FIDELIS CYBERSECURITY

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…

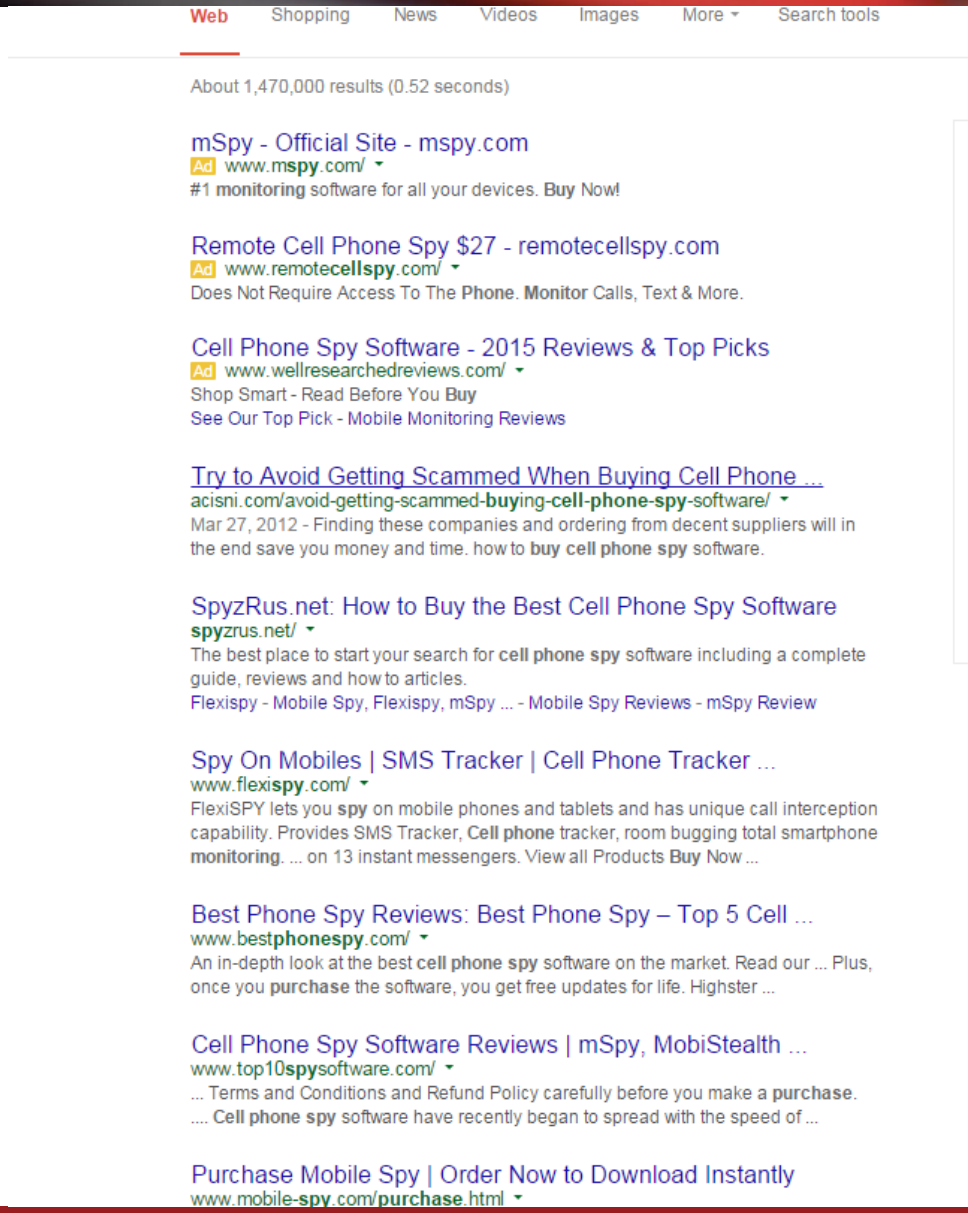
Overview

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

Spyware Introduction

Mobile spyware is:

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



What We Know

Lacoon Mobile Security /Check Point Study:

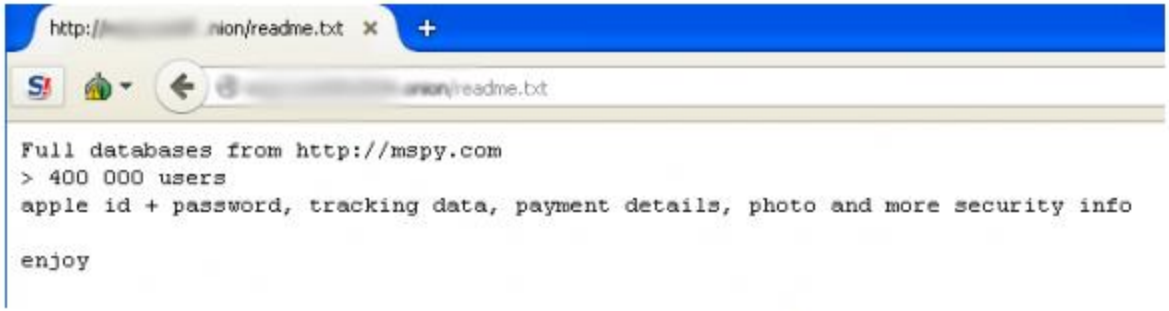
- Sampled nearly 1 million devices (50% Android, 40% iOS, 10% Other) communicating through corporate Wi-Fi .
- Detected over 20 variants and 18 different families of spyware products.
- Two spyware programs (SpyToMobile and Mspy) accounted for more than half of all infections.
- Organizations with 2,000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

