Android - Security Metrics

Alexandru Babeanu 4881133
Antoine d'Estalenx 5149371
Irène Förstel 5149398
Arjen Brussen 4974484

September 23, 2019

1 Introduction

Android is an operating system developed by Google to be used for mobile devices. First released in 2008, it has become the dominant operating system for such devices, with a market share of 84% (Fig. 1). Its large user-base makes this operating system a very appealing target for threat agents, since the more victims are impacted by an incident, the more revenue is generated for the attacker. Figure 2 shows the most common types of malware that target mobile devices. The most common malicious activities that target mobile devices include:

- The theft of personal information thorough spyware applications. This data may involve address details, location data, bank account information, etc.
- Performing unauthorized calls or messaging to increase the revenue of specific services at the expense of the victim.
- Presenting unwanted advertisement to users via adware.
- The theft of computational resources by cryptocurrency miners.

The programs that run on these devices, called "applications", or "apps" for short, offer various attack vectors for threat agents, such as exploiting vulnerabilities found in existing legitimate applications, or intentionally publishing applications with vulnerabilities or malicious behaviour. These programs are offered by a large number of vendors and distributed through public online marketplaces called "app stores". Most Android applications are distributed through Google Play (Fig. 3), an app store run by Google, but many other app stores exist. Each store has its own set of rules and requirements regarding the software that can be published on them, with varying attitudes towards security and privacy, and with different moderation capabilities.

This brings into question how trustworthy some of these app stores are, and introduces the need for a method of evaluating how safe the products published

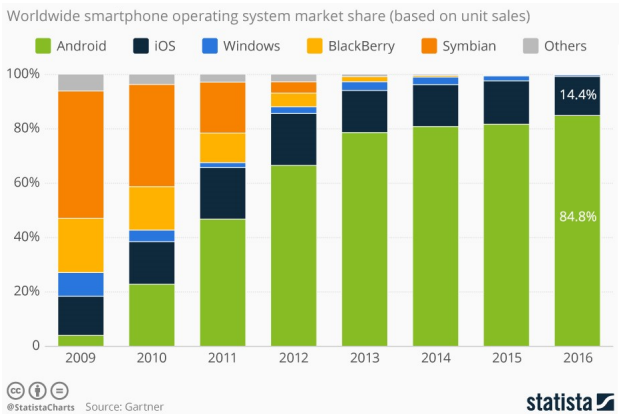


Figure 1: Worldwide smartphone operating system market share (based on unit sales), source: [5]

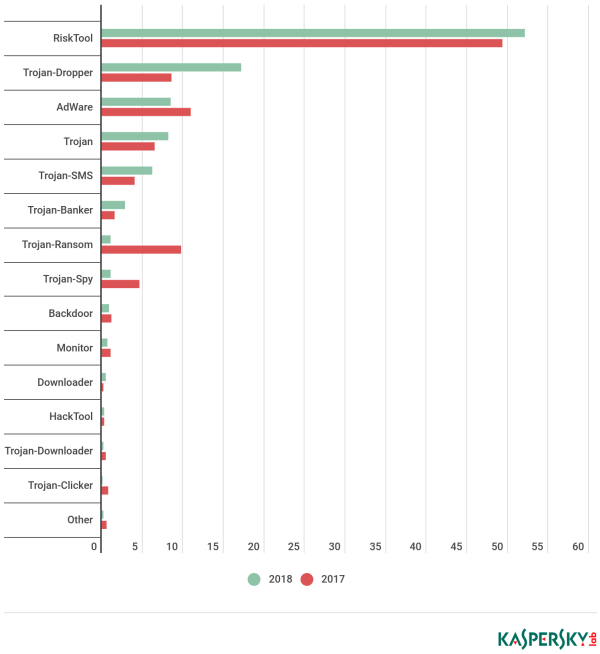


Figure 2: Distribution of new mobile threats by type (2017 and 2018), source: [7]

on these stores are. In paper [4], the authors perform a security comparison between various app stores, considering the controls they have in place and how efficient they are at combating malware. In some of the stores considered for

