- Less powerful and easier to remove than sophisticated banking Trojans but also less prone to detection due to a lack of advanced techniques acting as triggers for Google's security measures, researchers and users

Stealth techniques and detection evasion

The stealth techniques used by fake banking apps typically do not go beyond code obfuscation.

Impact on users compared to sophisticated banking Trojans:

- Less advanced detection evasion techniques than sophisticated banking Trojans, however, the lack of advanced techniques acting as triggers might balance out the overall effect

COMPARISON OF THE THREATS

To sum up, **sophisticated banking Trojans** have a potentially wider target group and reach than fake banking apps. They are characterized by extensive capabilities and stealthy operation. However, the same attributes that make them powerful also make them prone to being detected – and not just by security measures and researchers, but also noticed by users before they have fallen victim.

Fake banking apps, on the other hand, have a more limited target group and reach and are simpler and less invasive than sophisticated banking Trojans. However, their strategy ensures that those who fall for the initial impersonation and install them are very likely to become victims.

HOW TO STAY SAFE FROM ANDROID BANKING MALWARE

This section provides advice addressing the most common Android banking malware attack scenarios, including the more advanced persistence techniques used by some sophisticated banking Trojans.

How to prevent, spot and remove sophisticated banking Trojans

Prevention

- Only install apps from Google Play; this does not ensure the app is not malicious, but apps like these are much more common in third-party app stores where they are rarely removed once uncovered, unlike on Google Play
- **Before installing an app from Google Play, always check its ratings, content of reviews, number of installs, and permissions requested by the app, specifically paying attention to SMS permissions in apps that have no reason to require them**
- **After installing, keep paying attention to further permission requests and be extra cautious before activating any intrusive permissions, specifically paying attention to requests to draw over other apps, and requests for device administrator rights or accessibility permissions**
- Keep your device and applications updated
- Use a reputable mobile security solution

Spotting

The most reliable way to detect banking Trojans on your device is to run a scan using a reputable mobile security solution.

Removing

If malware is detected on your Android device, you can use a reputable mobile security solution to clean it.

In case you wish to remove a banking Trojan from your Android device manually, you need to know the names the malware and its further potential payloads use for their various forms and disguises, and locate and remove each of them. This may include:

- Malware as a Trojanized app in Apps/Application manager
- Malware as an active device administrator
- An active malicious Accessibility service

If advanced persistence techniques are used, booting the device in Safe mode and then locating and removing the malware might be necessary.

Mitigating damage

Apart from cleaning your device, it is advisable to take the following measures:

- Change your credit/debit card PIN codes as well as internet banking passwords
- Check your bank account for suspicious transactions
- If there are suspicious transactions, contact your bank
- Consider replacing your credit/debit card

How to prevent, spot and remove fake banking apps

Prevention

- **Only trust mobile banking and other finance apps if they are linked from the official website of your bank or the financial service**
- **If you are inclined to download a banking app because it offers some attractive extra features, or the bank previously hasn't offered a mobile app, always check the official website of the bank for a link to the app**
- Only enter your sensitive information into online forms if you are sure of their security and legitimacy
- Keep your device updated
- Use a reputable mobile security solution

Spotting

The lack of fuctionality usually makes victims realize they have installed a fraudulent app, so spotting such apps should not be a problem. If you are not sure, we recommend scanning your device using a reputable mobile security solution.

Removing

The apps usually do not take extra measures to secure persistence on affected devices. In most cases, they can be simply uninstalled in Apps/Application manager.

Mitigating damage

As well as cleaning your device, it is advisable to take the following measures:

- Change your credit/debit card PIN codes as well as internet banking passwords
- Check your bank account for suspicious transactions
- If there are suspicious transactions, contact your bank
- Consider replacing your credit/debit card

CONCLUSION

In this white paper, we have identified the two main categories of banking malware currently preying on Android users.

While sophisticated banking Trojans have long been regarded as a serious threat to Android users, fake banking apps have sometimes been viewed as "just scams" due to their limited capabilities. Despite not being technically advanced, we believe fake banking apps are a serious threat to Android users.

Sure – the damage done by sophisticated banking Trojans can go beyond phished banking credentials, and they are overall a more worrying threat to cross paths with. But as far as credential and money theft are concerned, fake banking apps might be just as effective – and thus dangerous for users – as sophisticated banking Trojans.

Besides this, fake banking apps are an increasingly prevalent threat, which is not all that surprising as the apps are easier to create and confronted with fewer obstacles in their operation – and criminals motivated by money tend to favor the easiest path to financial gain.

We can only speculate what type of malware will dominate the Android threat landscape in the coming years. However, it is beyond doubt that mobile devices will continue to be an attractive target for cybercriminals – which makes taking extra measures for keeping them safe worthwhile, if not necessary.

It is important to note that all the apps discussed within these categories are detected and blocked by ESET systems.

IoCs

Sophisticated banking Trojans

Package name	Hash	ESET detection name
jhgfjhgfj.tjgyjgjgjy	1C555B35914ECE5143960FD8935EA564	Android/Spy.Banker.AJZ
com.puredevlab.powermanager	7C13ADEFC2CABD85AD8F486C3CBDB6379811A097	Android/TrojanDropper.Agent.CIQ
com.apps.callvoicerecorder	DA926010056A75E7DA0DE1292B0FC7C2DCD727A7	Android/Spy.Banker.AIX
com.mygamejewelsclassic.app	B556FB1282578FFACDBF2126480A7C221E610F2F	Android/Spy.Banker.LA
com.flashscary.widget	CA04233F2D896A59B718E19B13E3510017420A6D	Android/Charger.B

Fake banking apps

Package name	Hash	ESET detection name
ch.post.finance	FE1B2799B65D36F19484930FAF0DA17A0DBE9868	Android/Spy.Banker.AIF
au.money.go	DE09F03C401141BEB05F229515ABB64811DDB853	Android/Spy.Banker.AIF

ABOUT ESET

For 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn *100 Virus Bulletin VB100* awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on *LinkedIn*, *Facebook* and *Twitter*.

ENJOY SAFER TECHNOLOGY™