Let's Talk About FlexiSpy

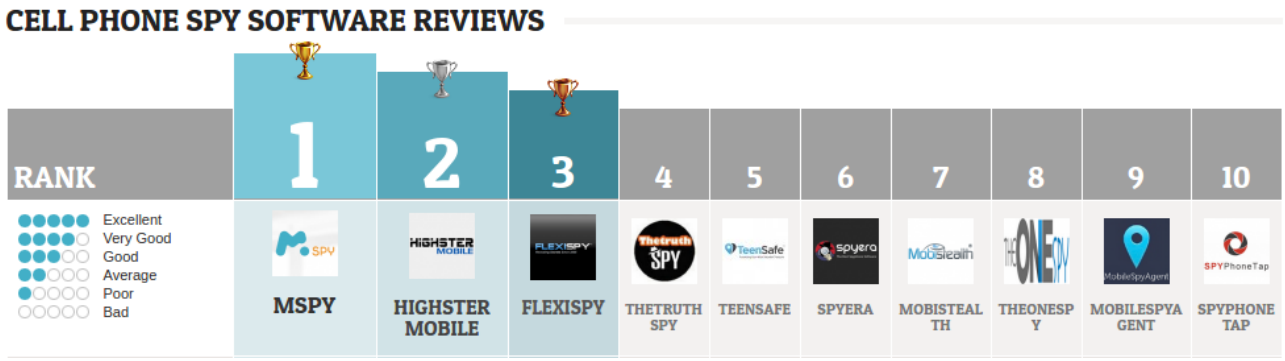
randhome.io/blog/2017/04/23/lets-talk-about-flexispy/

23 Apr 2017 · 7 minutes read

Introduction: I started this blog post to explain the context of FlexiSpy leaks and show some information I have found during my analysis. This information is incomplete and there is still plenty analysis of source code or binaries to be done. I have uploaded the source code and binaries on github so that everyone can help with it. I will try to report in this articles the publications I have seen on it, but feel free to ping me on Twitter if you see new information or have any question.

FlexiWho?#

FlexiSpy is one of these companies selling surveillance software to people who want to spy on their wife/husband/partner (a.k.a. StalkerWare). You think that it is creepy? Well, it is likely worse than you imagine. First, there are dozens of companies like FlexiSpy, selling software allowing to remotely track everything the other person is doing : emails, calls, chat apps, calendar… The market is so developed that you can even find websites ranking them:



And the impact is really awful : a 2015 women's aid survey showed that 29% of women experiencing domestic abuse had a spyware or GPS locator installed on their phone.

FlexiSpy is not even the bigger StalkerWare seller (Mspy seems to have more than one million customers) but they have something specific : in February a Forbes article showed that FlexiSpy is sharing part of its code with a tool called FinFisher, done by a UK-German company called Gamma International.

Screenshot of FinFisher website...

FinFisher is also a tool to spy on computers and smartphones but specifically for Law Enforcement and Intelligence agencies, and although their website pretends that it is used against crime, we have seen consistent utilization of this spyware against activists or political opponents:

- In March 2011, Egyptian protesters who broke into the headquarters of the Egyptian intelligence service found contracts between Gamma Group and the Egyptian government
- Since 2012, it was used several times against Bahrain political activists. Gamma denied selling FinFisher to the Bahrain government and stated that their software could have been stolen but leaked Gamma documents later showed that not only Gamma sold their product to the Bahraini government but also that they knew that their tool was used to target journalists and political dissidents
- In 2013, Citizen Lab researchers identified FinFisher samples used against political groups in Ethiopia, in Vietnam and in 25 other countries. An Ethiopian political dissident in exile in London, Tadesse Kersmo, discovered with this report that he was targeted and that his computer was successfully compromised with FinFisher.
- In 2015, Privacy International researchers confirmed the use of FinFisher against political opponents in Uganda

In 2015, Citizen Lab researchers scanned the Internet for FinFisher server and identified 33 countries using the product:

Map of government suspected to use FinFisher (CitizenLab - 2015)

So What?#

Last week, we learned something interesting : two persons decided that the StalkerWare business was not ethically acceptable and went after FlexiSpy and another company called Retina-X. They found vulnerabilities in their systems, successfully hacked them, stole all their information and wiped the disks. They finally shared some of their files with Motherboard journalists through their SecureDrop instance.