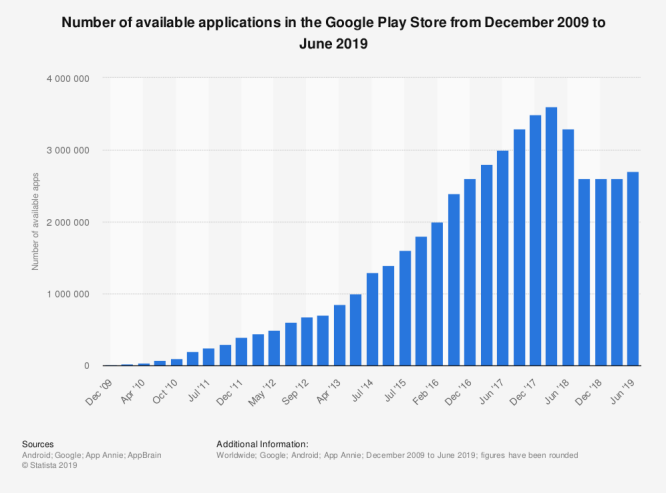


Figure 3: Number of available applications in the Google Play store from December 2009 to June 2019, source: [6]

this study, the percentage of apps that were detected to contain or be malware was over 50%. This showcases the importance of evaluating these markets for the safety of their users.

2 What security issue does the data speak to?

The data, acquired from [1], can be described as a list of applications with some information about them: the category an application belongs to, the amount of downloads, and the results of malware-analyses conducted through VirusTotal.com. The latter property can be used to differentiate between legitimate and malicious applications within each store. Therefore, the security issue at hand is related to the amount of malware made available to Android-phone users by various application stores. The data at hand is a compilation of datasets corresponding to multiple online application stores:

- eoemarket.com
- freewarelovers.com
- gp09, which is now apkmonk.com
- liqucn.com
- mumayi.com
- playdrone, which analyses applications from the Google Play store

The actors involved in the security issue are the application publishers, some of which are threat actors, the app-stores themselves, and the Android-phone users, who represent the primary victims of mobile malware and the primary targets of malware publishers.

For our study, we choose to focus on the perspective of the app-stores. The threat consists of malicious software being published on their platform. In this case, the assets that need protection are their clients, or more specifically, the safety, privacy, comfort, and trust of the people who generate revenue for the store by downloading applications. A very important asset that is under threat is the reputation of the app-store. If a store gets the reputation of having lax security controls or that a high percentage of their applications contain malware then users will be deterred from buying their products, and the revenues of the business will suffer. An application store with a relatively high amount of malware will see a sharp decline in popularity, and once the trust of their clients is lost, it is almost impossible to gain back. Furthermore, the reputation of lax security may cause a feedback-loop, since this information will attract more malware publishers to the platform, which will further aggravate the issue.

3 What would be the ideal metrics for security decision makers ?

In terms of control-based metrics, knowledge about the internal security controls, malware detection tools, and validation processes used by each store would offer insight into the amount of effort and level of sophistication they invest into security. However, a high amount of effort does not necessarily translate into good results. In order to measure the actual security of a system, incident-based metrics are required. In our case, the incidents are represented by malicious applications that bypass the security controls of the app-stores and become published. Some ideal metrics that would help measure the security of the Android app-stores consist of measuring the prevalence of malware in each store, while normalizing for factors that are unrelated to security, such as the size of each store, their popularity, their openness, or the popularity of each application category.

As a start, having the total number of daily downloaded applications and the total amount of malware downloaded per day could allow us to have a representation in time of the number of infections, and give us an overview of the quality of the controls in the stores (i.e. how much malware reaches the end-consumer), even if it also depends on the behaviour of the attacker.

Another interesting metric would be the ratio of malware that is rejected by the security controls of each store. This way, the analysis takes into account the popularity of the store with threat agents. For example, when measuring only the published malware, a store with no security controls that never gets attacked may appear more secure than one that is attacked often, but has a good level of security which prevents most of the incidents.