What could possibly go wrong?

14 MAY 15 Mobile Spyware Maker mSpy Hacked, Customer Data Leaked

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

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

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 if 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 phones 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."

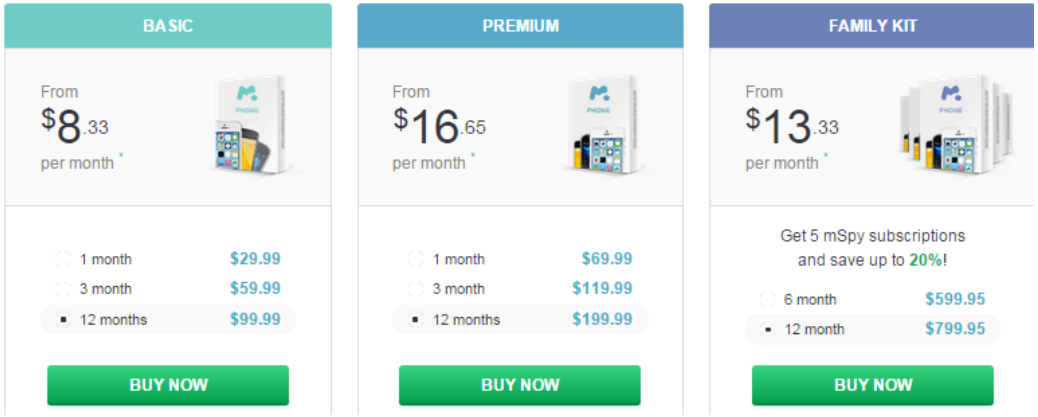
"Mr. Akbar is the first-ever person to admit criminal activity in advertising and selling spyware that invades an unwitting victim's confidential communications," said FBI Assistant Director in Charge McCabe. "This illegal spyware provides individuals with an option to track a person's every move without

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

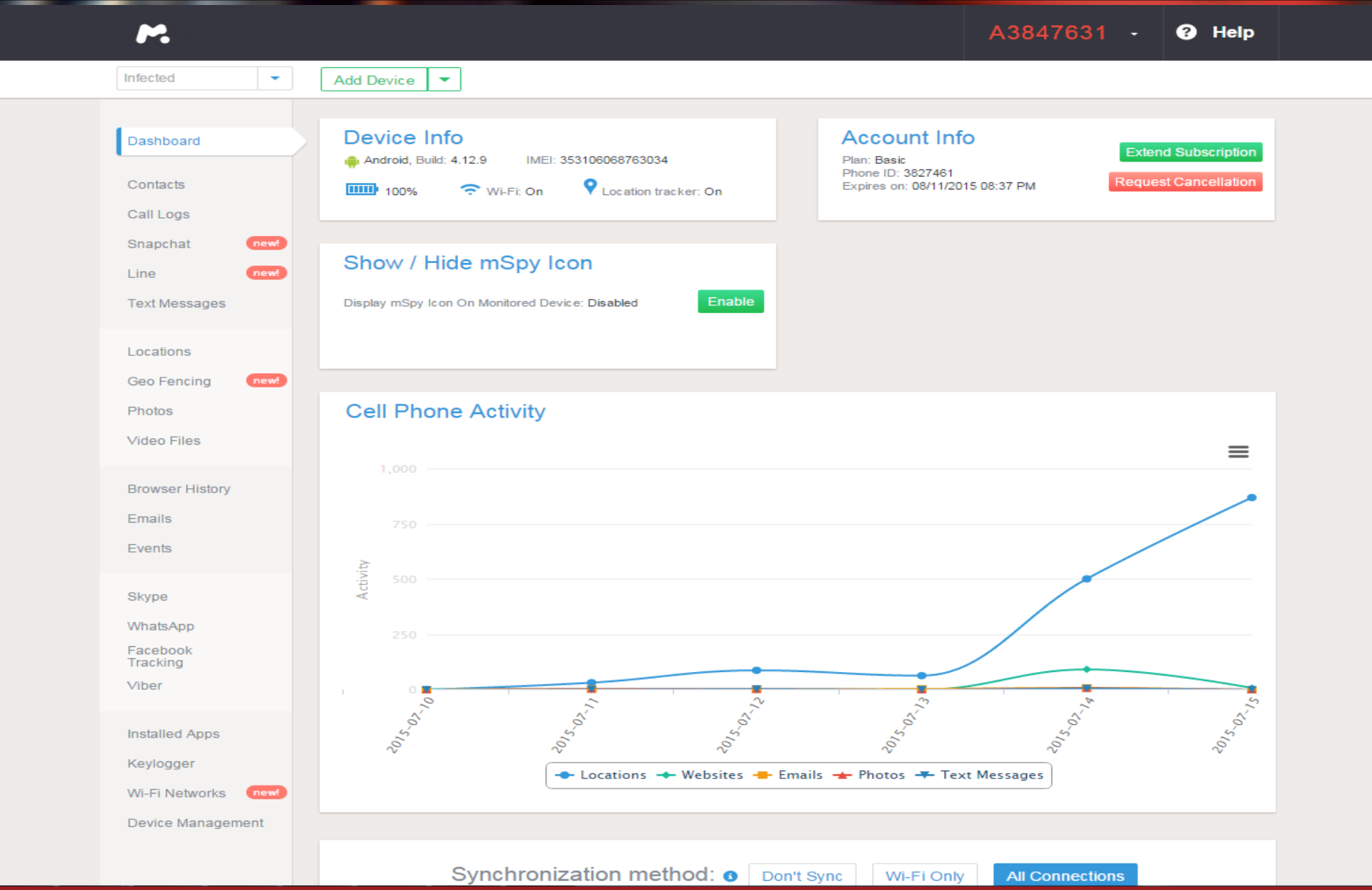
Experiencing difficulties with an installation? Having hard times with setting up the features? Or simply tired of reading technical manuals? Relax! We'll do everything for you.

