Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets

Yajin Zhou  Zhi Wang  Wu Zhou  Xuxian Jiang

North Carolina State University
Motivation: Smartphones

Worldwide Smartphone Sales

Data source: gartner.com
Motivation: Apps

Number of Apps in Official Android Market

$^{2}$Data source: androlib.com
Motivation: Markets
Motivation: Malware in Markets

What is the overall health of Android Markets?

The security of Google Android has once again been called into question after an academic researcher discovered 12 malicious apps hosted in the operating system's official app store.
Design Goals

• Accuracy
  • Detect malware with low false positives and negatives

• Scalability
  • Scale to hundreds of thousands of apps

• Efficiency
  • Process all apps in a reasonable amount of time
DroidRanger Overview

Representative Android Markets

Malware Samples

Permission-based Behavioral Footprints

Footprint-based Detection Engine

Infection from Known Malware

Heuristics-based Detection Engine

Infection from Zero-day Malware

Heuristics

DroidRanger

App Repository
## Footprint-based Detection Engine

- Filter apps with essential permissions

<table>
<thead>
<tr>
<th>Malware</th>
<th>Essential Permissions</th>
<th>Apps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geinimi</td>
<td>INTERNET, SEND_SMS</td>
<td>7,620 (4.17%)</td>
</tr>
<tr>
<td>ADRD</td>
<td>INTERNET, ACCESS_NETWORK_STATE, RECEIVE_BOOT_COMPLETED</td>
<td>10,379 (5.68%)</td>
</tr>
<tr>
<td>Pjapps</td>
<td>INTERNET, RECEIVE_SMS</td>
<td>4,637 (2.54%)</td>
</tr>
<tr>
<td>Bgserv</td>
<td>INTERNET, RECEIVE_SMS, SEND_SMS</td>
<td>2,880 (1.58%)</td>
</tr>
<tr>
<td>DroidDream</td>
<td>CHANGE_WIFI_STATE</td>
<td>4,096 (2.24%)</td>
</tr>
<tr>
<td>zHash</td>
<td>CHANGE_WIFI_STATE</td>
<td>4,096 (2.24%)</td>
</tr>
<tr>
<td>jSMSHider</td>
<td>INSTALL_PACKAGES</td>
<td></td>
</tr>
<tr>
<td>Zsone</td>
<td>RECEIVE_SMS, SEND_SMS</td>
<td></td>
</tr>
</tbody>
</table>

Filtering apps with essential permissions reduced to 0.64% when considering a broadcast receiver.
Footprint-based Detection Engine

- Match apps to malware behavioral footprints in multiple dimensions
  - Information in manifest file
    - Declare a receiver listening to SMS_RECEIVED
  - Semantics in the byte-code
    - Register a receiver listening to SMS_RECEIVED
    - Call `abortBroadcast` in the receiver
    - Send SMS messages to premium numbers
  - Structural layout of the app

Behavioral footprint of Zsone
Heuristics-based Detection Engine

• Select apps with dynamic Java/native code loading
• Monitor their runtime behavior
  • Java code: permission-related framework APIs
  • Native code: system calls requiring root privileges
Evaluation: Overall

• Data set
  • Crawled the official & four alternative markets
  • Collected 204,040 free apps during 05/2011-06/2011

• Process time
  • Used four and half hours for all 204,040 apps
## Evaluation: Overall

<table>
<thead>
<tr>
<th>Malware</th>
<th>Official Market</th>
<th>eoeMarket</th>
<th>alcatelclub</th>
<th>gfan</th>
<th>mmoovv</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known</td>
<td>21</td>
<td>51</td>
<td>48</td>
<td>20</td>
<td>31</td>
<td>171</td>
</tr>
<tr>
<td>Zero-day</td>
<td>11</td>
<td>9</td>
<td>10</td>
<td>1</td>
<td>9</td>
<td>40</td>
</tr>
<tr>
<td>Total</td>
<td>32 (0.02%)</td>
<td>60 (0.35%)</td>
<td>58 (0.39%)</td>
<td>21</td>
<td>40 (0.47%)</td>
<td>211</td>
</tr>
</tbody>
</table>

Total infected apps detected by DroidRanger
Evaluation: Footprint-based Detection Engine
Evaluation: Infected Apps

First report: 10/2010
Evaluation: Accuracy

- **Pjapps**: 31/15
- **BaseBridge**: 4/1
- **jSMSHider**: 9/6
- **Bgserv**: 0/0
- **ADRD**: 3/3

Legend:
- **DroidRanger**
- **LookOut Ver 6.11 (11/2011)**
- **LookOut Ver 6.3 (08/2011)**
Evaluation: Accuracy

• 24 samples in 10 known families from *contagio*

• DroidRanger detected 23 samples (96%)
  • Missed a payload of DroidDream, not the malware itself
  • Found one mis-categorized sample for ADRD
Evaluation: Heuristics-based Detection Engine

Malware Samples

Permission-based Behavioral Footprints

Footprint-based Detection Engine

Infected from Known Malware

Infection from Zero-day Malware

Heuristics-based Detection Engine

Heuristics

DroidRanger

App Repository
Evaluation: Infected Apps

- Detected two zero-day malware using heuristics
  - Plankton: dynamic loading of Java code
  - DroidKungFu: dynamic loading of native code