We could also measure the ratio of malware per application type (whether it's a game, a fitness app, a messaging app, etc.) to understand which types are targeted and why (i.e. because they have better controls or because one type of application leaks more information than others). We have done this in figure 6, but this analysis is only done on a subset of all applications, which may not reflect the real distribution on the application store.

To assess the correct amount of malware applications, an ideal antivirus would also be needed. In the given dataset, some malware detection tools consider an application as malware and some do not, which creates uncertainty when measuring the amount of malware.

4 What are the metrics that exist in practice ?

In paper [4], the authors perform a comparison between various app-stores that operate in China. They also compare them with Google Play in order to relate their findings to the characteristics of the global leader of the app-store market. When performing this comparison, the researchers consider various metrics.

Some of these metrics relate to the security controls the app-stores have in place to limit malicious behaviour, for example:

- **Openness** relates to who is allowed to publish applications. Some stores allow vendors to publish their apps for free, while some demand a fee. Obviously, the ones which allow free publishing are more appealing to attackers. Additionally, some stores only allow registered companies to publish apps, only distribute apps from certain categories (e.g. games, tools, etc.), or only allow apps that are compatible with certain devices (e.g. OPPO, Xiaomi).
- **Copyright checks** are performed by most stores to reduce the amount of fake or cloned apps.
- **Publishing incentives** relate to what a store offers publishers to motivate them to publish their apps on said tore. This usually involves exposure through in-store promotion and recommendations.
- **Auditing process** relates to the inspection and vetting processes performed by each store to limit the amount of malicious applications. Most of these processes are automated, but some stores (e.g. Google Play, Tencent, Xiaomi) claim to also use human inspection.
- **App quality ratings** relate to the internal scoring performed by each store on their apps, based on downloads, user comments, developer level and other metrics.
- **Transparency** relates to whether the app-stores inform their clients about the privacy policies, advertisement practices, and in-app purchases of the published apps.

Other metrics relate to the security incidents that app-stores face, namely the percentage of malicious behaviour that bypasses their controls. This category includes:

- The percentage of fake or cloned apps out of the total amount of apps published in each store.
- The percentage of applications that contain malware.
- The percentage of applications that request more privileges than required by their functionality.
- The persistence of malicious applications over time. To measure this, the authors performed a second analysis 8 months after the first, and discovered that Google Play has removed 84% of the malware detected by the first analysis, while the removal rates of other stores range from 0.01% to 35%.

5 A definition of the metrics that can be designed from the dataset

In our analysis, we consider an application to be malicious if it has been detected to contain malware by at least one of the antivirus programs used by VirusTotal to analyse it. In other words, we assume that there are no false positives (or false negatives for that matter) in the results of the virus scans.

For the given data we have defined the following three metrics that offer insight into the security levels of the application markets:

- The ratio of malware within each app-store is defined as the number of applications identified as malicious divided by the total amount of applications within a store. This metric represents how likely it is for a customer to download malware from each store, which translates into how (un)safe the store is for its clients. This metric is also used in practice when assessing the security level of an app-store.
- The ratio of malware within each application category is defined as the number of malware instances from each category divided by the total amount of applications within that category. This metric will offer insight into which application categories are prioritized by malicious publishers. We expect these priorities to be similar to the popularity of each category, for example, we expect game applications to have a higher malware ratio than most categories. Figure 4 shows a ranking of the application categories on *Eoemarket* based on the amount of downloads, which can also be interpreted as a ranking based on the popularity of each category.
- The ratio of malware for application downloads is defined as the total amount of downloads of malicious applications divided by the total amount

of downloads within each app-store. Unlike the first metric, this also accounts for the impact of each incident, since a malicious application will technically become a security issue only if it reaches the customers of the store.