We learned some interesting facts from the first article published by Motherboard but also in the interview they gave and in the last Motherboard article about FlexiSpy:

- FlexiSpy started from a small Thai company called Vervata in 2004, developing software until they started a first spying tool for Symbian in 2006. They later started a company called “Digital Endpoint” selling products to monitor employees.
- They started a sister company called “RaySoft” selling to Law Enforcement agencies, and then a partnership with Gamma in 2011 on this market
- Around 130 000 people had an account on Retina-X or Flexispy platforms
- The hack was apparently quite easy and exploited a bug in the API
- The hacker called Leopard Boy (a reference to the classic 1995 Hacker Movie) is apparently gonna continue targeting companies doing this business : *“It’s the beginning of a reign of terror across this entire industry. I’m going to burn them to the ground, and leave absolutely nowhere for any of them to hide.”*

Map of compromised smartphones with FlexiSpy (motherboard - 2017)

But more interesting, the Leopard Boy hacker started yesterday to publish documents and code on his Twitter account @fleximinx. I have uploaded the source code and binaries on a github repository and I will go through the interesting information I got from them during the past days.

What did we get?#

So what did we get in these leaks:

- Documents about the FlexiSpy and sisters companies
- Source code of Flexispy Android App v1.00.1 and 1.00.4
- Source code of Blackberry spyware v.1.03.2 (from Jan 2012)
- Source code of iPhone spyware version 4.9.1
- Binaries of FlexiSpy malware for all platforms:

A View Of FlexiSpy Market Strategy#

One document named *Flexi - Battleplan* gives an interesting view of FlexiSpy market strategy (the document is from June 2009):

Executive Summary

Time to fight back; competitors are eroding our market share.

Playing to our strengths will produce greater wins, quickly, easily, and cost effectively.

We intend to improve our competitive position against other spy phone vendors, particularly Mobile-Spy; and include affiliate program development in this effort. To beat down mobile-spy.com we need to get more presence in related keyword organic SERP and position Adwords against their campaigns.

Because we have intelligence on competitor Google Adword keyword selection and CPC budget we can easily match them ad for ad and have a Flexispy or SpyPhoneReview.com ad wherever their ads are placed.

We can also take this a bit further in sophistication by targeting keywords, copy and budget based on where buyers are in their sales cycle: discovery – research and evaluation – purchase. As they move through the sales cycle, they become more valuable and we can assign a higher CPC budget.

So their strategy focus mainly on buying Adwords, and bid more on Adwords used by their competitors on which they did an advanced analysis:

Then they define different Adwords campaigns including a creepy one:

Campaign: Cheating Bastards and Bitches

- Discovery Phase of Sales Cycle. People exploring their options to deal with infidelity.

Adgroup	CPC	Geo	Keywords	Ad Copy	Search	Landing Page	Traffic Estimate
Cheaters_search		global	CheaterList1		search		
Cheaters_placement		global	CheaterList1		Selected related sites		

Google Traffic Estimator (Guestimator) – Google is a usually a bit optimistic in CTR percentage, these figures should be used for budgeting purposesand idea of scope of interest in the market.

