



Commercial Spyware- Detecting the Undetectable

July 2015

About the Authors

Joshua Dalman

Second generation
digital forensics
examiner

M.S. Digital Forensics
(University of Central
Florida)

Certifications: ACE,
CCE, CFE, CFCE, EnCE,
etc...



About the Authors

Valerie Hantke

M.S. Cybersecurity
(UMUC) and B.S.
Electrical Engineering
(USNA)

Certifications: EnCE,
ACE, GCIH, GMOB,
CEH...



Overview

- Mobile Spyware Introduction
- Research Methods
- SpyToMobile Results
- mSpy Results
- Conclusion

Spyware Introduction

Web Shopping News Videos Images More Search tools

About 1,470,000 results (0.52 seconds)

Mobile spyware is:

- Easily available
- Easy to install
- Lots of features
- Stores data on remote server
- Already in your enterprise network?

[mSpy - Official Site - mspy.com](#)

Ad www.mspy.com/ ▾

#1 monitoring software for all your devices. Buy Now!

[Remote Cell Phone Spy \\$27 - remotecellsy.com](#)

Ad www.remotecellsy.com/ ▾

Does Not Require Access To The Phone. Monitor Calls, Text & More.

[Cell Phone Spy Software - 2015 Reviews & Top Picks](#)

Ad www.wellresearchedreviews.com/ ▾

Shop Smart - Read Before You Buy

[See Our Top Pick - Mobile Monitoring Reviews](#)

[Try to Avoid Getting Scammed When Buying Cell Phone ...](#)

acisni.com/avoid-getting-scammed-buying-cell-phone-spy-software/ ▾

Mar 27, 2012 - Finding these companies and ordering from decent suppliers will in the end save you money and time. [how to buy cell phone spy software](#).

[SpyzRus.net: How to Buy the Best Cell Phone Spy Software](#)

spyzrus.net/ ▾

The best place to start your search for cell phone spy software including a complete guide, reviews and how to articles.

[Flexispy - Mobile Spy, Flexispy, mSpy ... - Mobile Spy Reviews - mSpy Review](#)

[Spy On Mobiles | SMS Tracker | Cell Phone Tracker ...](#)

www.flexispy.com/ ▾

FlexISPY lets you [spy](#) on mobile phones and tablets and has unique call interception capability. Provides SMS Tracker, Cell phone tracker, room bugging total smartphone monitoring. ... on 13 instant messengers. [View all Products](#) [Buy Now](#) ...

[Best Phone Spy Reviews: Best Phone Spy – Top 5 Cell ...](#)

www.bestphonespy.com/ ▾

An in-depth look at the best cell phone spy software on the market. Read our ... Plus, once you purchase the software, you get free updates for life. Highster ...

[Cell Phone Spy Software Reviews | mSpy, MobiStealth ...](#)

www.top10spysoftware.com/ ▾

... Terms and Conditions and Refund Policy carefully before you make a purchase.

... Cell phone spy software have recently began to spread with the speed of ...

