

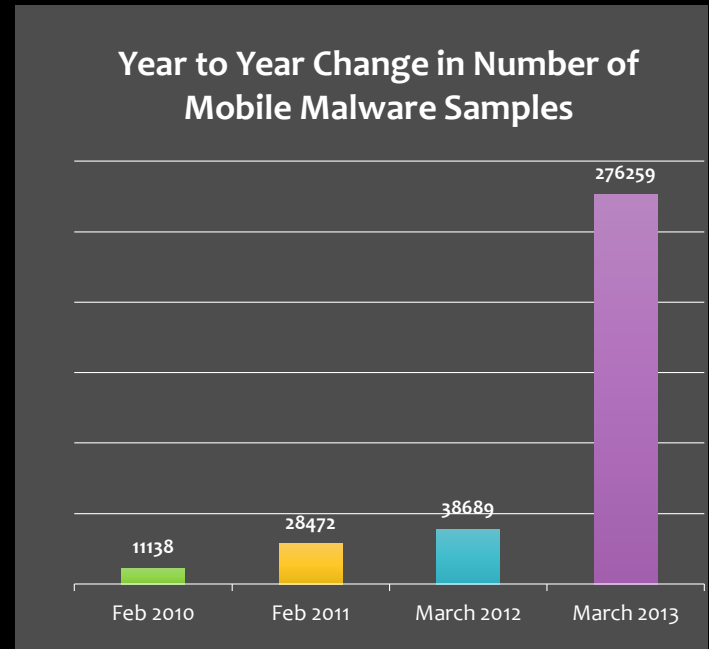
Mobile Malware and Spyware: Working Through the Bugs

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>



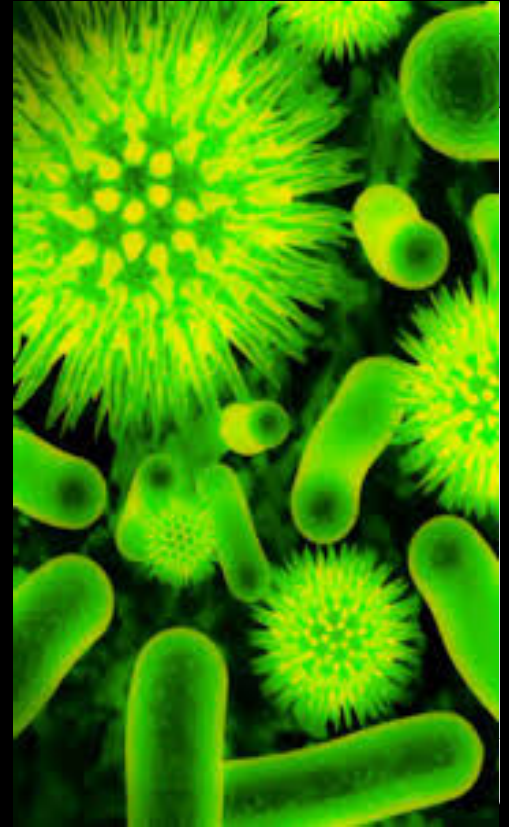
Types of Mobile Malware & Potentially Unwanted Applications

- 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 - Androids with outdated OS versions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



