Android - Security Investments and Management
- Draft -

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

September 30, 2019

1 Introduction

In this report, we want to define the different actors in the problem of the infected malware applications. We will also define the possible strategies for each actor.

2 Problem owner

In our previous report, we defined metrics to measure the threat of malwares on Android application stores. Malware are developed by malicious developers, who embed it in an application and subsequently upload it on the app stores. The users, who potentially download these applications, are the victims of malware.

Application stores depend on their users for their business. Some, like the Google Play Store, take a percentage of every transaction that happen on the store (like buying an application). But since a majority of the applications on these stores are free, these stores mostly earn money by advertising applications. For example, developers can pay to have their applications appear first in the user searches on to be highlighted on the front page.

As the Google Play store is the official application store for Android and because the data is more detailed than the data about some other application stores, we will mostly focus on this store.

3 Security Performance

In the previous paper, we defined multiple metrics to measure the security performance of the different application stores. In figure 1, we looked at the proportion of downloaded infected applications to measure the risk of downloading a malware depending on the application store used.

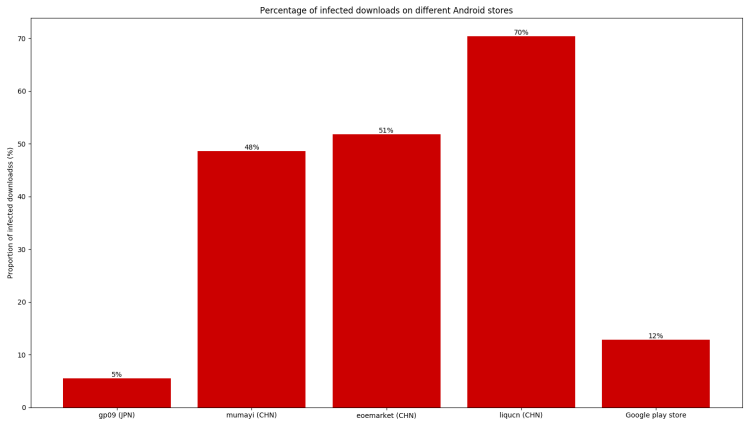

Figure 1: Proportions of malwares in application downloads

In Figure 2, one can see that the markets which had the higher proportion of malwares in downloads in figure 1 are also the ones which have the higher proportion of malwares in the available applications. These measures are of course linked together (the more malwares there are, the higher the chance users download malwares).

These metrics reveal that the stores do not have the same controls quality, both in mitigating the risk and preventing it.

4 Risk strategies

The metrics presented in Figures 1 and 2 reveal that the stores do not have the same risk strategies against malware. Most choose risk acceptance as their strategy (i.e. they ignore the issue at hand). The Google Play store chooses to reduce the risk by analysing each uploaded or updated application for potential malware. They also promote very popular, useful and safe applications by pushing them to the top of search results ('Editor's Choice'). These measures do not reduce the security issue completely, but it is the most optimal solution out of ignoring or avoiding the issue (e.g. by removing categories which have a high proportion of malware), or even transferring the risk by being insured for potential lawsuits.

As shown in Figure 3, the proportions of malware are not equally distributed in the store categories. This metric can also help to refine the controls to analyse the applications that are most likely to be malwares.

The Google Play Store can mitigate the risk of having malware applications in the store by :

