Evaluating Malware Mitigation by Android Market Operators

Yosuke KIKUCHI*, Hiroshi MORI*, Hiroki NAKANO*, Katsunari YOSHIOKA*, Tsutomu MATSUMOTO*, Michel VAN EETEN**

*Yokohama National University
**Delft University of Technology

9th USENIX Workshop on Cyber Security Experimentation and Test
Motivation

• The number of Android apps is continuously increasing
• There are many third party app markets (e.g. Amazon App Store)
• At the same time, the number of Android malware are increasing [1]
• In this situation, we are interested in whether these market operators make effort for mitigating malware and if yes, how well they do
Agenda

• Motivation
• Agenda
• Method
• Result of Evaluation
• Conclusion
• Limitations
Method

1. Download apps and meta-data (# of downloads and date of last update)
What markets we have selected?

• We measured five markets
• Why did we select these markets?
  – We wanted to track survival period of apps, so we selected popular (at least once) and not too new markets

<table>
<thead>
<tr>
<th>Market</th>
<th>Collected Apps</th>
<th>Collection Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Play (GP_PO)</td>
<td>12280</td>
<td>2015/09/21 – 2015/09/28</td>
</tr>
<tr>
<td>Goolge Play (GP_PD)</td>
<td>8966</td>
<td>2014/08/07 – 2014/11/03</td>
</tr>
<tr>
<td>Mumayi (MY)</td>
<td>19794</td>
<td>2015/07/14 – 2015/08/09</td>
</tr>
<tr>
<td>Liqucn (LQ)</td>
<td>6844</td>
<td>2015/09/02 – 2015/09/04</td>
</tr>
<tr>
<td>eoeMarket (EM)</td>
<td>10203</td>
<td>2015/09/15 – 2015/09/19</td>
</tr>
<tr>
<td>Freeware Lovers (FL)</td>
<td>3652</td>
<td>2015/06/20 – 2015/06/23</td>
</tr>
</tbody>
</table>
We collected apps from Google Play in two ways

1. Top popular apps for each categories (GP_PO)
   - e.g. games, tools and etc...
   - We could collect 12,280 apps
   - Note: There is a bias, because these apps are popular and could have been more closely examined by market operator

2. We also use PlayDrone DataSet[3] (over 1.4M apps) that were collected for research purpose. And we used 8,966 apps finally (GP_PD)
   - We selected 15,000 free apps from the dataset at random
   - Since Play Drone was collected in 2014, we then checked whether these apps still exist in the Play store at the time of the study
   - We picked up 8,966 apps that are still in Google Play
   - Note: Collection period of this dataset is older than our other app dataset

Data Collection
- Other Markets -

• We could collect apps by crawling web pages of apps in other markets
  – Mumayi(EM): 19,794 apps
  – eoeMarket(EM): 10,203 apps
  – Liqucn(LQ): 6,884 apps
  – Freeware Lovers(FL): 3,652 apps
1. Download apps and meta-data (# of downloads and date of last update)
Method

1. Download apps and meta-data (# of downloads and date of last update)

2. Submit the apps to VirusTotal and log results
   - Detection Ratio
   - Labels
Method

Detection Ratio: How many AV vendors flag the app as malicious?

Detection ratio: 43 / 55
Analysis date: 2016-07-25 07:53:40 UTC (1 week ago)

Label: What kinds of malware (Note: sometimes adware is included)
1. Download apps and meta-data (# of downloads and date of last update)

2. Submit the apps to VirusTotal and log results
   - Detection Ratio
   - Labels

3. Evaluate with three metrics
Method
- Metrics for Evaluation -

• We calculate three security metrics for each market for evaluation:
  – the malware presence ratio (MPR)
    • percentage of all collected apps that are detected as malware
  – the malware download ratio (MDR)
    • percentage of all downloads of all collected apps that are detected as malware
  – the survival period of malware
    • how long apps detected as malware remain in the app store
Positive Detection Ratio

• We defined Positive Detection Ratio (PDR)
  – Ratio of number of AV products that flag the app “malicious” (=Detection Ratio)

\[ PDR(S, a) = \left| \{ \text{av} \in S | \text{av}(a) = \text{malicious} \} \right| / |S| \]

a : Android App
av: Anti Virus Product
S : Set of AV products with which VirusTotal used to scan the app
Positive Detection Ratio

Detection Ratio: How many AV vendors flag the app as malicious?

