spy vs. spy
examining spyware on mobile devices
michael robinson | christopher taylor
Introduction: The newest spy
Spyware can easily run on mobile devices.
It’s in malware and it’s commercially available.
Mobile malware up 273% in first half of 2011

Malware for smartphones and tablets is up 273% in the first half of 2011, compared with the same period in 2010, a study has shown.

Research from G Data Security Labs shows cyber criminals are increasingly targeting mobile devices, with cross-platform Trojans dominating the malware landscape.

In the first half of 2011, researchers recorded one new malware strain every twelve seconds on average. G Data believes there is no end in sight to this malware flood.

"With mobile malware, cyber criminals have discovered a new business model," said Eddy Willems, security evangelist at G Data.

Even though this special underground market segment is still being set up, there is an enormous risk potential for mobile devices and their users, Willems said.

NickiBot Spyware

- Spyware (GPS monitoring, sound recording, call logs, e-mail uploading)
- Fully controlled by SMS messages
- Appears as “Android System Log” under installed applications

(See www.csc.ncsu.edu/faculty/jiang/NickiBot.)
Soundminer
- Monitors phone calls (voice and keypad)
- Sends credit card data over the network
- Paired app with another Trojan
F-Secure: Photoscraping for harassment and blackmail.
Does Your Smartphone Need Anti-Virus Protection?

After hearing about what happened to Scarlett Johansson it seems like everyone is talking about what they can do to keep the private data on their smartphone private. While it is important to follow best practices, it might be time, depending on which OS you rock on your smartphone, to consider adding an extra level of protection.

Commercialization of spyware
BlackBerry Spyware

Monitor, Trace and Track BlackBerry Smartphones

BlackBerry Spyware Spyphone Software

BlackBerry Spy technology delivers find out the specifics as to what people are saying on their Android as well as who they really are talking to. Trace BlackBerry Phone Calls, Track BlackBerry Location; and determine what is in SMS texts and email; find out internet activity; and a whole lot more. With BlackBerry Mobile Phone Spy Software programs you may even cell phone tap to listen to smartphone calls and spy call transform the smartphone right into a covert bug device. The BlackBerry operating system is particularly popular with mobile device software developers and normally BlackBerry Spy applications are packed with features unavailable with other systems; making BlackBerry Spy software powerful as solutions to Parental Monitoring, Workforce Monitoring and uncovering Cheating.

Go to Phone Monitoring Websites

Compare Phone Monitoring Software

BlackBerry Spy

Monitoring and Tracking applications is designed for most type of BlackBerrys but there are a few limitations — if you’re looking to capture a history of Website Visits or Check MMS multi-media messages (images, music and video), unfortunately BlackBerry will not support keeping track of that. BlackBerry Tracker, Review SMS Texting & E-mail, Call Event Logging, Cell Phone Tap Calls and much more.

Go to Phone Monitoring Websites

Compare Phone Monitoring Software
Did you catch the list of compatible devices?
And this is the short list.
Some commercial versions don’t require rooting of the phone.*

* iPhones need to be jailbroken.
So what does it do?
Commercial spyware may capture:

<table>
<thead>
<tr>
<th>SMS activity</th>
<th>Inbound/outbound call logs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location/GPS coordinates</td>
<td>Browser activity (URLs)</td>
</tr>
<tr>
<td>Pictures</td>
<td>E-mail</td>
</tr>
<tr>
<td>Videos</td>
<td>Identify SIM card changes</td>
</tr>
</tbody>
</table>
Interactive mode may include:

- Taking pictures
- Recording videos
- Record conversations/background via calls
- Wiping the phone
- Viewing the target phone’s screen
Harvested data sent back to a server.
For example:
## List of Text Messages

### SMS History

<table>
<thead>
<tr>
<th>Phone</th>
<th>SMS Type</th>
<th>ALL</th>
<th>Sort By</th>
<th>SMS Date/Time</th>
<th>Order</th>
<th>Descending</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Download in CSV**
- **Current Page**: All Pages
- **SMS Type**: Received, Sent

### List of Functions

- Account Home
- Add New Phone
- View Phones
- Installation Guide
- Blackberry Messenger
- Configurations
- How Spy Call Works
- Invoices
- Update Profile
- Change Password
- Logout

