



## Commercial Spyware-Detecting the Undetectable

July 2015

Fidelis Cybersecurity  
1601 Trapelo Road, Suite 270  
Waltham, MA 02451

# Commercial Spyware-Detecting the Undetectable

*Last fall on a popular digital forensics email listserv a police officer posed a question. “Is there a way to tell if commercial spyware had been installed on an Android phone and if so what evidence could be found?” Nobody responded to his request for help. This paper and presentation seek to answer this question.*

## I. Introduction

Mobile spyware, also referred to as mobile Remote Access Tools (mRATs), poses an increasing threat to both smartphone users and corporate enterprises. MRATs are readily available, easy to install, and frequently marketed as completely undetectable.

This is a serious problem for organizations as it increases the chance of corporate data loss including intellectual property, network credentials, privileged communications, and employee locations. A study conducted by Check Point and Lacoon Mobile Security released in February 2015, found companies with over 2,000 mobile devices had a 50% chance of six or more infected devices on their network.

The presence of these tools puts the individual user’s privacy at risk in addition to jeopardizing sensitive corporate data, such as emails, proprietary information, and business partners. MRATs allow the attacker to eavesdrop on phone calls, activate the camera and microphone, obtain all emails on the device, as well as monitor a number of other invasive activities.

Last fall, the FBI arrested the CEO of the company that advertised and sold the mRAT Stealth Genie. The owner pleaded guilty, shut down the company, and paid a \$500,000 fine. However, many other commercial spyware programs are still available, easily located, and simple to install.

### **mRAT Overview**

Obtaining a commercial mRAT is simple and there are numerous mRATs available for purchase and download. The Lacoon-Checkpoint study identified 18 different families of mRAT. Most of these tools are marketed towards individuals who are interested in monitoring cheating spouses, child monitoring, or employee monitoring. The tools are sold on a subscription basis where the customer purchases the mRAT for a period of time. The Lacoon-Checkpoint research indicated that just two mRATs, mSpy and SpyToMobile, account for over fifty percent of the market share. Both can be found and purchased online and offer the following functionality:

mSpy	SpyToMobile
Text Messages	Text Messages
Call History	Call History
Contact List	Contact List
Web History	Online tracking
Calendar, Notes, Tasks,	Travel History
Emails	WhatsApp
Photos and Videos	
List of Installed Applications	
GPS Location	
Uninstall Alert	

This research will focus on forensic analysis of these two programs using both free and open-source tools as well as popular and widely used commercial forensic tools.

## II. Research Methodology

### ***Device Used***

The device used in this research is a Samsung Galaxy S3, model number GT-I9800I, Android Version 4.4.4 (KitKat). KitKat was selected for this research due to its current popularity. According to Google, KitKat is the most widely used Android version with a 39.2% distribution.

### ***Application Memory Exploitation***

Recovering memory from Android devices yields valuable evidence; data written to flash memory must pass through RAM. However, forensically retrieving the memory can be complicated. Acquiring memory requires root access to the device. Typical rooting of a device requires that the phone be powered off and booted into download mode. This results in data stored within the device's memory to be lost. It is also possible to be given a phone to analyze that has already been rooted. In this research, the device was rooted prior to infection of the mRATs.

There are several free open source tools available for capturing memory from Android devices. Linux Memory Extractor (LIME) is a fairly well known tool, but requires the forensic examiner to compile it from source code. A second tool known as mem is also available. An advantage of mem is it is a binary file that can be pushed and executed from the device. Mem allows the examiner to either acquire the entire memory of the device or to specifically capture the memory from a single process.

Google's Android Debug Bridge (ADB) is the final tool required to exploit application memory. ADB is a command line tool that allows communication between a computer

and a connected Android device. If the device is rooted, the forensic investigator can issue commands to the phone with root privileges using ADB.

Before starting analysis on the Android device, the following specific default settings had to be changed:

- **Turn On Developer Options:** With Android 4.2 and later developer options are hidden by default. To enable the options browse to *Settings* and select *About Phone* and then select *Build number* seven times.
- **Enable USB debugging:** Turning on USB debugging enabled system level clearance from the computer to the phone. This feature is found by navigating to *Settings and Developer options*.
- **Enable stay awake:** Enabling stay awake prevents the Android device from locking after a period of time. This feature is found by navigating to *Settings and Developer options*.

At this point the device is ready for analysis. The device was connected and the following commands were run:

Command	Description
adb forward tcp:9999 tcp:9999	This forwards the ADB port so captured data can be sent over netcat to minimize the footprint on the device.
adb devices	ADB will list connected Android devices.
adb shell	Opens the shell to begin issuing commands on the device.
su -	If the shell did not open as root user this command can be used to escalate privileges.