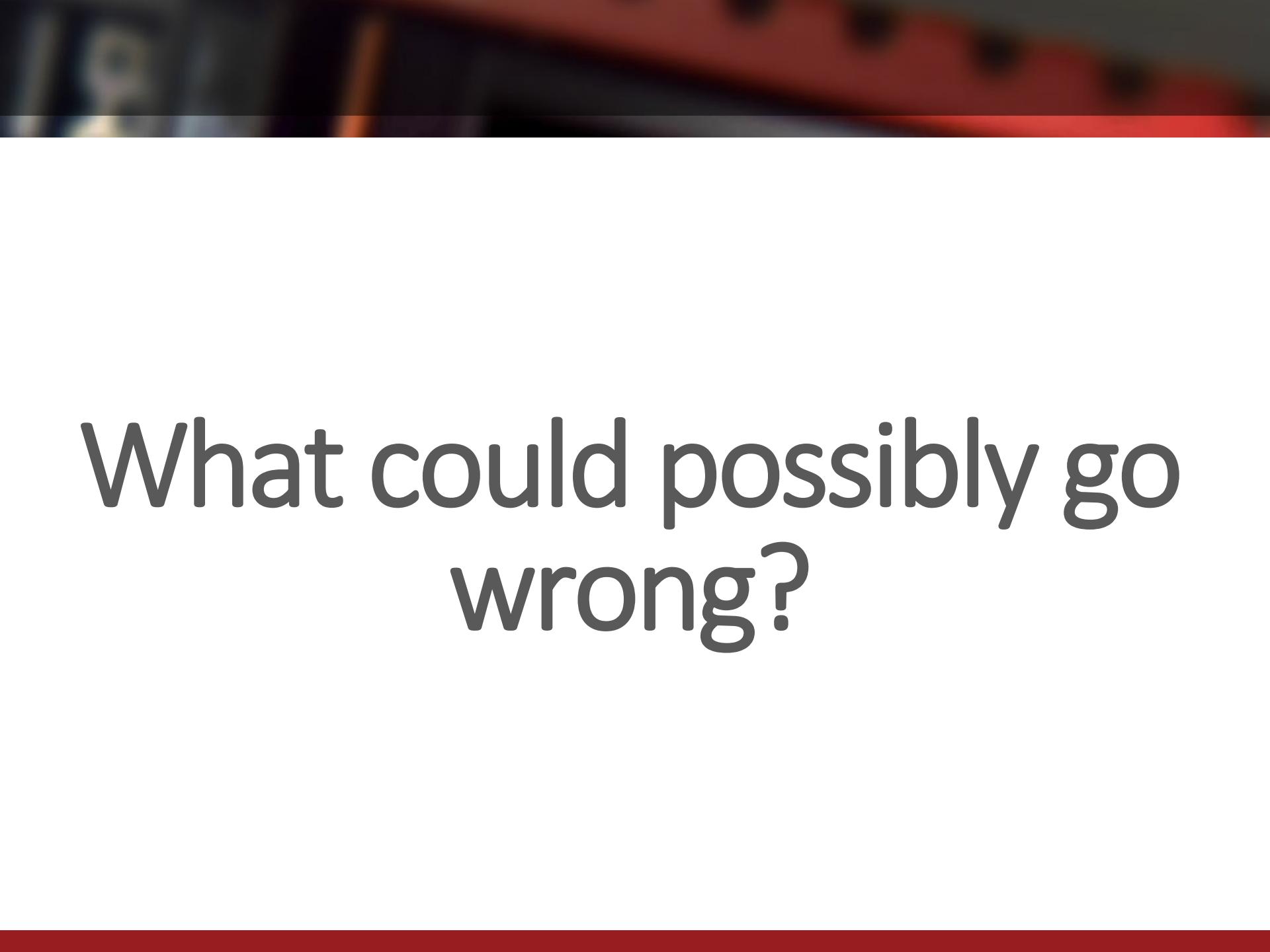
[Purchase Mobile Spy | Order Now to Download Instantly](#)

www.mobile-spy.com/purchase.html ▾

What We Know

Lacoon Mobile Security /Check Point Study:

- Sampled nearly 1 million devices (50% Android, 40% iOS, 10% Other) communicating through corporate Wi-Fi .
- Detected over 20 variants and 18 different families of spyware products.
- Two spyware programs (SpyToMobile and Mspy) accounted for more than half of all infections.
- Organizations with 2,000 devices on their enterprise have 50% chance of infection.



What could possibly go
wrong?



BLOG ADVERTISING

ABOUT THE AUTHOR

14 Mobile Spyware Maker mSpy Hacked, Customer Data Leaked



MAY 15
mSpy, the makers of a dubious software-as-a-service product that claims to help more than two million people spy on the mobile devices of their kids and partners, appears to have been massively hacked. Last week, a huge trove of data apparently stolen from the company's servers was posted on the Deep Web, exposing countless emails, text messages, payment and location data on an undetermined number of mSpy "users."

mSpy has not responded to multiple requests for comment left for the company over the past five days. KrebsOnSecurity learned of the apparent breach from an anonymous source who shared a link to a Web page that is only reachable via [Tor](#), a technology that helps users hide their true Internet address and allows users to host Web sites that are extremely difficult to get taken down.

The screenshot shows a web browser window with the URL [http://\[REDACTED\].ion/readme.txt](http://[REDACTED].ion/readme.txt). The page content is as follows:

```
Full databases from http://mspy.com
> 400 000 users
apple id + password, tracking data, payment details, photo and more security info
enjoy
```

The Tor-based Web site hosting content stolen from mobile devices running mSpy.

Advertisement



Detect Communications with Malicious IPs in Minutes

Try NEW ThreatFinder
(It's FREE!)



TRY THREATFINDER NOW ▶

My New Book!



Spyware Features

Most spyware programs collect at minimum the following types of information:

- Text Messages
- Call History
- Contact List
- Web History
- Wi-Fi Networks
- Emails
- Calendar, Notes, Tasks
- GPS Location

Are These Legal?

- Previously marketed towards cheating spouses.
- Tools now marketed towards employee and child monitoring.
- Legal disclaimer during installation.
- Many spyware companies still running.

Washington Field Office (WFO)

[Home](#) • [Washington](#) • [Press Releases](#) • [2014](#) • **Man Pleads Guilty for Selling StealthGenie Spyware App and Ordered to Pay \$500,000 Fine**

 Twitter (28)  Facebook  Share 

Man Pleads Guilty for Selling StealthGenie Spyware App and Ordered to Pay \$500,000 Fine

U.S. Attorney's Office
November 25, 2014

Eastern District of Virginia
(703) 299-3700

WASHINGTON—A Danish citizen today pleaded guilty in the Eastern District of Virginia and was ordered to pay a fine of \$500,000 for advertising and selling StealthGenie, a spyware application (app) that could remotely monitor calls, texts, videos and other communications on mobile phones without detection. This marks the first-ever criminal conviction concerning the advertisement and sale of a mobile device spyware app.

