Android Applications

Introduction

Assignment draft - It should contain the methodology, a description of the steps you will follow to solve the assignment and any preliminary result. This draft must be a pdf file located in the root directory.

Methodology:

For performing this assignment we will:

1. Brainstorming to gather ideas regarding problem owners of security issues on Android applications, risk strategy management, external actors influencing different strategies, and risk strategies to tackle the problem.

2. Conducting a desk research to complete the missing information regarding the topics explained above.

3. Selecting the most viable strategy to evaluate its Return on Security Investment.

4. Calculating the ROSI of the selected strategy.

5. Analyzing the results of the calculations and deriving some conclusions.

6. Providing the information, analysis, and results as a scientific document according the questions of the assignment.

1. Who is the problem owner of the security issue as measured in your first assignment?
2. What relevant differences in security performance does your metric reveal?

3. What risk strategies can the problem owner follow to reduce the security issue as measured in your first assignment?

This report centers around the app-market and sees the app-market owners as the problem owner. According to the data both app-markets suffer from a high amount of malware. If this issue is deemed to be detrimental to the company goals it has to implement certain strategies to prevent and mitigate the problem of malware. Before any strategy can be formed the life cycle of an app must be understood.

A developer first needs to be registered with the app-market. After registration the app is uploaded to the market. The market owner checks if content is complying with their terms. The app is finally listed and downloadable off the app-market. The developer at this stage still able to update and pull their content.

The app-market owners (APO) play a significant role as the hub for apps. Nonetheless their risk reduction strategies are limited to control strategies, in which they control access and distribution of apps. These control strategies fall in to the categories of Prevention, Interdiction, Detection and Response.

PREVENTION

The old saying goes as: "Preventing is better than curing". This also rings true for any cyber security issue. Preventing any calamity is preferred than fixing the damage it has caused. This idea can be translated to the app-markets too. The goal is to decrease the amount of malicious apps turned in by developers.The strategy must stimulate developers to not include any malware in their products. A possible "carrot" solution can be a program as a "trusted developer" certification. This is a program that rewards developers that let their firm to be audited and hold a clean track record. In being trusted they are then rewarded for it by better rankings etc.. On the "stick" end of the solutions is a punishment strategy that dolls out fines or holds back deposits when there is foul play. Of course a punishment system is only effecive if fines are more costly than profit made with malicious content.

INTERDICTION

Interdiction is actually a part of prevention, but the mechanism is so different that it warrants its own section. Interdiction in the context of app-market owners is the process in which an app is

checked after it has been offered for publishing and then blocked from being published on the market when malware is detected/found. Code can be manually reviewed, which is time consuming and costly. A large skilled workforce is needed to check if certain code seems to be malicious. Alternatives are automated malware scanning and sandboxing. Sandboxing involves the app-market owner installs and runs the app in a special protected environment that closely monitors if the app shows malicious behaviour.

DETECTION

Even if prevention and interdiction are done at a high intensity it is still possible for malware to slip through the cracks. It is now important that a detection mechanism is present that will detect and pull malicious apps from the market. In essence there are modes of detection, active and reactive. In the active mode, the appmarket owner analyzes app behaviour sent in by monitoring plugins that runs on the platform or is added by the app-market owner. An AI can flag the results for further investigation. On the reactive end, market owners can use information provided by antivirus companies or user review/flagging as a data source to act upon.

RESPONSE

Once a compromise is found the problem owner has to make a decision on how to respond. Depending on the business strategy, philosophy and malware type it can choose to do nothing, pull the app from the market and issue a warning to the installed user base or remotely uninstall it off of android devices.

STRATEGY

It is important to understand that if at any stage security was circumvented that it offers no protection on later stages. It is therefore imperative to adopt a risk strategy that minimizes risk at every stage thus a mixed risk strategy is prefered. But to what extent this strategy should take form is dependent on a number of factors. The problem owner must first of all know what level of security it wants to adopt, then it should look at its financial means to see if it is possible to realize. Since both markets are free app markets, receive their profits from advertising and considering their unique position in the Chinese market they can get away with much more. They are much more served with the cheapest solution, Simple developer sign up, automated malware scan and short sanboxing period and only react to large amount of responses.