- Calls History
- SMS History
- Contacts
- Appointments History
- Internet Browsing History
- Bookmarks History
- Emails History
- Messenger Chat History
- Recent Location
- Location History
- Calls Recording History
- Surround Recording History
- Pictures History
- Videos History
GPS Coordinates
(Actually cell phone towers)
<table>
<thead>
<tr>
<th>Phone</th>
<th>Observed Number</th>
<th>Stealth Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>700</td>
<td>2012-05-22 17:10:06</td>
<td></td>
</tr>
<tr>
<td>703</td>
<td>2012-05-21 17:50:18</td>
<td></td>
</tr>
<tr>
<td>571</td>
<td>2012-05-20 15:53:38</td>
<td></td>
</tr>
<tr>
<td>419</td>
<td>2012-05-20 13:44:06</td>
<td></td>
</tr>
</tbody>
</table>

Recorded phone calls
Alerts can be sent to a monitoring phone via SMS directly from target or from the website.
Commands can be sent to the target phone via the observing phone or website.
Principle differences between malware and commercial versions:
Attack vector
(delivery method)

Logging
Installation

• Physical access: required.
• Android rooting: not always required.
• iPhone Jailbreaking: required.
• Internet connection: required.
• Ability to install apps from unknown sources.: required
• Device may need to be rebooted.
The **BIG** question:
How do you know if you’ve been PWN’d?
You wouldn’t know, would you?
Spyware is “undetectable.”

Q: Will other people know that SpyBubble is installed or running on the mobiles I provide them with?
A: No, there is no icon or symbol that shows the status of SpyBubble on the screen of the mobile.

Will users know MobiStealth is installed or running?
MobiStealth uses the latest innovations in mobile monitoring to keep your monitoring safe and secure. There are no indications that MobiStealth is running while it is active. It runs in completely stealth mode.

Will users know Mobile Spy is installed or running?
Mobile Spy uses the latest innovations in mobile monitoring to keep your monitoring safe and secure. There are no indications that Mobile Spy is running while it is active. The program has no entries in the User Menu, and its files are extremely discreet. Best of all, when Mobile Spy is running, there is NO entry for it in the Task Manager. So it is your responsibility to notify any user they are being monitored.
Here’s what we did:
We forensically examined smart phones infected with different commercial spyware products.
HTC Wildfire S (rooted) on T-Mobile

LG Optimus Elite on Virgin Mobile

LG Optimus V on Virgin Mobile

Samsung Galaxy Prevail on Boost/Sprint

Apple iPhones 4s (jailbroken) on T-Mobile
LEGAL DISCLAIMER

Get the facts and understand your liability

Flexispy Ltd. Full Legal Disclaimer

Updated 2011

In some areas it may be a Federal or State offense to install software onto a phone you do not own, without the owner's awareness & consent. We do not condone the use of our software for any illegal purpose. By purchasing, downloading or using our software in any way, form or fashion, you acknowledge & approve the following:

1. You represent that FlexiSPY will be used exclusively in a lawful manner. If you're in doubt as to the legality of your planned usage we require you consult with a registered attorney for the jurisdiction where you intend to use FlexiSPY.

2. You acknowledge you own the mobile phone you will install the software on, or have consent from the owner to administrate the device & install software onto it.

3. FlexiSPY Ltd will never release any of your private information or account data for any reason whatsoever, EXCEPT under threat of legal action or court order. If you use our software to commit a crime & a warrant or subpoena for records is issued by court order as part of an ongoing investigation, we are legally bound to comply. This may include the release of purchase information or other customer data as ordered by a judge.

4. You acknowledge that you are solely responsible for how you use the software, & for complying with all relevant laws in your area. You also acknowledge that neither FlexiSPY Ltd, nor any of its agents, affiliates, directors, employees & associates may be held liable, responsible or accountable for any type of damage, litigation or other legal action, which may arise either from your legal or illegal use of FlexiSPY software, websites, or any other software & under no circumstances will you be eligible for any form of compensation from the aforementioned.
End User License Agreement

End User License Agreement (EULA)

It may be a federal and/or state offense to install monitoring/surveillance software onto a Phone/Computer which you do not own or have proper authorization to install. It may also be an offense in your jurisdiction to monitor the activities of other individuals. Check all state, federal and local laws before installing any Monitoring Software such as MobiStealth. You may also have to notify a person that they are being monitored if they are over age 18. Federal or local law governs the use of some types of software; it is responsibility of the user to follow such laws.