Assistant Attorney General Leslie R. Caldwell of the Justice Department's Criminal Division, U.S. Attorney Dana J. Boente of the Eastern District of Virginia and Assistant Director in Charge Andrew G. McCabe of the FBI's Washington Field Office made the announcement after a hearing before U.S. District Judge Leonie M. Brinkema in the Eastern District of Virginia.

"Spyware is an electronic eavesdropping tool that secretly and illegally invades individual privacy," said Assistant Attorney General Caldwell. "Make no mistake: selling spyware is a federal crime, and the Criminal Division will make a federal case out of it. Today's guilty plea by a creator of the StealthGenie spyware is another demonstration of our commitment to prosecuting those who would invade personal privacy."

"The defendant advertised and sold a spyware app that could be secretly installed on smart phones without the knowledge of the phone's owner," said U.S. Attorney Boente. "This spyware app allowed individuals to intercept phone calls, electronic mail, text messages, voice-mails and photographs of others. The product allowed for the wholesale invasion of privacy by other individuals, and this office in coordination with our law enforcement partners will prosecute not just users of apps like this, but the makers and marketers of such tools as well."

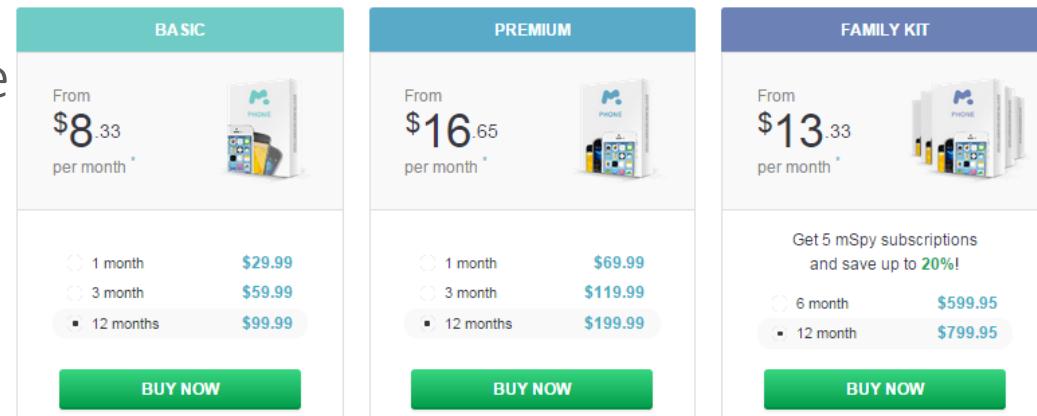
"Mr. Akbar is the first-ever person to admit criminal activity in advertising and selling spyware that invades an unwitting victim's confidential communications," said FBI Assistant Director in Charge McCabe. "This illegal spyware provides individuals with an option to track a person's every move without

Research Conducted

- Device Used: Samsung Galaxy S3
 - Model: GT-I9800I
 - Android Version: 4.4.4 (KitKat)
- Application Memory Exploitation
 - Android Debug Bridge (ADB)
 - Mem and Netcat
 - Strings
- Physical device acquisition and analysis
 - Cellebrite UFED4PC 4.2.1.3
 - Cellebrite Physical Analyzer 4.2.1.7

About mSpy

- Most common mobile spyware application, accounting for nearly one third of infections
- Sold on a subscription basis
- Claims to have over one million customers



Installation and Monitoring

- Requires physical access to the phone
- Modify security settings to allow untrusted apps.
- Browse to <http://kypler.com/android>
- Download and install bt.apk
- Enter unique passcode that is generated and emailed after purchase.
- And if you have trouble installing the spyware...



mAssistance

With **mAssistance** we'll gladly perform initial installation of mSpy on your target mobile device or computer.

Within 24 hours upon the purchase of the service, you'll be e-mailed to the e-mail you provide here by our field service representative to fix the best time for the procedure.

Platforms: [Android](#) , [MacOS](#) , [Windows 2000](#) , [Windows 7](#) , [Windows 8](#) , [Windows Vista](#) , [Windows XP](#)

Unit price: 37.99 USD

Total price: 37.99 USD

< Back to shopping

Add to cart

Experiencing difficulties with an installation? Having hard times with setting up the features? Or simply tired of reading technical manuals? Relax! We'll do everything for you.

With **mAssistance** we'll gladly perform initial installation of **mSpy** on your target mobile device or computer. We'll complete Keylogger setup, Locations, disable SMS apps, activate USB-debugging and more.

