Quick Heal

Security Simplified

The Evolution of Fake Apps

and the ways they can damage Android Devices

Whitepaper

Authors:
Pramod Shinde and Prachi Sudame

Table of Contents

Introduction

In the past few years, we have seen a surge in FakeApps on the Android Platform. This paper will shed light on several ways used by FakeApps to enter into users' mobile devices.

Fake mobile applications mimic the look and/or functionality of the legitimate mobile applications to widen their reach and trick users to install them.

All malware (and PUA) use some level of deception to get into users' devices. Most of them use fake icons, fake app-names, fake developer-names or show fake functionality (which they never provide). There are FakeApps for almost every popular app, including Google Play, WhatsApp, Flash Player and many Bank-Apps. People tend to use these apps more often because of their uncanny resemblance or exaggerated functionality offerings free of cost becoming a target of malware authors regularly. Some of them make their way to Google Play (or other official markets) as well.

The number of Android malware have increased drastically in recent years. To cope-up with this, all security products use some automated procedures or machine learning to identify and categorize these malicious applications. Sometimes users may fail to notice a FakeApp when an Anti-Virus (AV) detects it with some other name and category. So, to make it simple, Quick Heal explicitly detects such apps under the category of FakeApps.

Background

Why FakeApps are created

Before we examine FakeApps and various tricks they use, let us take a look into the motivation and economy behind the FakeApps. Earning some easy money has been the prime motive behind the development of FakeApps. Mobile advertisements are a multi-billion[1] dollar industry. Some of us might have heard about how popular games and apps earn per-month or per-year[2]. With billions of dollars moving around mobile advertisements, many app developers try to use the popularity of famous apps by creating similar fake applications to earn some quick cash. Most of these FakeApps are poorly developed —these apps do not have proper privacy-policy or 'terms and conditions' (and they do not follow any, even if they have poorly assembled one).

Google has created a good set of policies [3] for app developers, but FakeApps do not adhere to these policies even if they publish their apps on Google Play Store. In recent years, many frameworks have been developed to make mobile app development easier. Some of these frameworks need little knowledge of programming and platform. Such apps developed with frameworks make their analysis and screening a little difficult for App-Stores and AVs. But developing a FakeApp and integrating advertising kit into it is a lot easier with these frameworks. Many FakeApps show ads aggressively to generate more revenue in less time. Other malware categories like Ransomware, Trojan-Banker, Spyware, Backdoor etc. are more dangerous and bigger threats than FakeApps. They generally have complex architecture, multiple malicious modules, use multi-layered evasive techniques and have advance functionalities.

Data and credential stealing is another prominent reason why FakeApps are created. FakeApps that imitate bank-apps or other popular apps are developed to steal the user's data and credentials.

[1] https://www.appannie.com/en/insights/market-data/2017-predictions-app-economy/

https://www.businessinsider.com/mobile-video-is-the-growth-area-2014-10

[2] https://www.businessinsider.com/crazy-angry-birds-earning-1-million-a-month-from-advertising-2010-12

https://blog.getsocial.im/mobile-app-growth-study-why-the-angry-birds-are-so-popular

[3] https://developer.android.com/distribute/best-practices/develop/understand-play-policies

https://play.google.com/about/developer-content-policy/#!?modal_active=none

How FakeApps are distributed

Google Play has good screening and filtering when it comes to bad apps, yet many FakeApps make it to its store. According to Google, more than 700,000 apps that violated the Google Play policies were taken down in 2017[4] —Google also took down 100,000 bad developers in 2017. However, taking FakeApps down from Google play does not mean bad app developers would give up on publishing. Most of these apps will be published on Third-Party app stores. Many Third-Party app stores do not have very strong screening and filtering mechanisms. There are many tools available to protect and modify applications' internal structure (viz. obfuscators, protectors and packers). Most of the malware use these to bypass the security of app-stores and AVs. So even after Google taking these apps down from play stores, the versions available on third-party markets may survive from Google Play protect whereas many others will keep trying different methods to bypass Google's security.

