Evolution of the mobile threat landscape - 2018

THREAT FABRIC

ThreatFabric B.V.

Naritaweg 106A
1043 CA Amsterdam

E-mail: info@threatfabric.com
Web: www.threatfabric.com

Table of Contents

1. Executive summary

Although cyber-criminal motivations are numerous, the prominent one remains money. Threat actors motivated by financial gain have noticed the shift of consumers from desktop towards mobile based online banking. The dominant market share and the flexibility offered by the Android operating system, combined with the shift towards mobile banking has resulted in a surge in Android malware visible since early 2014.

Despite mobile based attacks not yet having reached their full potential, they already represent a threat with which many financial institutions are not familiar enough. This year the challenges for financial institutions will be multiple, not only having to keep an eye on traditional threat developments, but also on the new risks for the payment chain introduced by PSD2, such as but not limited to third party access to sensitive information, banks' fraud detection based on the limited customer/device information available, third party lower security standards and broader attack scope due to multi-tenancy.

Threat actors keep on improving their tools, overlay attacks being one of their favorites as they are a simple way to social-engineer victims and new overlay screens can be made very easily. Using these overlays, criminals no longer limit themselves to banking apps, but increase their non-banking targets including mail clients, web stores, chat/communication tools, social networking apps, booking apps and even app stores.

To grow the ROI from fraud, malware distribution also has been improved, having certain actors specialize in spreading malware through several different means such as social networks, cloud-based file sharing and even the official application stores themselves, making even these official stores a place to keep on your toes when installing a new app.

In line with their continuous efforts to bypass detection measures, threat actors started working on Remote Access Trojan (RAT) capabilities, making their malware even more powerful by providing them remote hands-on access to the infected devices. Although the main aim is to bypass 2FA and fraud detection, such capabilities bring potential to evolve towards data exfiltration or espionage. The open ecosystem of Android makes it easy to gain access to sources of sensitive information, in addition, a vast majority of people have a smartphone and carry it around all day long, making these devices the ideal spying tool.

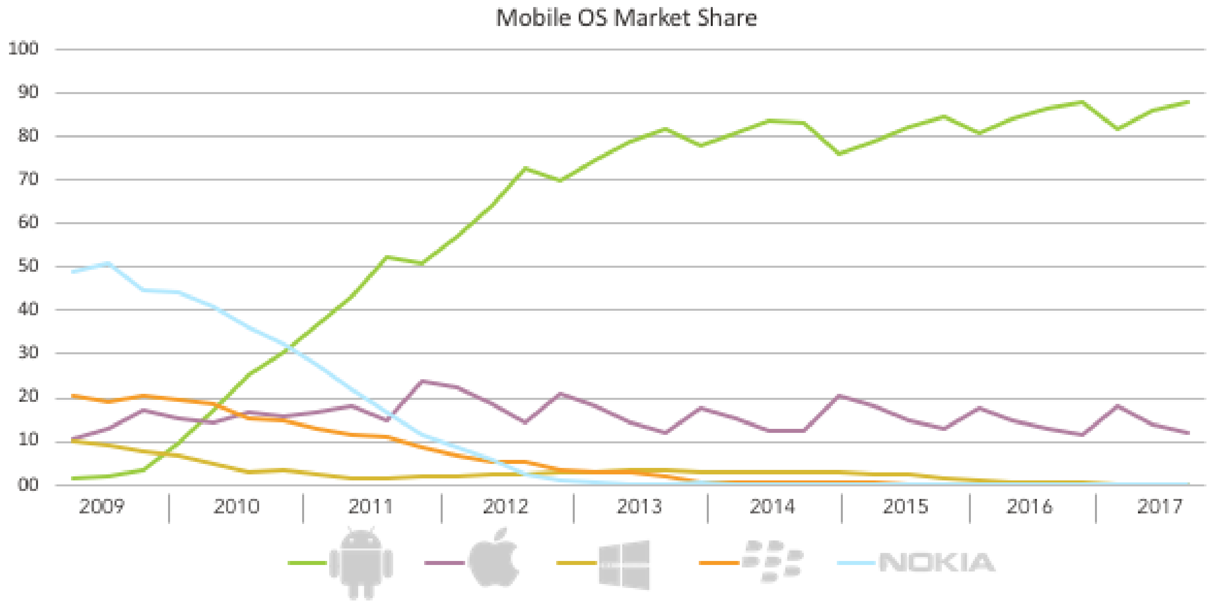
This report provides insight on the evolution of the Android threat landscape since it's early beginning and how ThreatFabric experts expect it to evolve in the coming years.

2. Introduction

2.1 Context

Although cyber-criminal motivations are numerous, the prominent one remains money. Threat actors motivated by financial gain have noticed the shift of consumers from desktop towards mobile based online banking. This trend shouldn't come as a surprise as numerous banks bet on their mobile services to conquer the market, some banks are even only available through digital channels.

Due to the limitation of hardware partners and general interest in the platform, Windows Phone represents approximately 0,1% of the mobile operating system market share, the second position is held by Apple's iOS oscillating between 11% and 17% of the market share depending on the release of its new devices. In an impressive leading position comes Google's Android, with a market share between 82% and 87%, mostly affected by the variations in iOS numbers.



The dominant market share and the flexibility offered by the Android operating system, combined with the shift towards mobile banking has resulted in a surge in Android malware visible since early 2014.

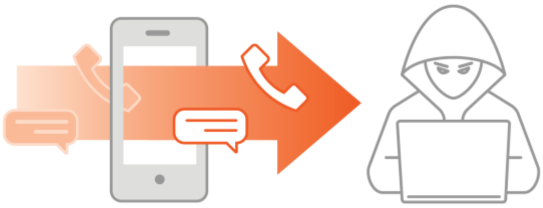
Since their early stage, mobile based threats haven't ceased evolving and regularly offer new features or improvements, allowing criminals to remain undetected and reach their fraudulent goals. Due to the nature of the targeted platforms, mobile malware capabilities are nowadays surpassing their desktop-based ancestors.

The purpose of this report is to share the knowledge gathered by ThreatFabric experts during investigations over the years and provide an overview of their expectations regarding future trends on the mobile threat landscape.

2.2 State of the art

The surge of Android malware since early 2014 can be split into different eras, each distinguishable by specific techniques built to gather the information needed to perform fraud. Understanding those eras and techniques is an important pre-requisite before talking about future trends and expected developments.

2.2.1 SMS and call forwarding



In order to understand the motivation behind the creation of the first Android banking malware we have to look at the existing computer-based malware and the security measures implemented by financial institutions. To perform fraud, computer-based malware involves interaction with the victim in order to gather the information required to perform transactions. To make it more difficult for fraudsters to be successful, many financial institutions have implemented second factor authentication mechanisms (2FA) to validate transactions, often based on the mobile channel.