In Section 1030(e), CFAA provides that "any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. 1030(e). CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." Id. at § 1030(e)(6); CFAA defines "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." Id. at § 1030(e)(11).

"It is the responsibility of the user to determine, and obey, all applicable laws in their country and/or local jurisdiction regarding the use of the software and services. The software and service is intended to provide the Licensee with the ability to capture, store and control their own access to information.

Installing MobiStealth, you represent that MobiStealth will be used in only a lawful manner. Logging other people's Call Phone or Computer data or installing MobiStealth on another person's Phone/Computer without their knowledge can be considered as an illegal activity in your country. MobiStealth assumes no liability and is not responsible for any misuse or damage. It is the final user's responsibility to obey all laws in their country and/or State.

Regardless of the state, it is almost always illegal to record a conversation to which you are not a party, do not have consent to tape, and could not naturally overhear. Federal law and most state laws also make it illegal to disclose the contents of an illegally intercepted call or communication.

Federal law and most state laws also make it illegal to disclose the contents of an illegally intercepted call or communication.

We do not manage the data, nor control distribution of data, nor access personal data captured or stored on servers and databases we provide. We cannot, and have no responsibility to, access, recover, retrieve or read any data or information captured by Licensee or other party use of the software and service. The publisher and vendor make no warranty, assume no liability, and are not responsible in any way for any misuse or damage caused by using the software or services. The software user must accept all risk and liability for use. Use of the software and service constitutes acceptance of these terms & conditions and grants indemnification of the software supplier. All trademark, copyright images and trademarks displayed on this website are property of their respective owners.

Refund Policy

1. If there is any issue with functionality of MobiStealth on your Phone/Computer then we shall work with you to resolve the issue. If issue cannot be resolved only then a refund will be issued. Customer is required to report the issue within 10 days of purchasing MobiStealth.
2. Customer bears the responsibility of installation of software on the target Phone/Computer that needs to be monitored. In the event a purchase is made under the false assumption that physical access is not needed to install the software on the target/monitored Phone/Computer, MobiStealth is not liable to issue any refund.
Disclaimer: SpyBubble is a Mobile Phone Spy Software, basically designed for monitoring your spouse, children or employees having Smartphone. Either you should own the phone or you should have permission to monitor from the user of smartphone.

If you fail to comply, depending on federal and state laws, you could be breaking the law. The SpyBubble will allow you to monitor Mobile phones as a tool NOT for illegal purposes. Use only at your discretion. The use of the software is done at your own discretion and risk and with agreement that you will be solely responsible for any damage to your Mobile or loss of data that results from such activities. No advice or information, whether oral or written, obtained by you from us or from the SpyBubble web site shall create any warranty for the software. In addition, you agree to hold harmless the publisher and authors personally and collectively for any losses of relationships, capital (if any) that may result from the use of this application. Your use of SpyBubble like other software agreements, indicates your acceptance of these disclaimers.

NOTE: All trademarks on this site are property of their respective owners. These companies are not affiliated with SpyBubble.com in any way. Mentioned trademarks are used solely for the purpose of describing phone and carrier compatibility for our mobile phone spy software.
User Legal Agreement
Information regarding our products and services.

All users are required to accept these terms as well as the terms located on the Legal Information page when creating your account and upon purchase.

It is a federal and state offense to install surveillance software onto a device which you do not have proper authorization.

We absolutely do not condone the use of our software for illegal purposes.
In order to purchase our software you MUST agree to the following conditions.

1. You acknowledge and agree that you own the device you will install the software onto OR that you have the expressed written consent of the owner to be an authorized administrator of the device and its users.

2. If you install our software onto a phone which you do not own or have proper consent, we will cooperate with law officials to the fullest extent possible. This includes turning over requested customer data, and any other purchase/product related information.

3. You agree that you will check all local, state and federal laws to make sure you are complying with all laws in your region. It may be illegal in your region to monitor other individuals on your own device. You will never monitor any adult without their valid permission.

4. You agree to the conditions in our EULA (End-User License Agreement). This includes the fact that we are not liable for any type of damage, litigation, or legal predicaments that may arise due to use or abuse of Mobile Spy or any other product.