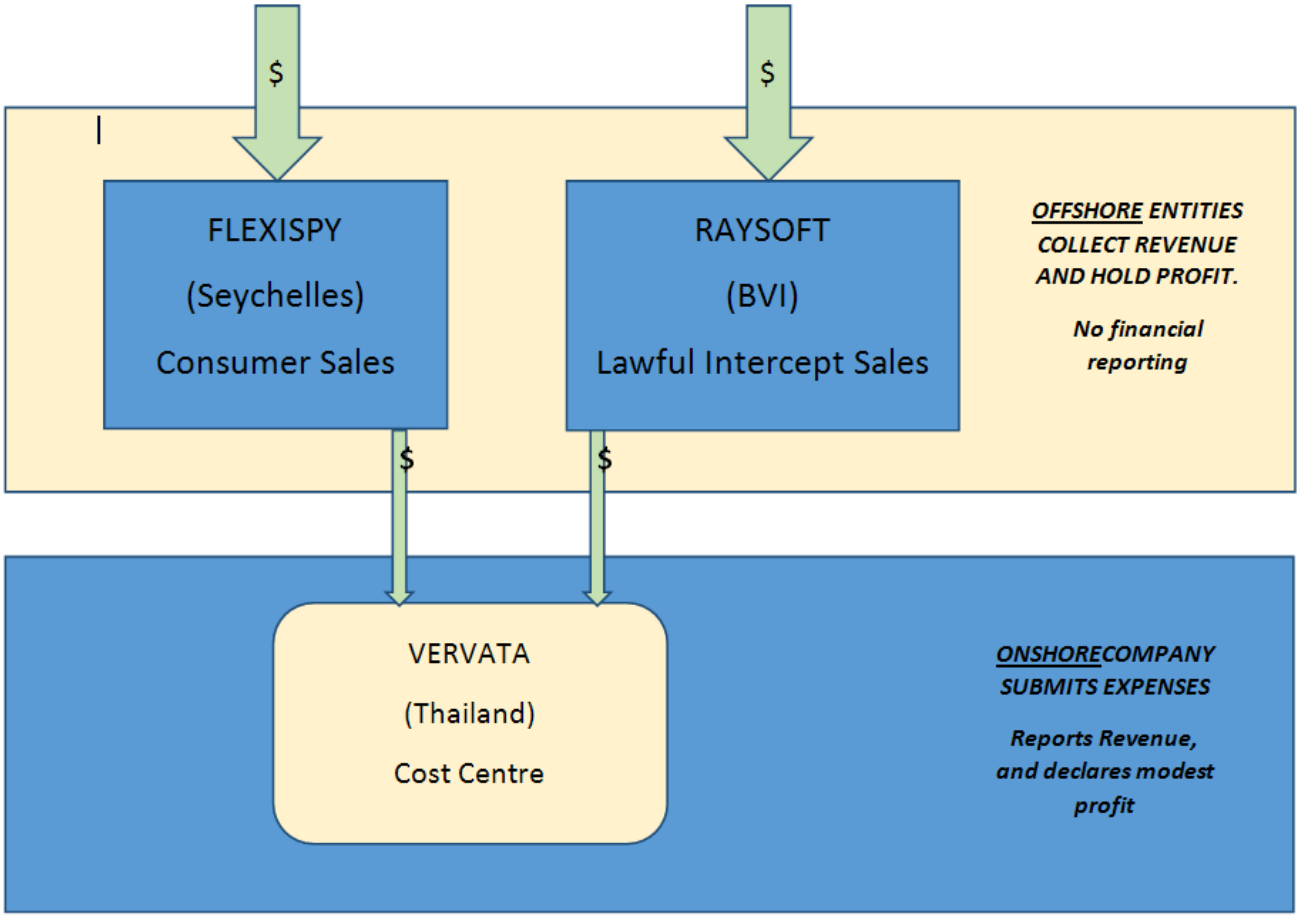
This group could be expanded or segmented to include inquiries regarding private investigators under the assumption that if looking for investigator would be interested in spy phone.

We also learn that they created a website reviewing spy software (which is not online anymore but I bet FlexiSpy had good reviews):

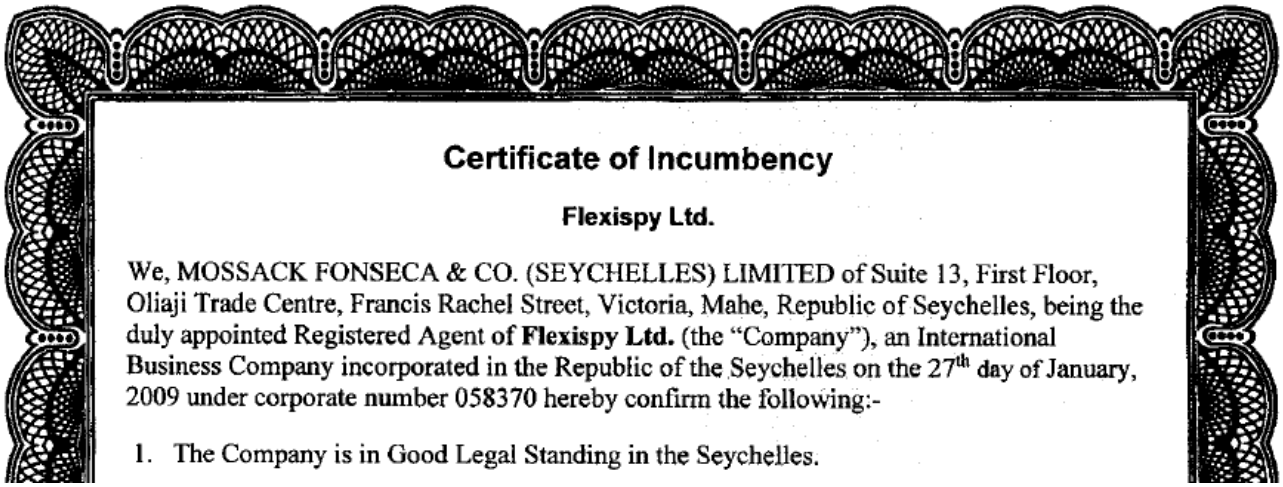
The question remains whether it is more beneficial to make an effort to drive people to SpyPhoneReview.com or cut to the chase and direct them to review and comparison pages on Flexispy.com. Also, www.flexispy.com as the display URL is going to get better aCTR click through rate.

