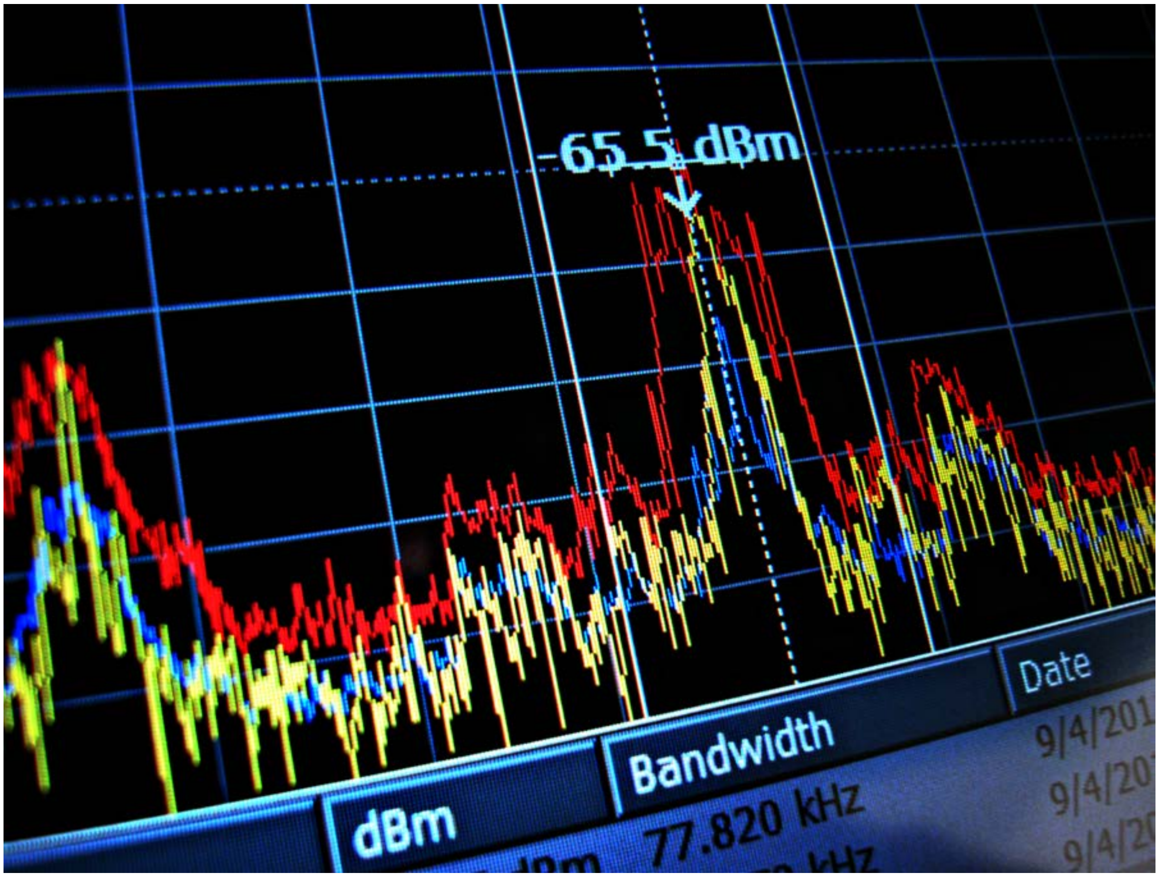
Smartphone Spyware Detection Clues

Report

PRIVILEGED & CONFIDENTIAL



Contents

Introduction 3

General Advice 4

iPhone 4

About Cydia 5

Android 6

Spyera 7

MobileSpy 7

FlexiSpy 8

Mobistealth 9

SpyBubble 10

mSpy 10

Phone Control 11

TeenSafe 11

iFunBox 12

PhoneSheriff 12

Introduction

The following are clues I have picked up about how to spot spyware on a smartphone. Since virus programs change frequently, understand that some of these clues may already be out of date. Please feel free to contribute to this document with additional clues and tips you may come across.

Provided free to the law enforcement community in appreciation for all you do.

Kevin D. Murray

General Advice

iPhone

- Look for items called **Cydia**, **MBackup, Pangu** or **Absinthe** which would indicate jailbreaking, the first step to installing any unauthorized app.

- Find invisible malware apps that loaded onto a non-jailbroken phone.
  These are apps that are tagged as "hidden" by a special developer tag, and can even be made to run in the background. For more information on this kind of malware, see the paper **Mactans: Injecting Malware into iOS Devices via Malicious Chargers**; Billy Lau, Yeongjim Jang, Chengyu Song, Tielei Wang, Pak ho Chung, Paul Royal; Georgia Institute of Technology; Black Hat 2013
  https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf

  To detect this kind of malware, download Apple's Xcode program onto your Mac (it's a free developer tool you can get from the Mac app store).

  1. Go to Window -> Organizer
  2. Click on the phone.
  3. Click on "Applications" under the phone.

  A list of applications loaded onto the phone should show up. Unlike iTunes, Xcode will also show you any applications that are marked as hidden.