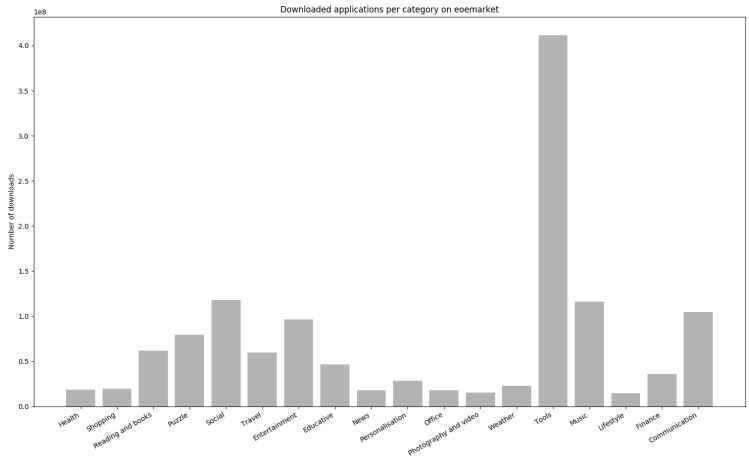


Figure 4: Downloaded applications per category on eoemarket.com

6 An evaluation of the defined metrics

6.1 Malware proportion per market

In figure 5 we can see that the application market has different ratios of infected applications for the stores. For example, in the Google Play Store, one out of ten (10%) applications is or contains malware (note that the distribution is not uniform over all categories). In other stores, for example Eoemarket, the ratio of malicious applications goes as high as 62%.

This metric can be used to asses how likely it is for a user to download malware when using each application store, and therefore how secure each store is. From this analysis, it seems that Google Play, Freewarelovers, and gp09 have better security than Eoemarket, Liqcn, or Mumayi. In fact, Google has a lot of security checks. These controls are not only in the store, but also on the side of the user: when the user downloads the application, it is checked again before it is being installed [8].

Calculating the ratio of malware in a store helps remove the size factor of the app-store. However, there are a few other parameters not taken into account, such as the popularity of each store, store/application age or the types of applications offered. For example, one store is entirely dedicated to games,

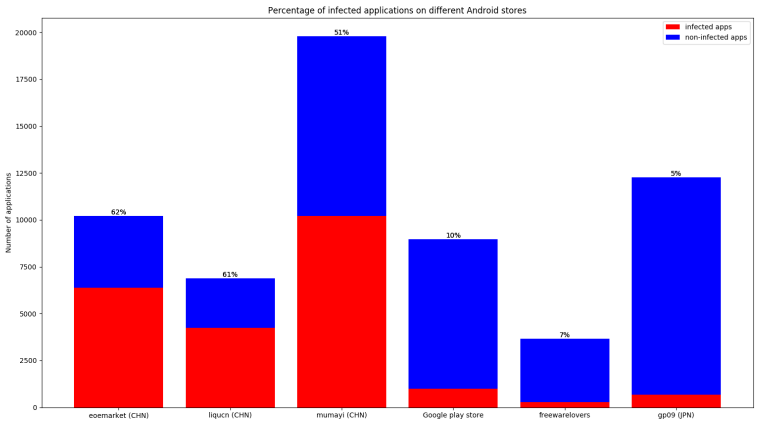
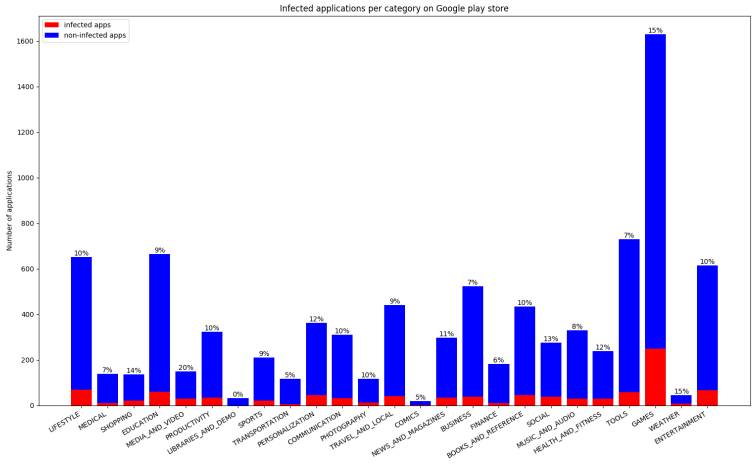


Figure 5: Amount and ratio of infected applications for several application stores Note that we assume the distributions of infected/non-infected applications of this dataset to be representative of the *entire* app-stores, even though the dataset only contains a subset of the applications in each store.