5. All logs are subject to deletion after thirty (30) days for maintenance purposes.

© 2002-2011 Retina-X Studios, LLC. All rights reserved.
End User License Agreement

NOTICE TO USER: PLEASE READ THIS CONTRACT CAREFULLY. BY USING ALL OR ANY PORTION OF THE SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT

1. The user hereby undertakes to use the software responsibly and obey all applicable laws in which ever jurisdiction the software is operating.

2. The user understands that the Server side data is held for the purposes of downloading to their own systems and that this should be done on a regular basis and at least every seven (7) days. If data is not downloaded within this period Spyera reserve the right to permanently delete it.

3. The user explicitly indemnifies Spyera for any harm financial or by reputation that may arise as a result of the misuse of this software.

4. Intellectual Property Rights. The Software and any copies that you are authorized by Spyera to make are the intellectual property of and are owned by Spyera Software LLC (Hong Kong). The Software is protected by copyright, including without limitation by international treaty provisions and applicable laws in the country in which it is being used. You may not copy the Software, you may however transfer the license from one phone to another providing the original device is first deactivated. You agree not to modify, adapt or translate the Software. You also agree not to reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software without the express written permission of Spyera. This Agreement does not grant you any intellectual property rights in the Software.

5. Transfer. You may not rent, lease, sublicense or authorize all or any portion of the Software to be copied onto another users phone except as may be expressly permitted herein. You may, however, transfer all your rights to use the Software to another person or legal entity provided that:
(a) you also transfer this Agreement to such person or entity;
(b) you retain no copies, including backups and copies stored on a computer; and
(c) the receiving party accepts the terms and conditions of this Agreement and any other terms and conditions upon which you legally purchased a license to the Software.

6. It is the responsibility of the user of Spyera to ascertain, and obey, all applicable laws in their country in regard to the use of Spyera for “sneaky purposes”. If you are in doubt consult your local attorney before using Spyera. By downloading and installing Spyera, you represent that Spyera will be used in only a lawful manner. Logging other people’s SMS messages & other phone activity or installing Spyera on another person’s phone without their knowledge can be considered as an illegal activity in your country. Spyera assumes no liability and is not responsible for any misuse or damage caused by our Software. It’s final user’s responsibility to obey all laws in their country. By purchasing & downloading Spyera, you hereby agree to the above.
Forensic Tools
URL history
Title: FlexiSPY Product Download
URL: http://djp.cc

Cookie
Name: JSESSIONID
Domain: djp.cc

Search of physical dump
http://djp.cc/checkkey?key=06107769107469&Submit=Download.FSXGAD_2.03.3.apk/mnt/sdcard/download/FSXGAD_2.03.3.apkapplication/vnd.android.package-archive

SD Card
\download\FSXGAD_2.03.3.apk
ATTRIBUTION!
Registration Key (in the picture)

/support@flexispy.com

/bookmark_thumb1/s7ea2c639.jpg
A couple of glitches...

On the version we tested, we noticed:

• Messages appeared periodically that “unknown” obtained “superuser access.”

• The software didn’t always launch on reboot.

• On CDMA phones, stealthy messages sent to the target phone appeared to the user, i.e., they were not stealthy.

• Stealthy phone calls did not work on CDMA phones.

Note: A new version of the product has since been released.
152 Running Apps

Superuser
(Evidence of rooting)
/data/system/usagedata/usage-20120207 contains a reference to: “com.android.msecurity”
Hidden SMS command: 

<#*50>

Confirmation of response sent to remote system:

Software version PROX
getMobileDataEnabled: true

Confirmation of Connection
Starting process: com.slacker.radio
Includes PID

Monitoring other services, e.g., charging.

/data/misc/dm/logcat
Calls to several daemons:
- com.fx.callmgrd.CallMgrDaemon
- com.fx.pmon.MonitorDaemon
- com.fx.main.MainDaemon

Database maintenance:

Library loading:
/data/misc/dm/libexec.so
Image5 (mtd5_userdata.bin)

Deleted log data found.
01-31 17:59:11.043: WARNING/SimChangeThread(514): verifySim # Previous subscriber ID: 3102

01-31 17:59:12.428: WARNING/SimChangeThread(514): verifySim # Current subscriber ID: 3102

01-31 17:59:12.897: WARNING/SimChangeThread(514): verifySim # SIM is not changed..