You'll still need to have a physical access to the target device with an Internet connection.

Available for:

- Android mobile OS

Command and Control

Infected ▼ Add Device ▼

A3847631 ? Help

Dashboard

- Contacts
- Call Logs
- Snapchat new!
- Line new!
- Text Messages
- Locations
- Geo Fencing new!
- Photos
- Video Files
- Browser History
- Emails
- Events
- Skype
- WhatsApp
- Facebook Tracking
- Viber
- Installed Apps
- Keylogger
- Wi-Fi Networks new!
- Device Management

Device Info

Android, Build: 4.12.9 IMEI: 353106068763034
100% Wi-Fi: On Location tracker: On

Show / Hide mSpy Icon

Display mSpy Icon On Monitored Device: Disabled Enable

Account Info

Plan: Basic
Phone ID: 3827461
Expires on: 08/11/2015 08:37 PM

Extend Subscription Request Cancellation

Cell Phone Activity

Date	Locations	Websites	Emails	Photos	Text Messages
2015-07-10	~10	~10	~10	~10	~10
2015-07-11	~20	~10	~10	~10	~10
2015-07-12	~100	~10	~10	~10	~10
2015-07-13	~80	~10	~10	~10	~10
2015-07-14	~500	~100	~10	~10	~10
2015-07-15	~850	~80	~10	~10	~10

Synchronization method: ? Don't Sync Wi-Fi Only All Connections

Customizable Settings

Phone Settings

Auto Update [?](#)

All changes made on the web panel will be applied in N minutes. N minutes equal one update interval.

Update Interval:	<input type="text" value="1"/> minutes	Location Update Interval:	<input type="text" value="1"/> minutes	Units:	<input type="text" value="foot"/> ?
Locations:	<input type="text" value="All Connections"/> ?	Call logs:	<input type="text" value="All Connections"/> ?	SMS:	<input type="text" value="All Connections"/> ?
Address Book:	<input type="text" value="All Connections"/> ?	Events:	<input type="text" value="All Connections"/> ?	E-mails:	<input type="text" value="All Connections"/> ?
Browser History :	<input type="text" value="All Connections"/> ?	Installed Apps:	<input type="text" value="All Connections"/> ?	Photos:	<input type="text" value="Wi-Fi Only"/> ?
Videos:	<input type="text" value="Wi-Fi Only"/> ?	Skype:	<input type="text" value="All Connections"/> ?	WhatsApp:	<input type="text" value="All Connections"/> ?
Viber:	<input type="text" value="All Connections"/> ?	Facebook:	<input type="text" value="All Connections"/> ?		
Keylogger:	<input type="text" value="All Connections"/> ?	Snapchat:	<input type="text" value="All Connections"/> ?		
Wi-Fi Networks:	<input type="text" value="All Connections"/> ?	Line:	<input type="text" value="All Connections"/> ?		

Wi-Fi is usually used when there's no data plan on the target device or it's too expensive. If you have Wi-Fi enabled all checked logs will be uploaded once the phone appears in Wi-Fi area. Please note that no data will be lost. mSpy will collect the logs and upload them once there's a connection.

'All Connections' means Cellular Internet and Wi-Fi. If there is a signal from both connections the first priority is always set to Wi-Fi connection.

Forensic Analysis Results: mSPY



Application Memory Exploitation Results

mSPY settings found:

```
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,"wifionly":false}, "note":{"enable":true,"wifi only":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}
```

Application Memory Exploitation Results

mSpy also captured the location of the device:

```
locations": [{"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": ""}]
```

mSpy Domains:

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

Packet Capture Results

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

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	32.439913	10.10.16.35	136.243.253.185	TCP	1514	[TCP segment of a reassembled PDU]
1933	32.439939	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	1	Follow TCP Stream
1940	32.440297	10.10.16.35	136.243.253.185	TCP	1	
1941	32.440322	10.10.16.35	136.243.253.185	TCP	1	
1942	32.440348	10.10.16.35	136.243.253.185	TCP	1	
1943	32.440373	10.10.16.35	136.243.253.185	TCP	1	
1944	32.440398	10.10.16.35	136.243.253.185	TCP	1	
1945	32.440421	10.10.16.35	136.243.253.185	TLSV1	1	

Frame 1931: 1514 bytes on wire (12112 bits), 1514 bytes captured
Ethernet II, Src: aaaa:03:00:00:00 (aaaa:03:00:00:00:00), Dst: 2e:
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: 0x010 (ACK)
Window size value: 123
Calculated window size: 157441