- Detected 40 samples using behavioral footprints
  - 11 samples from the official Android Market
  - 29 samples from alternative Android Markets
Evaluation: Malware Behaviors

- **Plankton**
  - Uploads a list of permissions before downloading a payload
  - Contains a bot-like command & control channel

```
ACTIVATION = new Commands("ACTIVATION", 1, "Activation", "/activate");
HOMEPAGE = new Commands("HOMEPAGE", 2, "Homepage", "/homepage");
COMMANDS_STATUS = new Commands("COMMANDS_STATUS", 3, "CommandsStatus", "/commandstatus");
BOOKMARKS = new Commands("BOOKMARKS", 4, "Bookmarks", "/bookmarks");
SHORTCUTS = new Commands("SHORTCUTS", 5, "Shortcuts", "/shortcuts");
HISTORY = new Commands("HISTORY", 6, "History", "/history");
TERMINATE = new Commands("TERMINATE", 7, "Terminate", "/terminate");
STATUS = new Commands("STATUS", 8, "Status", "/status");
DUMP_LOG = new Commands("DUMP_LOG", 9, "DumpLog", "/dumplog");
UNEXP_EXCEPTION = new Commands("UNEXP_EXCEPTION", 10, "UnexpectedException", "/unexpectedexception");
UPGRADE = new Commands("UPGRADE", 11, "Upgrade", "/installation");
INSTALLATION = new Commands("INSTALLATION", 12, "Installation", "/installation");
```
Discussion

• Need more comprehensive heuristics
  • Background sending of unauthorized SMS messages?
  • Bot-like behavior controlled by SMS messages?

• A call for rigorous vetting processes
  • A large number of users can be infected
  • Malware remains in alternative markets for a long time
  • Zero-day malware exists in Android Markets
Related Work

• Smartphone platform security
  • TaintDroid (Enck et al., OSDI 10), PiOS (Egele et al., NDSS 11), Stowaway (Felt et al., CCS 11), Cells (Andrus et al., SOSP 11), AppFence (Hornyack et al., CCS 11), Quire (Dietz et al., USENIX Security 11), A Study of Android Application Security (Enck et al., USENIX Security 11), TISSA (Zhou et al., TRUST 11), Woodpecker (Grace et al., NDSS 12) ...

• Malware detection on mobile devices
  • pBMDS (Xie et al., WiSec 10), VirusMeter (Liu et al., RAID 09), Crowdroid (Burguera et al., CCS-SPSM 11) ...

• Other systematic security study
  • HoneyMonkey (Wang et al., NDSS 06), Systematic Web Spyware Study (Moshchuk et al., NDSS 06), All Your iFRAMEs Point to Us (Provos et al., USENIX Security 08) ...
Conclusion

- DroidRanger is a system to systematically study the overall health of existing Android Markets

<table>
<thead>
<tr>
<th>Malware</th>
<th>Official Market</th>
<th>eoeMarket</th>
<th>alcatelclub</th>
<th>gfan</th>
<th>mmoovv</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known</td>
<td>21</td>
<td>51</td>
<td>48</td>
<td>20</td>
<td>31</td>
<td>171</td>
</tr>
<tr>
<td>Zero-day</td>
<td>11</td>
<td>9</td>
<td>10</td>
<td>1</td>
<td>9</td>
<td>40</td>
</tr>
<tr>
<td>Total</td>
<td>32 (0.02%)</td>
<td>60 (0.35%)</td>
<td>58 (0.39%)</td>
<td>21</td>
<td>40</td>
<td>211</td>
</tr>
</tbody>
</table>
Thank You!
# Evaluation: Known Malware Samples

- 20 samples from 10 malware families

<table>
<thead>
<tr>
<th>Malware</th>
<th>First Report</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geinimi</td>
<td>10/2010</td>
<td>Trojan with bot-like capability</td>
</tr>
<tr>
<td>ADRD</td>
<td>02/2011</td>
<td>Trojan with bot-like capability</td>
</tr>
<tr>
<td>Pjapps</td>
<td>02/2011</td>
<td>Trojan with bot-like capability</td>
</tr>
<tr>
<td>Bgserv</td>
<td>03/2011</td>
<td>Trojan with bot-like capability</td>
</tr>
<tr>
<td>DroidDream</td>
<td>03/2011</td>
<td>Root exploit with Exploid, Rageagainstthecage</td>
</tr>
<tr>
<td>zHash</td>
<td>03/2011</td>
<td>Root exploit with Exploid</td>
</tr>
<tr>
<td>BaseBridge</td>
<td>05/2011</td>
<td>Root exploit with Rageagainstthecage</td>
</tr>
<tr>
<td>DroidDreamLight</td>
<td>05/2011</td>
<td>Trojan with information stealing capability</td>
</tr>
<tr>
<td>Zsone</td>
<td>05/2011</td>
<td>Trojan that sends premium-rate SMS</td>
</tr>
<tr>
<td>jSMSHider</td>
<td>06/2011</td>
<td>Trojan that target third-party firmware</td>
</tr>
</tbody>
</table>