01-31 18:18:20.805: WARNING/SocketSmsThread(514): Found a new SMS.

01-31 18:18:20.837: WARNING/SocketSmsThread(514): SMS Command is detected! -> Hide..

01-31 18:18:20.890: WARNING/SocketSmsThread(514): Forward SMS: false..

01-31 18:18:20.909: WARNING/SmsCommandManager(85): processSmsCommand # +1571<#87>0861077<#87>CD>..

01-31 18:18:22.783: WARNING/EventDatabaseManager(84): countTotalEvents # TYPE_CALL: 2, TYPE_SMS: 0, TYPE_EMAIL: 0, TYPE_LOCATION: 0, TYPE_IM: 0, TYPE_SYSTEM: 8, Total: 10.

01-31 18:18:22.808: WARNING/EventManager(84): processNumberOfEvents # Number of events: 10 / 10..

01-31 18:18:22.880: WARNING/EventManager(84): processNumberOfEvents # Request deliver all events..

01-31 18:18:23.294: WARNING/EventDatabaseManager(84): countTotalEvents # TYPE_CALL: 2, TYPE_SMS: 0, TYPE_EMAIL: 0, TYPE_LOCATION: 0, TYPE_IM: 0, TYPE_SYSTEM: 8, Total: 10

**/*


01-31 12:29:11.093: WARNING/SocketSmsThread(584): Set keywordId: ""


01-31 12:29:11.152: WARNING/SocketSmsThread(584): Set keywordId: ""

01-31 12:29:11.205: WARNING/SocketSmsThread(584): Set keywordId: ""

01-31 12:29:11.292: WARNING/SocketSmsThread(584): Set keywordId: ""


01-31 12:29:11.364: WARNING/SmsCommandHelper(85): WL StatusWatch all number..


01-31 12:29:11.659: WARNING/SocketSmsThread(584): Set keywordId: ""

01-31 12:29:11.716: WARNING/SocketSmsThread(584): Set keywordId: ""

**/*
01-31 17:59:11.043: WARNING/SimChangeThread(514): verifySim # Previous subscriber ID: 3102...
01-31 17:59:12.426: WARNING/SimChangeThread(514): verifySim # Current subscriber ID: 3102...
01-31 17:59:12.897: WARNING/SimChangeThread(514): verifySim # SIM is not changed..
01-31 18:18:20.837: WARNING/SocketStmcSms(514): SMS Command is detected! -> Hide..
01-31 18:18:20.890: WARNING/SocketStmcSms(514): Forward SMS: false..
01-31 18:18:20.909: WARNING/SmsCommandManager(85): processSmsCommand # [1571]...<"#87>
01-31 18:18:22.753: WARNING/EventDatabaseManager(84): countTotalEvents # TYPE_CALL: 2, TYPE_SMS: 0, TYPE_EMAIL: 0, TYPE_LOCATION: 0

ATRIBUTION!
Controlling Number

01-31 12:29:11.093: WARNING/SocketStmcSms(584): setKeyword1: ""
01-31 12:29:11.323: WARNING/SocketStmcSms(584): setMonitorNumber: "+1571..."
URL history
http://www.spybubble.com/android/adv/radio.apk

downloads.db entry
uri: http://www.spybubble.com/android/adv/radio.apk
hint: radio.apk
_data: /mnt/sdcard/Download/radio.apk

(Phone not shipped with an SD Card.)
Outgoing call log #999999*

There was an error with the operation of the software.

This should not appear in the log.

This number can be changed. Regardless of the number, it will start with # and end with *.
When SpyBubble is installed, it automatically sends an SMS from the target phone to the observer.

This text appears in blk0_mmcblk0.bin: “this phone is now having Radio installed in it and has added you as the observer”

This text found here is identical to the SMS message. The phrase appears in different languages before and after the English version.
data/data/com.radioadv
/databases
/files
/shared_prefs
InCallRecording: enable
OutCallRecording: enable
AutoEnvRec: enable
AutoLivePic: enable
AutoLiveVideo: enable
AutoEnvRecDur: 120
AutoEnvRecInterval: 0.5
AutoLivePicInterval: 2
AutoLiveVideoInterval: 3
TrackMode: WebCallTrack: enable
DataTrack: enable
LocationTracking: enable
GPSINT: 15
UrlTrack: enable
PhotoUpload: enable
ContactUpload: enable
CalendarTrack: enable
ATTRIBUTION!