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



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:	1 minutes	Location Update Interval:	1 minutes	Units:	foot
Locations:	All Connections	Call logs:	All Connections	SMS:	All Connections
Address Book:	All Connections	Events:	All Connections	E-mails:	All Connections
Browser History :	All Connections	Installed Apps:	All Connections	Photos:	Wi-Fi Only
Videos:	Wi-Fi Only	Skype:	All Connections	WhatsApp:	All Connections
Viber:	All Connections	Facebook:	All Connections		
Keylogger:	All Connections	Snapchat:	All Connections		
Wi-Fi Networks:	All Connections	Line:	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,"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}

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":"-

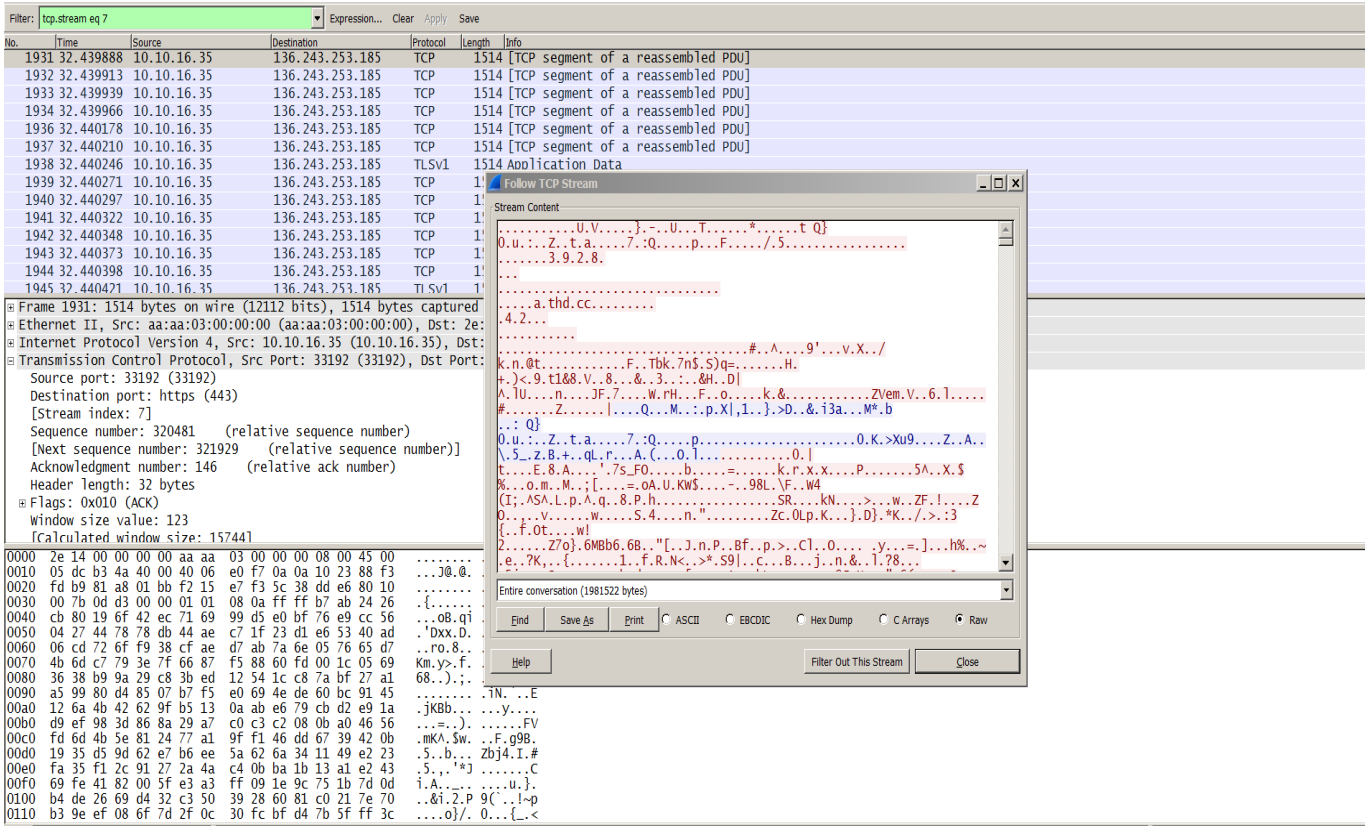
76.8511957","latitude":"39.1704807"},{"timestamp":"1436895210","accuracy":26.86199951171875,"longitude":"-76.8511427","latitude":“