At this point, we are ready to copy the mem and netcat tools to the memory of the device. In forensics, it is important to minimize the digital footprint on the device; therefore, the best place to save the tools is to the device's RAM, also known as tmpfs in the Android operating system. This is the best alternative over storing the files to the devices storage and potentially overwriting evidence. The command *cat /proc/mounts* can be used to determine where tmpfs is mounted.

```
root@s3ve3gds:/ # cat /proc/mounts
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,seclabel,nosuid,relatime,size=694700k,nr_inodes=130262,mode=755 0 0
devpts /dev/pts devpts rw,seclabel,relatime,mode=600 0 0
none /dev/cpuctl cgroup rw,relatime,cpu 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,seclabel,relatime 0 0
```

*tmpfs is mounted to /dev with read and write permissions.*

The next step is to create a directory in /dev and use ADB to upload the mem acquisition tool and netcat for Android. In the other terminal, issue the ADB push command to upload the tools.

```
examiner@examiner-Precision-M6700: ~/Desktop
examiner@examiner-Precision-M6700:~/Desktop$ adb push mem /dev/forensics
2728 KB/s (457334 bytes in 0.163s)
examiner@examiner-Precision-M6700:~/Desktop$ adb push old_nc /dev/forensics
2747 KB/s (92156 bytes in 0.032s)
examiner@examiner-Precision-M6700:~/Desktop$
```

At this point, the tools have been uploaded, but do not have execute permissions. Use chmod +x to add execute permissions. The memory of the entire device can be captured or the memory of a specific application. In this case, the application was identified and the memory associated with the process was captured. To capture the memory of a specific application, the process identifier (PID) is required. The *ps* command is used and piped to *grep* to quickly locate the malicious process.

```
root@s3ve3gds:/dev/forensics # ps | grep android.sys.process
u0_a40    17997 14800 938856 30580 ffffffff 400be938 S android.sys.process
```

*The malicious process for mSpy*

Once the process is identified, the application memory exploitation can begin. The examiner can either save the memory dump to the phone, the sd card, or send it to the computer via netcat. The syntax of the mem command is: ./mem pid out\_put path. The netcat option will leave the smallest footprint on the infected phone, therefore it is the best choice for forensic examinations.

```
root@s3ve3gds:/dev/forensics # ./mem 17997 | ./old_nc -l -p 999
9
```

Run netcat on the host computer to receive the memory acquisition. Additionally, other commands such as netstat can be run and sent to the host computer through netcat to collect information about running processes and connections.

Once the memory is acquired commercial forensic tools or tools such as strings can be used to search through the data. In this case, strings was run on the memory dump files.

### **Network Traffic**

Network traffic was captured and analyzed for evidence of the mRATs. Shark for Root, a free packet capturing tool was used to capture the traffic. Wireshark 1.10.0 was used to analyze the captured packets.

### ***Forensic Analysis of Physical Acquisition***

Forensic analysis was conducted on the Samsung Galaxy S3. Three physical acquisitions were made using Cellebrite UFED 4PC version 4.2.1.3. A baseline image was taken prior to any interaction with the mRATs. The device was wiped and re-imaged in-between tests to ensure that cross contamination did not occur. The physical images were analyzed with Cellebrite's UFED Physical Analyzer 4.2.1.7.

## **III. mSpy Results**

### ***Memory Analysis***

Numerous artifacts were found in the exploited application's memory, to include the configuration for mSpy. The configuration information depicts what data is being captured and how the data should be transmitted back to the mSpy servers. The options are to transmit data through Wi-Fi only or through both Wi-Fi and the cellular network. Wi-Fi only false indicates that the data will be transmitted either through Wi-Fi or cellular connection. The screen capture below shows which applications are enabled (gps, email, viber, etc).

```
sh": "87b3ed68bae3bc270445984a76e00d79", "config": {"gps": {"enable": true, "interval": "1", "force_gps": true}, "sms": {"enable": true, "wifionly": false}, "email": {"enable": true, "wifionly": false, "call": {"enable": true, "wifionly": false}, "memos": {"enable": true, "wifi only": false}, "note": {"enable": true, "wifionly": false}, "event": {"enable": true, "wifionly": false}, "task": {"enable": true, "wifionly": false}, "contact": {"enable": true, "wifionly": false}, "apps": {"enable": true, "wifionly": false}, "audio": {"enable": true, "wifionly": false}, "photo": {"enable": true, "wifionly": true}, "video": {"enable": true, "wifionly": true}, "browser": {"enable": true, "wifionly": false}, "callrecording": {"enable": true, "wifionly": false}, "skype": {"enable": true, "wifionly": false}, "line": {"enable": true, "wifionly": false}, "whatsapp": {"enable": true, "wifionly": false}, "facebook": {"enable": true, "wifionly": false}, "viber": {"enable": true, "wifionly": false}, "keylogger": {"enable": true, "wifionly": false}, "update": {"interval": "1"}, "logs": {"enable": false}, "build_version": {"is_trial": false}, "photospying": {"enable": true, "wifionly": false}, "snapchat": {"enable": true, "wifionly": false}, "wifi_networks": {"enable": true, "wifionly": false}, "version_available": 0}, "commands_list": [], "status_code_text": "OK - Everything worked as expected.", "status": 200}
```