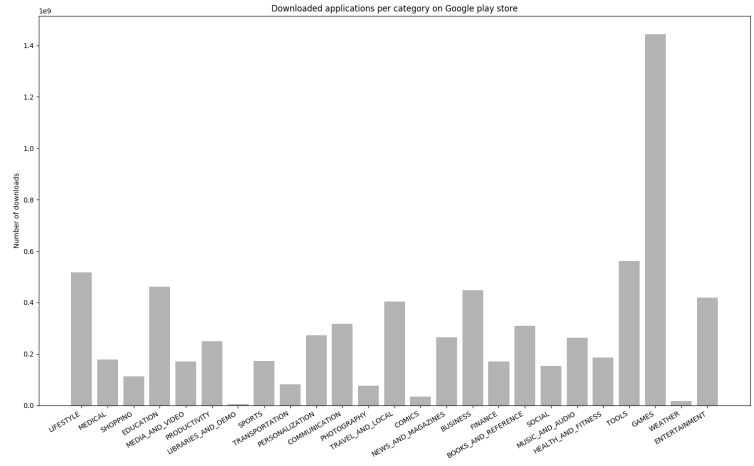
while others offer a large variety of applications. This can influence our analysis because attackers may favor some application categories over others.

6.2 Analysis of the malware per category

In figure 6, we clearly see that the proportion of infected applications depends on the category of the app. Judging by the prevalence of malware in each category, we can see that the categories most popular with attacker are media and video (20%), games (15%), weather (15%), shopping (14%), and social (13%). This analysis can be used to account for application types when measuring security. For example, if an app-store offers mainly games than it is expected for it to have a higher malware ratio than a store which offers a broad selection of application types. Therefore, when comparing the security levels of multiple app-stores, the malware ratio should also be measured within each application category. One obstacle that makes this task difficult though, is that different app-stores use different methods of categorizing their applications, so a translation needs to be performed to a standard categorization. This metric indicates that the application stores could develop controls related to a specific category in addition to the generic controls they already have. But the proportion of infected applications in one category is not threatening if the applications are never downloaded or downloaded by very few users. For example, as seen on figure 6b the media category is not very popular, while the games category is very popular in terms of downloads. So the security risk is higher in this



(a) Infected applications per category on Google Play store

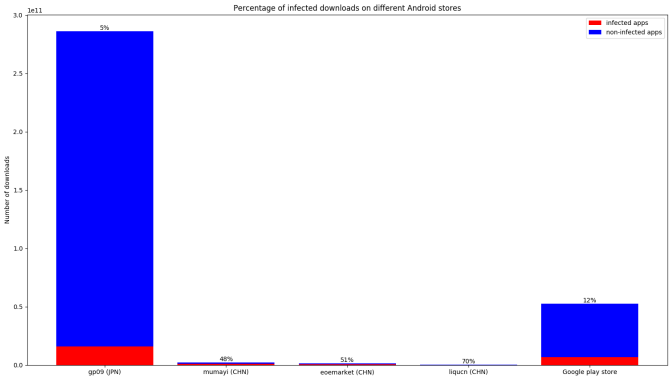


(b) Downloaded applications per category on Google Play store

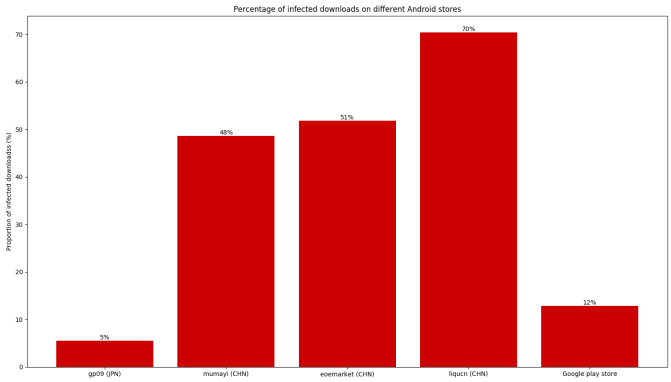
Figure 6: Analysis of Google play store categories