There are many other ways for app developers to widen their reach — using Social engineering, SMS, Mails, fake WhatsApp messages are a few more ways preferred by malicious developers. Further, sharing these apps by Bluetooth, Wi-Fi and File-Sharing apps spread FakeApps even more.

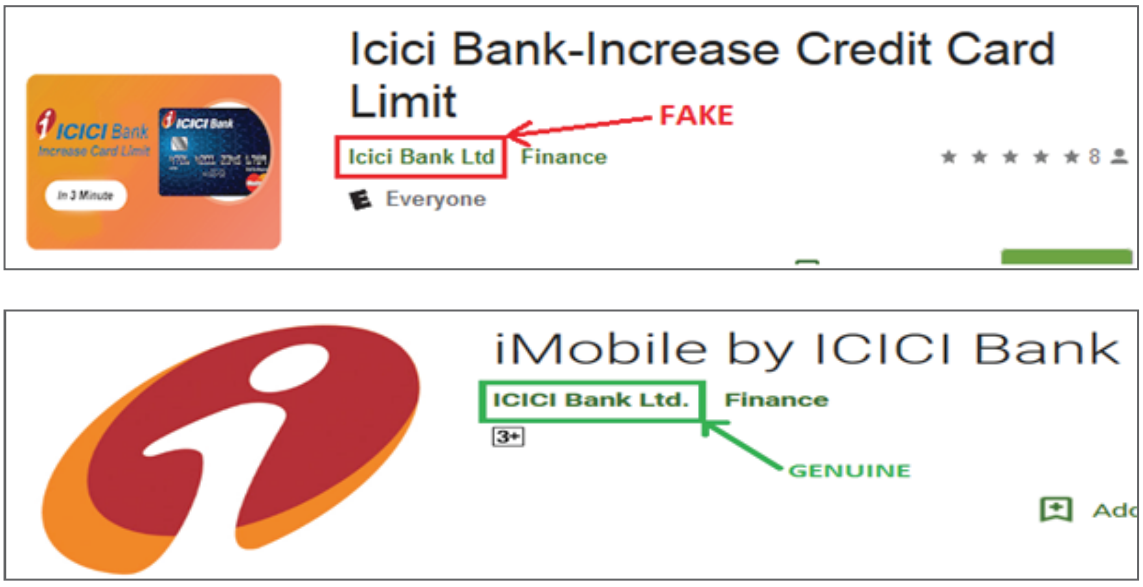
[4] https://android-developers.googleblog.com/2018/01/how-we-fought-bad-apps-and-malicious.html

Tricks used by FakeApps

FakeApps use many tricks to deceive users —some of the tricks used by them over the past years are shown below with examples and references. While FakeApp developers will always keep inventing new tricks to deceive users, security products will always be there to catch them. Most FakeApps keep using a combination of below tricks. You will find these tricks neat and elegant enough to deceive anyone. Beware of these tricks and always make sure you are downloading genuine apps only.

1] Disguising the Developer's Name

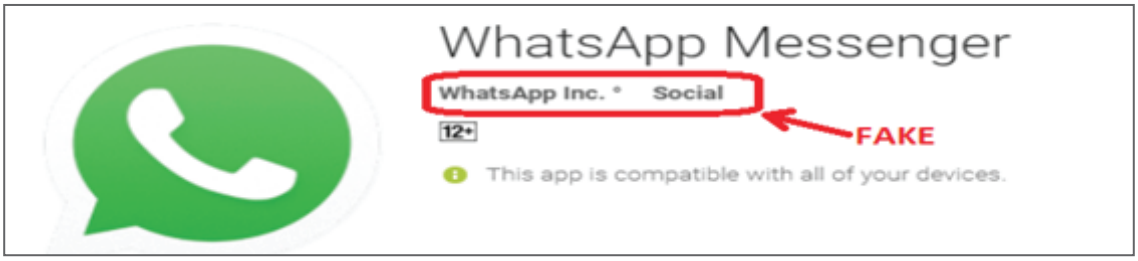
Mentioned below is a fake banking app which was present on Google Play. It uses the same developer name but with different cases. The fake one was designed to collect bank credentials along with credit card details.