Evidence of the mRAT capturing the location of the device was also detected.

```
cations": [{"timestamp": "1436894811", "accuracy": 17.525999069213867, "longitude": "-76.851205", "latitude": "39.1704729"}, {"timestamp": "1436894876", "accuracy": 19.06599998474121, "longitude": "-76.8512033", "latitude": "39.1704794"}, {"timestamp": "1436894937", "accuracy": 25.166000366210938, "longitude": "-76.8511666", "latitude": "39.1705094"}, {"timestamp": "1436894998", "accuracy": 16.844999313354492, "longitude": "-76.8511917", "latitude": "39.1704879"}, {"timestamp": "1436895059", "accuracy": 16.844999313354492, "longitude": "-76.8511881", "latitude": "39.1704956"}, {"timestamp": "1436895120", "accuracy": 15.015000343322754, "longitude": "-76.8511957", "latitude": "39.1704807"}, {"timestamp": "1436895210", "accuracy": 26.86199951171875, "longitude": "-76.8511427", "latitude": ""}]
```

Lastly, evidence of domains associated with the mRAT was detected.

url LIKE '%mspy%' OR url LIKE '%thd.cc%' OR url LIKE '%mspyonline.com%'

## Analysis of Network Traffic

Analysis of network traffic indicates the mRAT communicated with IP Address 136.243.253.185 using TCP over port 443.

Filter: **tcp.stream eq 7**

No.	Time	Source	Destination	Protocol	Length	Info
1931	32.439888	10.10.16.35	136.243.253.185	TCP	1514	TCP segment of a reassembled PDU
1932	32.439910	10.10.16.35	136.243.253.185	TCP	1514	TCP segment of a reassembled PDU
1933	32.439919	10.10.16.35	136.243.253.185	TCP	1514	TCP segment of a reassembled PDU
1934	32.439966	10.10.16.35	136.243.253.185	TCP	1514	TCP segment of a reassembled PDU
1936	32.440178	10.10.16.35	136.243.253.185	TCP	1514	TCP segment of a reassembled PDU
1937	32.440210	10.10.16.35	136.243.253.185	TCP	1514	TCP segment of a reassembled PDU
1938	32.440246	10.10.16.35	136.243.253.185	TLSv1	1514	Application data
1939	32.440271	10.10.16.35	136.243.253.185	TCP	1514	Follow TCP Stream
1940	32.440302	10.10.16.35	136.243.253.185	TCP	1514	Stream Content
1941	32.440322	10.10.16.35	136.243.253.185	TCP	1514	0.u...z.t.a...7.Q..p..F.../3.....
1942	32.440348	10.10.16.35	136.243.253.185	TCP	1514	0.u...z.t.a...7.Q..p..F.../3.....
1943	32.440373	10.10.16.35	136.243.253.185	TCP	1514	3.9.2.8.
1944	32.440398	10.10.16.35	136.243.253.185	TCP	1514	136.243.253.185
1945	32.440421	10.10.16.35	136.243.253.185	TLSv1	1514	TLSv1

# Frame 1931: 1514 bytes on wire (2212 bits), 1514 bytes captured  
# Ethernet II Src: a.thd.cc (00:0c:29:1e:00:00) Dst: 2e:80:00:00:00:00 (aa:aa:03:00:00:00)  
# Internet Protocol Version 4, Src: 10.10.16.35 (10.10.16.35), Dst:  
# Transmission Control Protocol, Src Port: 33192 (33192), Dst Port:  
# Source port: 33192 (33192)  
# Destination port: https (443)  
# [Stream index: 7]  
Sequence number: 320481 (relative sequence number)  
Next sequence number: 321929 (relative sequence number)  
Acknowledgment number: 146 (relative ack number)  
Header length: 32 bytes  
# Flags: 0x0100 (ACK)  
Window size: 123  
Calculated window size: 157441

0000 2e 14 00 00 00 aa 03 00 00 00 08 00 45 00 :.  
0001 3c de b2 48 00 00 06 00 00 00 00 00 00 00 :.  
0020 fd 6d 01 01 01 01 f2 07 ff 00 00 00 00 00 :.  
0030 00 7b d3 00 00 01 01 08 00 ff ff b7 ab 24 26 :.  
0040 cb 80 19 6f 42 ee 71 69 99 d5 e0 bf 76 e9 cc 56 :.  
0049 00 27 34 78 00 db ae 07 ab 23 01 bf 52 00 00 :.  
0060 06 07 77 79 f9 28 cf 4d 07 ab 23 01 05 65 d7 00 :.  
0070 4b 6d c7 79 3e 77 66 87 f5 88 60 fd 00 1c 05 69 : Km.y.-f.  
0080 36 38 b9 9a 29 c8 3b ed 12 54 1c c8 7a bf 27 a1 :68.):.  
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 :.  
00a0 12 64 4b 42 62 9f b5 13 0a eb e6 79 cb d2 e9 1a :jKB8...y..  
00b0 d9 e9 9b 86 88 29 a7 c0 c3 c8 08 ab a0 46 56 :m=.)...FV  
00c0 fd 6d 4b 5e 81 29 77 ee 04 f1 46 dd 11 39 42 23 :mK.Sw...F.998  
00d0 69 fe 41 82 00 5f e3 a3 ff 09 1a ba 9c 75 1b 7d 0d :2034.1.#  
00e0 fa 35 f1 2c 91 27 2a 24 ea 0b ba 1b 13 a2 e2 43 :5...A;...  
00f0 69 fe 41 82 00 5f e3 a3 ff 09 1a ba 9c 75 1b 7d 0d :1.A;...;...;C  
0100 b4 de 69 d4 32 c3 50 39 28 60 81 c0 21 7e 70 :.8!2.P 9C..!-P  
0110 b3 9e 08 6f 7d 2f 0c 30 c4 bf d4 7b 5f ff 3c :...)./.0...<