PDR = 78%
Malware Presence Ratio

• We define Malware Presence Ratio (MPR)
  – This means percentage of all collected apps that are detected as malware
• How to judge malware or not?
  – We judge an app as malware if PDR of the app above \( m[\%] \)

\[
M_{PR}(m,S,M) = \left| \left\{ a \in M \mid PDR(S,a) > m \right\} \right| / |M|
\]

a : Android App
av : Anti Virus Product
S : Set of AV products with which VirusTotal used to scan the app
M : Set of Apps in a market
m : Threshold
Malware Presence Ratio

![Graph showing the relationship between Malware Presence Ratio and Positive Detection Threshold.](graph.png)
Malware Presence Ratio
- What is a reasonable value of “m”? -

MPR depend on “m” (Positive Detection Threshold), so this value is important. If we set m to too high value (e.g. m= 70[%]), almost all apps are counted as not malware. In this study, we decided m = 30[%] is reasonable value according to other studies[4][5]

Google Play is Really Safe?
- MPR for Google Play via Keyword Search -

• The MPR for GP_PO is low, but we have explored whether this risk was perhaps concentrated, and thus higher, in certain areas of the market.

• For this purpose, we collected another sample of apps, via keyword searches.
Google Play is Really Safe?  
- MPR for Google Play via Keyword Search -  

• We used 155 popular keywords listed on the keyword ranking sites [6-8], and 11 keywords in the security report by Symantec [9]  

• We then collected the 40 apps that are shown on the first page of search results  

MPR for Google Play via Keyword Search

Malware Presence Ratio (m = 30[%])

Keywords:
- sms
- adult
- megami
- hulu
- bejeweled
- screenshot
- justin bieber
- jokes
- olympics 2012
- keyboard
- weather
- hotmail
- ringtones free
- temple run
- send sms
- live wallpapers
- video downloader
- emoji
- hotspot
- GP_PD
- GP_PO
Google Play is Really Safe?
- MPR for Google Play via Keyword Search -

• We used 155 popular keywords listed on the keyword ranking sites [6-8], and 11 keywords in the security report by Symantec [9]

• We then collected the 40 apps that are shown on the first page of search results

• Keywords like "sms” and "adult” lead users to apps with an MPR that is more than 50 times higher than the rate for GP_PO.
Malware Download Ratio

- We define Malware Download Ratio (MDR)
  - This means percentage of all downloads of the collected apps that are detected as malware

\[
MDR(m, S, M) = \frac{\sum_{a \in M'} DL(a)}{\sum_{a \in M} DL(a)}
\]

- \( m \): Threshold
- \( S \): Set of AV products VirusTotal used to scan
- \( M \): Set of Apps in a market
- \( M' \): Set of Malware in \( M \)
- \( a \): Android App

Total download number of all malware
Total download number of all apps
Malware Download Ratio

*In FL, the number of downloads is unpublished. For reference, we calculated the index on the assumption that each app was downloaded same times.
Malware Survival Period

• We measure malware survival period
  
  – The survival period of an app is the time that an app has been present in an app store.

• To calculate a survival period, we count the number of days between the date when we downloaded the app and the date when it was last updated

• We expected that if market operators make effort to mitigate malware, high positive detection ratio (PDR) apps cannot live a long time
Google Play Popular (GP_PO)

Positive Detection Ratio [%]

Malware Survival Period [days]

- Average PDR
- Apps in GP_PO
- #Submitted Apps

#Submitted Apps
Color of Dots

- Detected with **no** "Adware" labels
- Detected with **some** "Adware" labels
- Detected with **many** "Adware" labels

Positive Detection Ratio [%]

Malware Survival Period [days]
Google Play Play Drone (GP_PD)
Mumayi (MY)
Liqucn (LQ)
eoeMarket (EM)
Freeware Lovers (FL)

No app submission was accepted in this period.
Conclusion

• At a PDR of 30%, around one in five apps are flagged as malicious in EM, MY and LQ.

• MPR, MDR are relatively low for GP and FL but when users of Google Play search with specific keywords, they may have a 50 times higher probability of encountering malware that when selecting from the popular app list.

• EM, MY, LQ and FL do not seem to act against malware even when PDRs are very high.

• Google Play is the only market that seems to conduct active malware removal.
Limitations

• Our results depend on VirusTotal (Anti Virus products)

• We simply count numbers of detection. We did not delve deeply into the labels

• There are some markets becoming popular in last few years that we didn’t evaluate. (e.g. Baidu)
Thank You for Your Attention!