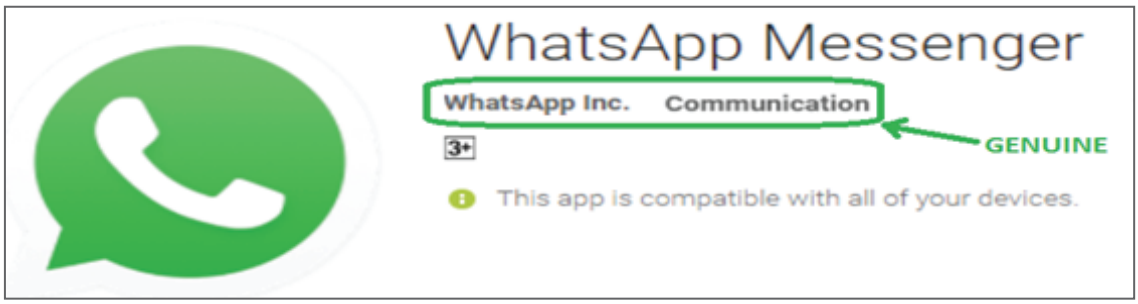


Ref.: https://www.welivesecurity.com/2018/07/26/fake-banking-apps-google-play-leak-stolen-credit-card-data/

2] Genuine Icon but Not the App:

Many FakeApps use icons of genuine apps and in almost all cases they succeed to confuse unaware users. Below is a fake WhatsApp App which was present on Google Play. This one used the icon and app name of genuine WhatsApp and developer name very similar to the genuine one. It seems app developer intended to earn some money by showing ads.





Ref.: https://blogs.quickheal.com/fake-whatsapp-apps-google-play-analysis-quick-heal-security-labs/

3] Some FakeApps Provide No Functionality:

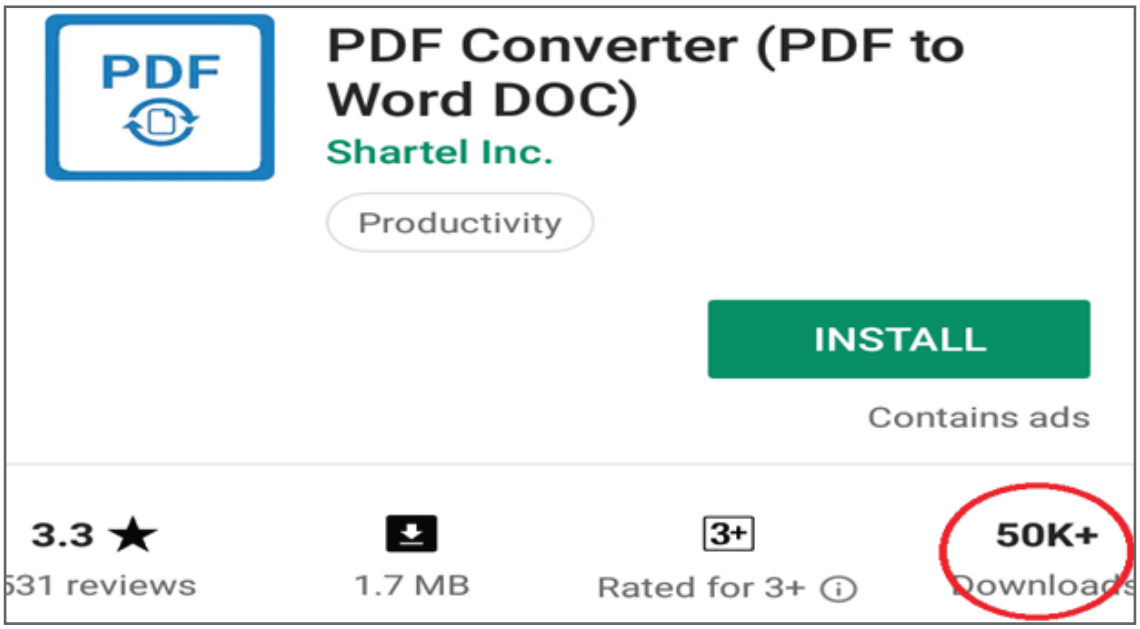
Nowaday's mobiles play an important role in the day to day life and every user wants his/her phone safe from an increasing number of cyber-attacks. For securing devices users trust on anti-virus protection and malware authors take undue advantage of this technique to spread FakeApps among users. Quick Heal Security Labs found fake antivirus apps on Google play. What's more alarming is that one of these fake AV Apps that have been downloaded 100000+ times already. These Apps appear to be genuine Anti-virus/virus-removal Apps with names like Virus Cleaner, Antivirus security, etc., but do not have such functionality related to malware scanning or identifying any other security issues. These apps only show a fake virus detection alert to the user and eventually show lots of advertisements.