0000 2e 14 00 00 00 aa aa 03 00 00 08 00 45 00
0010 05 d6 b3 4a 40 00 46 e0 f7 0a 0a 10 23 88 f3@. @.
0020 fd b9 81 a8 01 bb f2 15 e7 f3 5c 38 dd e6 80 10
0030 00 7b 0d 3d 00 00 01 01 08 0a ff ff b7 ab 24 26 .{.
0040 cb 80 19 6f 42 ec 71 69 99 d5 e0 bf 76 e9 cc 56 ..0.., q1
0050 04 27 44 78 78 db 44 ae c7 1f 23 dt e6 53 40 ad .Dxx, D.
0060 06 cd 72 6f f9 38 cf ae d7 ab 7a 66 05 76 d7 ..r0.8..
0070 4b 6d c7 79 3e 7f 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 a5 99 80 d4 85 07 b7 f5 e0 69 4e de 60 b0 91 45T.N..E
00a0 12 66 4b 42 62 9f b5 13 0a ab 69 cb 2d e9 1a .jKBb.....y....
00b0 d9 ef 98 3d 86 8a 29 a7 c0 c3 c2 08 ab 04 56 ...=..).FV
00c0 fd 6d 4b 5e 81 24 77 a1 f1 46 dd 67 39 42 0b .mK^, Sw ..F.g98.
00d0 19 35 d5 9d 62 e7 b6 ee fa 56 2a 34 11 49 e2 23 .5.., t*] ..C
00e0 Fa 35 f1 2c 91 27 2a 4a c4 0b 1a 13 a1 e2 43 .5.., t*] ..C
00f0 69 fe 41 82 00 5f e3 a3 ff 09 1e 9c 75 1b 70 0d i.A.....u.}.
0100 b4 de 26 69 d4 32 c3 50 39 28 60 81 c0 21 7e 70 ..&1.2.P 9(..!-p
0110 b3 9e ef 08 6f 7d 2f 0c 30 fc bf d4 7b 5f ff 3co/. 0...{.<

Entire conversation (198152 bytes)