The most frequent implementation of 2FA uses one-time-passwords (OTP) sent via SMS to the user. As this security measure made it more difficult to perform fraud, some actors behind desktop malware decided, between 2013 and 2014, to create Android malware to intercept SMS messages sent by the banks, giving them access to the one-time-passwords. Another implementation of the 2FA used automated phone calls to transmit the OTP to the user. To also be able to intercept OTP's sent using this method, the actors added call forwarding functionality to their Android malware.

ZitMo, *mTan*, *Perkele* and *iBanking* are examples of mobile malware used in the so-called SMS and Call forwarding attacks. To perform fraud the actors where still harvesting login credentials on the desktop but didn't need to rely on the victim anymore to provide the OTP from the mobile device. This reduced the required interaction with the victim and increased the fraud success rate.

2.2.2 Overlay attacks

2014 and 2015 show an important shift from desktop banking to mobile banking (according to certain banks, in late 2015 most logins to online banking were already taking place via mobile apps). This overall shift from desktop to mobile made actors even more motivated to focus on mobile attack vectors.

In early 2014 the first Android banking malware making use of an overlay attack appeared. The overlay attack, as the name suggests, is an attack where the malware will overlay the screen with a phishing page whenever a targeted application is started on the infected device.

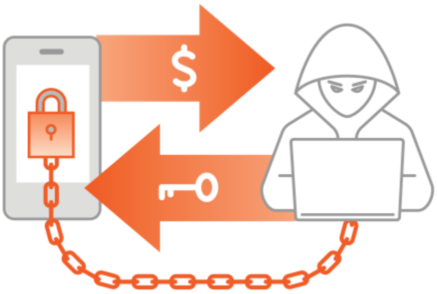
The overlay window is often indistinguishable from the expected screen (such as a login screen for a banking app) and is used to steal the victim's banking credentials, or other information such as credit card details. The list of targeted apps and overlay screen content can, in most cases, be dynamically updated via the C&C server of the malware, significantly increasing the flexibility of this attack.

In early 2016 malware called MazarBot surfaces. This malware combines both the overlay attack vector and the SMS interception, enabling the malware to steal login credentials through phishing and then use them to perform transactions by intercepting the OTP's.

MazarBot was created based on the source code of another Android malware called GMBot, which was leaked in December 2015. MazarBot was not the only malware however that used the leaked source code as a basis. Other families such as MBOT, Android KNL, Cerus, Abrevel, AceCard, Shiz, Catelites, CronBot, Marcher, Exobot and Bankbot also have their roots in the GMBot malware. Most of these new malware families are rented malware, meaning the creators rent panels (backend system to control the malware) and Android malware to other criminals to perform fraud.

The popularity of the overlay attack vector resulted in several actors selling packages of overlays on underground forums, just like web-injects for desktop malware.

2.2.3 Ransomware functionality



It is 2016 that the first Android banking malware with ransomware capabilities appears. The combined functionality was first observed in the Catelites malware, which has an option to encrypt all files on the SD card and present the victim with a message urging them to pay to get their files back. This functionality however was not used by default but triggered by the actor from the control panel. What also stands out for this malware is that it has the ability to overlay most banking apps in the world using a generic template. In 2017 another banking malware embedding ransomware capabilities appeared. This malware named Lokibot, however, didn't need interaction from the actor to trigger encryption of files on the victim's device. Instead this functionality was triggered when a user tried to remove the malware from the device. It seems that the actors behind the Lokibot malware used the ransomware as a last resort to try to monetize the infected device. Ransomware will always be part of the threat landscape, but it is alarming the see that it is now becoming an integral part of the default banking malware kit, possibly hurting victims by not only the banking malware MO, but also taking their personal files hostage and making the advice to remove the malware a bad choice in some cases.

2.2.4 Device rooting

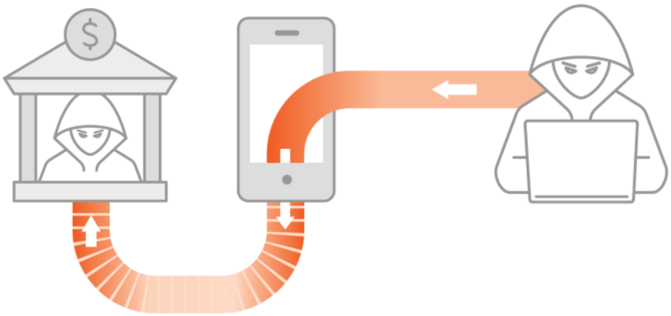
End 2016 two banking Trojans, Shiz and Zniu, were found to have rooting capabilities, enabling the malware to exploit vulnerabilities in the device's security to gain the highest possible privileges. The actors behind the malware were aiming to use the gained privileges to bypass mobile security applications by simply terminating the application process. Once the antivirus or security application was disabled, the malware would proceed to download and installation more advanced components to efficiently perform fraud.

During the same period the Dvmap Android malware was discovered. This malware, which wasn't used for banking fraud, used root privileges for more advanced exploitation. It modified the code of the Android system to disable the built-in security mechanism that prevents users (and therefore apps) from installing applications from other sources than the Google Play Store. By doing so the malware could install applications from other sources on the device. This functionality was possible used as a malware distribution service for other actors.

2.2.5 Key strokes logging

During 2017 a new Android Trojan named CryEye (often also referred to as Svpeng) surfaced. It offered a powerful new key-logging feature, logging key strokes by abusing the Android Accessibility Service. The Accessibility service has been created to enable application developers to build apps that can assist users with disabilities in using the device (i.e. screen readers). In the first step of the keylogging process, the malware takes a screenshot of every key stroke made on the device. As a result, it obtains images of every character typed on the virtual keyboard before characters are put into the password field and replaced by dots. The second step involves sending all the screenshots to the criminal infrastructure (C&C server), where each set of pictures is stored in sequence for future use by the actors. While the use case here is banking fraud, the information can obviously also be used for other purposes, such as espionage.

2.2.6 Proxy feature



Although overlay attacks, just like the more traditional phishing attacks, are very effective against users of banking environments that implement no or very limited fraud detection capabilities, they are ineffective against banks using fraud detection patterns. Pattern based fraud detection is making use of information such as but not limited to the public IP address of the connecting device. If deviations of characteristics occur during online banking, the fraud engine will attribute a higher risk score to the related session.