While, anything that comes FREE might come across as a temptation for users to buy, remember that FREE can also be FAKE! So, beware that you don't fall prey to the free security software available on Play Store. Go only for trusted brands like Quick Heal when it comes to guaranteed security of your device.

Ref- https://blogs.quickheal.com/free-mobile-anti-virus-using-can-fake/

Sometimes users download an app for some functionality they are looking for. Some FakeApps do not imitate any popular app but they claim to provide some functionality that users are looking for. So unsuspecting users may end up installing such FakeApps. Below is an example of one such case —these applications appear to be genuine as a PDF reader, PDF Downloader,

PDF Scanner etc. but don't have such functionality. The basic intention of these applications is to increase the download count, rating and earn some revenue through ads.



Ref.: https://blogs.quickheal.com/fakeapp-discovered-google-play-store-increases-download-count-rating-applications/

https://blogs.quickheal.com/28-fake-apps-removed-google-play-store-post-quick-heal-security-lab-reports/

4] FakeApps follow Social Trends:

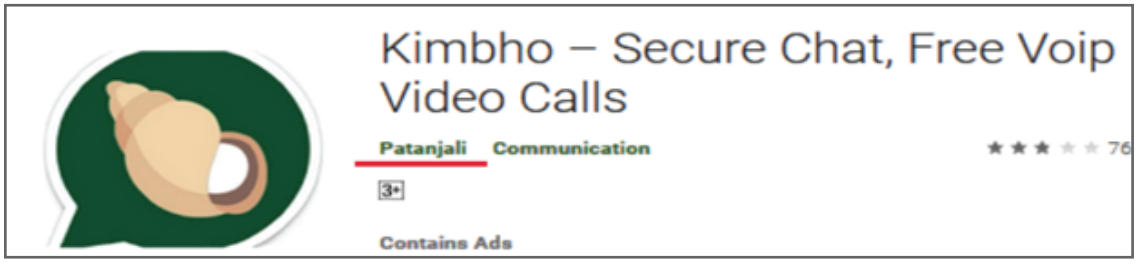
Whether it is a FakeApp or some other malware category app, author will try to increase its user base. So, whenever something is trending, there are very high chances of FakeApps to ride on the wave of the trend. All the FakeApps mentioned below were designed to show ads aggressively.

- When cryptocurrency was gaining a lot of attention and there was a news about Jio's move to launch a cryptocurrency viz. JioCoin, many Fakeapps were published.

• When the Government of India made it mandatory for all mobile users to link their Aadhaar to their mobile number, many people were searching for the apps which will ease the task. FakeApp developers saw this as an opportunity and did not miss.

Link Aadhar Card to Mobile Number & SIM Online | **Link Aadhaar Card With Mobile Number Online** | **Link Aadhar Card with Mobile Number**

• Patanjali launched Kimbho app on Google Play Store but took it down from after some time. A fake Kimbho app was published on Google Play which had nothing to do with the original app.



