



# Stalk Awareness

A Presentation for  
**OWASP Newcastle**

September 2019  
By Cian Heasley

**OWASP**

# whoami

## Cian Heasley

Studied Computer Security & Digital Forensics at Napier University

Security Engineer at Adarma



@nscrutables



@nscrutables



@diskurse

“But ultimately, it was Guzmán’s own fondness for surveillance that helped federal agents charge him. Rodriguez testified in court that, at Guzmán’s behest, he personally installed 50 BlackBerry phones with monitoring software called “*FlexiSpy*.” The software is undetectable and can read text messages and call logs, steal passwords saved to the device, and remotely switch on and listen to the microphone.”

**‘The Spyware That Brought Down El Chapo’s Drug Empire’,**  
Sidney Fussell, The Atlantic, Jan 15 2019

“Turner had shown the informant an app on her mobile telephone which allowed her to track the location of the intended victim’s telephone. On Wednesday, the informant called Turner and asked where the victim was located at that moment. Turner allegedly provided the location of the intended victim and confirmed that the informant would be paid for the murder. The FBI then contacted the victim and arrested Turner.”

**‘Bellflower Woman Charged In Murder-For-Hire Plot Against Boyfriend’,**  
CBS Los Angeles, December 16th 2017

# This Spyware Data Leak Is So Bad We Can't Even Tell You About It

A consumer spyware vendor left a lot of incredibly sensitive and private data, including intimate pictures and private call recordings, for all to see or still hasn't take

**MOTHERBOARD**  
TECH BY VICE

## Hosting Provider Finally Takes Down Spyware Leak of Thousands of Photos and Phone Calls

After Motherboard reported that a consumer spyware vendor left a lot of incredibly sensitive and private data online, the company's hosting provider took it down.

Technologie

# Spyware company leaves private customer data on the internet

A manuf

incredib

available

The com

with the

10.09.201

☰ **SPIEGEL ONLINE** SPIEGEL

Stalking via Smartphone

## Anti-virus apps overlook spyware

Some people monitor their partners or employees with secretly installed spyware on their smartphones. This is illegal, but hard to discover, as confirmed by a test with seven antivirus apps.



By *Patrick Beuth* ▼

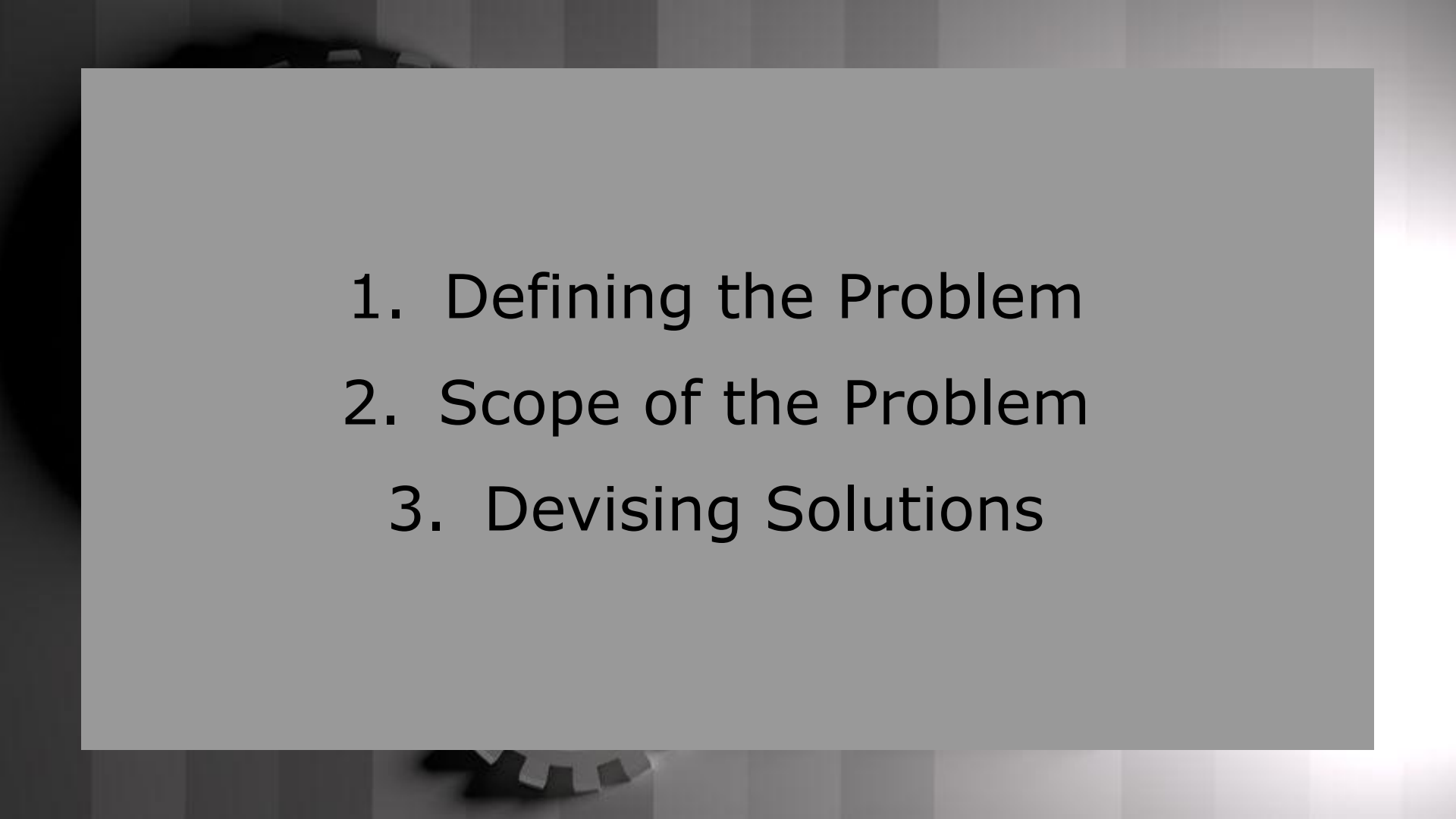
## DroidBox

Uses the Android SDK to run a custom Android Virtual Device (running Android 4.1.2) with some extra patches to track file operations and outputs to JSON to aid in dynamic apk analysis.