This is why late 2016 some actors started experimenting with proxy functionality enabling the actors to use the IP address of the victim to perform fraud, basically fooling IP-based fraud detection. At the end of 2017 for example, the Exobot malware (often wrongly referred to as Marcher) got equipped with SOCKS proxy functionality, enabling the actor to route the network traffic through the infected mobile device, making it seem to banking systems that the traffic is coming from their banking customer.

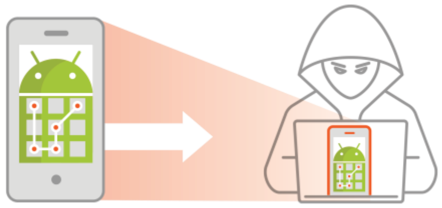
2.2.7 Distribution as a service

At the end of 2016 an actor nicknamed Maza-In published a blog on an underground forum detailing how to write an Android banking Trojan, even including sample code for the bot and the control panel, based on his own malware dubbed Bankbot. This blog resulted in an important surge of Android banking malware based on this source code. The many variants of the Bankbot malware were not only spread via Smishing (SMS phishing) or pornographic sites (using fake Flash Player apps), but also via the Google Play Store. Many different malware samples were discovered in the Google Play Store, targeting over 500 different Android banking apps in total. Although Bankbot isn't very advanced malware, it's effective distribution campaigns resulted in high infection rates, make it very successful.

After several waves of distributing malware directly through the Google Play Store a new underground service appeared: malware distribution. This service consists of selling dropper apps (often called loaders by the actors) that are already installed on many devices through the Google Play Store. These dropper apps can then be used by the malware actors to install their own malware on devices. The advantage of such as service for the actors behind the Android banking malware is that they can focus on improving their malware and performing fraud as the distribution is outsourced. The droppers are mimic legitimate apps such as games, flashlights, battery boosters or video players to bypass Play Store security mechanisms and trick users into installing the app. Once the dropper is installed on the victim's device it will performed the tasks the victim will expect it to perform, but in the background will install the malware.

During 2017 at least 4 different actors have been selling dropper services to the actors behind the infamous Red Alert, Exobot and Bankbot banking Trojans. One of the actors behind such services was GanjaMan, author of the GMBot malware and the actor who introduced the use of overlays in 2014. The appearance of services such as these show that the Android banking malware threat landscape is evolving and becoming more mature.

2.2.8 Remote Access Trojan



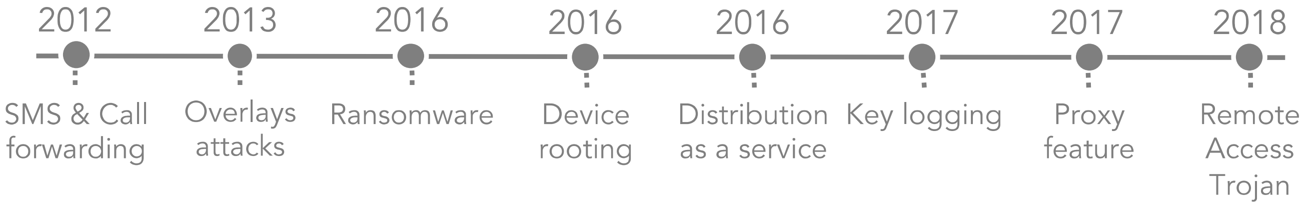
The latest feature added to the Android banking malware arsenal is again one already seen before in desktop malware: remote access. The technology used (VNC) is often used by administrators to remotely manage devices, and now abused to provide actors the ability to remotely control the victim's device as if they have the device in their own hands. The power of this feature is pretty clear: it enables actors to bypass any security measures, including fraud detection, which are based on the device. This includes things like device binding and IP-address checks. After obtaining the login code of the victim, the actor can simply log in to the banking app on the victim's device and perform transactions. This can be done for example at a moment the victim is not using the device as to not raise any suspicion.

In the end of 2017, an actor nicknamed Maza-in started developing VNC functionality for his private Android Trojan named Anubis II (also called Bankbot v2). At the time of writing, this is still an ongoing project. He seems to work hard on features to hide the remote connection from the end user to avoid raising suspicions. Currently there seem to be two options to achieve this goal: On one side the actor can lock the screen of the Android device to keep the victim away from seeing what is happening. On the other side the actor can create a hidden VNC session, allowing him to manipulate the device at any moment even while the victim is using it for other purposes. In additional to the VNC functionality, the actor seems to also be writing code to get access to the file system of the infected device, giving read access into all folders and files on each victim's phone.

2.3 Conclusion

What we observe through the evolution of the Android-based banking malware is that threat actors' interest in mobile malware started with the motivation to bypass 2 factor authentication mechanisms. This interest kept growing stronger with the ongoing shift from desktop to mobile banking, resulting in the continuous development of new features.

An important step for the criminals to increase the fraud ROI was to scale-up their operations through new distribution techniques, with a strong focus on the official Google app store to avoid raising suspicions.



As many financial institutions have at least minimal fraud detection functionality, financially motivated threat actors keep on building tools to evade detection, of which the most recent one gives actors full remote access to the victim's device, enabling them to bypass most fraud detection techniques but also to steal all data on infected devices for potential monetization.

3. Future trends

Threat actors continuously try out new techniques to perform fraud and therefore build new tools to improve their attack capabilities. An observed phenomenon is that those improvements will, after some time, end-up being copied or leaked, resulting in a wave of threats with new properties to counter.

3.1 Continuing shift from desktop to mobile

Criminals follow the money. Although this shouldn’t come as something new, the fact that a large majority of online banking users have made the shift towards mobile banking is a signal for adaptation of Modus Operandi for those criminals.

Another interesting fact is that a predominant part of criminals will choose the easiest path to money. Complex procedures might represent a higher ROI but also a lower chance of success. The fact that the weakest link of online banking remains the customer, combined with the shift to mobile, is a reason for mobile-based malware to be an attractive attack vector for scalable fraud.

Although we might still be surprised by some spectacular fraud scenarios from time to time, the vast majority of financially motivated attacks will use similar patterns to what has taken place during the last decade. Looking at mobile attacks, the Modus Operandi seem very similar to those of desktop malware, for a very simple reason: it works. Unless there are other ways to easily increase their financial gains, there is no reason for the criminals to spend time on creating new attacks.

Another important reason that makes mobile such an attractive platform for fraud is that the platform is used for many more purposes than the desktop and has become part of many consumers’ daily life, making it a resource rich in information and possibilities.

3.2 Chronic waves of ransomware

While ransomware is one of those old and not very advanced techniques to racket device owners, it still chronically comes back on the threat landscape like rolling waves. Although ransomware has one main goal, locking the victim away from its data or device, two different types can be distinguished.