**buddy.txt**

Cell phone number for remote control
Pin: 999999
ATTRIBUTION!
serial.txt
Serial number for this purchase
<?xml version='1.0' encoding='utf-8' standalone='yes'?>
<map>
  <long name="LastCall" value="1337648857776"/>
  <long name="LastIncomingSMS" value="1337648486047"/>
  <long name="LastHeartBeat" value="1337647996962"/>
  <string name="OutCallRecordConfig">MR-1,1,1</string>
  <long name="LastURL" value="1337649293803"/>
  <long name="LastPhonebook" value="1337648219159"/>
  <long name="LastSMS" value="1337647927461"/>
  <long name="LastPhoto" value="1337648720000"/>
  <string name="InCallRecordConfig">MR-1,1,1</string>
  <long name="LastEnv" value="1337686404056"/>
  <boolean name="State" value="true"/>
  <long name="LastOutgoingSMS" value="1337648503040"/>
  <long name="LastHeartBeatRecorder" value="1337688158849"/>
  <long name="LastLiveVideo" value="1337681859237"/>
  <long name="LastLivePic" value="1337687259195"/>
  <long name="LastCalendar" value="1337648885027"/>
</map>
Live capture pictures:

Retrieved from the website.

Not recovered from the phone.

The phone was in my pocket. Not that useful.

The phone was in my hand. The raw photo does not focus.
Table: exception_blobs

/mpt/MPT_MainData.db

com.radioadv.CameraActivity$Preview.surfaceChanged
(CameraActivity.java:132)
ANR in com.radioadv
Reason: Executing service com.radioadv/.LivePicService
Load: 12.16/16.72/15.64
CPU usage from 16515ms to 0ms ago:
1% 4261/com.radioadv: 1% user + 0% kernel / faults: 145 minor

Table: exception_blobs

/mpt/MPT_MainData.db
<table>
<thead>
<tr>
<th>pkg_name</th>
<th>install_time</th>
<th>delete_time</th>
<th>last_version</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.radioadv</td>
<td>133764770715</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table: app_history

/mpt/MPT_MainData.db

Mon May 21 2012 20:48:27 GMT-0400 (EDT)

Pkg Name: com.radioadv  Install Time: 133764770715
Table: acc_recent_activity

pkg Name: com.radioadv

/mpt/MPT_MainData.db
Table: acc_usage

Pkg Name: com.radioadv
Pid: 666
uid: 10079
URL history
  http://www.mobistealth.com/asset/mobistealthv2.apk

downloads.db entry
  uri:     http://www.mobistealth.com/asset/mobistealthv2.apk
  Hint:    mobistealthv2.apk
  _data:   /mnt/sdcard/download/mobistealthv2.apk

SD Card
  \download\mobistealthv2.apk
84 Running Apps

LookOutSecure
Attribution!
• Trigger word: “location”
• Source phone number
Attribution!
• Trigger word: “location”
• Source phone number
data/data/lookOut.Secure/files/debugLog
Names of Services & Functions:
- debugLog
- Location:
  - Lat: 36.145
  - Long: -115.324

“Service is already running”
- data/data/lookOut.Secure/files/debugLog
Location (Lat 36.145, Long -115.32444444444444) matches one of the addresses listed. Identical value recovered from the phone.

Locations are based on cell phone towers.

Actual location was nearby.
List of pictures that have been uploaded.

data/data/lookOut.Secure

files

loggedpictures.ser
The MD5 hash of this downloaded file matches the MD5 hash of the picture stored on the phone.
Contents:

- IMEI
- FTP connection information
- CDMA
- Phone Model

Attribution!
FTP credentials (names and passwords)
URL history
  http://asd-ms.com/ms5-a/ms5-2.1-above.apk

downloads.db entry
  uri: http://asd-ms.com/ms5-1/ms5-2.1-above.apk
  Hint: ms5-2.1-above.apk
  _data: /mnt/sdcard/download/ms5-2.1-above.apk

SD Card
  \download\ms5-2.1-above.apk
A couple of glitches...

On the version we tested, we noticed:

- E-mail alerts were sent back to a monitoring e-mail address; however, no data appeared on the website.