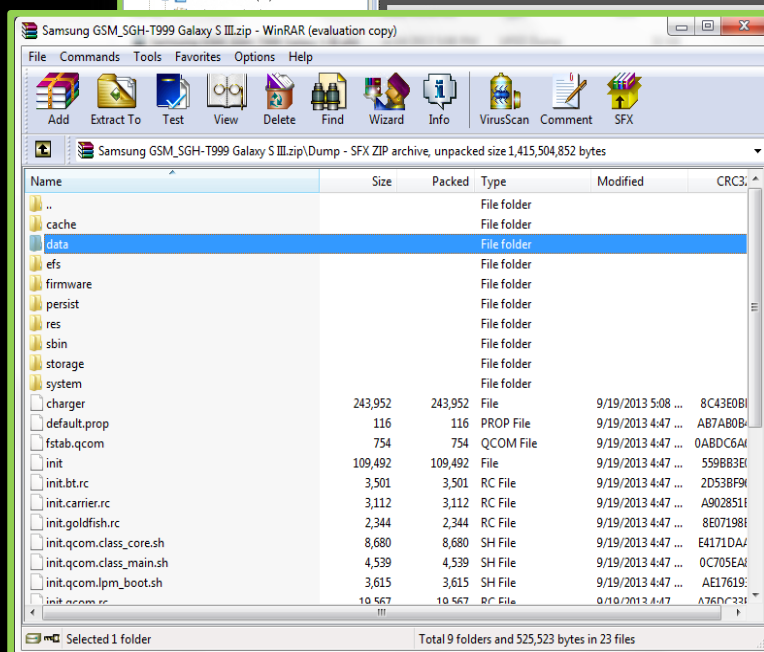
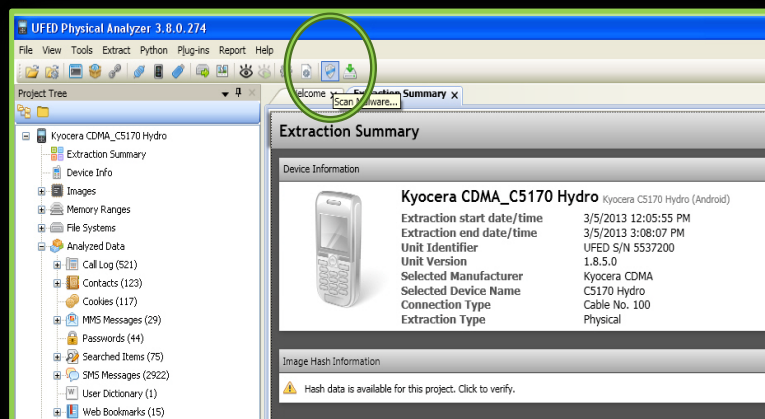
OUCH! ?

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

Malware Scanner (13)			
	_37_YO~1.JPG (Gen:Variant.Kazy.206505)	<input checked="" type="checkbox"/>	104
	flv_player_installer.apk (Android.Trojan.FakeInst.F	<input checked="" type="checkbox"/>	103
	Play_Movie-1.exe (Trojan.GenericKD.1014484)	<input checked="" type="checkbox"/>	58
	Play_Movie-2-1.exe (Trojan.GenericKD.1014531)	<input checked="" type="checkbox"/>	171
	Play_Movie-2.exe (Trojan.GenericKD.1014531)	<input checked="" type="checkbox"/>	128
	Play_Movie.exe (Trojan.GenericKD.1014484)	<input checked="" type="checkbox"/>	140
	Play_Video1054.exe (Gen:Variant.Kazy.206505)	<input checked="" type="checkbox"/>	211
	Play_Video1280-1.exe (Gen:Variant.Kazy.239970)	<input checked="" type="checkbox"/>	182
	Play_Video2890-1.exe (Gen:Variant.Kazy.206505)	<input checked="" type="checkbox"/>	177
	Play_Video3007.exe (Gen:Variant.Kazy.250089)	<input checked="" type="checkbox"/>	89
	Play_Video3062.exe (Gen:Variant.Kazy.206505)	<input checked="" type="checkbox"/>	20
	Play_Video4379.exe (Gen:Variant.Kazy.250089)	<input checked="" type="checkbox"/>	174
	Play_Video_Now.exe (Trojan.GenericKD.V.1071457;	<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171
		<input checked="" type="checkbox"/>	128
		<input checked="" type="checkbox"/>	140
		<input checked="" type="checkbox"/>	211
		<input checked="" type="checkbox"/>	182
		<input checked="" type="checkbox"/>	177
		<input checked="" type="checkbox"/>	89
		<input checked="" type="checkbox"/>	20
		<input checked="" type="checkbox"/>	174
		<input checked="" type="checkbox"/>	129
		<input checked="" type="checkbox"/>	104
		<input checked="" type="checkbox"/>	103
		<input checked="" type="checkbox"/>	58
		<input checked="" type="checkbox"/>	171

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!



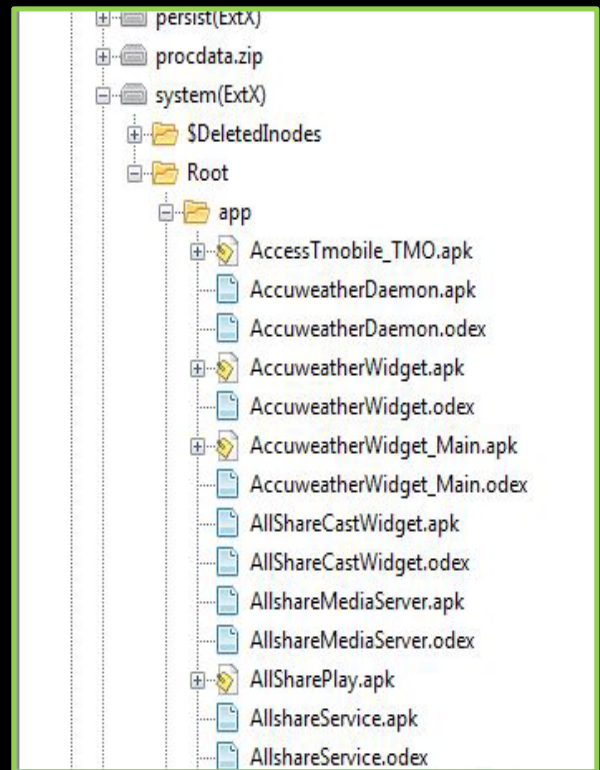
If you still suspect a problem...