Picture “Ransomware, your data or your money”

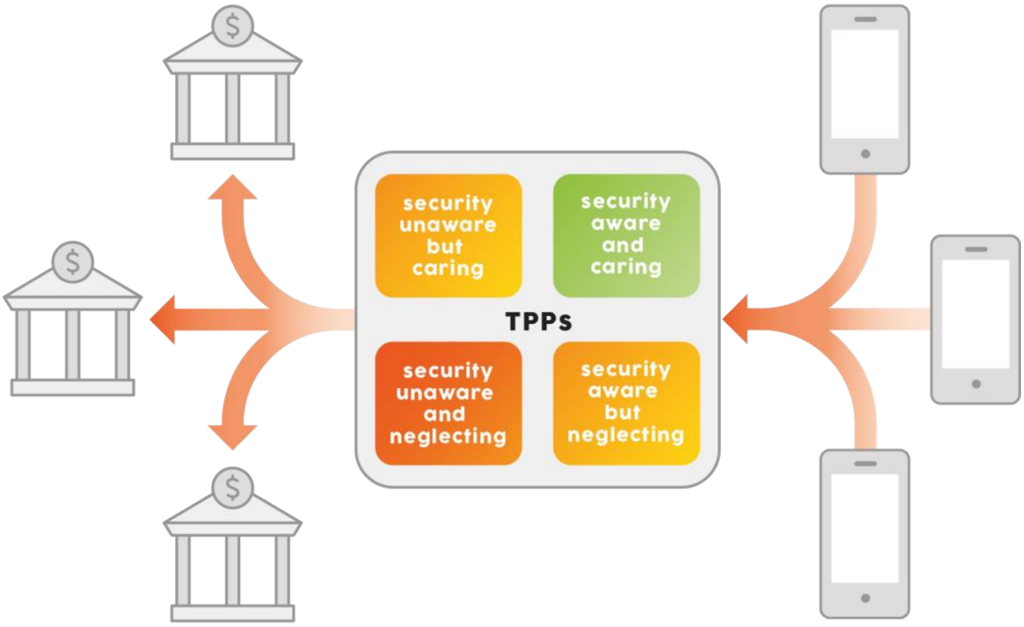
On one side the crypto-lockers that will encrypt data on the device, offering the victim restoration of data in exchange of payment. On the other side the blockers that will block the device from working properly, either blocking access or blocking specific software.

Until now the most popular form of mobile ransomware are blockers, just showing a persistent overlay with a threatening message, which is easier to create and maintain than an actual crypto-locker. The problem of mobile ransomware is the nature of the device and/or data taken hostage. Mobile phones have become an essential part of everyday life, meaning that a blocked/encrypted device can turn into a major handicap for personal and professional life.

The reason for which the ransomware concept persists is the simplicity yet effectiveness to affect a wide group of people and so earning money even without advanced technical skills. Although no major improvements or developments are forecasted, ransomware can be expected to remain one of the malware types regularly active on the threat landscape.

3.3 Risks of PSD2 and mobile

The PSD2 payment directive designed by the European Union has been created to revolutionize the payments industry. The opening of banking services to third parties should indeed offer a lot of new possibilities for consumers, but the lack of attention for security and fraud matters leave experts sceptic. The concept is rather simple: banks should allow Third Party Providers (TPP) access to customer information through APIs, enabling those providers to build financial services on top of the banks' data and infrastructure. There are two types of TPP, the AISP (Account Information Service Provider) able to access account information of bank customers and the PISP (Payment Initiation Service Provider) able to handle payment transactions on behalf of the bank customers.


security unaware but caring
security aware and caring
TPPs
security unaware and neglecting
security aware but neglecting

Picture "The 4 types of TPP and associated risk level"

We foresee four major challenges with PSD2: The first one is that we expect a lot of new mobile banking apps in the stores with significant security flaws which can be abused by malicious actors. With more than a decade of experience in the financial industry we can attest that most mobile (banking) apps are not developed with security in mind. In fact, most of the FinTech companies are not even aware of the basics such as the OWASP mobile top 10 risks. For those companies, secure development is unfortunately not a priority. Furthermore, according to the General Data Protection Regulation (GDPR), although banks are required to give third-parties control over customer data, the banks will remain liable for the security of that data. This lack of responsibilities on the side of the TPPs won't push them to guarantee security and safety of their service.

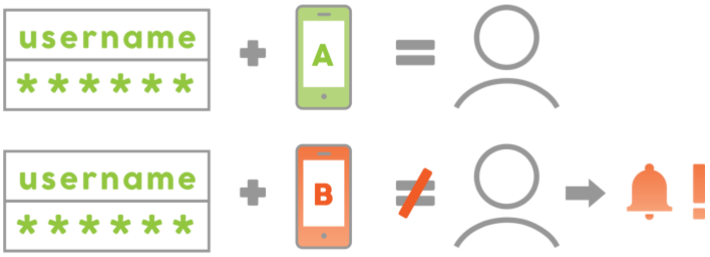
Once threat actors will get familiar with the PSD2 concept flaws, the second challenge we expect are untrusted TPPs (threat actors operating as TPPs). The concept would be to act as regular TPP during a certain period to gain consumers' trust, once being trusted and having most consumer data act as Man-in-the-Middle to perform fraud. The requirements to become a TPP are ridiculously low: PISPs need to hold a minimum of €50,000 in reserve and both AISPs and PISPs must have suitable professional indemnity insurance. No check of criminal record seems to be required.

The third challenge we predict is the general decrease of security when using TPPs services. Applying the PSD2 model to mobile banking, TPPs would be standing in between the banks and the consumers, meaning that the banks will lack visibility on the end user, their behavior and their devices. Fraud detection based on remaining, limited information will be difficult and the added security of features such as device binding won't be used in the PSD2 model. If TPPs use their own authentication mechanisms to allow user to access their services, the banking environment is no longer subject to the authentication and security rules that banks have built over the years. The only way for banks to settle this would be by enforcing their own authentication standards via the API to the consumer and TPP.

The fourth challenge we can expect with TPP acting as central access point to multiple banking services (multi-tenant), is the potential fraud multiplier effect that it can have. As multitenant online banking service it would represent a valuable target for threat actors, for example using a single overlay attack to gain access to accounts at multiple banks.

3.4 Device registration fraud

To prevent fraud with stolen login credentials banks introduced the concept of device binding: before the user can log in to an account through mobile banking for the first time, it is required to use an out-of-band authentication mechanism such as a token to register the device on the account. This way the bank knows for sure that the user using the device is actually the owner of the account.



Picture: "Device registration: association and detection"

This out-of-band authentication is only required during the registration process. For usability purposes, further log in actions only require for example a passcode.