## MARA Framework

Android apk static analysis toolkit that outputs results to text files, incorporates tools like androbugs, androwarn and OWASP Top Mobile Top 10 and the OWASP Mobile Apps Checklist. Shares regexes with MOB.SF project.

- 
1. Defining the Problem
  2. Scope of the Problem
  3. Devising Solutions



# Defining the Problem

You wonder if your wife/husband is cheating on you.

You wonder if your partner does something behind your back.

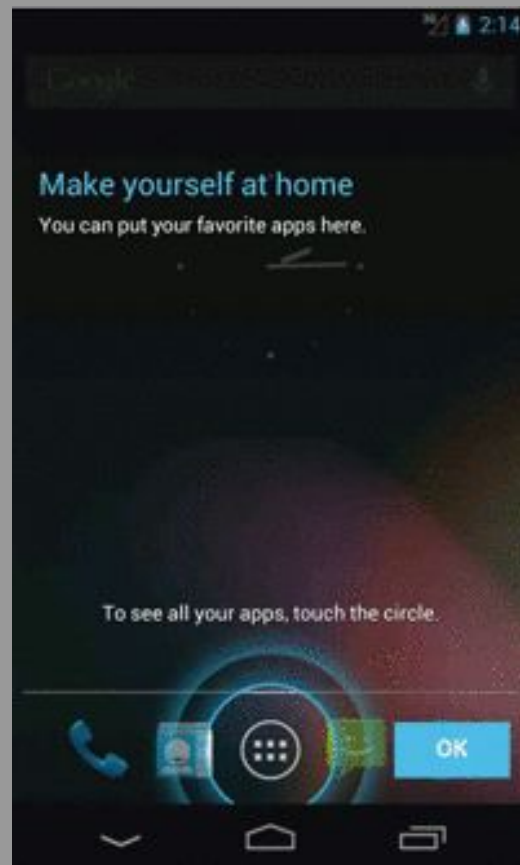
You feel your spouse keeps distance from you.

You suspect your wife/husband is lying to you.

Find out the truth and bring peace to your mind with [TheTruthSpy](#)

# Stalkerware basics

- Physical access to device needed
- Changes to device security settings
- C2 server controls app functions
- Collects, monitors, exfiltrates data
- Exfiltrated data stored on server
- Basic functionality similar in all apps



# Stalkerware is variously described as

- Mobile RAT
- Spouseware
- Spyware
- Intimate Partner Surveillance



# Stalkerware companies describe their products as

- Child monitoring tools
- Employee monitoring tools
- Anti-theft apps
- For monitoring phones with permission/knowledge of device owner
- Sometimes called “dual use” apps



Promotional material from stalkerware provider “hellospy”.

Imagery and language that evokes paranoid jealousy or depicts domestic violence or implies adultery is often used for marketing purposes by some companies.



The screenshot shows a web browser window with the URL [hellospy.com/hellospy-for-personal-catch-cheating-spouses.aspx?lang=en](https://hellospy.com/hellospy-for-personal-catch-cheating-spouses.aspx?lang=en). The page title is "Mobile Spy App for Personal Catch Cheating Spouses". The navigation menu includes "Home", "Uses", and "HelloSpy for Business". The main content area features the heading "Cheating by the numbers..." followed by text discussing the prevalence of infidelity and extramarital affairs, citing a 2002 study by Joan D. Atwood & Limor Schwartz. A photograph of a man and a woman is included, with the man appearing to be in a physical altercation with the woman. The text continues to discuss the accessibility of infidelity due to technology and mentions that up to 90% of marital affairs may involve mobile phones or email. It concludes with a statement that technology can also be used to detect and reveal infidelity.


Mobile Spy App for Personal Catch Cheating Spouses

Home Uses HelloSpy for Business

### Cheating by the numbers...

One of the unpleasant truths most married individuals are blissfully ignorant of is the surprisingly high occurrence of infidelity & extramarital affairs.

According to a study by Joan D. Atwood & Limor Schwartz, published in 2002, by the Journal of Couple & Relationship Therapy, 45-55% of married women and 50-60% of married men engage in extramarital sex at some time or another during their relationship. If that is not alarming enough, another study puts the average nonpaternity rate at above 3.3%, or in other words, 33 children in every thousand are not fathered by the man everybody thinks they are...



The past two decades has made infidelity more accessible than ever mostly because of the ascent of two majorly disruptive technologies: online social networks and mobile phones.

Up to 90% of marital affairs may include the use of a mobile phone or email as a preferred means for communication.

Good news is that technology can also be used to detect & reveal infidelity.

Stalkerware is a global phenomenon but with often highly localized companies and franchises.

## ALGUNAS CARACTERÍSTICAS

### CÁMARA EN VIVO



Activa de forma remota la cámara y toma fotos en forma secreta para ver los alrededores del Teléfono.

### GRABAR ALREDEDOR



Active de forma remota el micrófono y escuche todo lo que está sucediendo. De forma secreta, escuche todo lo que sucede alrededor.

### CAPTURAS DE PANTALLA



Tome capturas de pantalla en tiempo real y observe todo lo que sucede en la pantalla del dispositivo.

Source: Catwatchful

Stalkerware is a global phenomenon but with often highly localized companies and franchises.

These target specific customer bases, whether these be linguistic, national or cultural.

## Witaj w LET ME SPY

Kontroluj telefon on-line

LetMeSpy (LMS) to niewielki program instalowany w Twoim telefonie z systemem Android™. Rejestruje przychodzące i wychodzące SMSy, połączenia telefoniczne, lokalizacje telefonu i przesyła je do Twojego konta użytkownika.

Wystarczy pobrać plik instalacyjny i zainstalować aplikację na telefonie, który chcesz namierzać. Do danych masz dostęp 24h/dobę poprzez stronę [www.letmespy.com](http://www.letmespy.com).