- 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...

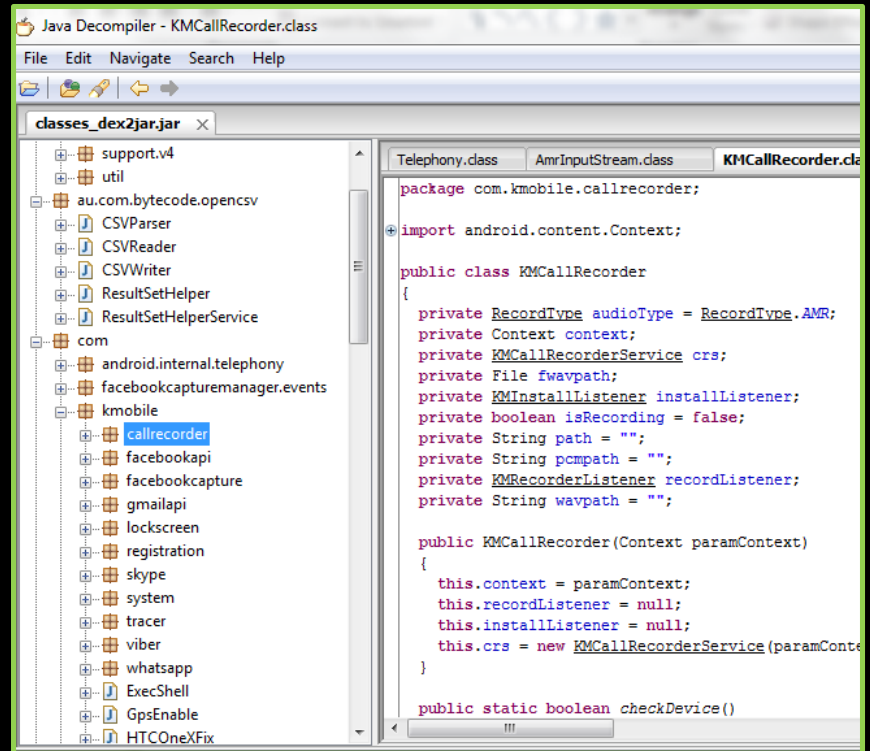
- **Root\App** folder contains downloaded .apk files
- Most .apk files will be legitimate applications
- Individual suspicious .apk files can be exported for further examination
- ANY .apk file can be unpacked and decompiled or submitted to a sandbox site for analysis



Mobile Malware Reverse Engineering & Analysis

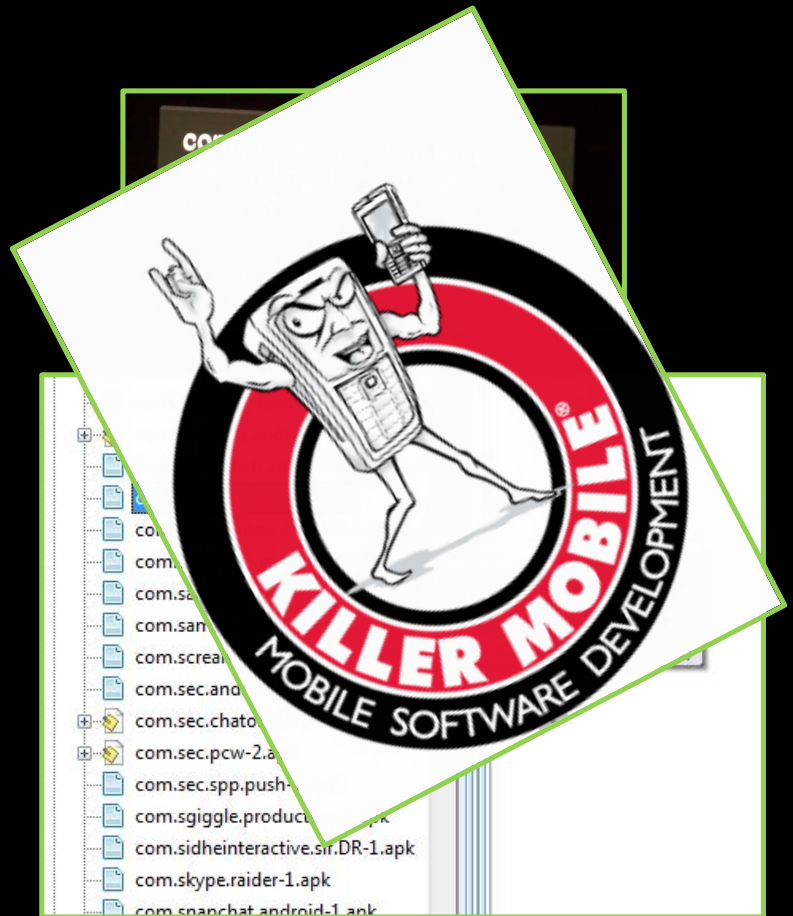
- Mobile Malware Analysis
& Reverse Engineering
Tools:

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



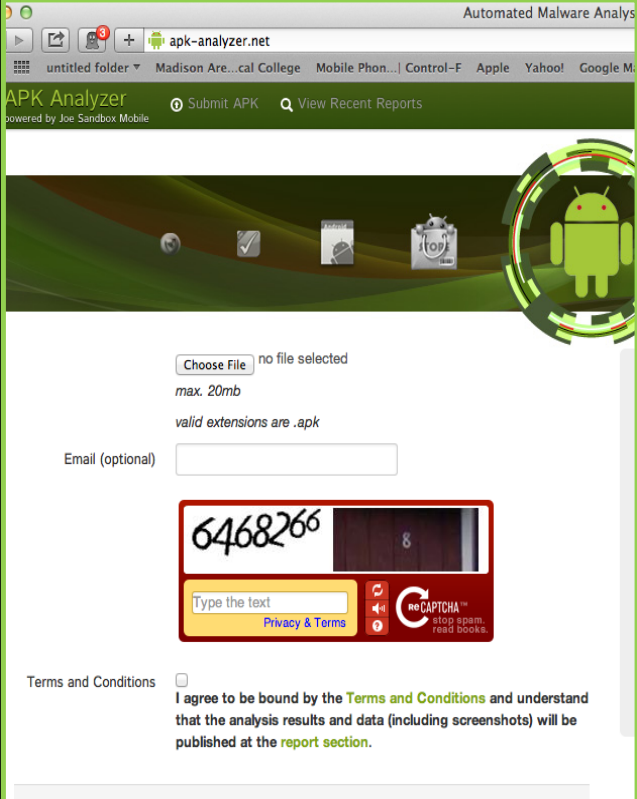
Locating Problem .apk files

- 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 address bar displaying '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 links for 'Submit APK' and 'View Recent Reports'. The interface includes a file upload section with a 'Choose File' button, indicating 'no file selected', a 'max. 20mb' limit, and 'valid extensions are .apk'. An optional email field is present. A CAPTCHA challenge is shown with the number '6468266' and a 'Type the text' input field. Below the CAPTCHA is a 'Privacy & Terms' link. At the bottom, there is a 'Terms and Conditions' checkbox and a paragraph stating: '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.



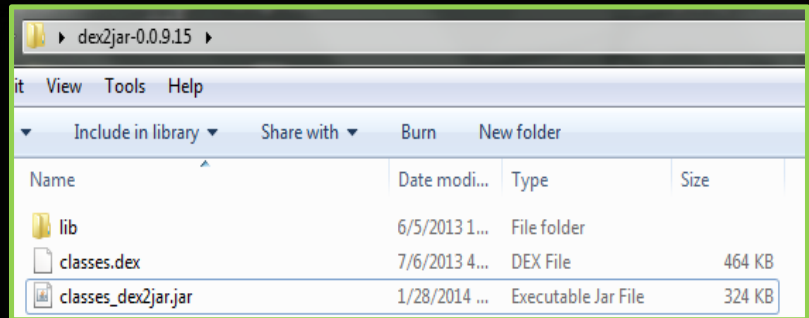
Static Analysis Step 2: “Decompiling” the .apk file