Entire conversation (1981522 bytes)

Find Save As Print ASCII EBCDIC Hex Dump C Arrays Filter Out This Stream Close

A query was made to Domain Tools, which retrieved the registration information for the IP address.

<b>IP Location</b>	 Germany Berlin Bitex Group Ltd
<b>ASN</b>	 AS24940 HETZNER-AS Hetzner Online AG (registered Jun 03, 2002)
<b>Resolve Host</b>	a.thd.cc
<b>Whois Server</b>	whois.ripe.net
<b>IP Address</b>	136.243.253.185
% No abuse contact registered for 136.243.253.184 - 136.243.253.191	
inetnum:	136.243.253.184 - 136.243.253.191
netname:	BITEX-GROUP-LTD
descr:	Bitex Group LTD
country:	DE
admin-c:	PD7003-RIPE
tech-c:	PD7003-RIPE

```

status: LEGACY

notify: ripe-mntner@hetzner.de

mnt-by: HOS-GUN

changed: ripe-dbm-updates@robot.first-ns.de 20141126
created: 2014-11-26T02:10:55Z
last-modified: 2014-11-26T02:10:55Z
source: RIPE

person: Pavel Daletski
address: Bitex Group LTD
address: 306 Victoria House
address: 0000 Victoria
address: SEYCHELLES
phone: +18007137528
e-mail: info@bitexgroupltd.com
nic-hdl: PD7003-RIPE
notify: ripe-mntner@hetzner.de
mnt-by: HOS-GUN
changed: ripe-dbm-updates@robot.first-ns.de 20130108
created: 2013-01-08T03:10:37Z
last-modified: 2013-01-08T03:10:37Z
source: RIPE

```

## Analysis of Physical Image

The mRAT mSpy is marketed as undetectable, however, it left numerous artifacts on the infected phone. Using UFED Physical Analyzer, a list of the installed application indicates that the mRAT is named: android.sys.process and has permissions to the following: Accounts, User Dictionary, Application INfor, Bookmarks, Display, Locations, Messages, Network, Personal Info, Phone Calls Social Info, and Storage.

Additional artifacts of the installation and setup were located using UFED Physical Analyzer 4.2.1.7.

Path	Object	Description
/Root/data/com.android.chrome/app_chrome/ Default/History	http://kypler.com/android	Visited URL
/Root/data/com.android.chrome/app_chrome/	bt.apk	Downloaded

Default/History		spyware installer.
/data/dalvik-cache	References to mRAT	mSPY left evidence in dalvik-cache directory

The mRAT is installed at `/Root/data/android.sys.process`. This directory contains several files of importance:

**File name:** Settings.xml

**Path:** /Root/data/android.sys.process/shared\_prefs/Settings.xml

**Description:** XML file containing mRAT settings.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <boolean name="LOCATION_FIRST_DATA_GATHERED" value="true" />
    <boolean name="EMAIL_WIFI_ONLY" value="false" />
    <long name="LAST_DELETED_CALLS_TRACKED_TIME" value="1436900577285" />
    <boolean name="TRACK_AUDIO" value="true" />
    <boolean name="FORCE_GPS" value="true" />
    <boolean name="APP_SENSOR_FIRST_START" value="false" />
    <boolean name="KEYLOGS_WIFI_ONLY" value="false" />
    <boolean name="AUDIO_WIFI_ONLY" value="false" />
    <boolean name="SENSORS_FIRST_DATA_GATHERED" value="true" />
    <boolean name="CONTACTS_WIFI_ONLY" value="false" />
    <long name="LAST_DELETED_SMS_TRACKED_TIME" value="1436900577248" />
    <boolean name="TRACK_WHATSAPP" value="true" />
    <long name="BROWSER_S_LAST_HISTORY_TIME" value="1436895967325" />
    <boolean name="PHONE_INFO_WIFI_ONLY" value="false" />
    <boolean name="WHATSAPP_WIFI_ONLY" value="false" />
    <boolean name="VIBER_WIFI_ONLY" value="false" />
    <boolean name="SNAP_CHAT_WIFI_ONLY" value="false" />
    <boolean name="TRACK_WIFI_NETWORKS" value="true" />
    <boolean name="TRACK_PHONE_CALLS" value="true" />
    <boolean name="TRACK_SKYPE" value="true" />
    <boolean name="ICON_VISIBLE" value="false" />
    <long name="BROWSER_S_LAST_BOOKMARK_TIME" value="0" />
    <boolean name="INSTALLATION_COMPLETED" value="true" />
    <boolean name="TRACK_PHONE_INFO" value="true" />
    <boolean name="TRACK_CONTACTS" value="true" />
    <boolean name="SKYPE_WIFI_ONLY" value="false" />
    <boolean name="BROWSER_WIFI_ONLY" value="false" />
    <long name="LAST_PHONE_CALL_TIME" value="1436899627398" />
    <int name="APPLICATION_CODE" value="497" />
    <boolean name="WIFI_NETWORKS_WIFI_ONLY" value="false" />
    <boolean name="TRACK_SNAP_CHAT" value="true" />
    <boolean name="APP_SYSTEM" value="true" />
    <boolean name="CALLS_WIFI_ONLY" value="false" />
    <boolean name="TRACK_LINE_MESSENGER" value="true" />
    <boolean name="TRACK_BROWSER" value="true" />
    <string name="HASH">d381bfa2f46229c5becc7f5d55be4259</string>
    <boolean name="TRACK_EMAIL" value="true" />
    <long name="GPS_INTERVAL" value="60000" />
    <boolean name="SHOW_ICON" value="false" />
    <boolean name="TRACK_PHOTOS" value="true" />
    <long name="WIFI_CONNECTION_START_TIME" value="1436881549" />
    <boolean name="TRACK_MESSAGES" value="true" />
```