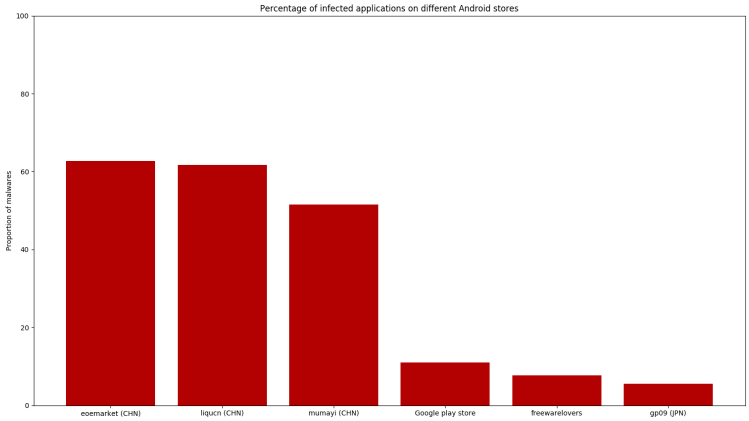

Figure 2: Proportions of malwares in application stores

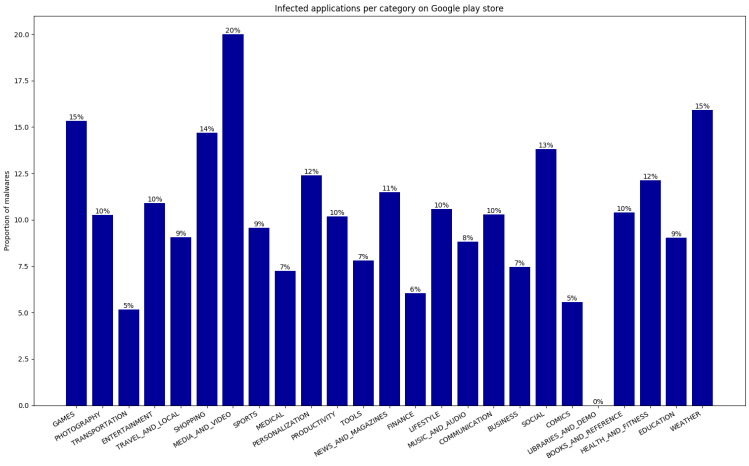

Figure 3: Proportion of infected applications per category on Google Play store

- Having stronger security checks before the application can be uploaded on the Play Store (especially in the most targeted categories, such as *Media and Video* or *Games*).
- Reducing the impact of an uploaded malware application by not promoting it and removing it shortly after its upload.

5 Actors

Malware developers are the main actors aside from the application store itself, because they are the threat source.

Application markets are actors. They have assets such as their reputation, user base and services (application storage) to protect. Application developers pay them to get on top of the application lists. Therefore, they have to attract a lot of users which is not possible if they are known to be full of malwares.

Users are also actors of this security issue since they dominantly influence the consequences of an untreated security issue. If the users are faced with malware-infected applications from an application store, they are discouraged from visiting that particular store again. The loss of revenue and popularity, as discussed in the first assignment, weighs heavily on the severity of the security issue.

Antivirus developers are actors since they work on the malware detection. They influence the effectiveness of mitigating this risk, whether it is by improving their detection rates or by providing cheaper antiviruses.

6 Choosing a strategy

The different actors here can have different strategies, because they all have different goals and assets to protect : a user wants to protect the integrity of its phone and the confidentiality of its credentials, the stores want to protect their reputation and the availability of the network, the malware owners want to have a maximum number of downloads...

One possible strategy for the users could be the risk avoidance : if one store (or one category of a specific store) contains too much malwares, the user can decide not to download any application that comes from this store or this specific category. However, this strategy is probably not efficient in long term, because malware developers focus on the most popular categories and stores and will simply change the category of their applications or try another store (even if some stores look more secure than others, because they have better controls).

Another strategy for the users could be to mitigate the risk by using an anti-virus application to detect the malware application after its installation. The success of a such strategy is however strongly correlated with the efficiency of the anti-virus. And we see in the dataset that anti-viruses don't always agree on which application is a malware. Users can also be careful about the permissions they give to each application, if they are well enough informed to

detect incoherent permissions (for example, an image editing application which asks for the permission to access the user's contacts).

7 ROSI calculation

7.1 Benefits

We have the price P of each application defined in the dataset of the PlayStore. We assume that there is no other transaction (no 'in app purchases') that the Play Store could charge and get benefit on. So each time a user buys an application, the Play Store gets 15% of the price. Therefore, we can compute the benefits on the Google Play store by multiplying the number of downloads for an application by 15% of this application price. Note that the dataset does not contain all the available applications, but that we will assume that the distributions for prices and malwares proportions are the same in dataset and in the store.

For each different developer, there is also a $25 fee. Because a developer can upload many apps, we need to compute the number of different developers in the dataset. But this is a one time fee, so this won't be present in the costs.

We need then to estimate the benefits (the prevented loss) when a malware application is not uploaded on the store. The main prevented loss is the reputation loss.

Possible approach : once a customer gets a malware, he never downloads an app on the store again. We can try to find average price spent for each customer on the Play Store, and take 15% of it to have an estimation of the loss of one customer.

7.2 Costs

The total costs for the Google Play Store, for example if they choose to implement stronger controls at the upload :

- the cost of the control themselves (paying developers to code a tool that has a better detection of malware applications) ;
- the costs of the malware applications that have not been uploaded.
- the costs of the false positives : when a non-malicious application is refused by the store (that detects it as a malware), the store loses the 15% fee on every transaction (including the price of the application).

Possible approach : To compute the costs of the false positives, we can compute the price distribution of the applications in the dataset and define what the false positives could be (for example, an application detected as malware by one anti-virus but not two) with a probability.

Other approach on the preventive controls: If Google detects all malwares before their being uploaded, there are less applications on the store. For each

application that is a malware, compute how much google earned thanks to this app (number of downloads multiplied by 15% of the price). This is money that Google would not earn if the controls were perfects.

8 Conclusion

9 References

Interesting links :
https://support.google.com/googleplay/answer/2812853?hl=en
https://www.google.com/about/unwanted-software-policy.html