Threat actors are aware of such mechanisms and will try to collect the information needed to perform the so-called binding of their own device and ensure that it's considered trustworthy by the bank. This attack can be cross-platform as observed in attacks performed with the Ramnit and Zeus-Panda desktop malware where victims were tricked into providing specific information, such as one-time passwords, which would then be used by the attacker to register a device. After the registration the device could then be used to perform transactions. Because in this scenario binding a new device is a precursor to fraud, this action is an important signal for fraud detection. In addition to this the newly bound device will come from a different IP address as the user's current device(s). These flaws in the attack are forcing attackers to become even more inventive by using the victim's device as a proxy or even taking over the victim's device to perform a transaction.

Even though device binding and other client-based security mechanisms can be bypassed, they still provide an important role in the defense against fraud. As stated in the section related to PSD2, having a third party in between the banks and their customers will nullify the benefits of these security mechanisms.

3.5 Broadening attack scope

Since the first appearance of banking malware on Android we've seen the malware mainly targeting mobile banking apps, sometimes including the Google Play Store in its target list. For a while now we see a trend where more and more non-banking apps are added to the targets, mainly using overlays requesting credit card details. The main reason for this seems to be that actors want to use their malware after infecting the device as soon as possible, not wanting to wait for a long time for a rarely used app to be started. After all, if they don't act soon after infection, the malware could be noticed by the user, blocked or removed by antivirus or the command and control server could be taken offline. Apps that we often see being targeted are for example WhatsApp, Instagram, Facebook, Twitter, Viber, Skype, Uber, Airbnb, eBay and Amazon, with the latest addition being some cryptocurrency wallet apps.

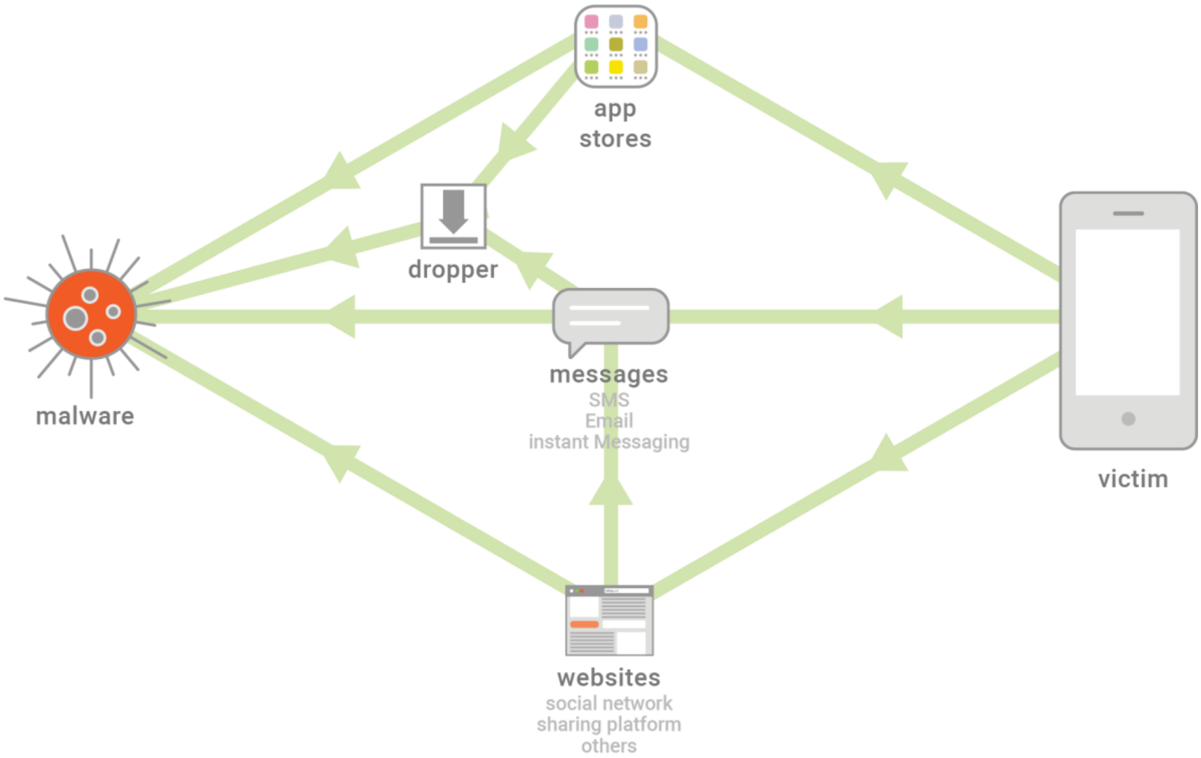
Picture: "Numerous potential mobile vectors for criminal usage"

As overlays usually are just simple html pages, it's very easy for actors to grow the list of targeted applications, making the main challenge monetization of the stolen data.

We can expect criminals to continue to broaden their target scope, adding apps that require personal data or login credentials, not only using the credit card overlays but also requesting app specific details for later monetization.

3.6 Evolution of malware distribution

The success of financially motived threat actors doesn't depend solely on the capacity of the malware to remain undetected but also on the infection campaigns spreading that malware. After all, having more infected devices means more chances to perform fraudulent transactions. To achieve higher infection rates actors have been experimenting with new means of distribution and will keep doing so for as long as they think it can increase their ROI. Early 2017 we discovered a dropper campaign spreading more than 20 different malware samples via the official Google Play Store. The actor uploaded the droppers disguised as different, seemingly benign apps which were found to be benign by Google's internal malware scanner (Bouncer) and remained undetected for more than half a year. Once one of these droppers was installed on a device it was used to provide the dropper service to different actors, downloading and installing different banking malware on the infected devices. Because the droppers come from the Play Store and are disguised as useful apps, the average user will simply install the dropper without suspecting a thing, making this distribution MO very powerful.