- After installation, the battery life dropped to 8-10 hours from nearly 20 hours.

- The website requires the user to update his/her password. As a result, the password stored on the device needs to be updated, which means physical access is required again.
Installed applications are listed in:
/data/data/com.sprint.zone/databases/zone.db

Package: com.retina22.ms6
Name: Android Toolkit
Date: 21 May 2012 11:06:57 PDT
Version: 5.0

Incidentally, “Seizure Service” is Paraben’s Device Seizure.
Package: com.re=na22.ms6
Name: Android Toolkit
Date: 21 May 2012 11:06:57 PDT
Version: 5.0
/data/system/Packages.xml has a list of installed apps and the set of permissions.
/data/data/com.retina22.ms6
/databases
/shared_prefs
<?xml version='1.0' encoding='utf-8' standalone='yes'?>
<map>
  
  <boolean name="KEY_IS_GPS_INFO_CMD" value="true"/>
  <boolean name="KEY_CELLID_LOG" value="true"/>
  <int name="KEY_GPS_INTERVAL" value="15"/>
  <string name="KEY_USER_NAME">Prevail</string>
  <long name="KEY_SMS_ID" value="12"/>
  <long name="KEY_PICTURE_ID" value="2"/>
  <boolean name="KEY_IS_EMAIL_GPS" value="true"/>
  <string name="KEY_EMAIL_ID">michaelkirbyrobinson@gmail.com</string>
  <boolean name="KEY_IS_SIM_CHANGE_NOTIFICATION" value="true"/>
  <boolean name="KEY_IS_EMAIL_ALERT" value="true"/>
  <boolean name="KEY_IS_EMAIL_REPORT" value="true"/>
  <int name="KEY_XML_UPLOADER_TIME" value="30"/>
  <boolean name="KEY_LOCK_LOG" value="true"/>
  <long name="KEY_LAST_REPORTING_TIME" value="1337649226670"/>
  <boolean name="KEY_IS_SIM_INFO_CMD" value="true"/>
  <string name="KEY_IMSI_NUMBER">310007038550995</string>
  <boolean name="KEY_IS_EMAIL_SMS" value="true"/>
  <boolean name="KEY_IS_ACTIVE" value="true"/>
  <boolean name="KEY_WIPE_LOG" value="true"/>
  <long name="KEY_CONTACT_ID" value="8"/>
  <int name="KEY_ACCOUNT_PULLER_TIME" value="345"/>
  <boolean name="KEY_IS_EMAIL_CALL" value="true"/>
  <boolean name="KEY_GPS_LOG" value="false"/>
  <string name="KEY_FRIEND_NUM">4109409782</string>
  <boolean name="KEY_IS_EMAIL_URL" value="true"/>
  <long name="KEY_CALL_ID" value="7"/>
  <boolean name="KEY_IS_FIRST_TIME" value="false"/>
  <int name="KEY_EMAIL_INTERVAL" value="15"/>
  <string name="KEY_USER_ID">100062555</string>
  <boolean name="KEY_IS_LIVE_PANEL" value="true"/>
</map>

Attribution!
Email ID
(Monitoring Address)
<?xml version='1.0' encoding='utf-8' standalone='yes'?>
<map>
  <boolean name="KEY_IS_GPS_INFO_CMD" value="true" />
  <boolean name="KEY_CELLID_LOG" value="true" />
  <int name="KEY_GPS_INTERVAL" value="15" />
  <string name="KEY_USER_NAME">Prevail</string>
  <long name="KEY_SMS_ID" value="12" />
  <long name="KEY_PICTURE_ID" value="2" />
  <boolean name="KEY_IS_EMAIL_GPS" value="true" />
  <string name="KEY_EMAIL_ID">michaelkirbyrobinson@gmail.com</string>
  <boolean name="KEY_IS_SIM_CHANGE_NOTIFICATION" value="true" />
  <boolean name="KEY_IS_EMAIL_ALERT" value="true" />
  <boolean name="KEY_IS_EMAIL_REPORT" value="true" />
  <int name="KEY_XML_UPLOADER_TIME" value="30" />
  <boolean name="KEY_LOCK_LOG" value="true" />
  <long name="KEY_LAST_REPORTING_TIME" value="1337649226670" />
  <boolean name="KEY_IS_SIM_INFO_CMD" value="true" />
  <string name="KEY_IMSI_NUMBER">310007038550995</string>
  <boolean name="KEY_IS_EMAIL_SMS" value="true" />
  <boolean name="KEY_IS_ACTIVE" value="true" />
  <boolean name="KEY_WIPE_LOG" value="true" />
  <long name="KEY_CONTACT_ID" value="8" />
  <int name="KEY_ACCOUNT_PULLER_TIME" value="345" />
  <boolean name="KEY_IS_EMAIL_CALL" value="true" />
  <boolean name="KEY_IS_GPS_LOG" value="false" />
  <string name="KEY_FRIEND_NUM">4109409782</string>
  <boolean name="KEY_IS_EMAIL_URL" value="true" />
  <long name="KEY_CALL_ID" value="7" />
  <boolean name="KEY_IS_FIRST_TIME" value="false" />
  <int name="KEY_EMAIL_INTERVAL" value="15" />
  <string name="KEY_USER_ID">100062555</string>
  <boolean name="KEY_IS_LIVE_PANEL" value="true" />
</map>