4. What other actors can influence the security issue as measured in your first assignment?

The app-market owners aren't the only actors in this game. Governments, consumers and app developers are all a part of this ecosystem.

In this case the Chinese government can be a very strong actor. The Chinese government has been known with its near totalitarian governance. It too can have a major impact on the malware density of the market by supporting regulations that prohibit the programming of malware in commercial apps and make it mandatory that each app-market adopts an extensive risk strategy. Consumers control their own actions, their choices are instrumental to the malware creators. The consumer can be educated or educate himself. By becoming a much more aware consumer it is possible to prevent infection and know how to mitigate the damage caused by accidental infection. The caveat is that it is very hard to discern between legitimate apps and shady ones. The consumer is actually the weakest actor in this ecosystem because they are the least skilled with the least of means.

App developers on the other hand are the root of this problem. They make a conscious decision to incorporate or withhold malware in their apps. The dominant motive is profit. Legitimate developers suffer from a compromised market. The only thing that can be done in an organized fashion are developer collectives. These collectives review the code of their peers and as a collective guarantee malware free apps. These collectives are also recognized by consumers. This way they reduce the load on a market owner for prevention and detection but also offer consumers a promise of clean apps. With the app-market owners help, apps from these collectives can be ranked higher. All of this helps dev-collectives to gain a competative advantage.

5. Identify the risk strategies that the actors can adopt to tackle the problem

1. are there actors with different strategies? why?

As it has been said above, there are also many other actors in our problem scope in addition to the market owner. Not surprisingly, it is highly likely for each of these actors to implement different security strategies. This might be the case because these actors are also likely to belong to a different category, which means they are likely to have different problems and objectives. Next, the strategies used by the various actors and how they have developed over time are going to be described.

2. have the strategies changed significantly over time in a way that reduces or increases risks?

The first actor that obviously affect the app marketplace security problem are the attackers. From the previous submission, it can be concluded that the attackers have quite successfully infected the app marketplace by looking from the infected apps statistic. The previous report also showed that the most common attack strategy is based on malware. However, the lack of time dimension in the data means that it will be hard to establish how the attacker strategies have changed over time. Nevertheless, since it is already determined that the attacker methods and strategies are always a response to the defender's implemented controls, it can be predicted that their methods and strategies will only be more sophisticated in the future. Therefore, it is almost certain that the advance of strategies and method by the attackers will always result in the increase of risk.

The second actor that highly influence the problem at stake is the regulatory authority. Since the app marketplace in the previous report based in China, then the relevant regulatory authorities are the Cyberspace Administration of China (CAC) and China's Ministry of Industry and Information Technology (MIIT). Although there is no clear conclusion about where the regulatory authority such as MIIT and CAC belong to in cyber security key player category, in this report it is determined that they are most closely resemble the security consumers.

There has been information about the activity of these two government entities. In May 2016, the MIIT released a list of 29 malicious apps after inspecting 43 app stores, four of which are from Baidu app store (http://www.youngchinabiz.com/en/internet-regulator-criticizes-baidu-mobile-assistant/). This might be a good sign that the government agency has been implementing risk reduction strategy to reduce harm suffered by customers. In June 2016, the CAC ordered various app marketplace to record users' activity for up to 60 days (http://www.bloomberg.com/news/articles/2016-06-28/china-orders-mobile-app-stores-providers-to-monitor-users). Although can be classified as risk reduction strategy, this action was arguably intended to support their "business strategy" instead of increasing real security level. Nonetheless, the risk reduction of regulatory authority through the release of regulations most likely have reduced the existing risk.

The third actor, in this case, are the app developers. <to be developed further>

The fourth actor is the consumers. <to be developed further>

6. Pick one of the risk strategies identified previously and calculate the Return on Security Investment (ROSI) for that particular strategy. I.e.,

1. Estimate the costs involved in following that strategy
2. Estimate the benefits of following that strategy (assume a particular loss distribution)