Picture: "All roads lead to Malware – multiple ways to infect a device"

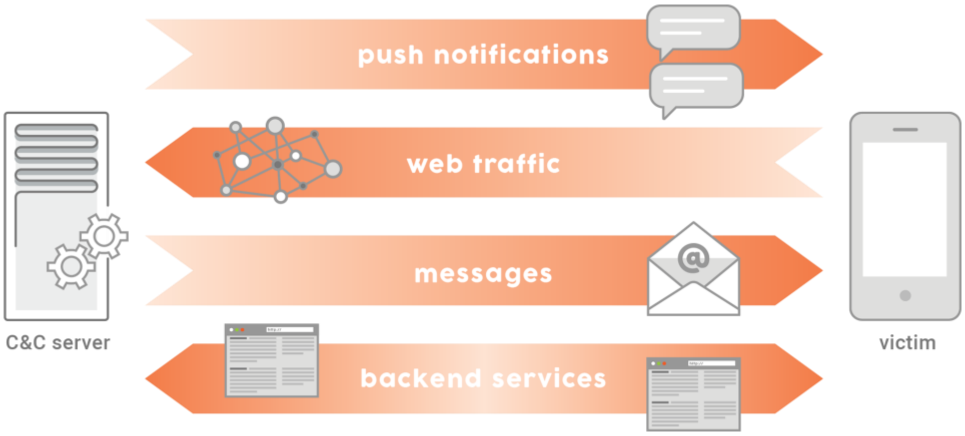
Interestingly enough, during 2017 we observed actors trying out new spreading techniques focused on social networks. The process is simple but effective: the malware is uploaded to Google Docs (Google's document sharing service) which results in a shortened URL that links directly to the malware. That link is then spread to the victims through social media. Because the link refers to a Google domain and the URL shortening hides the file extension, users will not quickly be alarmed. However, the downside of this technique is that the app installation file does not come from Google Play, requiring the unknown sources setting on the device to be enabled before the app can be installed.

Based on what we have seen so far, we can expect two main trends regarding malware distribution in the coming year. On one side the less technically advanced actors that will continue focusing on distribution through social networks and/or other websites, tricking victims into allowing installation from unknown sources on their devices (if it is not already enabled), on the other side more advanced actors that will rather spread through the official app store. At some point actors will start combining the above-mentioned MO's, putting malicious apps in official stores and spreading their existence on social media to ramp up infection rates.

3.7 Hiding and multiplying communication channels

To be able to run fraudulent operations with a minimum of disruptions, criminals put a lot of effort into making the communication between the infected device and their backend infrastructure robust and well hidden. This has resulted in several different channels and techniques currently in use by certain malware to connect to their Command and Control (C&C) servers.

Besides communicating directly with their respective C&C servers, many malware variants, such as Exobot, use SMS as a main or backup channel to receive commands and send information. Other channels being used are push messages using Google Cloud Messaging and the communication options of the Google Firebase platform (an information gathering tool for app developers). One malware variant named Red Alert even uses Twitter, though only to obtain the location of an active C&C server to communicate with in case the original one is unreachable.



Picture: “C&C communication via covert channels”

These communication channels used in addition to the direct communication with the C&C server present two challenges for targeted institutions: Because of the nature of these channels it is extremely difficult to detect infections through monitoring the communication. Especially the use of channels often used by legitimate apps is an issue. The second challenge is disruption of the communication channel. Where with direct communication with the C&C server it is often possible to take over the domain name or take down the server, when legitimate communication platforms are used this is more complex. In addition, fallback mechanisms as the one used by Red Alert make it even harder to permanently disrupt the malware.

Looking at the developments so far, we can expect features as described above to become more common among mobile malware variants, making detection and prevention increasingly difficult.

3.8 Device rooting

Until now we've seen several Android malware variants use exploits to obtain root privileges. So far only one of these variants was used to perform banking fraud, using the gained privileges only to prevent detection. Because these root privileges can do much more than just disable security measures, such as making the malware persistent on the device, even after a reset, or give access to areas outside the normal application sandbox, we can expect rooting to become more popular in banking malware, especially if an easy-to-use exploit kit becomes available.

One of the uses for the root privileges is to install additional malware without requiring any user interaction (which normally is required): The user simply installs a malicious app from the Play Store (disguised as a legitimate app) which will then install the actual banking malware on the device.

Picture: “Rooting, the root of all evil”

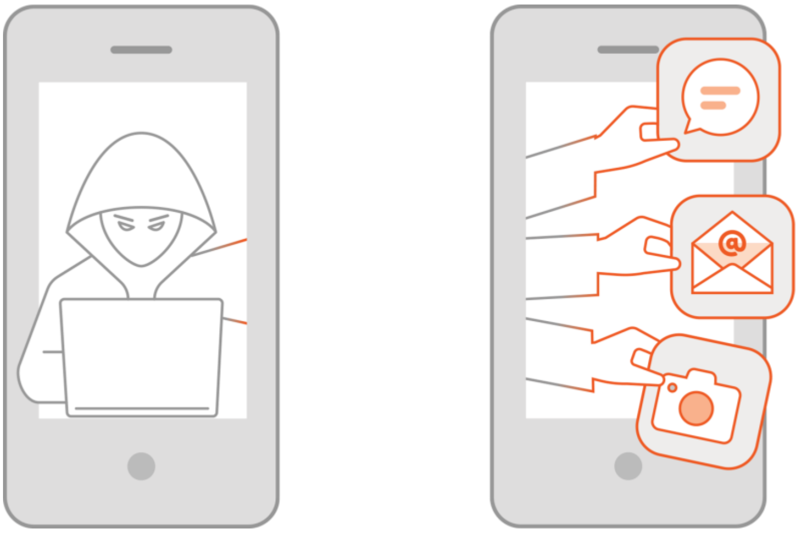
Then there is the option for the malware to steal sensitive data from the device which can be used for fraud, such as device binding details (effectively cloning the banking app to another device).

Another, more advanced use case is that malware will modify low level system functionality to redirect certain internet traffic to different servers to perform Man-in-the-Middle attacks against banking traffic or show a fake banking web site.

3.9 Remote Access Trojan functionalities

As we are starting to see banking malware include features similar to those of remote access Trojans, it is interesting to think of what these features can be used for. The first thing that come to mind is of course working around 2FA barriers and server-side fraud detection, since that is a priority for banking malware. It is however also good to realize that the actors using the malware will not limit themselves to online banking fraud if other opportunities to monetize the infected devices arise. If for example they find out the device contains valuable information, they will not hesitate to steal it.

This means that banking malware will cause a risk not only to the users of the device, but also to the companies these users work for (in case the device is used for work). VNC capabilities make it easy for malware to for example access (business) email or file storage.



Picture:"RAT infestation, criminals getting remote access"

An example of a similar MO is the Dridex malware, the actors behind this malware were selling infected devices inside specific organizations to other threat actors who would then install RAT malware on them to perform their attacks.

Looking at the ongoing technical developments and the requests for RAT functionality on underground forums, we can be sure such functionality will play an important role in the future mobile threat landscape.

