Android - Actors and Security Strategies
-Draft-

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

October 14, 2019

1 Introduction

In the previous reports, we described metrics about the security of mobile applications, by comparing the number of malwares and downloaded malware applications in the Play Store and in other stores (for example, Chinese stores).

We continue with three actors for this report: the Play Store itself, the customer who install applications on its phone, and the antivirus companies.

2 Strategies for three actors

2.1 The Play Store

The Play Store can, as described in the previous report, develop an anti-virus to better detect the malwares among the uploaded applications on the store (e.g. by improving the Google Play Protect tool, that since 2017 tries to detect and remove malwares on the platform using machine learning).

The main costs of such a tool would be the developing costs: Google needs to hire a lot of Computer Engineers/Scientists to develop a tool (i.e. a tool with a very low false positive rate, since the Play Store does not want to remove applications that are not a malware). For scale, an antivirus company such as McAfee works with more than 6,000 people and a smaller one like Avast with 1,700 employees worldwide, which means that Google would require a very high initial investment, because of employment costs and the rent of offices and computer material.

The main benefit for the store would be the avoidance of reputation loss: when a customer downloads malware on the Play Store, the customer could blame the Play Store for letting a malware inside in the first place and leave. Even if a customer spends very little on the Play Store, the amount of downloads (even for the malware applications) makes it interesting for the store to mitigate the issue.

This control tool can be an externality for the users of the store: even if they don't pay for it, they will have a better security while downloading applications - which leads to a better security hygiene of the Android network in general.

2.2 The customer

The customers cannot directly act on the applications in the Play Store, but they can take countermeasures to avoid security problems. For example, by installing an antivirus on their phone. The antivirus will detect some (maybe not all) the malicious applications and avoid potential data leaks.

The cost of such a solution is the cost of the antivirus. However, plenty of free antivirus tools exist. Since it's difficult to assess the quality of an antivirus (because of the lack of available data and the difficulty to measure security), people will probably choose a free antivirus. So the only cost remaining is the time it takes for a customer to choose an antivirus and install it.

The benefit of such an installation are difficult to measure. Often, the antivirus will not detect anything (since the customer is more likely to download non-malicious applications rather than infected applications). Most antivirus software use a great deal of processing power, negatively affecting battery life and performance of a device. When it does prevent the installation of a malicious application, the prevented loss could be anything. Loss of personal information, Loss of device performance, loss of credit or money. It could also just be some simple ads that are not being shown anymore.

Customers, therefore, do not have many incentives to install antivirus applications on their phone, unless required to do so by, for example, their employer. Installing an antivirus is not a priority, because most customers have never experienced (the effects of) a serious data breach.

The hacked phone could be used as an bad externality, though. For example, an email hacked by a malicious application can send spam to other contacts of this email-address. However, since this does not directly concern the owner of the phone (which is not the one receiving spam), he could ignore that problem.

2.3 The antivirus companies

The countermeasure for the issue designed by antivirus companies is obvious. More R&D on developing better algorithms for detecting malicious code is an effective long-term countermeasure.

The costs are directly tied to the product of these companies. Employee salaries, office rent and hardware are the most common costs. However, if we assume the company to have been operational for some time already, such as McAfee, then the costs are negligible as it requires no initial investment, but rather a continuous R&D cost.

The benefits are, once the product is released, initially very significant. However, over time the relative increase of quality in updates to the antivirus software decreases. Most malware will be detected by the antivirus and, therefore, the security issue reduces in risk.

Obviously, the antivirus companies have a high priority in developing this countermeasure, as it is their sole source of income.

The externality of this is that malware developers are less inclined to create 'lazy malware'-applications. With antiviruses, these developers must invest time and money in their applications in order to fool the antivirus software. Therefore, it would also result in a lower proportion of malware vs. non-malware applications, as less malware applications would be built.

3 Differences in the metrics

The main difference observed in the metrics is on the proportion of malicious applications in application stores which is represented in figure 1. This graph shows that all the stores don't have the same security controls. Furthermore comparing the American store (the Google Play Store) and Chinese stores show that Chinese stores have far more malicious applications on it.

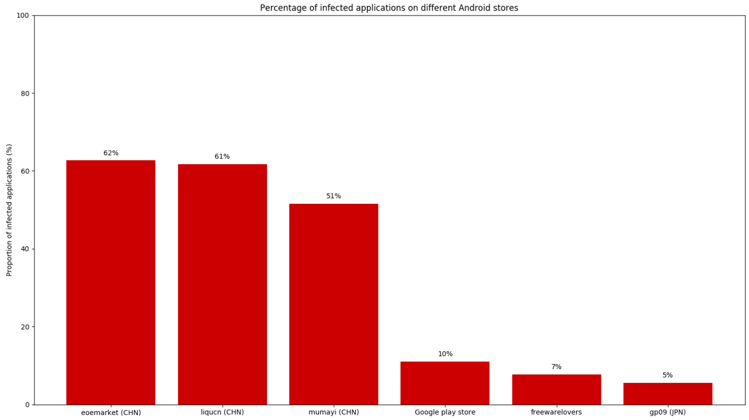

Figure 1: Percentage of infected applications on each store

3.1 Factors

We have identified various factors that can influence our metric:

1. **The laws and regulations specific to the regions where the app-stores operate.** For example, some US states have regulations about data breach disclosures that force the companies suffering from a data breach to inform the customers and the authorities as soon as possible.

Because this will result in loss of reputation, it is an incentive for the app markets to install better security controls.

2. **The size of the user-base of each app-store.** Our metric accounts for the size of the platform by normalizing the amount of malware based on the total amount of applications, but the size of the platform by itself constitutes an incentive to the attackers. It is very likely that malicious developers will prioritize platforms with larger user-bases, since this translates to more potential victims.

3. **The openness of the application market.** Malicious developers are more likely to target app-stores with less security controls, lower publishing standards, and lower publishing prices.

4. **The types of applications available on each market.** If attackers have a preference for certain application categories, then stores that specialize in these categories will have higher malware ratios than stores that don't.

3.2 Statistical analysis

How exact should this analysis be? Due to the lack of data and external data fitting with our problem context, we have difficulty quantifying the variance of our factors. For us, the variance is more speculation than actual numbers.

Our ideas so far:

1. Find data on the number of users for each market and look for a correlation between this number and the malware ratio. Alternatively, approximate the number of users from the amount of downloads in the provided dataset.

2. Find data on the publishing requirements of each platform, namely the publishing cost or whether they perform quality checks or background checks on the developers, and look for a correlation to the malware ratios. Note: with a few exceptions, this data is very hard to find for Chinese app-stores.

3. Perform a simple difference of means between malware ratios based on the regulatory environments in which the stores operate.

4. Compute the correlation between malware ratios and the ratios for certain categories (e.g. games, social media, etc.) in each store.

4 References

Interesting link for potential strategies on the customer point of view: https://www.forcepoint.com/cyber-edu/mobile-malware

About the regulations on private data in China: https://technode.com/2019/06/19/china-data-protections-law/

https://iclg.com/practice-areas/data-protection-laws-and-regulations/china

Google play definition of malwares

Evaluating Malware Mitigation by Android Market Operators: they did the same analysis as we did and found that Chinese stores had "alarmingly high" malwares ratios. They state that "Google Play is the only market that seems to conduct active malware removal".

China forces tourists to install malwares