category. A possible control could be to focus on a better analysis of typical malwares in games to lower the malware proportion in this category, which is the most popular on Google Play.

6.3 Malware downloads per market



(a) Downloads of infected and non-infected applications in the markets



(b) Percentage of downloads of infected applications in the markets

Figure 7: Metrics about applications downloads

In figure 7, stores are compared on the ratio of infected application downloads. Even if an infected application is uploaded on an application store, the store can protect its users by selecting the order in which the applications are displayed (it is well known that users often look for the first results of a search query). Since applications are often sorted by popularity, an unpopular infected

application would have fewer downloads, and therefore poses a lower threat than a popular one. This metric could reflect the popularity of infected applications on these markets.

Our analysis shows that the percentage of malware downloads is close to 50% in Eoemarket and Mumayi, and 70% in Liqucn. In these markets, which have higher proportions of infected applications, malicious applications are popular because they have a high number of downloads. On the other side of the spectrum, only 12% of application downloads from Google Play are malware, and only 5% for gp09. This means that malicious applications are not very popular on these platforms, which lowers the impact of security incidents.

However, this metric has limitations because the applications are not the same in each dataset. While the datasets for Mumayi, Liqucn, Eoemarket and Google Play contain few popular apps (in the Mumayi dataset, only 8 applications have been downloaded more than 100 000 times), the gp09 dataset contains very popular applications like Facebook or Yahoo News - these applications are not malicious and count for a lot of safe downloads, i.e. more than one million downloads for Facebook. These applications also exist on some other stores (Facebook is also on the Google Play store), but are not in the corresponding datasets. Therefore, the datasets used when performing the above measurements do not properly represent their stores, because they do not include all applications or applications with equal popularity.

7 Conclusion

In conclusion, we designed two metrics that can be used to measure the security levels of the app-stores in our data set. Both the malware ratio within published apps and the malware ratio within downloads imply higher levels of security for Google Play, gp09, and Freewarelovers, while the other stores seem to be exposing their users to a high amount of malicious software. We have also measured the popularity of each application category for both users and attackers, which can influence the results of our metrics for application stores with a more focused range of application types. In relation to the metrics used in practice, our data allows us to calculate the ratio of malware published on each store, but the absence of publishing dates limits our analysis. For example, we cannot differentiate between popular applications and old applications, since both have a high amount of downloads. Additionally, we are unable to asses the ability of a store to discover and remove malware after publication.

References

[1] Yosuke Kikuchi, Hiroshi Mori, Hiroki Nakano, Katsunari Yoshioka, Tsutomu Matsumoto and Michel Van Eeten: "Evaluating malware mitigation by android market operators". In 9th Workshop on Cyber Security Experimentation and Test (CSET 16).

[2] Paul E. Black, Karen Scarfone and Murugiah Souppaya: "Cyber Security Metrics and Measures". In Wiley Handbook of Science and Technology for Homeland Security, 2008.

[3] D. R. Thomas, A.R.Beresford, A. Rice: "Security Metrics for the Android Ecosystem". Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, p. 87-98, 2015.

[4] Haoyu Wang, Zhe Liu, Jingyue Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, Juan Tapiador, Jingcun Cao, Guoai Xu: "Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets" in Proc. IEEE 38th Annu. Comput. Softw. Appl. Conf., 2014, pp. 509–518.

[5] escalesolutions.com/blog/market-share-android-ios-other-operating-systems/

[6] statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

[7] securelist.com/mobile-malware-evolution-2018/89689/

[8] android.com/play-protect/