SAND2014-15266PE

Towards an Android Exfiltration Detection System

Xisen Tian & Daniel Jung

United States Naval Academy

xtian@sandia.gov
sjung@sandia.gov

June 18, 2014

Overview

1. Inherent Vulnerabilities of Android Apps
2. Methods of Combating Malware
3. Possible Solutions
4. Wrap Up

Background

Android's Popularity

- Last year 4 out of 5 phones shipped carried Android OS [1]

Open Development

- Promotes large base of developers consisting of both amateurs and professionals
- Unlike Apple's App Store, anybody can upload any Android App onto the Google Play Store without a rigorous screening process...

[1] Bradley, 2013

Sensitive Hardware/Data

- Contacts
- Phone Records
- Camera
- Microphone
- Installed apps (Key Chain apps, etc)
- media (i.e. pictures, video, audio)
- SMS
- Web History

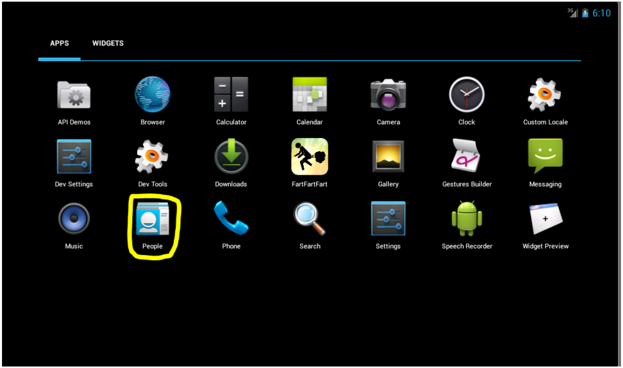
Malicious App Demo

Assumptions

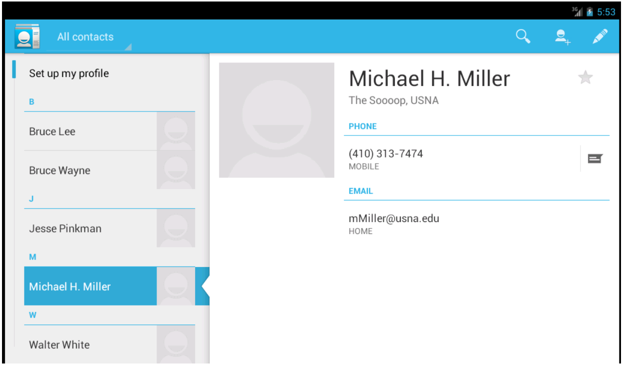
- People don't have any type of Exfiltration Detection Systems (EDS) installed
- People blindly click "Yes" during Install without reading everything
- People will install anything - i.e. fart apps[2]

[2] Crider, 2014

Malicious App Demo



Malicious App Demo



Set up my profile

B

Bruce Lee

Bruce Wayne

J

Jesse Pinkman

M

Michael H. Miller

W

Walter White

Michael H. Miller

The Soooop, USNA

PHONE

(410) 313-7474

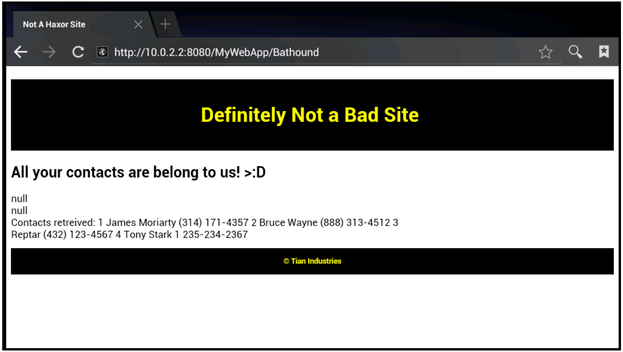
MOBILE

EMAIL

mMiller@usna.edu

HOME

Malicious App Demo



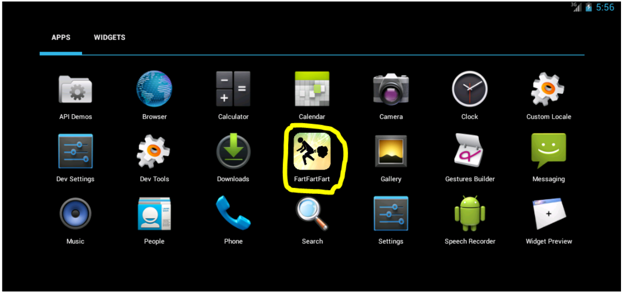
Definitely Not a Bad Site

All your contacts are belong to us! >:D

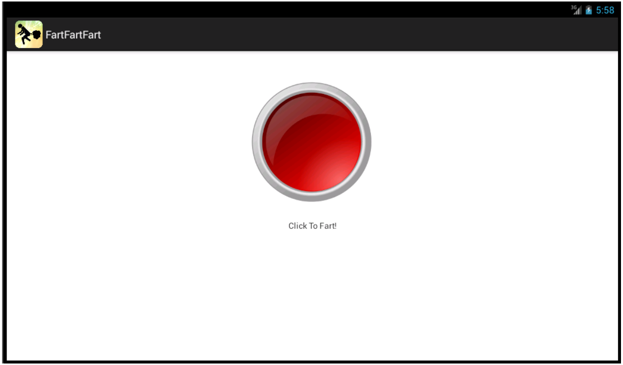
null
null
Contacts retreived: 1 James Moriarty (314) 171-4357 2 Bruce Wayne (888) 313-4512 3
Reptar (432) 123-4567 4 Tony Stark 1 235-234-2367