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.



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-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
```

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

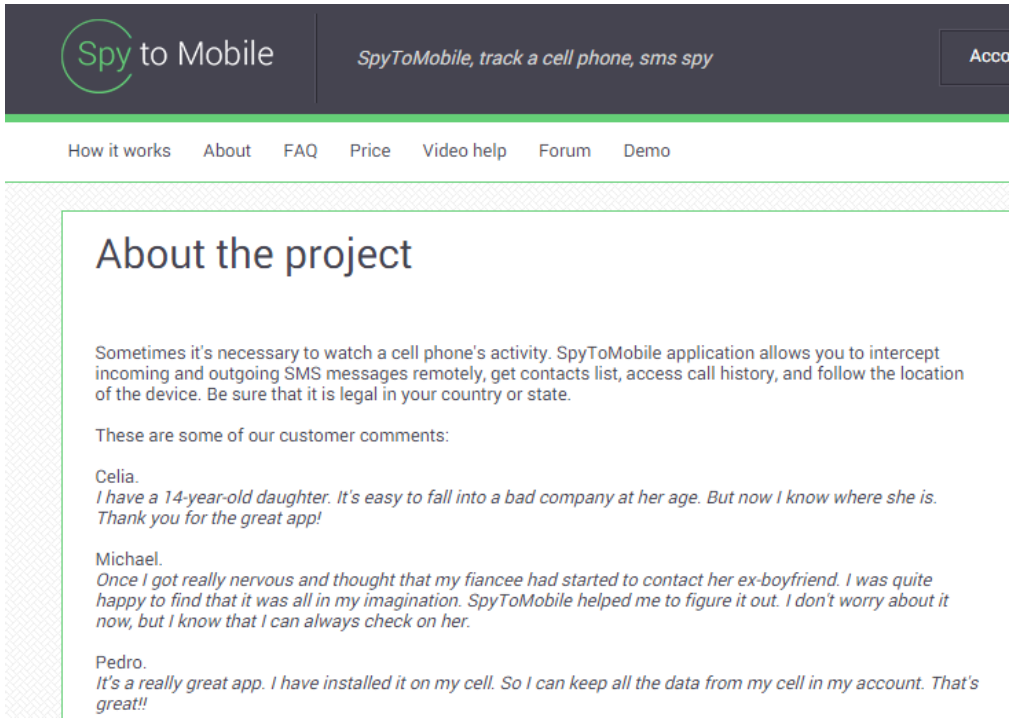
Database view | Hex View | File Info

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)

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

About SpyToMobile

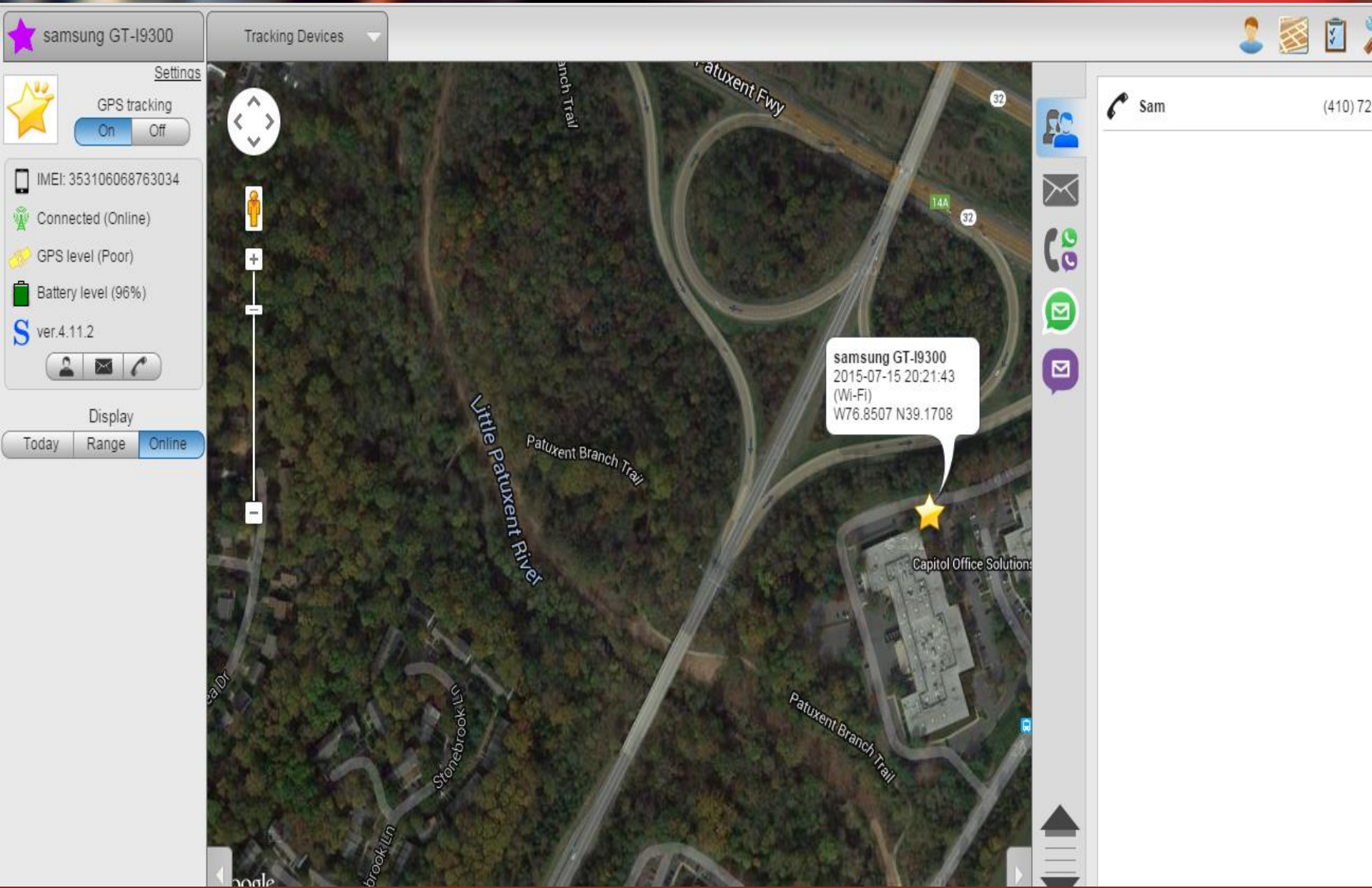
- Second most common mobile spyware
- Sold on a subscription basis
- Cost $0.99 per day



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



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