Zwracamy uwagę, że kontrola telefonu bez wiedzy i zgody jego użytkownika jest niezgodna z polskim prawem. Jeżeli używasz oprogramowania Let Me Spy na telefonie, z którego korzysta osoba trzecia - zawsze poinformuj go o ograniczeniu prywatności.

Source: LetMeSpy



Stalkerware is a global phenomenon but with often highly localized companies and franchises.

These target specific customer bases, whether these be linguistic, national or cultural.

Many companies market similar or identical apps to different markets.

## Minoyou Solution

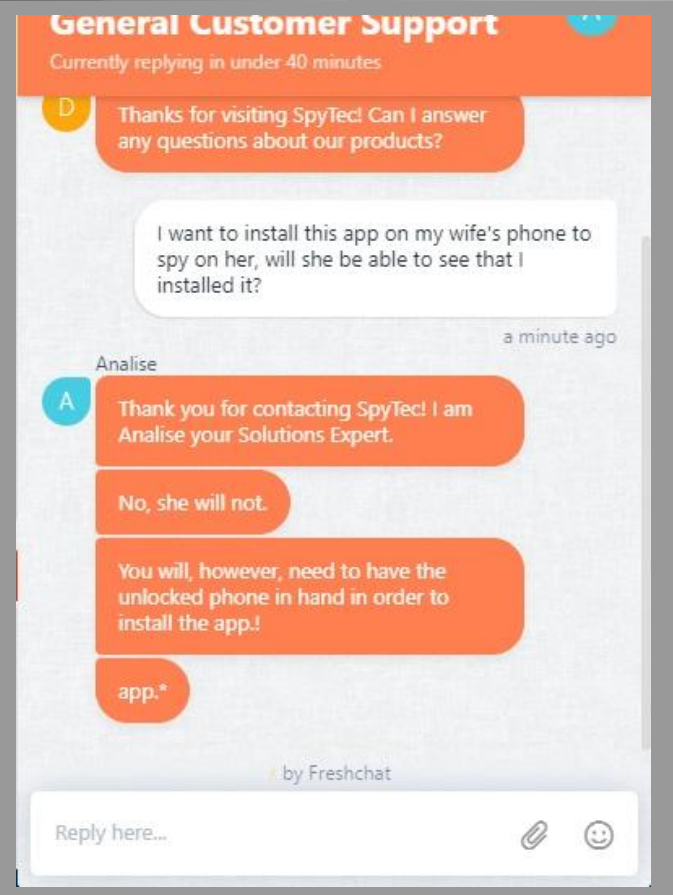
[Reverse Whois](#) » COMPANY [Minoyou Solution] { 12 domain names }

NUM	DOMAIN NAME	REGISTRAR
1	<a href="http://mobiispy.com">mobiispy.com</a>	GoDaddy.com, LLC
2	<a href="http://mobilespyblog.com">mobilespyblog.com</a>	GoDaddy.com, LLC
3	<a href="http://maxxspy.com">maxxspy.com</a>	GoDaddy.com, LLC
4	<a href="http://toplcd.net">toplcd.net</a>	GoDaddy.com, LLC
5	<a href="http://yuaphone.com">yuaphone.com</a>	GoDaddy.com, LLC
6	<a href="http://suaphone.net">suaphone.net</a>	-
7	<a href="http://suaphone.com">suaphone.com</a>	-
8	<a href="http://saiqoniphone.com">saiqoniphone.com</a>	-
9	<a href="http://chuyenhangmyviet.com">chuyenhangmyviet.com</a>	-
10	<a href="http://xososaigon.com">xososaigon.com</a>	-
11	<a href="http://getspyapps.com">getspyapps.com</a>	GoDaddy.com, LLC
12	<a href="http://cong-ty-tham-tu.com">cong-ty-tham-tu.com</a>	GoDaddy.com, LLC

An actual conversation that I had with a customer service representative of **Spytec**, through their web based chat interface.

A review on their site states:

*"I purchased the Datadrone to see what texts and calls my boyfriend gets during the day while he is at work and it actually works amazingly! I see every incoming/outgoing sms, mms, and phone call. **He has absolutely no idea it is even installed on his phone.**"*



```
<uses-permission android:name="android.permission.INTERNET"/>
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
<uses-permission android:name="android.permission.PROCESS_OUTGOING_CALLS"/>
<uses-permission android:name="android.permission.ACCESS_FINE_LOCATION"/>
<uses-permission android:name="android.permission.READ_PHONE_STATE"/>
<uses-permission android:name="android.permission.READ_CALL_LOG"/>
<uses-permission android:name="android.permission.RECEIVE_SMS"/>
<uses-permission android:name="android.permission.READ_CONTACTS"/>
<uses-permission android:name="android.permission.READ_SMS"/>
<uses-permission android:name="android.permission.RECORD_AUDIO"/>
<uses-permission android:name="android.permission.CAMERA"/>
<uses-permission android:name="com.android.browser.permission.READ_HISTORY_BOOKMARKS"/>
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"/>
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"/>
<uses-permission android:name="android.permission.GET_ACCOUNTS"/>
<uses-permission android:name="android.permission.CHANGE_WIFI_STATE"/>
<uses-permission android:name="android.permission.CHANGE_NETWORK_STATE"/>
<uses-permission android:name="com.google.android.c2dm.permission.RECEIVE"/>
<uses-permission android:name="android.permission.WAKE_LOCK"/>
```

These apps generally rely on outdated and insecure methods of obscuring or encrypting data, Base64 encoding, MD5 encryption and when SSL is used certificate pinning to thwart MiTM attacks is generally not implemented.

```
GET /protocols/check_device_registered.aspx?deviceid=d4bc-803e-25f0-8913 HTTP/1.1
Host: protocol-a810.thetruthspy.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-Control: private
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 17 Jan 2019 15:34:36 GMT

0
The device does not exist in the system.
```

```
GET /protocols/device_register.aspx?
username=emillio.esneider@plutocow.com&password=p4ssw0rd&deviceid=d4bc-803e-25f0-8913
HTTP/1.1
Host: protocol-a810.thetruthspy.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Cache-Control: private
Transfer-Encoding: chunked
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/8.5
X-AspNetMvc-Version: 5.2
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Thu, 17 Jan 2019 16:03:40 GMT
```

1

Most of these apps implement SSL for the stalker to access their control panel but transmit user data stolen from devices to their database server in the clear.