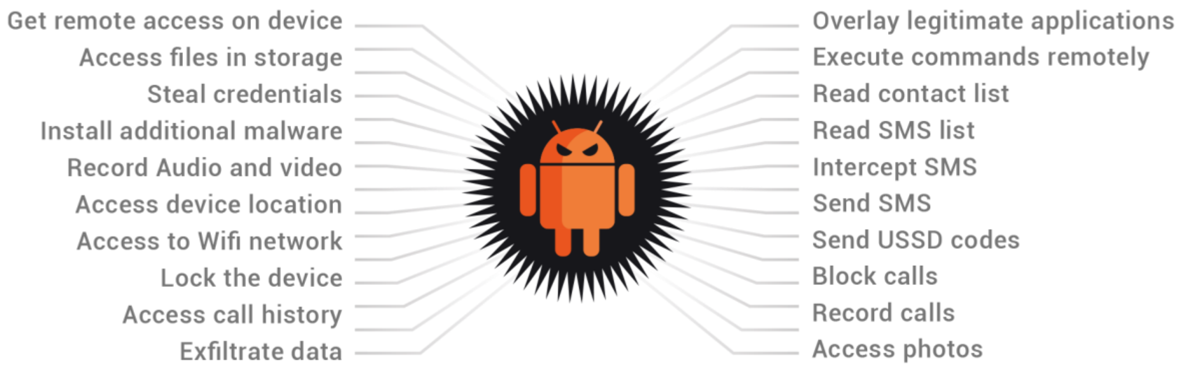
3.10 Increase in APT malware

The open ecosystem of Android makes it easy to gain access to sources of sensitive data by simply using system functionality. Examples of such data sources are the contact and SMS stores, SD card, microphone and camera, all accessible by simply requesting a permission. Because so many legitimate apps request these permissions, most users think nothing of it and simply grant them.

In addition to having many interesting data sources, almost everyone these days has a smartphone and carries it with them wherever they go, making these devices the ideal spying tool. The information gathered using the devices, such as Wi-Fi credentials and email conversations can also be used in further attacks on a corporate environment. That APTs have also realized the value of abusing mobile devices can be seen from the APT malware for Android that has been popping up.

A multi-platform cyber espionage campaign from early 2018 called Dark Caracal mainly made use of Android devices collecting SMS messages, contact details, call logs, installed applications, bookmarks, browser history, Wi-Fi details, account credentials, file and directory listings, audio recordings and pictures. As mentioned earlier, all this data can be accessed if the app has certain, often-asked-for, permissions.

Another spyware variant, called SkyGoFree, enabled audio recording based on GPS position and gained access to the sandbox of the WhatsApp application to gain to encryption keys for the WhatsApp chat database stored on the SD card. In addition, it contained functionality which enabled the actor to control the device remotely. Other examples of recent mobile APT campaigns using the Android platform as attack vector are Chrysaor Pegasus, Lazarus, GnatSpy, FrozenCell, xRAT, JadeRAT, ViperRAT.



Picture: “The many possiblitites of a mAPT”

Mobility itself is a key interest for criminals, there is a high chance that an infected smartphone will be connected to several different networks, meaning potential access to different environments and so a higher chance for criminals to reach their end-goal. Furthermore, smartphones also have their own data connection, transforming them into a perfect remote access node far away from the well monitored corporate network. We can expect a growth in hybrid forms of malware using the infected mobile device an entry point to get into corporate networks and spread computer malware for persistence, reusing the mobile device to exfiltrated the data without being detected.

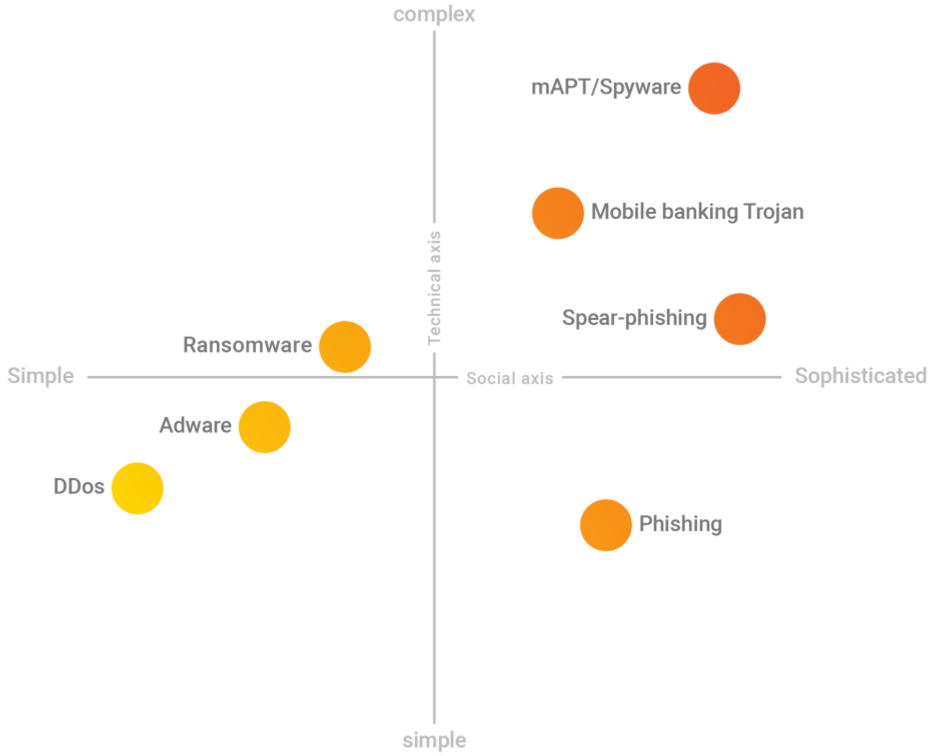
Seeing how easy it is to turn a phone into a spying device and considering the many already ongoing APT campaigns, makes us believe this is a trend that will continue to grow.

4. Conclusion

Even though it seems mobile based attacks have not yet become large enough to be a major problem for financial institutions, they already represent a threat that many don't know enough about. Fraud performed via mobile has yet to reach the level of fraud performed via desktop, but looking at the rate at which mobile malware is growing this will not take long. The development pace of new mobile malware has reached the stage at which desktop malware has been for some time now, with 4 to 6 major new mobile banking campaigns released per year.

With the introduction of the PSD2 directive, Third Party Providers will be positioned in between the banks and the banking customers, meaning: third party access to sensitive information, banks' fraud detection based on the limited information available, possibility of lower security standards and broader attack scope due to multi-tenancy. Financial institutions should draft rulesets for TPP access and enforce security policies via their APIs.

Overlay attacks are an easy way to social-engineer victims, therefore they became a popular tool to gather information. Due to the easiness with which overlay screens can be made criminals didn't limit themselves to banking apps. The list of targeted applications is not the only broadened factor, distribution also has been boosted with the services offered by actors specialized in spreading malware. This happened through several different supports such as but not limited to: Social-networks, cloud-based file-sharing and even the official application stores. Installing applications solely from official sources or known services is not sufficient security criteria, therefore financial institutions should monitor the devices and user behavior to ensure that fraudulent activity can be detected.