```

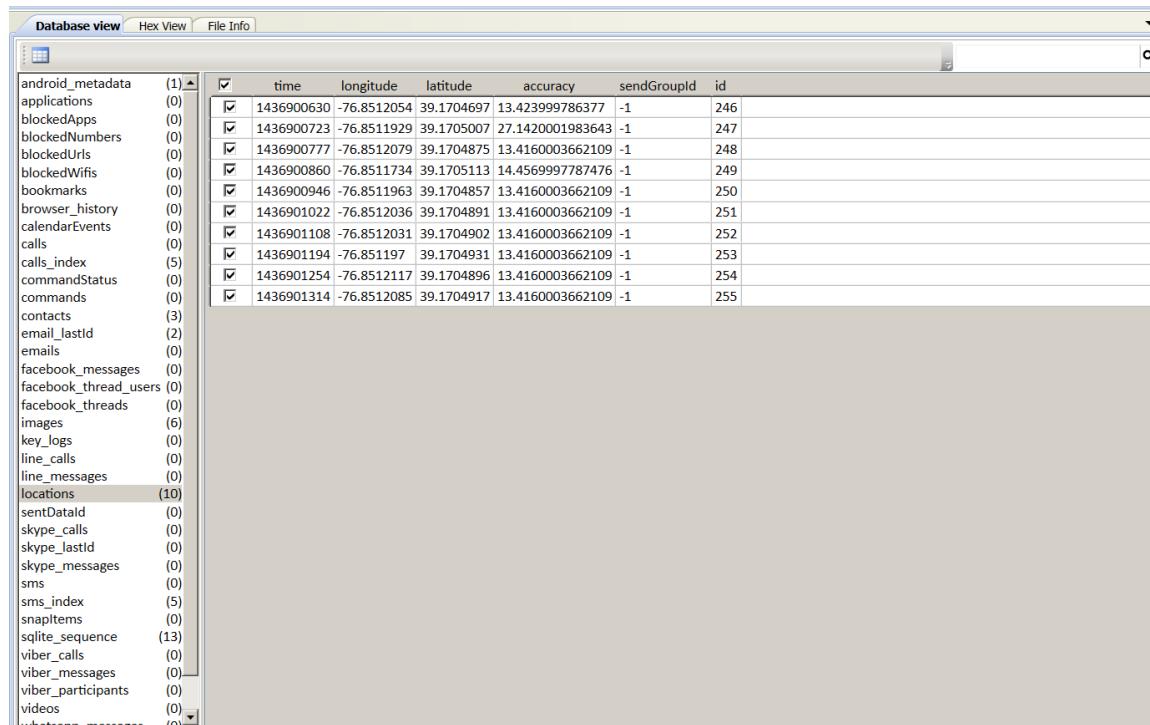
<string name="WIFI_CONNECTION_BSSID">54:a0:50:5c:d6:aa</string>
<long name="BROWSER_LAST_HISTORY_TIME" value="1436882133703" />
<boolean name="EVENTS_WIFI_ONLY" value="false" />
<boolean name="TRACK_EVENTS" value="true" />
<boolean name="FACEBOOK_WIFI_ONLY" value="false" />
<boolean name="PHOTOS_WIFI_ONLY" value="true" />
<boolean name="TRACK_VIBER" value="true" />
<long name="LAST_SMS_TIME" value="1436899610013" />
<boolean name="APP_INSTALLED" value="true" />
<boolean name="TRACK_LOGS" value="false" />
<string name="AUTH_ID">ae69d3df6f9d3891</string>
<long name="LAST_EXTERNAL_IMAGE_DATE_ADDED" value="1436899007" />
<long name="UPDATE_INTERVAL" value="0" />
<boolean name="CONTACT_SENSOR_FIRST_START" value="false" />
<boolean name="VIDEO_WIFI_ONLY" value="true" />
<boolean name="SMS_WIFI_ONLY" value="false" />
<string name="IMEI">353106068763034</string>
<boolean name="TRACK_VIDEO" value="true" />
<boolean name="TRACK_FACEBOOK" value="true" />
<boolean name="TRACK_LOCATION" value="true" />
<boolean name="TRACK_KEYLOGS" value="true" />
</map>

```

File name: Internal.db

Path:/Root/data/android.sys.process/databases/internal.db

Description: The tool utilizes a sqlite database with write-ahead logging and shared memory files. The write-ahead logins and shared memory file features creates two additional files in this directory with extensions .db-shm and .db-wal. Forensic analysis of the associated .db-shm and .db-wal files yielded additional evidence that was not readily apparent in the internal.db file, such as full emails



	id	time	longitude	latitude	accuracy	sendGroupId
checkbox	246	1436900630	-76.8512054	39.1704697	13.423999786377	-1
checkbox	247	1436900723	-76.8511929	39.1705007	27.1420001983643	-1
checkbox	248	1436900777	-76.8512079	39.1704875	13.4160003662109	-1
checkbox	249	1436900860	-76.8511734	39.1705113	14.4569997787476	-1
checkbox	250	1436900946	-76.8511963	39.1704857	13.4160003662109	-1
checkbox	251	1436901022	-76.8512036	39.1704891	13.4160003662109	-1
checkbox	252	1436901108	-76.8512031	39.1704902	13.4160003662109	-1
checkbox	253	1436901194	-76.851197	39.1704931	13.4160003662109	-1
checkbox	254	1436901254	-76.8512117	39.1704896	13.4160003662109	-1
checkbox	255	1436901314	-76.8512085	39.1704917	13.4160003662109	-1

## Internal.db

### IV. SpyToMobile Results

#### *Memory Analysis*

Analysis of the exploited application's memory yielded multiple noteworthy artifacts. The application was found to be storing information from a recent text of 'I love Black Hat 2015!' to phone number 555-2368 and the sms call time of: 1436290801

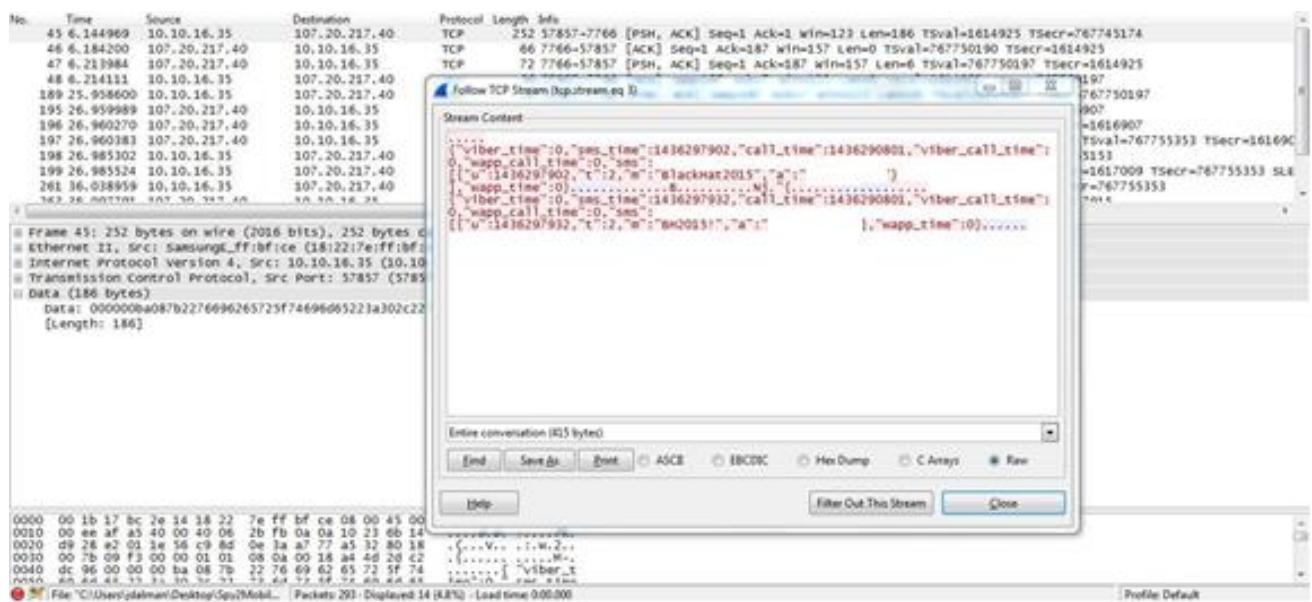
```
)7B
{ "viber_time":0,"sms_time":1436293687,"call_time":1436290801,"viber_call_time":0,"wapp_call_time":0,"sms": [{"u":1436293687,"t":2,"m":"I love Black Hat 2015!\n","a":5552368}], "wapp_time":0}
H<aB
duration
/data/data/com.spy2mobile.light/databases/msgstore.db
```

Additionally information was found that indicates the mRAT was capturing location data from nearby wireless networks.