They Don't Like Taxes#

Two documents give also an interesting view on their off-shore strategy, first with the link between their companies:



But also with a copy of their contract with the notorious Mossack Fonseca laywer firm in the Seychelles (Monssack Fonseca was the company at the center of the Panama Papers):



Certificate of Incumbency

Flexispy Ltd.

We, MOSSACK FONSECA & CO. (SEYCHELLES) LIMITED of Suite 13, First Floor, Oliaji Trade Centre, Francis Rachel Street, Victoria, Mahe, Republic of Seychelles, being the duly appointed Registered Agent of **Flexispy Ltd.** (the "Company"), an International Business Company incorporated in the Republic of the Seychelles on the 27th day of January, 2009 under corporate number 058370 hereby confirm the following:-

1. The Company is in Good Legal Standing in the Seychelles.

Installing Cyclops#

Cyclops is the name a surveillance tool used by Gamma and FlexiSpy (I don't know exactly what is the difference with FinFisher, it may be FlexiSpy internal name), and the install documentation (from 2011) leaked clearly confirms the collaboration between FlexiSpy and Gamma :

1. Introduction

Cyclops is a client/server monitoring platform for legally authorized Gamma customers, to be used with officially supported mobile phone clients (Windows Mobile, Symbian, and Blackberry defined models). The installation of this system is done on the Client site, and requires a minimum level of preparation and training to be successful.

The installation is officially executed by Gamma with specialists from FlexiSPY embedded into the installation team.

1.1 Purpose

The purpose of this document is to define the preparation and resourcing required from both FlexiSPY and Gamma to ensure the Client has a seamless installation experience delivered by Gamma.

Introduction of the Install Guide

4.4 CheckList of Deliverables

Intended use of this checklist :		This checklist should be used during installation		
	Finspy Mobile Brunei			
	Installation Checklist			
Sl.No	Description	Gamma	FlexiSPY	Confirm (Yes/No)
1	Server with Centos ver 5.5 and 64 BIT	X		
2	GSM modem (power and usb cable)	X		
3	2 SIM card for each operator	X		
4	Blackberry service enabled on SIM	X		
5	Blackberry device (Bold 9700 preferable)	X		
6	Symbian device (Nokia E72 preferable)	X		
7	Windows Mobile (Professional edition)	X		
8	UAT document	X	X	
9	IP Address (Server URL to access the system)	X		
10	Mobile Binary files		X	
11	License file		X	
12	Product definition file (contains remote commands)		X	
13	Deployment script	X	X	
14	SSH connection upon installation	X		
15	Repository server is online	X		
16	Backup repository server		X	
17	Network Engineer	X		
	Reviewer :			
	Review Date :			

List of Deliverables

This documents seems to indicate that FlexiSpy was actually developing Cyclops while Gamma was reselling it and maintaining it without involvement in the development of the tool. But as @Josephfcox pointed out on Twitter, it is possible that it was a proposal for a

customer that never happened (I doubt it though).

And Then Atlantis Arrived#

Atlantis is an enterprise product to monitor employees mobile devices. It seems to be a FlexiSpy product in this documentation, but it may be the product which later led to the creation of the Digital Endpoint company:

2 INTRODUCTION

Atlantis is a Mobile based Surveillance System that can be used by corporates to monitor employee mobile devices. *Atlantis* is ideal for situations where access to the mobile operator's network is not available or where Off Air Interception is not practical or limited due to encryption and accessibility.