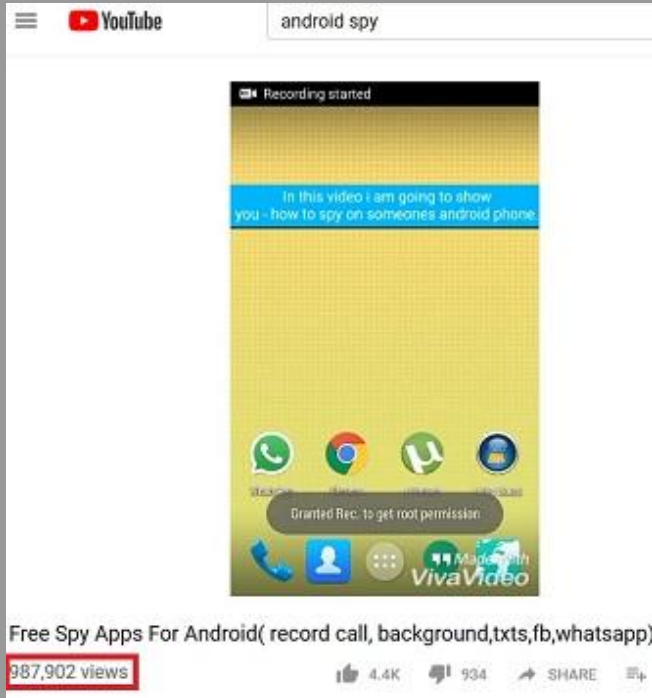
# Scope of the Problem



### How To Install Flexispy Without the Target Device

2,376,113 views

👍 80K    💬 2.6K    ➦ SHARE    ⌵ SAVE    ⋮



### Free Spy Apps For Android( record call, background,txts,fb,whatsapp)

987,902 views

👍 4.4K    💬 934    ➦ SHARE    ⌵

Sales channel:

eStore  Network cross-selling

**Build report**

avangate

Orders amount (USD)



**Export as CSV**

Orders amount (USD) Jul 1, 2016 - Aug 26, 2016

<b>2016 Aug</b>	66,699.52 USD
<b>2016 Jul</b>	96,796.42 USD
<b>TOTAL:</b>	<b>163,495.94 USD</b>

Source: Spyera leak

### Der er registreret malware

Følgende apps er blevet identificeret som malware. Vi anbefaler, at du afinstallerer dem for at beskytte din enhed og dine data.



SystemUpdate

IGN.

AFINSTALLÉR

SENERE

IGNORÉR ALLE

Brugt

840 MB ledig

Trusselsfund

RYD ALT

You can activate this product if you have an activation code.

.....

ACTIVATE

### SystemUpdate

Activation failed. Device ID 355320071938313 already registered to License 8570823783 (401).

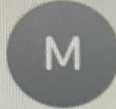
OK



etisalat

10:28 PM

100% 10%



Mum

Text Message  
Today 10:27 PM

< \*#2 > < 3177494344 > < D >

[5002 2.21.2][2] Error  
Product is not yet activated.

- May 2015 - **MSpy** hacked, **400,000** user accounts exposed
- June 2016 - **WtSpy** hacked, **179,802** user accounts exposed
- April 2017 - **Flexispy** hacked
- April 2017 - **Retina-X** hacked, **130,000** customer records exposed
- February 2018 - **Mobistealth** and **Spy Master Pro** hacked
- May 2018 - **Hellospy** database leak, **108,000** user accounts exposed
- July 2018 - **SpyHuman** hacked **440,000,000** phone call details exposed
- August 2018 - **TheTruthSpy** hacked
- September 2018 - **MSpy** leaks millions of records from infected devices
- October 2018 - **Xnore** hacked, **28,000** active user accounts exposed

## MobiiSpy Data leak

```
11/7/2017 4:37 AM <dir> bin
11/7/2017 1:36 PM 111 DataService.svc
11/30/2014 2:02 AM 91 Global.asax
5/28/2017 8:30 PM 293 packages.config
11/7/2017 1:36 PM 99 Photo.svc
2/5/2019 3:33 AM <dir> Pictures
8/18/2017 4:04 PM 49 PrecompiledApp.config
2/10/2019 9:03 PM <dir> RecordCall
11/7/2017 4:50 AM 3944 Web.config
```



```
12/28/2018 9:19 AM 166957 5c264d2d9479292058e52dbf.PNG
12/28/2018 9:20 AM 275228 5c264d319479292058e52dc0.PNG
12/28/2018 9:20 AM 275319 5c264d359479292058e52dc1.PNG
12/28/2018 9:20 AM 32901 5c264d4d9479292058e52df5.PNG
12/28/2018 9:20 AM 33269 5c264d4e9479292058e52df6.PNG
12/28/2018 9:20 AM 106784 5c264d4f9479292058e52df7.PNG
12/28/2018 9:20 AM 177565 5c264d519479292058e52df8.PNG
12/28/2018 9:20 AM 123504 5c264d559479292058e52df9.PNG
12/28/2018 9:20 AM 122830 5c264d589479292058e52dfa.PNG
12/28/2018 9:20 AM 124345 5c264d5c9479292058e52dfb.PNG
12/28/2018 9:20 AM 137972 5c264d5e9479292058e52dfc.PNG
12/28/2018 9:20 AM 76081 5c264d609479292058e52dfd.PNG
12/28/2018 9:20 AM 277407 5c264d639479292058e52dfe.PNG
12/28/2018 9:20 AM 166957 5c264d669479292058e52dff.PNG
12/28/2018 9:20 AM 275228 5c264d699479292058e52e00.PNG
12/28/2018 9:21 AM 275319 5c264d6d9479292058e52e01.PNG
12/28/2018 9:30 AM 33912 5c264f8f9479292058e52e35.PNG
12/28/2018 9:30 AM 33912 5c264f8f9479292058e52e36.PNG
12/28/2018 9:30 AM 32901 5c264f909479292058e52e37.PNG
12/28/2018 9:30 AM 33269 5c264f929479292058e52e38.PNG
12/28/2018 9:30 AM 32901 5c264f929479292058e52e39.PNG
12/28/2018 9:30 AM 33269 5c264f949479292058e52e3a.PNG
12/28/2018 9:30 AM 106784 5c264f949479292058e52e3b.PNG
12/28/2018 9:30 AM 106784 5c264f959479292058e52e3c.PNG
12/28/2018 9:30 AM 177565 5c264f979479292058e52e3d.PNG
12/28/2018 9:30 AM 177565 5c264f9a9479292058e52e3e.PNG
12/28/2018 9:30 AM 123504 5c264f9b9479292058e52e3f.PNG
12/28/2018 9:30 AM 123504 5c264fa09479292058e52e40.PNG
12/28/2018 9:30 AM 122830 5c264fa09479292058e52e41.PNG
12/28/2018 9:30 AM 124345 5c264fa49479292058e52e42.PNG
12/28/2018 9:30 AM 122830 5c264fa49479292058e52e43.PNG
12/28/2018 9:30 AM 137972 5c264fa69479292058e52e44.PNG
12/28/2018 9:30 AM 124345 5c264fa89479292058e52e45.PNG
12/28/2018 9:30 AM 76081 5c264fa89479292058e52e46.PNG
12/28/2018 9:30 AM 137972 5c264fa99479292058e52e47.PNG
12/28/2018 9:30 AM 76081 5c264fab9479292058e52e48.PNG
```