Picture: "Matrix of the threats technical complexity VS social complexity "

Financially motivated threat actors are working on Remote Trojan (RAT) capabilities, powering their malware up to next level by providing them direct hands-on the infected devices. At an early stage to bypass 2FA and fraud detection, this has the potential to evolve towards data exfiltration or espionage

Rooting the infected devices has so far be used only to perform banking fraud, but

the gained privileges can be used to do much more than just disable security measures, such as making the malware persistent on the device, or give access to data and functions normally not accessible.

The open ecosystem of Android makes it easy to gain access to sources of sensitive information, in addition, a vast majority of people have a smartphone and carry it around all day long, making these devices the ideal spying tool. Seeing how easy it is to turn a phone into a spying device, financial institutions should consider mobiles as one of the most important attack vectors. Mobile malware represents a risk for both the banking customers and the corporate mobile fleets, therefore threat awareness and detection measures are of utmost importance for the security strategy and business continuity in the coming years.

5. Our recommendations

Below are some of the recommendations we give to both mobile users and corporates handling fleets of mobile devices.

5.1 For mobile users

Automatic updates

Let your device automatically check and install OS and application updates. When new vulnerabilities are discovered the vendors will provide security updates for their software. Your device should have those updates installed as soon as available.

Keep unknown sources disabled

Make sure that the setting “Unknown sources” is not enabled. Allowing applications from unknown sources to be installed on the device opens the door for malware.

Install apps from the official store only

Only install apps from the official store. Although not all applications on the Google Play store are trustworthy, there is a higher chance to get malicious apps from 3rd party application stores.

Verify app permissions

When installing an application, verify that the list of required permissions makes sense with the application’s expected functionality. An application with many irrelevant permissions might be a sign of malicious behavior.

Avoid connecting to unknown or open WiFi

Avoid connecting to unknown or open WiFi networks. Such networks are often insecure (or created with malicious intent) and expose the device and data stored on it to additional risk due to possible insecure apps installed on the device. In case you still want to be able to use such networks, consider using a VPN service to improve security.

Don’t root or jailbreak your device

Manufacturers provide the devices with security restrictions to protect device integrity and security. Rooting or jailbreaking the device damages the security. If certain apps might only work with rooted devices, we strongly recommend to not use such apps as they require abnormal rights on the device. Even if the specific app is not doing anything malicious, other apps might be able to abuse the created security hole.

Enable strong authentication and use passwords

Just having to swipe the screen to unlock the device will not protect your data against attackers who have physical access to the device. Consider using a PIN, password or fingerprint to unlock the device and protect your data.

Automatically lock devices when not in use

Enable the automatic lock to ensure that the mobile device locks automatically when not used. This is a first barrier to prevent a security breach through physical access in case a device is lost or stolen.

Encrypt storage

To reduce chance of data theft, consider encrypting data stored on both built-in storage and removable media storage. Without the proper key/password undesirable access to the data will be difficult.

Install security software

Although antivirus or anti-malware software doesn't solve all problems, such solutions will help with early detection of infections and possibly remove malware before it can start performing troublesome actions.

Regularly backup the device

By regularly making a backup of the device data is safeguarded in case of loss or destruction of the device. A backup tool that automatically saves the data to a safe storage also allows fast recovery.

Enable remote device wiping

In case a device is lost or stolen, the option to remotely wipe the device comes in handy to avoid undesirable access to data stored on the device.

Don't answer or react to messages from unknown senders

Although it might sound very familiar, don't follow links from unknown senders (whether links are sent via SMS, email or chat messages). Be cautious when responding to calls from unknown or abnormal numbers. Such calls might result in charges to your phone bill or be used for social engineering.

Manage GPS settings

The GPS service, or location service, gives apps a way to determine where you are. Many malicious apps collect this information even though they don't require it for the purpose for which they were installed. Don't give apps access to this information unless you are sure they need it for their task, because location information can for example be abused for social engineering and/or espionage purposes.

5.2 For corporates

Remain ahead with Threat Intelligence

Be aware of trends and developments of the mobile threat landscape with the use of Cyber Threat Intelligence. A common mistake is to wait till painful events happen (such as fraud) before investing in relevant Threat Intelligence.

Regular security assessment

Re-assess risk exposure and security level of your mobile on regular basis. Consider writing attack scenarios and implement the related detection & incidents response plans.

Have a mobile device usage policy

Ensure you have a mobile device usage and security policy that defines what the corporate devices should be used for, which resources (public or corporate) can be accessed and what is allowed on the device (apps and data).
The security aspect of the policy should include all the point mentioned in the

Use an MDM tool to manage your fleet

Mobile Device Management is an import tool to have when owning a corporate mobile fleet. The MDM itself isn't a solution to security problems but allows to enforce policies and standards for the devices, push updates and remotely manage security settings.
The MDM should be used to:

- Enforce the mobile usage policy
- Restrict usage of applications and app stores
- Manage authentication to get access to corporate resources
- Manage authentication and access security level
- Remote admin for support and lockout
- Manage permissions and hardware (camera, GPS, Wi-Fi, Bluetooth, etc…)
- Be able to apply all the recommendations from section For mobile users
- Alert security operations if violation occurs

Endpoint protection is key

As stated, MDM is important but security of devices requires an endpoint protection solution, allowing real-time detection of threats or abnormal behavior.

- In the case of a corporate fleet endpoint protection and MDM are a perfect combination to safeguard devices and employees.
- In the case of online services, endpoint and backend monitoring are as important the one as the other. They provide complementary threat detection possibilities.

Educate users

Even when using an exhaustive set of security solutions or policies, the human variable remains the main risk to corporate security. Teaching employees about mobile threats and the related corporate security policies will help users knowing what can or can't be done with the mobile device and therefore lower the risk of malware on those.

6. About ThreatFabric

ThreatFabric experts at have experienced threats and risks for financial institutions for over a decade. That’s how it’s dedicated team has conceived and developed custom detection and analysis services to simplify response to complex cyber-threats.
Focus is key; ThreatFabric’s threat intelligence and threat detection solutions have enabled prevention of attacks and detection of numerous known and unknown threats, empowering financial institutions worldwide to remain ahead of cyber-criminals.

MTI (Mobile Threat Intelligence) is the key to gain visibility on the mobile threat landscape, enabling prevention of attacks and deflection of risk.
CSD (Client Side Detection) is a flexible and powerful detection solution allowing to detect known and unknown threats on devices in real-time.

More information about our solutions on our website at: www.threatfabric.com
For more information, feel free to contact us anytime at: info@threatfabric.com