Ref.: https://blogs.quickheal.com/beware-fake-apps-claim-help-invest-jiocoin/

https://blogs.quickheal.com/beware-fake-apps-claim-link-mobile-number-aadhaar/

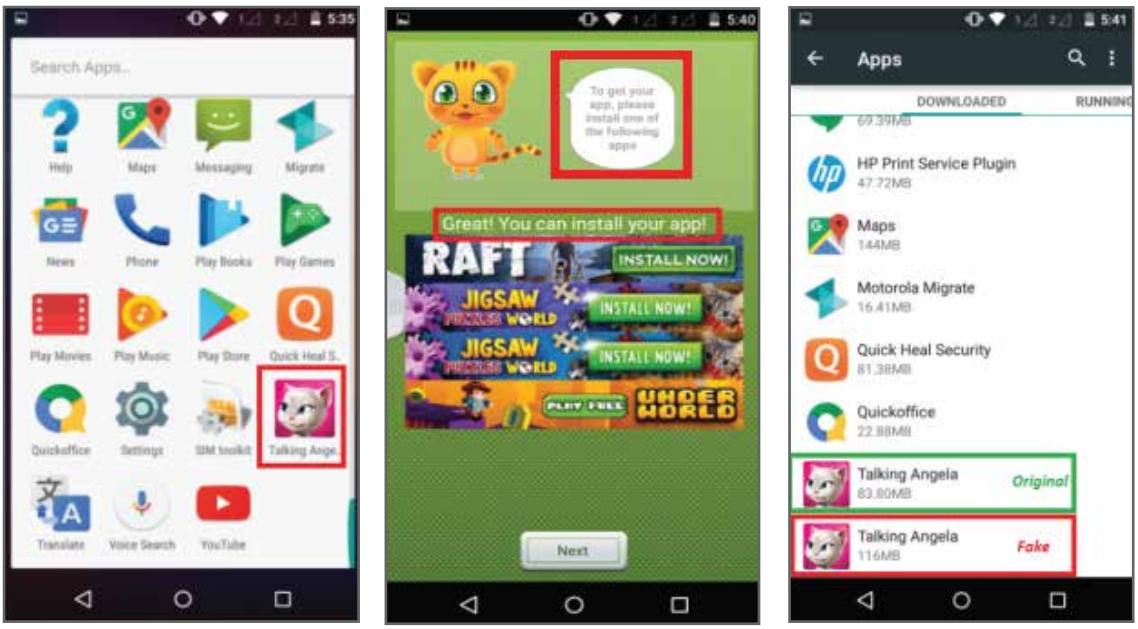
https://blogs.quickheal.com/quick-heal-detects-malware-misusing-fame-patanjalis-kimbho-app/

5] Offer a Free App for free after coating it in a FakeApp

There are many popular apps available on Google Play that are extremely popular with millions of downloads. Riding on this wave, FakeApp developers create an app and hide the orginal app inside it. Users fall for this trick due to the outstanding crafting of FakeApp developers in designing a replica of the original app. When a user installs this FakeApp, it shows many ads, asks users to install some additional apps to promote them and increase their download count. The worst part is after all this, it shows a prompt that redirects to a page asking the user to download the intended app.

We saw this phenomenon for Talking Angela's FakeApp (the app which is free and famous for entertainment, from the same app developer of Talking Tom) which pretended as a free app but in reality, carrying the original application within it and asking users to download some promoted applications, prompting to install the original 'Talking Angela application', afterwards. Malware authors take undue advantage of a novice user with the main intention being to increase the download count of the sponsored app.