WtSpy database leak in 2016 includes a user database with 179,802 entries and the following fields:

subscriber\_id, subscriber\_name, **country\_id**  
subscriber\_mobile, phone\_type, subscriber\_email  
subscriber\_pwd, subscriber\_date, subscriber\_status,  
payment\_gateway\_code

Taking the codes from the WtSpy registration page we can see that the country\_id codes are:

- 196 - Saudi Arabia
- 214 - Syria
- 146 - Morocco
- 1 - Afghanistan
- 244 - Yemen
- 225 - Turkey
- 65 - Egypt
- 110 - Jordan
- 120 - Lebanon
- 163 - Oman

country_id	Count
196	47298
214	13888
146	12723
1	11206
244	9642
225	7592
65	7510
110	7228
120	6852
163	5449

With a bit of grepping we can see that there are a number of .gov addresses among the subscribers, in particular Saudi Arabian government email addresses, with other Middle Eastern countries also making an appearance.

nalhadora@moh.gov.sa	hahmubarak@rca.gov.om
aalamer@tv.tc.gov.sa	Msada@pp.gov.qa
aalamer@tv.tc.gov.sa	salsulaiman@tv.tc.gov.sa
thakfans@scta.gov.sa	khadija.almemari@dubaied.gov.ae
bolkhima@dzit.gov.sa	ymmhathrami@rca.gov.om
asadeeq@moh.gov.sa	salsulaiman@tv.tc.gov.sa
badreyeh.alhantoubi@mopw.gov.ae	ghazouania@scta.gov.sa
helaziz@mcit.gov.eg	isglmic.cur@mo.gov.xsd
into@curriculum.gov.sl	akjhfl@moh.gov.sa
info@curriculum.gov.ll	abalalrashedi@moh.gov.sa
halsiddiqi@mot.gov.qa	mohd_khalifa@stc.gov.ae
halsiddiqi@mot.gov.qa	TMBayah@sdfa.gov.sa
nalaedi@coh.gov.sa	malajmi@kkia.gov.sa
Mohammad.sh@mopsd.gov.jo	npc.drug@sdfa.gov.sa

# HelloSpy

Email address

Password

Login

Forgot password



Sign Up

How To Install

Uses

FAQs

Live Demo

## Cell Phone Spy Software

Silently monitor text messages, GPS locations, call details, photos and social media activity. View the screen and location LIVE!

Download the free HelloSpy App



Android



iPhone

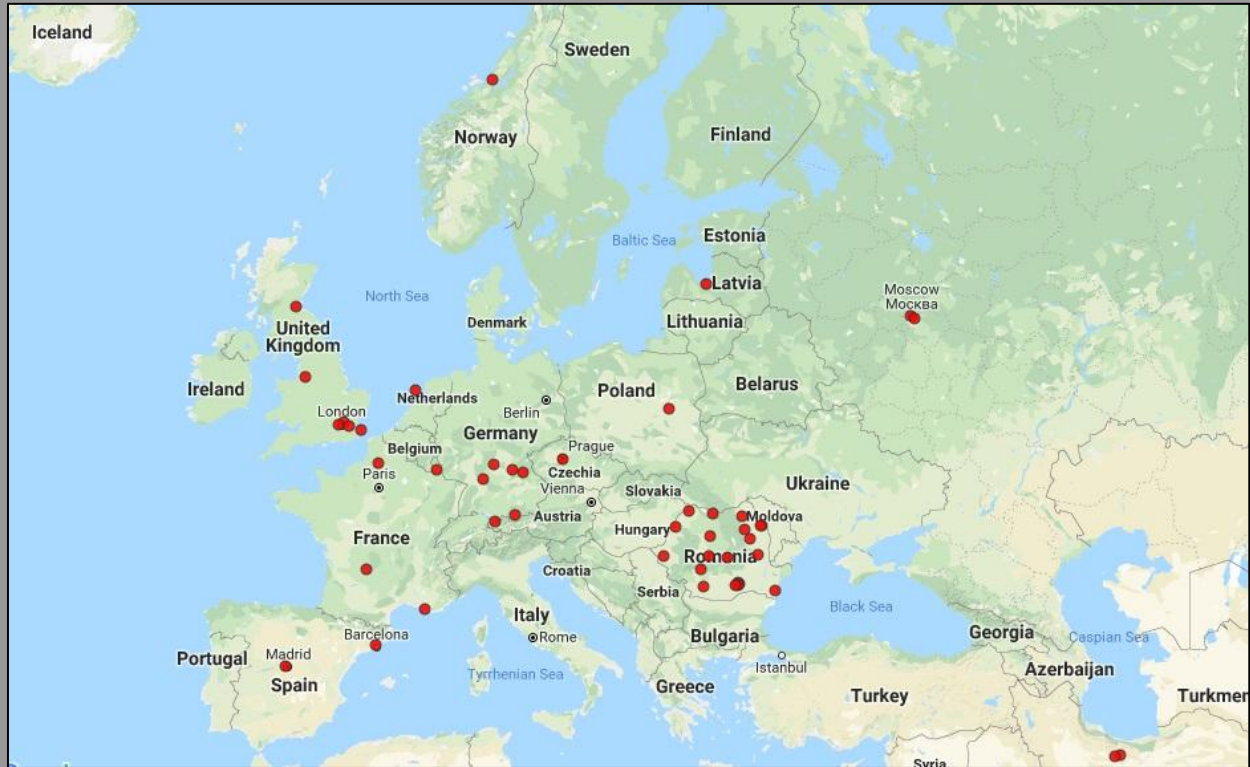
Free for **48 hours** with full features