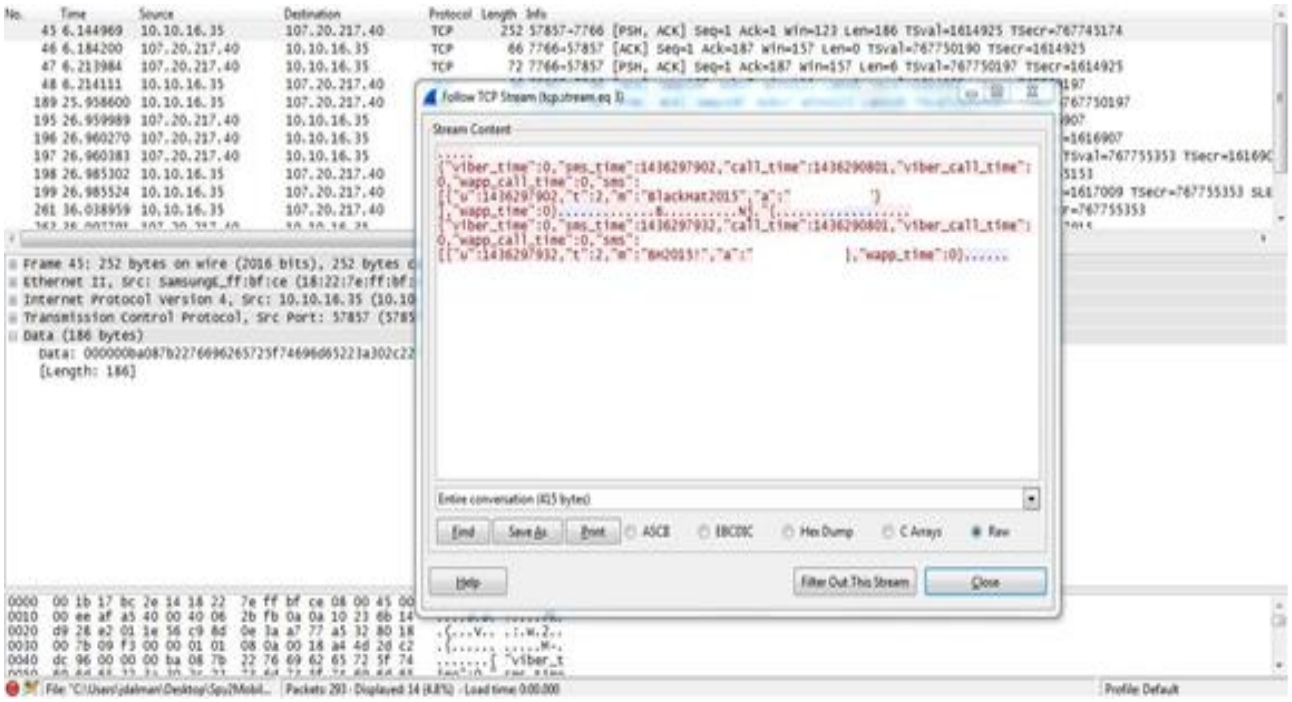
Application Memory Exploitation

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.

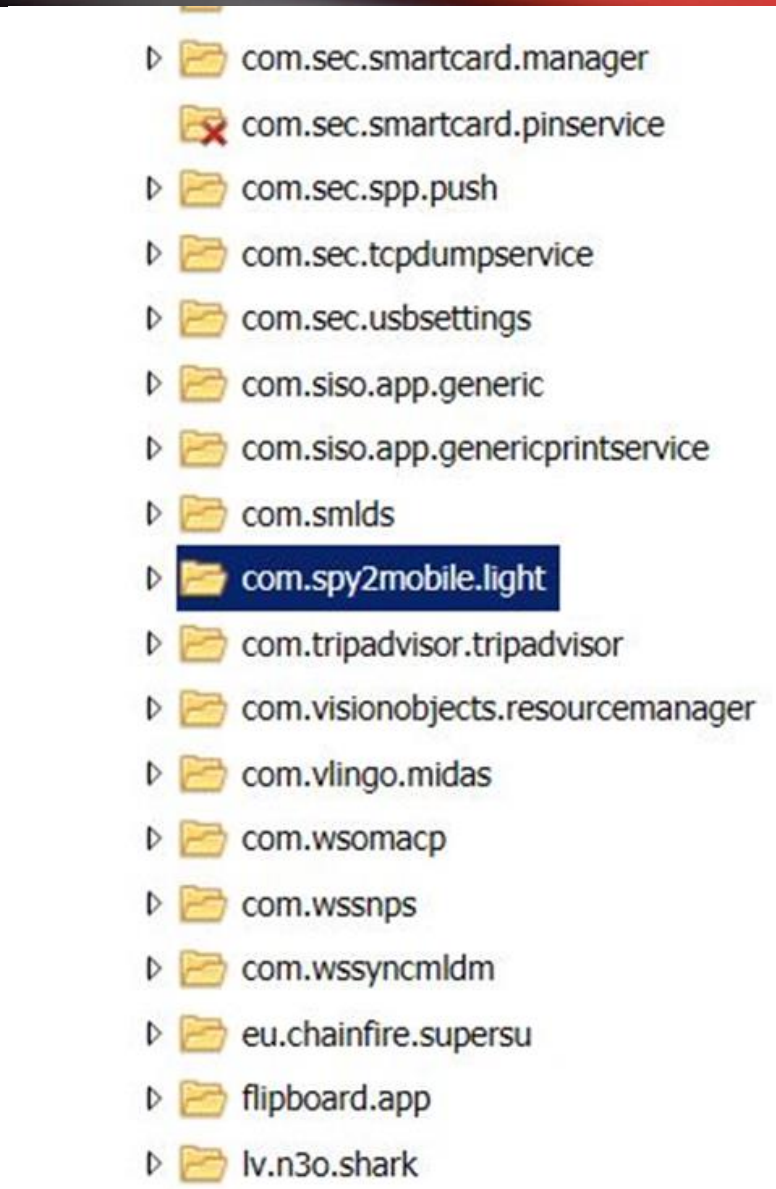


IP Address Information

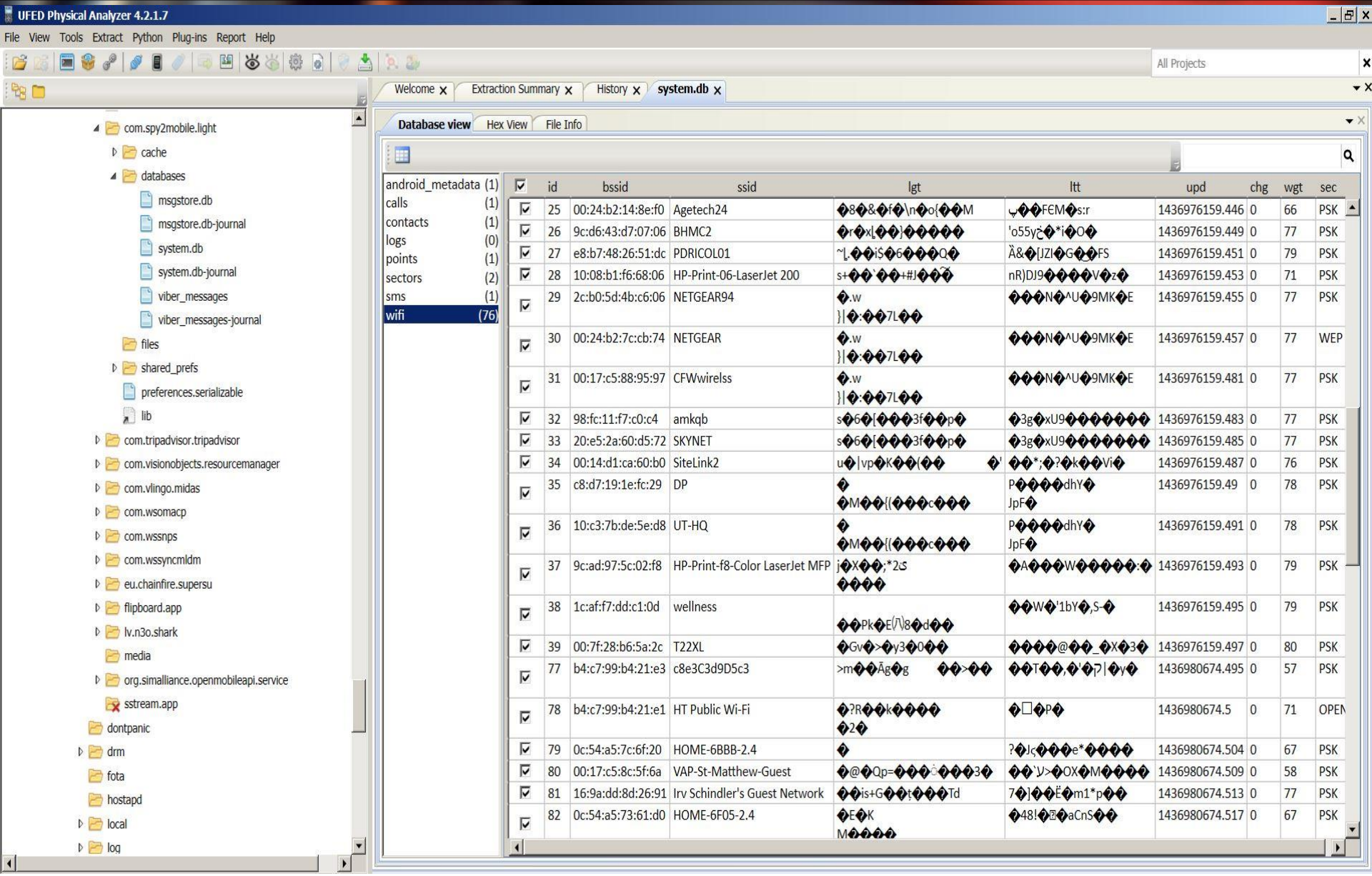
Registrant Org	Domains By Proxy, LLC was found in ~11,111,910 other domains
Registrar	WILD WEST DOMAINS, LLC
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	Created on 2012-02-15 - Expires on 2016-02-15 - Updated on 2015-01-19
Name 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.



System.db


UFED Physical Analyzer 4.2.1.7
File View Tools Extract Python Plug-ins Report Help
All Projects