Below screenshot shows the case:

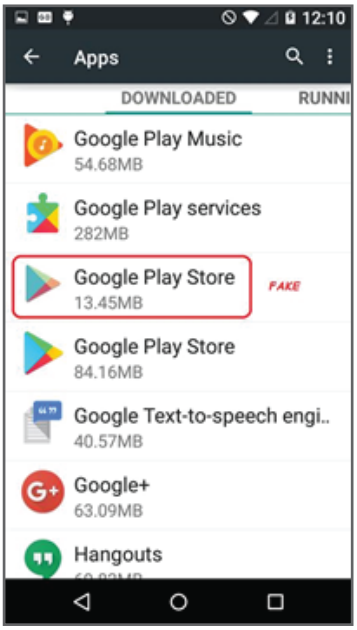


6] Bundled Bogus Applications:

Similar to the above method, malware authors sometimes bundle FakeApps with their regular apps. Malware authors use this trick to remain hidden from users. In the case shown below, gaming applications were published on Google Play that all carried fake Google Play applications inside them. After running the game, it showed an installation prompt for fake Google Play app. If users fell prey to this trap and installed the fake 'Google Play Store' app, then their device got infected by an Adware. On launching, it displayed some stored wallpaper and after that, it hid its icon.

The FakeApp will keep showing ads and users will not be able to identify easily which app is showing the advertisements. Also, if users decide to uninstall it, they will have difficulties in identifying the FakeApp.

REF-
https://blogs.quickheal.com/alert-27-apps-found-google-play-store-prompt-install-fake-google-play-store/



How to stay safe

- ✓ Malicious developers spoof original Application names and Developer names. So, make sure you are downloading genuine apps only. Often app descriptions contain typos and grammatical mistakes. Check the developer's website if a link is available on the app's webpage. Avoid using it, if anything looks strange or odd.
- ✓ When you search for an app, look at the app icon before installation — if there are many apps with similar icons then there is a chance of malware, because malware authors have used icons similar to the original app.
- ✓ The 'Editor's Choice' badge (in Google Play) is usually a good sign that the app is safe.
- ✓ Reviews and ratings can be fake but still reading user reviews of the app and the experience of existing users can be helpful. Pay attention to reviews with low ratings.
- ✓ Check download count of the app — popular apps have very high download counts. But do note that some FakeApps have been downloaded thousands or even millions of times before they were discovered.
- ✓ Install apps only from official stores such as Google Play.
- ✓ Avoid downloading apps from third-party app stores or links provided in SMSs, emails or WhatsApp messages. Also, avoid installing apps that are downloaded after clicking on an advertisement.
- ✓ Always keep 'Unknown Sources' disabled. Enabling this option allows the installation of apps from unknown sources.
- ✓ Read all app permissions carefully. A bit of common sense is what can help you tell the right from the wrong. The rule of thumb to remember here is, the permissions asked by an app must comply with its functions/features. For instance, if Skype app requires your permission to access SMS, call logs, media files, etc., then that's alright because these are required for obvious reasons. On the other hand, if a gaming app or a flashlight app requires similar permissions, stay away – that's a bad app!
- ✓ Install a reliable mobile security app that can detect and block fake and malicious apps.

About Quick Heal Mobile Security

Quick Heal Mobile Security is the mobile antivirus from Quick Heal Technologies Ltd. offering best-in-class cybersecurity solutions to smartphones. Our product portfolio includes Scanning of your Android phone for threats like viruses, fake or malicious apps services, Privacy Adviser helps you to identify such apps and Parental Control, Protects your sensitive information while you are shopping or banking on mobile payment apps, If anyone enters a wrong password 2 times consecutively (to unlock your phone), this feature will click a picture of the person using its front and rear camera,

It scans apps before you download them from Google Play and scans apps in the background to ensure they are safe

https://play.google.com/store/apps/details?id=com.quickheal.platform&hl=en

About Quick Heal Security Labs

A leading source of threat research, threat intelligence and cybersecurity, Quick Heal Security Labs analyses data fetched from millions of Quick Heal products across the globe to deliver timely and improved protection to its users.

Conclusion

FakeApps (Fake Applications) are all about the deception to trick users into installing them. In this paper, we saw commonly used tricks by FakeApps with many examples of actual cases that occurred in the past. For malware authors, they are easy to build and get some quick cash using the popularity of other apps. The problem of FakeApps is not going to end soon, in fact, it is going to get worse. Knowing their tricks and having awareness about them will always help you to identify FakeApps.