Start Free Trial

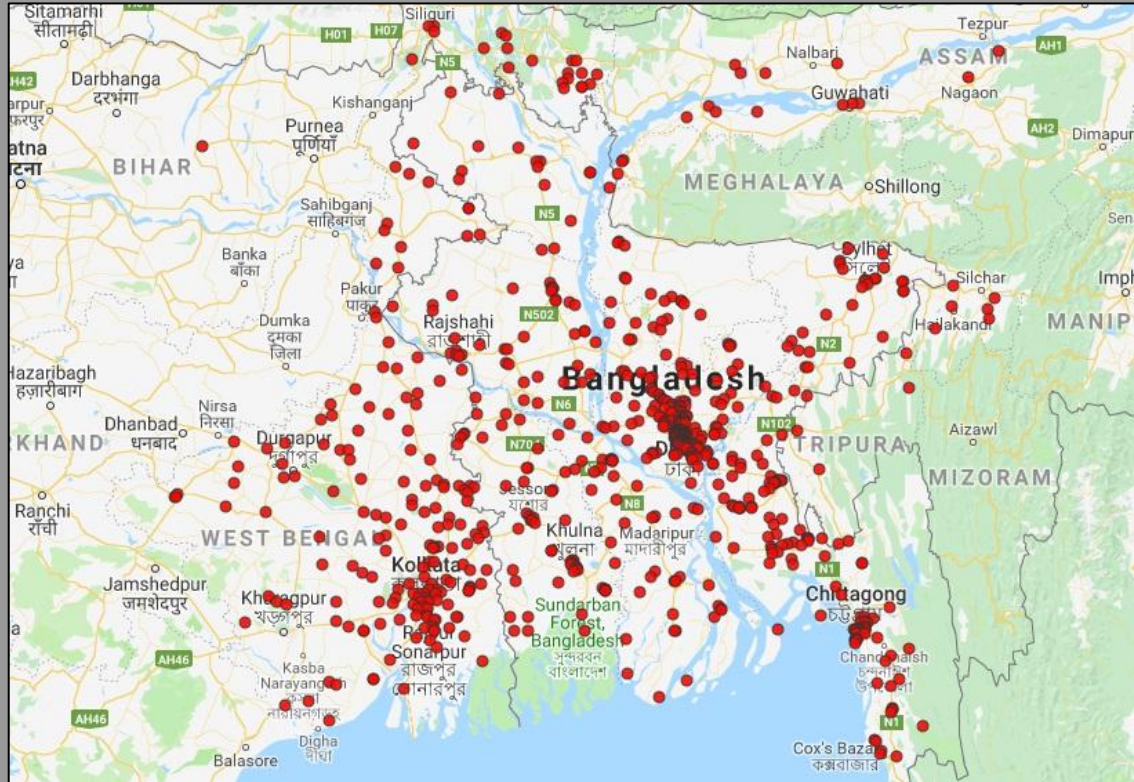




Data from Hellospy database leak



Data from Hellospy database leak



Data from Heliospy database leak

## KEY FACTS FROM THE REPORT

- Sampled more than 500k Android and 400K iOS devices
- Approximately 1,000 devices infected: 60% android, 40% iOS
- 0.12% of all the devices were infected with one of these mRATs
  - 0.21% for Large organizations in the US
- Corporate data at risk: emails, messages, keystrokes, calls, employee location
- Over 20 variants and 18 different mRAT families of products found
- Larger organizations are unevenly targeted by mRATs
- Over 100 countries were represented in this survey

Joint Enterprise mRAT Research  
Lacoon Mobile Security & Check Point (2015)

# Devising Solutions

“The best two AV engines were Cyren and WhiteArmor. Cyren flagged 6% of the on-store IPS apps, and 70% of the off-store spyware, but Cyren also flagged one of the top 100 apps (Pandora Radio). WhiteArmor flagged less dual-use apps than Cyren (only 5%), but flagged all of the off-store spyware, and did not have any false positives.”

- The Spyware Used in Intimate Partner Violence

## The Spyware Used in Intimate Partner Violence

Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad,  
Sam Havron, Jackeline Palmer, Diana Freed,  
Karen Levy, Nicola Dell, Damon McCoy, Thomas Ristenpart