```
Guest Network-columbia/xx:xx:xx:xx:xx:xx
RSSI:-44
W:87.0
C:-1
L:39.170727 -76.85074
Pentest_Lab2/xx:xx:xx:xx:xx:xx
RSSI:-49
W:85.0
C:-1
L:39.170727 -76.85074
/data/data/com.spy2mobile.light/database
/data/data/com.spy2mobile.light/databases/system.db
WiFi stored:
Guest Network-columbia/xx:xx:xx:xx:xx:xx
RSSI:-44
W:87.0
C:-1
L:39.170727 -76.85074
```

#### Analysis of Network Traffic

Analysis of network traffic indicated that the mRAT communicated with IP Address 107.20.217.40 using TCP over port 7766.



A query was made to Domain Tools for spy2mobile.com, which confirmed the IP address from WireShark.

<b>Registrant Org</b>	Domains By Proxy, LLC was found in ~11,111,910 other domains
<b>Registrar</b>	WILD WEST DOMAINS, LLC
<b>Registrar Status</b>	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
<b>Dates</b>	Created on 2012-02-15 - Expires on 2016-02-15 - Updated on 2015-01-19
<b>Name Server(s)</b>	NS29.DOMAINCONTROL.COM (has 38,773,043 domains) NS30.DOMAINCONTROL.COM (has 38,773,043 domains)
<b>IP Address</b>	107.20.217.40 - 2 other sites hosted on this server
<b>IP Location</b>	 - Virginia - Ashburn - Amazon.com Inc.
<b>ASN</b>	 AS14618 AMAZON-AES - Amazon.com, Inc. (registered Nov 04, 2005)
<b>Domain Status</b>	Registered And Active Website
<b>Whois History</b>	24 records have been archived since 2012-02-16
<b>IP History</b>	3 changes on 4 unique IP addresses over 3 years
<b>Registrar History</b>	1 registrar
<b>Hosting History</b>	1 change on 2 unique name servers over 3 years
<b>Whois Server</b>	whois.wildwestdomains.com
<b>Website</b>	
<b>Website Title</b>	 SpyToMobile, track a cell phone, sms spy

<b>Server Type</b>	nginx/1.1.19
<b>Response Code</b>	200
<b>SEO Score</b>	73%
<b>Terms</b>	379 (Unique: 163, Linked: 102)
<b>Images</b>	38 (Alt tags missing: 37)
<b>Links</b>	64 (Internal: 58, Outbound: 6)
<b>Whois Record</b>	( last updated on 2015-07-14 )
Domain Name:	SPY2MOBILE.COM
Registrar URL:	<a href="http://www.wildwestdomains.com">http://www.wildwestdomains.com</a>
Registrant Name:	Registration Private
Registrant Organization:	Domains By Proxy, LLC
Name Server:	NS29.DOMAINCONTROL.COM
Name Server:	NS30.DOMAINCONTROL.COM
DNSSEC:	unsigned

You must [Register](#) or [Log in](#) to view the Whois record for this domain name

## Analysis of Physical Image

The mRAT SpyToMobile left numerous artifacts on the infected phone. Using Cellebrite's UFED Physical Analyzer, listing the installed applications listed the mRAT with the identifier 'com.spy2mobile.light'. The mRAT has permissions to the following applications: Accounts, Application Info, Bluetooth, Locations, Messages, Network, Phone Calls, Social Info, and Storage.

Additional artifacts of the installation and setup were located using UFED Physical Analyzer 4.2.1.7. Spytomobile.com/d is the website used to download the mRAT onto the device. Spy2Mobile's installation file is named data\_backup.apk.

Path	Object	Description
/Root/data/com.android.chrome/app_chrome/Default/History	Spytomobile.com/d	Visited URL
/Root/data/com.android.chrome/app_chrome/Default/History	data_backup.apk	Downloaded spyware installer.

The mRAT is installed at */data/data/com.spy2mobile.light*. This directory contains several files of importance:

File Name: system.db

Path: /data/data/com.spy2mobile.light/databases/system.db

Description: The tool utilizes a sqlite database to store collected data.

Database view Hex View File Info

		id	bssid	ssid	
android_metadata	(1)	<input checked="" type="checkbox"/>	1	e4:f4:c6:02:d6:fe	MLwifi
calls	(1)	<input checked="" type="checkbox"/>	2	00:21:29:c7:08:01	Protechnology
contacts	(1)	<input checked="" type="checkbox"/>	3	68:7f:74:d7:20:a4	FSC-VISITORS
logs	(0)	<input checked="" type="checkbox"/>	4	00:17:c5:88:95:98	CFW-Public
points	(1)	<input checked="" type="checkbox"/>	5	24:a4:3c:b2:49:8a	Site Link Wireless
sectors	(3)	<input checked="" type="checkbox"/>	6	00:0f:66:81:76:ba	TNGMD
sms	(1)	<input checked="" type="checkbox"/>	7	9c:b6:54:5d:26:65	HP-Print-65-Officejet Pro 8600
wifi	(65)	<input checked="" type="checkbox"/>	8	68:7f:74:11:fa:36	executivehouse - conf B
		<input checked="" type="checkbox"/>	9	58:6d:8f:17:42:22	FSD CLUB HOUSE