- 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



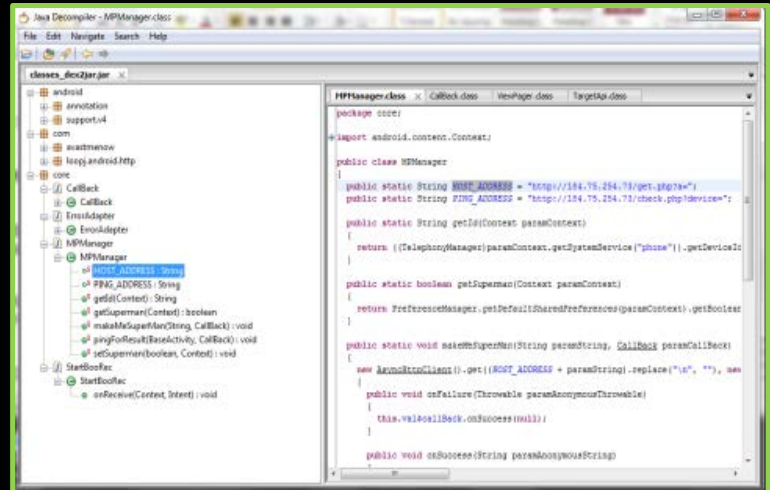
```
cmd Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

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
```



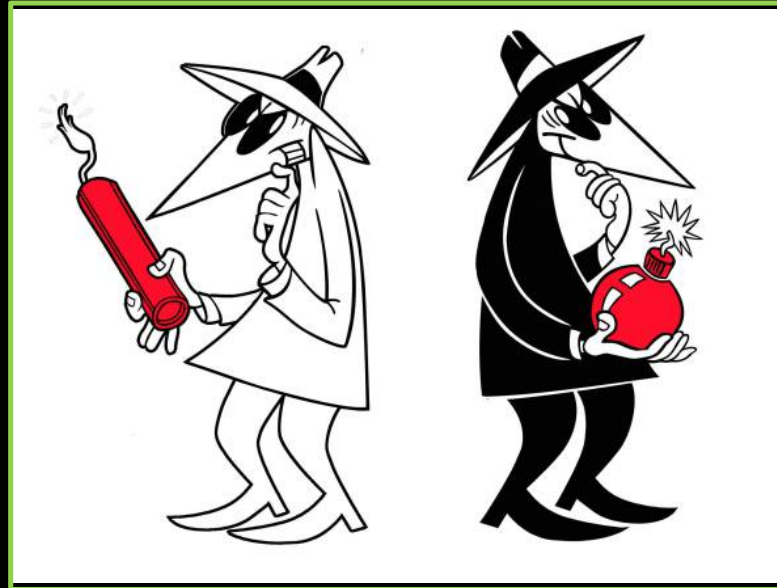
Static Analysis Step 3: Viewing Decompiled Code

- 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



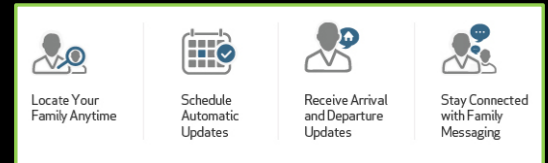
Mobile Spyware

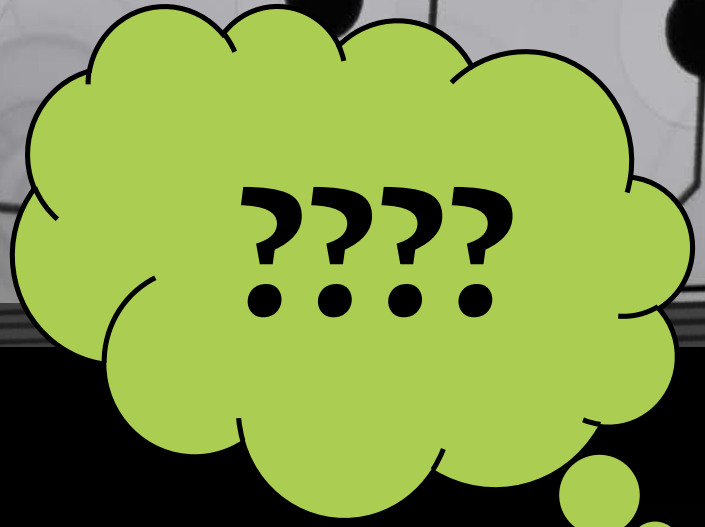
- Generally advertised for
 - Catching cheating spouses
 - Monitoring and protecting children
 - Monitoring employees
- Must have physical control of the target device to install
- Many, Many, Many varieties
 - mostly cheap or free
- Mobile malware scans may or may not detect the presence of spyware



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