Once the mobile device is infected with *Atlantis* the software will collect and deliver data to the central *Atlantis* server, intercept voice calls and allow listening to the targets surrounding. The *Atlantis* also accepts a full set of control commands enabling remote configuration of the device.

The *Atlantis Server* provides an easy to understand GUI that allows data mining of recorded communications, GPS position visualization on a map, Mobile Agent control functions and administration features.

The server comes with an option to connect a Call Interception using *Atlantis recording* server that will simultaneously record multiple intercepted calls.

These documents also gives an idea of the price (in 2012):

Item	USD	Notes
MSS Server Software	250,000	Base System with no License Pack
CIS Server Software	50,000	Delivers 30 line capabilities. Additional lines require purchase of extra PRI Cards.
10 Floating Licenses F10	6000	Pack of ten floating licenses
10 Fixed License Pack L10	2500	Pack of tem fixed licenses
Custom UI / Integration services	Price On Application	
Support Contract	25,000	Annual support including updates for one year
Training	1500 per day	Client sends their support technician to FlexiSPY offices for training

Android Source Code#

The Android source code leaked is for the version 1.00.1 while the Android APKs are in version 2.24.3 and 2.25.1m so it seems to be pretty old code.

Nevertheless, we can quickly get the IP addresses and domains used by the application (here, here, here or here):

- 192.168.2.60 and 192.168.2.116 are used as a dev IP

- 58.137.119.227
  - hxxp://58.137.119.227:880/RainbowCore/gateway/unstructured
  - hxxp://58.137.119.227:880/RainbowCore/gateway
- 58.137.119.229:
  - hxxp://58.137.119.229/RainbowCore
  - hxxp://58.137.119.229/RainbowCore/gateway
- 58.137.119.230
  hxxp://58.137.119.230/Core/gateway
- hxxp://www.vervata.com
- hxxp://www.flexispy.com
- trkps[.]com
  hxxp://trkps.com/m.php?lat=%f&long=%f&t=%s&i=%s&z=5

Please note that all the URLs in the code are in HTTP and not HTTPs :D :

```
$ find . -iname "*.java" -exec fgrep -iHn "https://" {} \; | wc -l
0
```

@ben_ra started an analysis of the Android source code and binaries here : Part 1 and Part 2.

According to @PaulWebSec, they achieve persistence by mounting /system as read/write and installing the spyware in the system folder (code is here):

> Funny. Looks like the persistence trick for the Android spyware leaked by @fleximinx is mounting /system as r+w pic.twitter.com/JrzkVFH9JL
>
> — Paul Sec.jpeg .exe (@PaulWebSec) April 23, 2017

Binaries#

The following binaries were leaked :

- d46af65cb7bd12ce77b4d88bbdd4a005 5000_1.1.4.sisx VirusTotal
- 39be87178c84d4afd07a80323a1d4b91 5002_2.24.3_green.APK VirusTotal
- a5b589f4edac1aea9952d3faff261817 5002_-2.25.1_green.APK VirusTotal
- 306adab7cfcb0d9a13956ca9e9dbd59a 5003_1.4.2.jad VirusTotal
- eb295fe2e40f12014cdb05de07edcae2 5006_-1.0.12.exe VirusTotal
- 8f6a42defdc8632c1baf961d7d9c3e5b 5006_1.0.13.exe VirusTotal
- fa26d3c6fe253a354ed95e5dbb5067c6 5006_1.0.13.ZIP VirusTotal
- 4efd37a38a56c650906d2ed76ceaaa6a 5007_1.1.1.pkg VirusTotal

Gamma Certificates#

Among the files leaked, we find two certificates used by the Gamma group to sign Symbian software. Both certificates are signed by a company called “Cyan Engineering Services SAL” :

```
Issuer: C=GB, ST=London, L=Southwark, O=Symbian Software Limited, CN=Symbian
Developer Certificate CA 280205A/emailAddress=developercertificates@symbian.com
Validity
    Not Before: May 25 04:07:05 2011 GMT
    Not After : May 25 04:07:05 2014 GMT
Subject: C=LB, L=Beirut, O=Cyan Engineering Services SAL (offshore), CN=Cyan
Engineering Services SAL (offshore), OU=Symbian Signed PublisherID, ST=Beirut
```

Links between this company and Gamma Group was already identified by Citizen Lab in their analysis of Symbian malware in 2012.

That’s all for now, folks. Ping me on Twitter if you have any question.

stalkerware