		<input checked="" type="checkbox"/>	10	12:c3:7b:de:5e:d9	UT-GUEST
		<input checked="" type="checkbox"/>	11	6c:b0:ce:14:3a:f2	MLwifiLL
		<input checked="" type="checkbox"/>	12	b8:c7:5d:04:2d:89	Next Level Fitness
		<input checked="" type="checkbox"/>	13	2c:b0:5d:a2:11:f9	IMPACT777
		<input checked="" type="checkbox"/>	14	00:24:b2:14:8e:f0	Agetech24
		<input checked="" type="checkbox"/>	15	9c:d6:43:d7:07:06	BHMC2
		<input checked="" type="checkbox"/>	16	e8:b7:48:26:51:dc	PDRICOL01
		<input checked="" type="checkbox"/>	17	10:08:b1:f6:68:06	HP-Print-06-LaserJet 200
		<input checked="" type="checkbox"/>	18	2c:b0:5d:4b:c6:06	NETGEAR94
		<input checked="" type="checkbox"/>	19	00:24:b2:7c:cb:74	NETGEAR
		<input checked="" type="checkbox"/>	20	00:17:c5:88:95:97	CFWwireless
		<input checked="" type="checkbox"/>	21	98:fc:11:f7:c0:c4	amkgb

## V. Conclusion

The purpose of this research was to demonstrate the two most popular Android commercial spyware programs (mRATS) were detectable using a combination of free, open source tools as well as commercial digital forensics tools. The results indicated that the mRATs were detected using every tool tested. Both were found through network traffic analysis, memory forensics, and the Cellebrite UFED acquisition. However, it is not necessary to have all those tools available for the average user to protect themselves and their privacy. Enabling a strong password and limiting physical access to the phone from would-be hackers is the first step in mRAT infection.. If a user is suspicious that a spyware program is already on the phone they should look in the following places:

- Navigate to **Settings** and then select **Security**. Determine if **Unknown Sources** is checked. If it is, and the user has no memory of turning this feature on, it may be indicative of mRAT presence and a deeper analysis should be conducted.
- Look for suspicious web browsing history or download history.
- Look for new Widgets or Apps on the desk.
- The mRATS may appear under running processes but they typically have names that are misleading and may be difficult to detect.

## VI. Similar Work

Robinson, M & Taylor, C. (2012, July). Spy vs. Spy: Examining spyware on mobile devices. Document presented at Defcon 20, Las Vegas, NV. Slides retrieved from <https://www.defcon.org/images/defcon-20/dc-20-presentations/Robinson/DEFCON-20-Robinson-Spy-vs-Spy.pdf>

## VII. Works Cited

Google Dashboards. (n.d.). Retrieved from  
<https://developer.android.com/about/dashboards/index.html>

Tamma, R. & Tindall, D (2015). Learning Android Forensics. Birmingham, UK: Packt Publishing Ltd.

Threat Research: Targeted Attacks on Enterprise Mobile. (2015, February). Retrieved from  
[https://www.checkpoint.com/downloads/product-related/Lagoon\\_CP\\_Enterprise\\_mRAT\\_Research.pdf](https://www.checkpoint.com/downloads/product-related/Lagoon_CP_Enterprise_mRAT_Research.pdf)

Whois Lookup 107.20.217.40. (n.d.). Retrieved from  
<http://whois.domaintools.com/107.20.217.40>

Whois Lookup 136.243.253.185. (n.d.). Retrieved from  
<http://whois.domaintools.com/136.243.253.185>

## VIII. About the Authors

Joshua M. Dalman is a second generation digital forensic examiner. Mr. Dalman has nearly a decade of digital forensics and incident response experience and has tackled hundreds of cases. Mr. Dalman has also earned recognition as an instructor, having

developed material and trained countless members of the law enforcement community. Mr. Dalman has a Master of Science degree in Digital Forensics from the University of Central Florida.

Valerie Hantke is currently a Cybersecurity Engineer at Fidelis Cybersecurity. She earned a Bachelor of Science in Electrical Engineering from the United States Naval Academy and a Master of Science in Cybersecurity from University of Maryland University College. After serving in the US Navy for six years, she began her digital forensics career. She has performed numerous mobile device forensic acquisitions and examinations, to include cellphones, tablets, GPS devices, wearable technologies, and many others. Ms. Hantke also teaches part time at her local community college in the Computer Technologies Department.