Dissecting Android Malware: Characterization and Evolution
Problems to solve
Requirement 1: Sufficient Malware dataset

Anti Virus Communities or Researchers are hampered by the lack of malware data set.

Requires a sufficient Android malware dataset.
Requirement 2: Current Malware Detection Rate

How good are top anti-virus software against latest Android malware?

Evaluating effectiveness of current Anti-virus software
Related work

• Felt et al. “A survey of mobile malware in the wild”
  – Survey 46 malware samples on iOS, Android and Symbian
  – Choice of breadth over depth
  – No mention of advanced trojans in the wild
Related work

What was missing?

• In-depth look at Android malware
  – A technical analysis of advanced attacks

• Large pool of malware
  – Perhaps A/V companies missed stuff? E.g. Malware in third-party markets

• Evolution of malware and evaluation of defense
Contribution

• Large malware dataset presented
  – 1260 different samples in all
  – 49 different families each with many variants
  – More info: http://www.malgenomeproject.org/
Malware dataset

How was it collected?
Malware dataset

Q. How was it collected?

A. Crawl app stores!

Search for *android marketplace crawler*
Contribution

• Large malware dataset presented

• Analysis of malware samples
  – Provenance, Design, Harm

Installation  Activation  Characterisation
Malware: Provenance

• Official Android market

• Alternate android markets
  – Eoemarket
  – Gfan

† http://thedroidguy.com/2012/04/android-market-share-doubles-in-china-even-symbian-is-ahead-of-ios/
Malware: Provenance

Month of the year

Number of new malware families discovered

In Android Market
In Both Markets
In Alternative Market

Third-party store only
Official store only

08 09 10 11 12 01 02 03 04 05 06 07 08 09 10
2010 2011

0 2 4 6 8 10
Malware: Installation

How to lure users into installing malware you have written?

OR

How do bad things happen to good people?
Repackaging

App developer (Good guy)

Official Android market

Monk Bowl

Third-party market

Repackage Meister (bad guy)

End-user

• Steal info
• Hijack phone
• Defraud
Repackaging

86% of malware samples repackage!
Repackaging

+ =
Update attack

Google SSearch

DroidKungFu

FinanceAccount.apk

Payload

Source:
https://www.mylookout.com/mobile-threat-report
Update attack

Original Benign app

Encrypted blog entry: blog.sina.com.cn

Payload

AnserverBot
Drive-by download

• “Benign” game with a malvertisement

Source: https://www.mylookout.com/mobile-threat-report
Malware: Activation

When do bad things happen?

• Standard Android event notifications
  – Phone boots up
    • BOOT_COMPLETED (83.3%)
  – SMS is received
    • SMS_RECEIVED
  – Host app is started
    • ACTION_MAIN
Malware: Purpose

What do they do?

Source: http://www.textspyware.com/android/android-spyware-software/
Malware: Purpose

• Harvesting user information (51.1%)

• What is sent?
  – Device ID
  – Phone number/operator
  – User’s email addresses

http://www.fortiguard.com/av/VID3148366
Malware: Purpose

• SMS to premium numbers (45.3%)

Malware: Design

• Social engineering

• Phones as bots controlled from C&C server (93%)

• Privilege escalation (36.7%)
  – Exploit security flaws in kernel code
Malware: Permission use

Frequency of top 20 permissions

<table>
<thead>
<tr>
<th>Permission</th>
<th>Malware</th>
<th>Benign app</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEND_SMS</td>
<td>553</td>
<td>43</td>
</tr>
<tr>
<td>CHANGE_WIFI_STATE</td>
<td>398</td>
<td>34</td>
</tr>
<tr>
<td>RESTART_PACKAGES</td>
<td>333</td>
<td>33</td>
</tr>
<tr>
<td>READ_CONTACTS</td>
<td>457</td>
<td>71</td>
</tr>
<tr>
<td>RECEIVE_BOOT_COMPLETED</td>
<td>688</td>
<td>137</td>
</tr>
<tr>
<td>CALL_PHONE</td>
<td>424</td>
<td>114</td>
</tr>
</tbody>
</table>

Multiple permissions have higher frequency in malware compared to benign apps.
Malware: Permission use

• Summary
  – Avg. no. of permissions per app
    • Malware: 11 | Benign apps: 4
  – Avg. no. of top 20 permissions per app
    • Malware: 9 | Benign apps: 3
Contribution

• Large malware dataset presented

• Analysis of malware samples

• Evolution of malware
  – Advanced techniques to beat defense

• How good is defense?
Malware: Evolution

How are malware writers trying to evade detection?

• Encryption
  – Payload and internal data
• Running without install
  – DexClassLoader, Reflection
• Thwart reverse engineering
  – Class name obfuscation
Malware: Detection Rate

A few malware samples went undetected!

- AVG: 54.7%
- Lookout: 79.6%
- Norton: 20.2%
- Trend Micro: 76.7%
Malware: Detection

Q. Any clue why some samples were NOT detected by any?

A. They most likely employ signature-based detection!
Takeaways

Malware

• Mostly in third-party markets/forums (~90%)

• Requests more permissions on average

• Is evolving and Anti-virus software needs to catch up
Future Work

How does one reduce the impact of malware?

Google’s “Bouncer”
Future work

Resilient 'SMSZombie' Infects 500,000 Android Users in China

By Mike Lennon on August 18, 2012

Well, Google has a kill switch at least...

...But, what about third-party markets?
THE SMARTPHONES GOT TOO SMART... AND DEVELOPED A TASTE... FOR BLOOD!

Fortunately, the only way they could move was by turning on their vibrate while on a sloped table.

Making xkcd slightly worse: www.xkcdsw.com