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

IP Address Information

IP Information for 136.243.253.185

Quick Stats

IP Location	 Germany Berlin Bitex Group Ltd
ASN	 AS24940 HETZNER-AS Hetzner Online AG (registered Jun 03, 2002)
Resolve Host	a.thd.cc
Whois Server	whois.ripe.net
IP Address	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-mntr@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@bitexgroup.ltd.com
nic-hdl:          PD7003-RIPE
notify:            ripe-mntr@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
```

Physical Acquisition Analysis Summary

- Google Chrome history contained evidence that the user visited <http://kypler.com/android> and downloaded bt.apk.
- The mSPY application installed to /Root/data/android.sys.process.
- The applications folder contained a sqlite database (internal.db) that stored all data collected by mSPY and a .xml file (settings.xml) which stores the spyware's settings.

Internal.db

Database view Hex View File Info

android_metadata (1)
applications (0)
blockedApps (0)
blockedNumbers (0)
blockedUrls (0)
blockedWifis (0)
bookmarks (0)
browser_history (0)
calendarEvents (0)
calls (0)
calls_index (5)
commandStatus (0)
commands (0)
contacts (3)
email_lastId (2)
emails (0)
facebook_messages (0)
facebook_thread_users (0)
facebook_threads (0)
images (6)
key_logs (0)
line_calls (0)
line_messages (0)
locations (10)
sentDataId (0)
skype_calls (0)
skype_lastId (0)
skype_messages (0)
sms (0)
sms_index (5)
snapItems (0)
sqlite_sequence (13)
viber_calls (0)
viber_messages (0)
viber_participants (0)
videos (0)
whatsapp_messages (0)

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

About SpyToMobile

- Second most common mobile spyware
- Sold on a subscription basis
- Cost \$0.99 per day

The screenshot shows the homepage of the SpyToMobile website. At the top, there is a dark header bar with the "Spy to Mobile" logo on the left, a search bar in the center containing the text "SpyToMobile, track a cell phone, sms spy", and a "Account" button on the right. Below the header is a navigation menu with links: "How it works", "About", "FAQ", "Price", "Video help", "Forum", and "Demo". The main content area has a light gray background with a green vertical bar on the left. The title "About the project" is centered at the top of this section. Below the title, there is a paragraph of text followed by a heading "These are some of our customer comments:" and three examples of customer reviews.

Sometimes it's necessary to watch a cell phone's activity. SpyToMobile application allows you to intercept incoming and outgoing SMS messages remotely, get contacts list, access call history, and follow the location of the device. Be sure that it is legal in your country or state.

These are some of our customer comments:

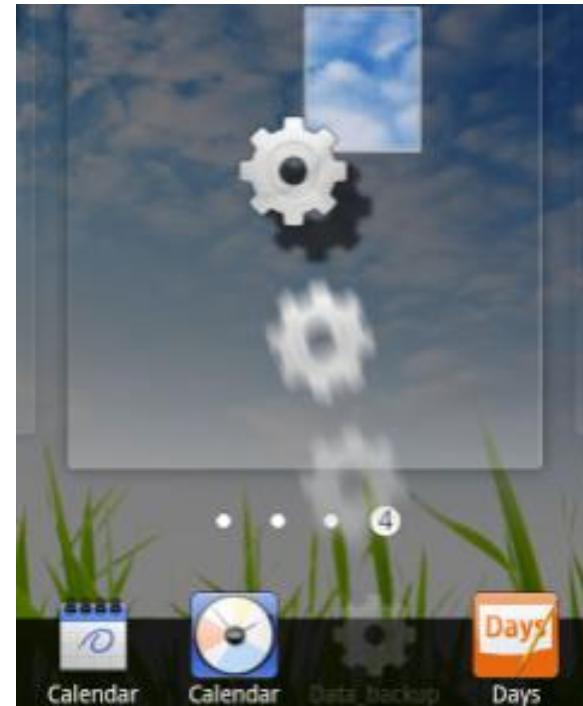
Celia.
I have a 14-year-old daughter. It's easy to fall into a bad company at her age. But now I know where she is. Thank you for the great app!

Michael.
Once I got really nervous and thought that my fiancee had started to contact her ex-boyfriend. I was quite happy to find that it was all in my imagination. SpyToMobile helped me to figure it out. I don't worry about it now, but I know that I can always check on her.

Pedro.
It's a really great app. I have installed it on my cell. So I can keep all the data from my cell in my account. That's great!!

Installing and Monitoring

- Requires physical access to the phone
- Modify security settings to allow untrusted apps.
- Browse to SpyToMobile.com/d
- Download and install Data_backup.apk
- Put ‘Data Backup’ widget on the screen.
- Enter email address.



Command and Control

The image shows a screenshot of a GPS tracking application interface. At the top left, there is a purple star icon followed by the text "Samsung GT-I9300". To the right of this is a dropdown menu labeled "Tracking Devices". The main area is a satellite map of a region featuring the "Little Patuxent River" running through a wooded area, with the "Patuxent Fwy" and "32" highway visible. A yellow star marker indicates the location of the tracked device. A white callout bubble provides detailed information about the tracked device: "samsung GT-I9300", "2015-07-15 20:21:43 (Wi-Fi)", and the coordinates "W76.8507 N39.1708". On the far left, there is a sidebar with various status icons and settings. These include a yellow star icon, a "GPS tracking" section with "On" and "Off" buttons, an "IMEI" number (353106068763034), a "Connected (Online)" status, a "GPS level (Poor)" indicator, a "Battery level (96%)", and the software version "ver.4.11.2". Below this are three small icons: a person, a mail, and a phone. Underneath the sidebar, there are three tabs: "Display", "Today", "Range", and "Online", with "Online" being the active tab. On the far right, there is a vertical sidebar with icons for "Sam" (a person icon), a telephone, an envelope, a speech bubble, and another envelope. At the bottom right, there is a vertical scroll bar.

Samsung GT-I9300

Tracking Devices

GPS tracking
On Off

IMEI: 353106068763034

Connected (Online)

GPS level (Poor)

Battery level (96%)

ver.4.11.2

Display

Today Range Online

samsung GT-I9300
2015-07-15 20:21:43
(Wi-Fi)
W76.8507 N39.1708

Patuxent Fwy

32

14A

Patuxent Branch Trail

Little Patuxent River

Capitol Office Solutions

Patuxent Branch Trail

Stone Brook Ln

Sea Dr

Brook Ln

Google

Sam

(410) 72

Forensic Analysis Results: SpyToMobile



Application Memory Exploitation

SpyToMobile recorded text message:

```
{"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}
```

duration

/data/data/com.spy2mobile.light/databases/msgstore.db

Application Memory Exploitation

Evidence of SpyToMobile recording wireless network locations:

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:7d

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

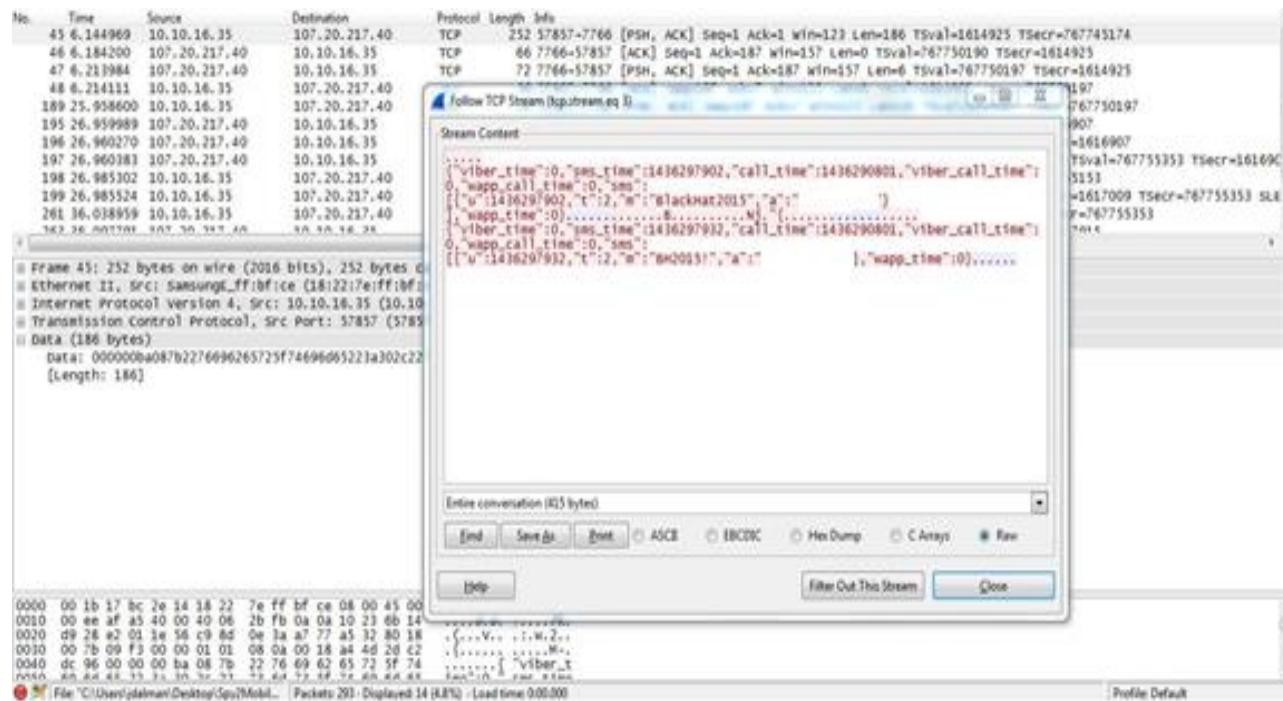
W:87.0

C:-1

L:39.170727 -76.85074

Packet Capture Results

Analysis of network traffic indicated that SpyToMobile communicates with IP Address 107.20.217.40 using TCP over port 7766.



IP Address Information

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

Physical Acquisition Analysis Summary

- Google Chrome History contained evidence that the user visited <http://spy2mobile.com/d> and downloaded a file named:
Data_backup.apk
- The SpyToMobile application is installed to
/data/data/com.spy2mobile.light
- The applications folder contained a sqlite database (system.db) that stored all data collected by mSPY.

- ▷ com.sec.smartcard.manager
- ▷ com.sec.smartcard.pinservice
- ▷ com.sec.spp.push
- ▷ com.sec.tcpdumpservice
- ▷ com.sec.usbsettings
- ▷ com.siso.app.generic
- ▷ com.siso.app.genericprintservice
- ▷ com.smlds
- ▷ com.spy2mobile.light
- ▷ com.tripadvisor.tripadvisor
- ▷ com.visionobjects.resourcemanager
- ▷ com.vlingo.midas
- ▷ com.wsomacp
- ▷ com.wssnps
- ▷ com.wssyncldm
- ▷ eu.chainfire.supersu
- ▷ flipboard.app
- ▷ lv.n3o.shark

System.db

UFED Physical Analyzer 4.2.1.7

File View Tools Extract Python Plug-ins Report Help

Welcome x Extraction Summary x History x system.db x All Projects

Database view Hex View File Info

com.spy2mobile.light

- cache
- databases
 - msgstore.db
 - msgstore.db-journal
 - system.db
 - system.db-journal
 - viber_messages
 - viber_messages-journal
- files
- shared_prefs
 - preferences.serializable
 - lib
- com.tripadvisor.tripadvisor
- com.visionobjects.resourcemanager
- com.vlingo.midas
- com.wsomacp
- com.wssnps
- com.wssyncldm
- eu.chainfire.supersu
- flipboard.app
- lv.n3o.shark
 - media
- org.simalliance.openmobileapi.service
 - sstream.app
- dontpanic
- drm
- fota
- hostapd
- local
- log

android_metadata (1)

	id	bssid	ssid	lgt	ltt	upd	chg	wgt	sec
✓	25	00:24:b2:14:8e:f0	Agetech24	ÿ8ÿ&ÿfÿ\nÿo{ÿÿM	ÿÿÿFEMÿs:r	1436976159.446	0	66	PSK
✓	26	9c:d6:43:d7:07:06	BHMC2	ÿrÿxÿÿÿÿÿÿÿÿ	'055ÿÿÿÿÿÿÿÿ	1436976159.449	0	77	PSK
✓	27	e8:b7:48:26:51:dc	PDRICOL01	~Lÿÿÿÿÿÿÿÿÿÿ	À&ÿJZIÿGÿÿÿÿFS	1436976159.451	0	79	PSK
✓	28	10:08:b1:f6:68:06	HP-Print-06-LaserJet 200	s+ÿÿÿÿÿÿÿÿÿÿ	nR)D9ÿÿÿÿÿÿÿÿ	1436976159.453	0	71	PSK