- To delete spyware and return phone to normal operating condition reload the iOS software onto the phone.

  1. Attached phone to iTunes account.
  2. Click Restore iPhone to reload the current iOS. This reverses the “jailbreak” and deletes the spyware.
  3. Do not reload information from the back-up file. Start fresh.

- How a Galileo RCS mobile trojan infects an iPhone (which first requires the phone to be jailbroken). Non-jailbroken iPhones become jailbroken when an attacker runs a jailbreaking tool like ‘Evasi0n’ via a previously infected computer and conducts a remote jailbreak. The infection is then injected.

Recommendations

1. Do not jailbreak the iPhone.

2. Update, or reload, the phone's iOS to prevent old jailbreaking techniques, or reverse a current jailbreak.

About Cydia

q.v. - http://acisni.com/how-to-jailbreak-your-iphone-simple-guide/
How to jailbreak iOS 7.1-7.1.2 (using Pangu) or iOS 7.0-7.0.6 (using evasi0n7).
How to jailbreak iOS 6.0-6.1.6.

The following is from:
http://acisni.com/how-to-hide-the-cydia-app-icon-after-jailbreaking-iphone/

(Note: SBSettings not yet available for IOS 7.0+ as of 7/14/14.)

Open Cydia and search for an app called "SBSettings" – download and install it for free. This app can do a few things but all we are interested in is that it can hide app icons from the main home screen.

Once it is installed, open SBSettings and hit "settings" – "more" – "hide icons". You will see a list of all icons on the phone and beside them a slider you can set to ON or Off.

Find Cydia on the list and set the slider to OFF. Off means that the icon will be hidden.

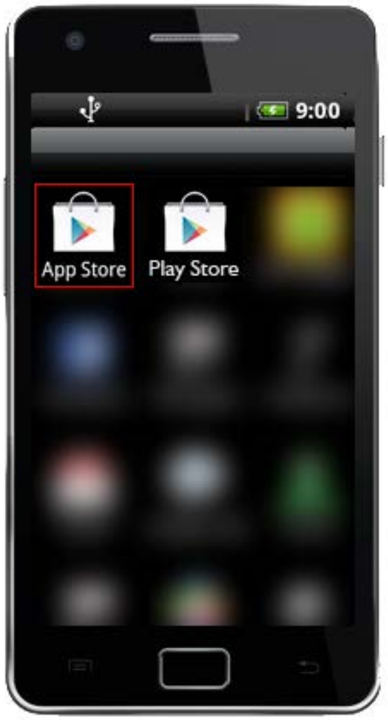
You can also hide the SBSettings app icon – just to be extra safe

That is it, the Cydia icon will be removed from the home screen but the app is not uninstalled. Hiding the Cydia App takes away the most obvious sign that the device has been Jailbroken and the person will be none the wiser.

Android

- **Android.DDoS.1.origin** creates an application icon, similar to that of Google Play. If the user decides to use the fake icon to access Google Play, (Google Play) will be launched, which significantly reduces the risk of any suspicion.

  The Trojan tries to connect to a remote server. It then transmits the phone number of the compromised device to criminals. Criminals then send it SMS commands.



Clues:
• Icon name and look is similar to Google Play.
• Reduced phone performance.
• Unwanted Internet and SMS service charges.
• Messages sent to premium numbers will be charged to the owner.
• General malicious activities.

Spread via social engineering tricks and as a disguised legitimate app.

Spyera

iPhone

- Look in a folder called “**Logs**” for a file called “**ownspy.log**”.
  (Note: This is a forensic examination procedure.)
- Assume there is an issue if the phone is jailbroken, especially if the owner did not do it.

Android

- Look in the SD card’s download folder for a file called “**Checkkey.XX.apk**”.
- Look for an image of the registration page called “**bookmark_thumb1**”.
- Look in the web history for “**http://spylogs.com/db**” and/or “**http://djp.cc**”.

  Note: These items are supposed to be deleted by the person installing the spyware, but this step is sometimes overlooked.

MobileSpy

iPhone

- Assume there is an issue if the phone is jailbroken, especially if the owner did not do it.

Android

- Look in the SD card’s download folder for “**ms5-−2.1-−above.apk**”.
- You can bring up the program’s interface by dialing **#123456789***.
- Also search for “**files/data/data/com.re=na22.ms6/MobileSpyData6.0.xml**” or similar. It shows the email address which is receiving your data.

FlexiSpy

iPhone

- Look for commands buried in received SMS messages. Commands are unique to avoid legitimate users sending commands to you by accident.
  Examples: “**HellO_**” or “**hI tHere_**” .

- Assume there is an issue if the phone is jailbroken, especially if the owner did not do it.

Android

- Look in the SD card’s download folder for “**FSXGAD_2.04.5.apk**” (or similar numbers)

- Look for an image of the registration page called “**bookmark_thumb1**”.

- Look for “**http://djp.cc**” in the web history file.

Note: These items are supposed to be deleted by the person installing the spyware, but this step is sometimes overlooked.