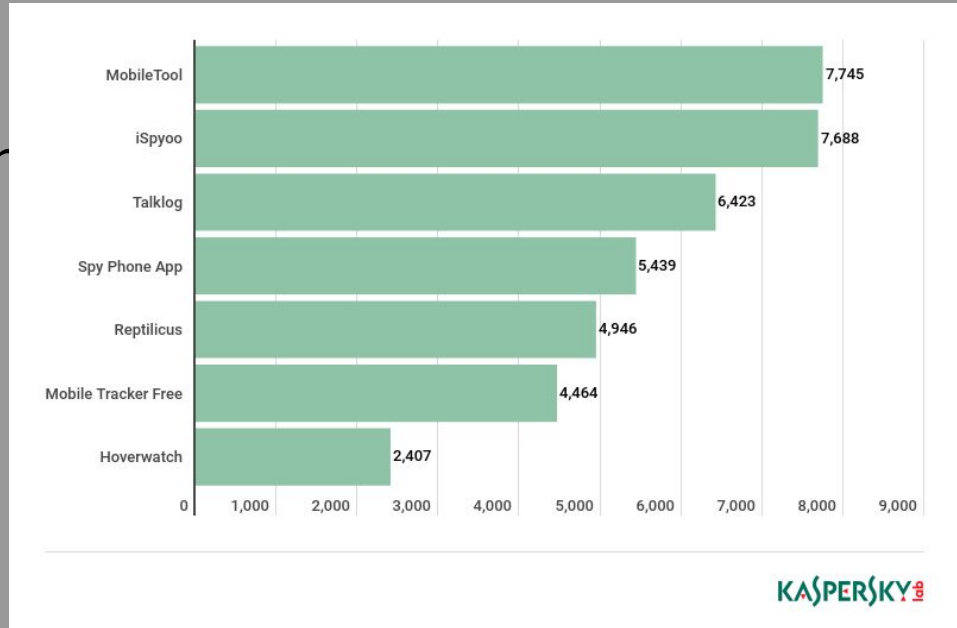
NYU

TANDON SCHOOL  
OF ENGINEERING



“Over the past year, more than 58,000 users have detected stalkerware on their phones or tablets with the help of our products alone. Of those, 35,000 had no idea about the stalkerware installed on their devices until our protection solution completed its first scan.”

- What's wrong with “legal” commercial spyware  
Leonid Grustniy, Kaspersky Lab Daily





STALKERWARE

## Parental monitoring apps: How do they differ from stalkerware?

Posted: July 22, 2019 by David Ruiz

kaspersky daily

Product ▾ Renew Downloads Support Resource Center Blog ▾

## What's wrong with "legal" commercial spyware

April 3, 2019

It's safe to say that almost everyone has wanted to spy on someone at least once in their life, whether to make sure your partner is faithful, your kid has not fallen in with the wrong crowd, or your employee is not being courted by competition. The technologies for spying on colleagues and families are in great demand, which is universally known to breed supply.



101 | CYBERCRIME | FYI | MALWARE

## When spyware goes mainstream

Posted: September 5, 2018 by Jovi Umawing

Last updated: September 28, 2018





**Eva** @evacide · Aug 7

Safety for victims of domestic abuse should not be a premium feature, @Trendmicro.

**Chris Cox** <sup>TM</sup> @Cyber\_Cox

The @TrendMicro booth at #BHUSA2019 told me that their free anti-virus scanner does NOT detect stalkerware /spouseware. They said that users concerned with this need to buy the commercial version. This seems tone deaf, since those that need it most may be least able to buy.

Show this thread



14



269



869



**Trend Micro**

@TrendMicro

Follow

Replying to @evacide

We are extremely surprised by this and investigating now. If this isn't included, it will be added immediately to the free version.