© Tian Industries

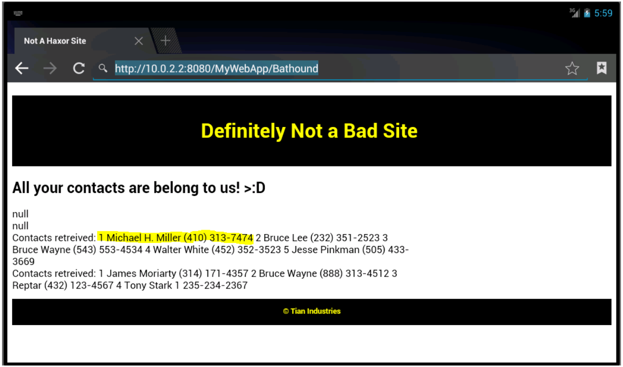
Malicious App Demo



Malicious App Demo



Malicious App Demo



Definitely Not a Bad Site

All your contacts are belong to us! >:D

null
null
Contacts retreived: 1 Michael H. Miller (410) 313-7474 2 Bruce Lee (232) 351-2523 3 Bruce Wayne (543) 553-4534 4 Walter White (452) 352-3523 5 Jesse Pinkman (505) 433-3669
Contacts retreived: 1 James Moriarty (314) 171-4357 2 Bruce Wayne (888) 313-4512 3 Reptar (432) 123-4567 4 Tony Stark 1 235-234-2367

© Tian Industries

Security Structure

Sandbox model

- Each app has its own allotted resources
- Apps use intents and binders for interprocess communication

Permissions

- App must request permission from the user during pre-installization to ultilize a feature
- Once permission is granted, the app has full access to the capabilities of the specified permission

3 Different Approaches

- Monitor Network/SMS Activity
- Reverse Engineer Source Code
- Monitor Hardware Anomalies

Monitor Network/SMS Activity

1. Check Permissions

android.permission.INTERNET
android.permission.CHANGE_CONFIGURATION
android.permission.WRITE_SMS
android.permission.SEND_SMS
android.permission.CALL_PHONE
android.permission.READ_*

2. Target Suspicious Apps

Focus on suspicious apps (over-privilaged/flagged) to increase efficiency and effectiveness

3. Alert User

The user must be responsible and vigilant

Monitor Network/SMS Activity

- Reroute all network traffic to external server to provide monitoring service via a VPN/SSH Tunnel
- Utilize existing packet sniffing tools and rules to create an Exfiltration Detection System using Tcpdump, Wireshark, Snort etc.

Reverse Engineer Source Code

1. Decompile APK

Decompile before install to ”scan” the app (small overhead).

2. Search source code for keywords related to malicious activity

Develop Algorithm to predict malicious Apps based on mapping of key words

3. Alert User

It is up to the user to decide to unistall the bad apps.

The Source Code

- To connect to the web, an app must call
  "URL.openConnection()"
- To upload data to a web server, an app must call
  "setDoOutput(true)"
  "setFixedLengthStreamingMode(int)"
  "setChunkedStreamingMode(int)"
- Use "getRoute()" to see where an app is uploading data to
- To use SMS, an app must call
  "void sendDataMessage(...)"
  "void sendMultipartMessage(...)"
  "void sendTextMessage(...)"

The Source Code

- Apps must import certain packages in order to communicate with webservers:
  ”import java.net.*”
  ”import org.apache.http.*”
- Apps must use ContentResolvers to access databases on the device
  ”import android.content.ContentResolver”

Inherent Vulnerabilities of Android Apps

Methods of Combating Malware

Possible Solutions

Wrap Up

Monitoring Hardware Anomalies

1. Set a baseline usage/behavior

i.e. battery, CPU

2. Monitor Hardware Usage

performance slowing down
temperature increase
spike in CPU/RAM usage

3. Flag Apps

Apps that are using an unusually high amount of hardware resources will get flagged for the EDS

Proposed Solutions

Monitor Network/SMS Activity

Use an external server to develop a Exfiltration Detection/Prevention System based on existing IDS/IPS software such as Snort.

Modify Android OS

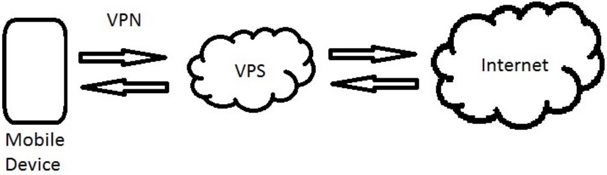
- Create shadow data based on encrypted device ID
- Limit applications' access to system/database resources [a]

[a] Hornyack, "These Aren't the Droids You're Looking For"

Implementation of Proposed Solutions

Steps

1. Establish VPN tunnel to VPS
2. Monitor the traffic (tcpdump)
3. Alert User



References

Michael Crider (2014)
The #1 New Paid App In The Play Store Costs $4, Has Over 10,000 Downloads, A 4.7-Star Rating... And It's a Total Scam
http://www.androidpolice.com/2014/04/06/the-1-new-paid-app-in-the-play-store-costs-4-has-over-10000-downloads-a-4-7-star-rating-and-its-a-total-scam/

Tony Bradley (2013)
Android Dominates Market Share, But Apple Makes All The Money
http://www.forbes.com/sites/tonybradley/2013/11/15/android-dominates-market-share-but-apple-makes-all-the-money/

References

Angel Alonso Parrizas (2013)
Monitoring Network Traffic for Android Devices
http://www.sans.org/reading-room/whitepapers/detection/monitoring-network-traffic-android-devices-34097

Peter Hornyack, Seungyeop Han, Jaeyeon Jung, Stuart Schechter, and David Wetherall (2011)
"These Aren't the Droids You're Looking For": Retroffiting Android to Protect Data from Imperious Applications
http://appfence.com/ccs210-hornyack.pdf

Special Thanks

Troy Stevens, Project Mentor

Staci Dorsey, MAC Program Coordinator

The End