- Be alert to periodic warning messages like “**unknown**” has “**superuser access**.”

- You may receive and see command text messages (beginning with **<*#10>** or alternate number). Note: The stealth feature works on GSM network phones. These may not automatically delete on CDMA networked phones. (Verizon and Sprint).

- Try dialing ***#900900900** as a call to see if you can open the registration screen.

Mobistealth

iPhone

- Assume there is an issue if the phone is jailbroken, especially if the owner did not do it.

Android

- Look in the SD card's download folder for a file called "**mobistealthv2.apk**". Note: This item is supposed to be deleted by the person installing the spyware, but this step is sometimes overlooked.
- Look for a folder called "**LookOut.secure**", a name similar to the security software, in the directory "data/data."
- Look for "**loggedpictures.ser**". This is the file containing photos Mobistealth captures and uploads.
- Look for a "**configuration.xml**" file. It contains the spy's FTP information.

SpyBubble

iPhone

- Assume there is an issue if the phone is jailbroken, especially if the owner did not do it.

Android

- Look for a file called “**radio.apk**” in the subdirectory “**/mnt/sdcard/Download**”.
- In the subdirectory called “**data/data**/“ look for “**com.radioadv**” and folders containing “**secret.txt**” (the spyware’s actual PIN number) and “**buddy.txt**” (the mobile phone number of the controlling phone).
- Check the phone’s call log. Look for an entry showing the default PIN - **#999999***, or similar code starting with a hash symbol and ending with an asterisk.

mSpy

iPhone

- Dial #000* then press CALL, wait for few seconds to bring up mSpy’s user interface. This is the default code. May have been change by the spy.
- Assume there is an issue if the phone is jailbroken, especially if the owner did not do it.

Android

- Dial #000* then press CALL, wait for few seconds to bring up mSpy’s user interface. This is the default code. May have been change by the spy.

Phone Control

iPhone

- Assume there is an issue if the phone is jailbroken, especially if the owner did not do it.

Android

- To launch the application: use the phone dialer to dial **74283.** Press the call button.
- If the spy has enabled the "**Secure uninstallation**" option, any attempt to uninstall the application will fail. To uninstall the application Phone Control must be launched with its secret code. Then the disable option will work.
- To ensure a maximum discretion the spyware is designed so the ”**Phone Control**" and "**Phone Control Key**" applications do not show *their* names in the application manager. Both the applications respectively show up with the "**Android System**" and "**Android Service**" names, and a system icon similar to the one of Android system components.

TeenSafe

iPhone

- You need to know the Apple ID and password for the phone to check for the app in iTunes. Neither the app nor logo shows up on the iPhone.

Android

- Does NOT appear among the application icons. Look in files for “**TS MDM**”. If clicked **TS MDM** will ask for a username and password.
  Note: TeenSafe app must be downloaded from Google Play.

iFunBox

iPhone

- This is a media import/export app. It imports music, videos and photos to the standard iOS apps, and also export them to PC as backup copy. Possibly useful for some spyware tasks. Able to browse iPhones without passcode (limited file access).

PhoneSheriff

iPhone, iPad, iPod

- PhoneSheriff Investigator Edition is different in that you don't have to Jailbreak the Apple device to use it. All you need to do is purchase the Windows software with a one-time charge, install it onto your computer and login using your child's Apple ID and password.

  Nothing needs to be installed onto the device and your child does not see that it is being monitored. Just access the Apple device to enable the cloud storage and backup. Unlike other systems, your Apple ID and password are never sent back to us. That's handled on your own computer by the standalone program. Therefore your ID is never seen by any third party.

Countermeasure:
Keep Apple ID and password private. Change password periodically.

Notes: From Retina X Software (the makers of Mobile Spy.)
http://www.phonesheriff.com/investigator.html

Special Requests:

- If ***you*** come up with additional clues, let me know and I will include them.
- I sincerely appreciated being recommended to businesses and organizations who can benefit from my Electronic Surveillance Detection services (TSCM).
  Thank you in advance for doing so. ~Kevin

About the Author

Kevin D. Murray, CPP, CISM is an independent, professional security consultant. He has been solving electronic eavesdropping, security, and counterespionage matters since 1973 while with Pinkerton's Inc., and from 1978 to present at his consulting firm, Murray Associates.

He is the author of "Is My Cell Phone Bugged?"[1], the Android app SpyWarn™[2] and Kevin's Security Scrapbook - Spy News from New York[3] and Spycam Detection Training[4].

Murray Associates provides advanced eavesdropping detection (technical surveillance countermeasures, TSCM) and counterespionage consulting services to business, government, and at-risk individuals.

Contact:
Kevin D. Murray
Murray Associates
PO Box 668
Oldwick, NJ 08858 (USA)
+1-908-832-7900
800-635-0811
murray@counterespionage.com

[1] http://www.IsMyCellPhoneBugged.com

[2] http://www.SpyWarn.com

[3] http://spybusters.blogspot.com

[4] http://spycamdetection.training