Welcome
Extraction Summary
History
system.db
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.wssyncmldm
eu.chainfire.supersu
flipboard.app
lv.n3o.shark
media
org.simalliance.openmobileapi.service
sstream.app
dontpanic
drm
fota
hostapd
local
log
android_metadata (1)
calls (1)
contacts (1)
logs (0)
points (1)
sectors (2)
sms (1)
wifi (76)
id bssid ssid lgt ltt upd chg wgt sec
25 00:24:b2:14:8e:f0 Agetech24 1436976159.446 0 66 PSK
26 9c:d6:43:d7:07:06 BHMC2 1436976159.449 0 77 PSK
27 e8:b7:48:26:51:dc PDRICOL01 1436976159.451 0 79 PSK
28 10:08:b1:f6:68:06 HP-Print-06-LaserJet 200 1436976159.453 0 71 PSK
29 2c:b0:5d:4b:c6:06 NETGEAR94 1436976159.455 0 77 PSK
30 00:24:b2:7c:cb:74 NETGEAR 1436976159.457 0 77 WEP
31 00:17:c5:88:95:97 CFWwirelss 1436976159.481 0 77 PSK
32 98:fc:11:f7:c0:c4 amkqb 1436976159.483 0 77 PSK
33 20:e5:2a:60:d5:72 SKYNET 1436976159.485 0 77 PSK
34 00:14:d1:ca:60:b0 SiteLink2 1436976159.487 0 76 PSK
35 c8:d7:19:1e:fc:29 DP 1436976159.49 0 78 PSK
36 10:c3:7b:de:5e:d8 UT-HQ 1436976159.491 0 78 PSK
37 9c:ad:97:5c:02:f8 HP-Print-f8-Color LaserJet MFP 1436976159.493 0 79 PSK
38 1c:af:f7:dd:c1:0d wellness 1436976159.495 0 79 PSK
39 00:7f:28:b6:5a:2c T22XL 1436976159.497 0 80 PSK
77 b4:c7:99:b4:21:e3 c8e3C3d9D5c3 1436980674.495 0 57 PSK
78 b4:c7:99:b4:21:e1 HT Public Wi-Fi 1436980674.5 0 71 OPEN