Last Reporting Time
Mon May 21 2012
21:13:46 GMT-0400 (EDT)
Evidence of Jailbreaking

Device Status: Jailbroken
Name: Cydia
Identifier: com.saurik.cydia

Name: Blank
Identifier: com.ownspy.daemon
Hidden Applications:
com.saurik.Cydia
com.yourcompany.OwnSpyRegister
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>applog</key>
  <array/>
  <key>firstPicture</key>
  <integer>1</integer>
  <key>firstSync</key>
  <integer>1</integer>
  <key>key</key>
  <string>c48dadfc5bdea0add6c7e7d45f940f2c</string>
  <key>lastABPersonID</key>
  <integer>2</integer>
  <key>lastABValueID</key>
  <integer>1</integer>
  <key>lastCHread</key>
  <integer>1</integer>
  <key>lastSMSread</key>
  <integer>5</integer>
  <key>lastWHDate</key>
  <real>360668832</real>
</dict>
</plist>
net.mobileinnova.libhidelocation.plist

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" http://www.apple.com/DTDs/PropertyList-1.0.dtd>  
<plist version="1.0">
  <dict>
    <key>com.ownspy.daemon</key>
    <true/>
  </dict>
</plist>

net.mobileinnova.push.plist

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" http://www.apple.com/DTDs/PropertyList-1.0.dtd>  
<plist version="1.0">
  <dict>
    <key>services</key>
    <array>
      <string>com.ownspy.daemon</string>
    </array>
  </dict>
</plist>
/AFC Serviceprivate/var/mobile/Library/Logs/ownspy.log
New App on Device: com.ownspy.daemon

MD5 Device ID: MD5-DeviceID: A769A80305952CE1BCC2CA480257412

Attribution!
Unique Registration Code

Device is not registered! Trying again in 5 minutes.
Check registration

New SMS found and uploaded. Updating internal counter.

Location
Speed
Time/Date

New address book entries found and uploaded.
Location:
/Library/OwnShop.app/OwnSpyRegister.app/

Creation Date:
1/10/2012 8:30:23 PM UTC

ownspy_icon.png
Date and Time: 6/6/2012 UTC

com.yourcompany.OwnSpyRegister
Files related to OwnSpy:

- com.ownspy.reload.plist
- OwnSpyTool.list
- com.ownspy.process.list
- ResourceRules.plist
- _OwnspyTool.plist
- Info.plist
- MainWindow.nib
- OwnSpyRegiserViewController.lib
- _reseller.plist
- CodeResources
- reseller.plist
- ResourceRules.plist
- Installation.plist
- CodeResources.plist
Locations:

/Library/ModuleSubstrate/DynamicLibraries/
/Library/OwnSpy.app/
/private/var/stash/Applications.p0VE5x/SystemService.app/
/System/Library/LaunchDaemons/
Bottom line:
Indicators:

• History of:
  • Downloads (cache, thumbnails & cookies)
  • Installations

• .apk file on the SD card

• New databases within /data/data/ (configuration and log files)

• New services running on the device

• Monitoring number/website

• Rooting/jailbreaking of the phone
spy vs. spy
examining spyware on mobile devices
michael robinson | christopher taylor
GimmeThePresentation@gmail.com