✓	29	2c:b0:5d:4b:c6:06	NETGEAR94	ÿ.w	ÿÿÿNÿÿÿÿÿÿÿÿ	1436976159.455	0	77	PSK
✓	30	00:24:b2:7c:cb:74	NETGEAR	ÿ.w	ÿÿÿNÿÿÿÿÿÿÿÿ	1436976159.457	0	77	WEP
✓	31	00:17:c5:88:95:97	CFWwireless	ÿ.w	ÿÿÿNÿÿÿÿÿÿÿÿ	1436976159.481	0	77	PSK
✓	32	98:fc:11:f7:c0:c4	amkqb	sÿ6ÿÿÿÿÿÿÿÿÿÿ	ÿ3gÿxU9ÿÿÿÿÿÿÿÿ	1436976159.483	0	77	PSK
✓	33	20:e5:2a:60:d5:72	SKYNET	sÿ6ÿÿÿÿÿÿÿÿÿÿ	ÿ3gÿxU9ÿÿÿÿÿÿÿÿ	1436976159.485	0	77	PSK
✓	34	00:14:d1:ca:60:b0	SiteLink2	uÿÿÿÿÿÿÿÿÿÿ	?ÿÿÿÿÿÿÿÿÿÿ	1436976159.487	0	76	PSK
✓	35	c8:d7:19:1e:fc:29	DP	ÿÿÿÿÿÿÿÿÿÿ	PÿÿÿÿÿÿdhYÿÿÿÿ	1436976159.49	0	78	PSK
✓	36	10:c3:7b:de:5e:d8	UT-HQ	ÿÿÿÿÿÿÿÿÿÿ	PÿÿÿÿÿÿdhYÿÿÿÿ	1436976159.491	0	78	PSK
✓	37	9c:ad:97:5c:02:f8	HP-Print-f8-Color LaserJet MFP	jÿXÿÿÿÿÿÿÿÿÿÿ	ÿAÿÿÿÿWÿÿÿÿÿÿÿÿÿÿ	1436976159.493	0	79	PSK
✓	38	1:caf:f7:dd:c1:0d	wellness	ÿÿPkÿÿEÿÿÿÿÿÿ	ÿÿWÿÿÿÿÿÿÿÿÿÿ	1436976159.495	0	79	PSK
✓	39	00:7f:28:b6:5a:2c	T22XL	ÿGvÿÿÿÿÿÿÿÿÿÿ	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	1436976159.497	0	80	PSK
✓	77	b4:c7:99:b4:21:e3	c8e3C3d9D5c3	>mÿÿÿÿÿÿÿÿÿÿ	ÿÿTÿÿÿÿÿÿÿÿÿÿ	1436980674.495	0	57	PSK
✓	78	b4:c7:99:b4:21:e1	HT Public Wi-Fi	ÿÿRÿÿÿÿÿÿÿÿÿÿ	ÿÿÿÿPÿÿÿÿ	1436980674.5	0	71	OPEN
✓	79	0c:54:a5:7c:6f:20	HOME-6BBB-2.4	ÿÿÿÿÿÿÿÿÿÿ	ÿÿJcÿÿÿÿÿÿÿÿÿÿ	1436980674.504	0	67	PSK
✓	80	00:17:c5:8c:5f:6a	VAP-St-Matthew-Guest	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	1436980674.509	0	58	PSK
✓	81	16:9a:dd:8d:26:91	Irv Schindler's Guest Network	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	1436980674.513	0	77	PSK
✓	82	0c:54:a5:73:61:d0	HOME-6F05-2.4	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	ÿÿÿÿÿÿÿÿÿÿÿÿÿÿ	1436980674.517	0	67	PSK

How do I know if I have been infected?

- Use a strong passcode and limit physical access to the phone.
- Check visited URLs and Download history.
- Examine security settings and determine if Unknown Sources is enabled.
- Look for new and unfamiliar Widgets or Apps.
- If still uncertain, take a pcap!

Similar Work

Robinson, M & Taylor, C. (2012, July). Spy vs. Spy: Examining spyware on mobile devices. Presented at Defcon 20, Las Vegas, NV.

Spyware Analyzed: FlexiSpy, SpyBubble, MobiStealth, Mobile-Spy, Spyera.

Works Cited

- Krebs, B. (2015, May 14). Mobile Spyware Maker mSpy Hacked, Customer Data Leaked. Retrieved from
<http://krebsonsecurity.com/2015/05/mobile-spy-software-maker-mspy-hacked-customer-data-leaked/>
- 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
- 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>



QUESTIONS?

Josh.Dalman@FidelisSecurity.com

Valerie.Hantke@FidelisSecurity.com