79 0c:54:a5:7c:6f:20 HOME-6BBB-2.4 1436980674.504 0 67 PSK
80 00:17:c5:8c:5f:6a VAP-St-Matthew-Guest 1436980674.509 0 58 PSK
81 16:9a:dd:8d:26:91 Irv Schindler's Guest Network 1436980674.513 0 77 PSK
82 0c:54:a5:73:61:d0 HOME-6F05-2.4 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

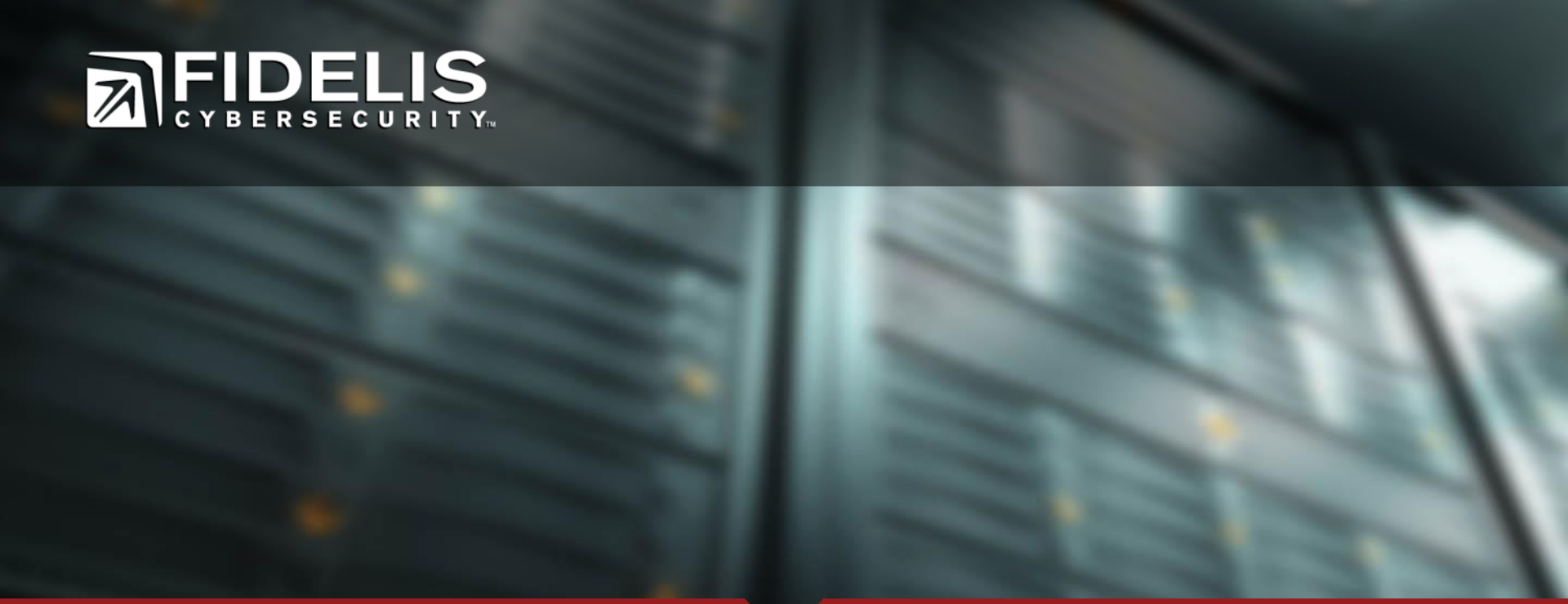
Krebs, B. (2015, May 14). Mobile Spyware Maker mSpy Hacked, Customer Data Leaked. Retrieved from http://krebsonsecurity.com/2015/05/mobile-spy-software-maker-mspy-hacked-customer-data-leaked/

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/Lacoon_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