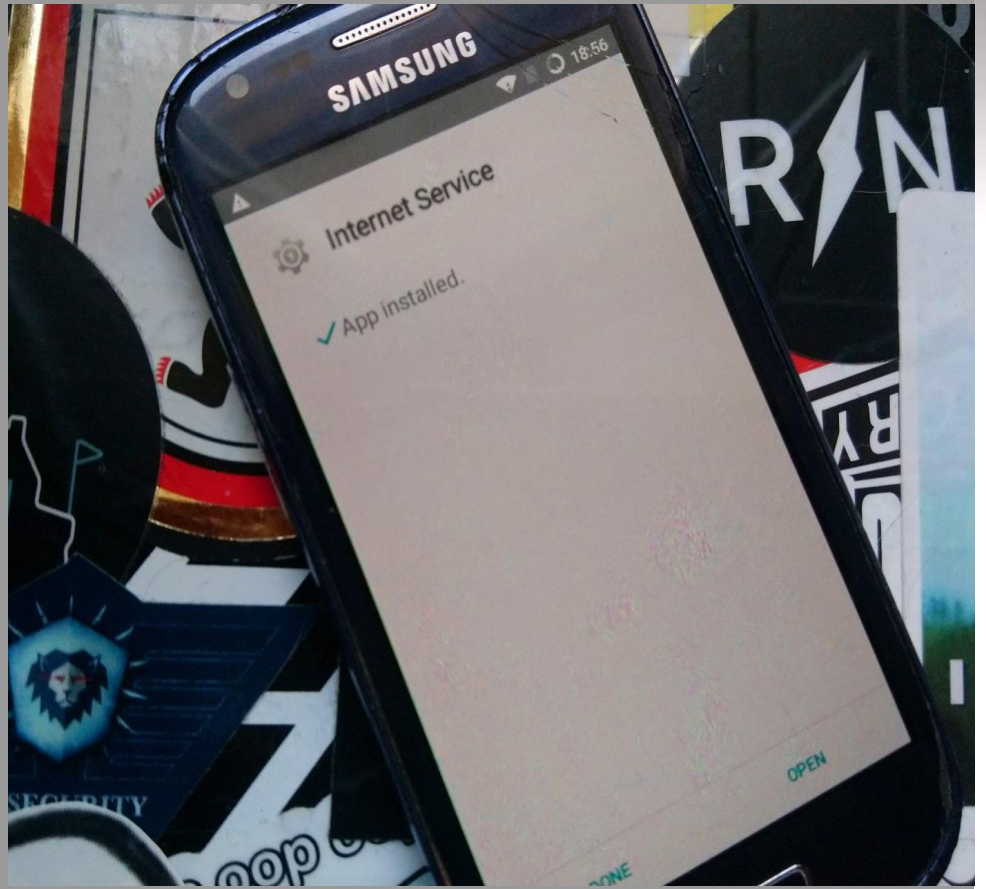
7:07 PM - 7 Aug 2019

39 Retweets 374 Likes



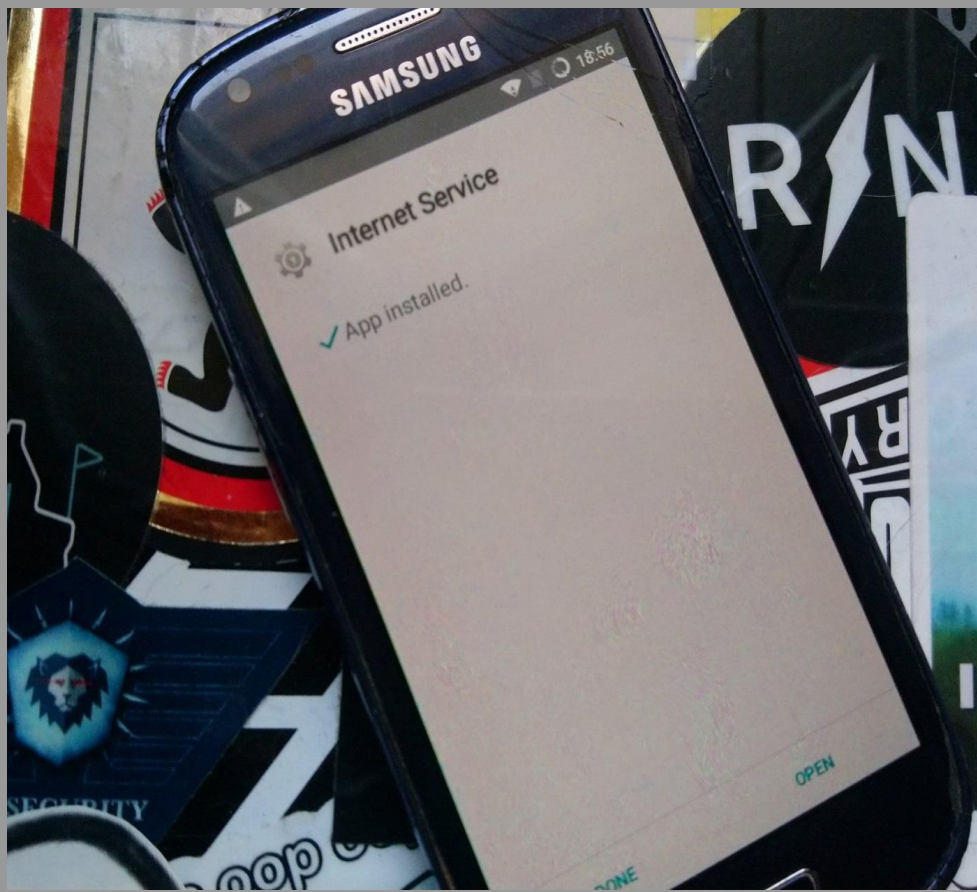
## Physical Device Antivirus Testing

- Galaxy S3 Mini phone
- Android 5.1.1 (rooted)
- 13 stalkerware apps installed
- 7 antivirus apps tested



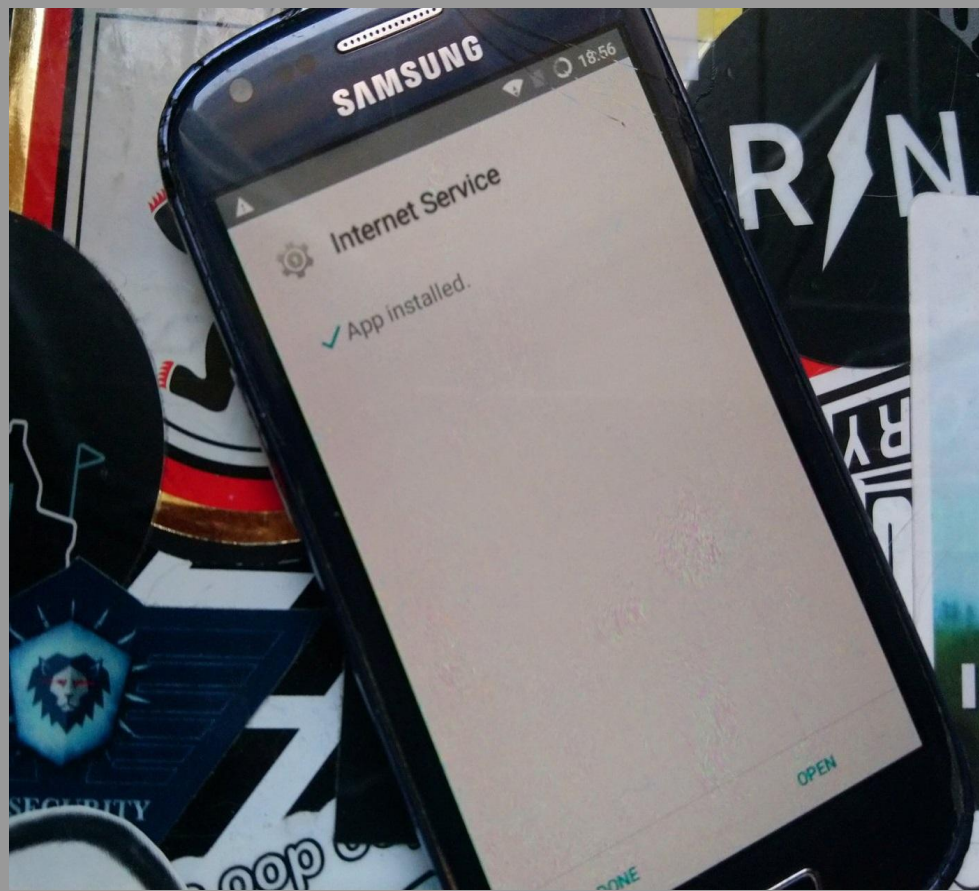
## Stalkerware Apps Installed

- BlurSpy
- EasyLogger
- hellospy
- hoverwatch
- iKeymonitor
- LetMeSpy
- MobileTrackerFree
- ShadowSpy
- Spyhuman
- spyzie
- TheTruthSpy
- trackview
- XnSpy

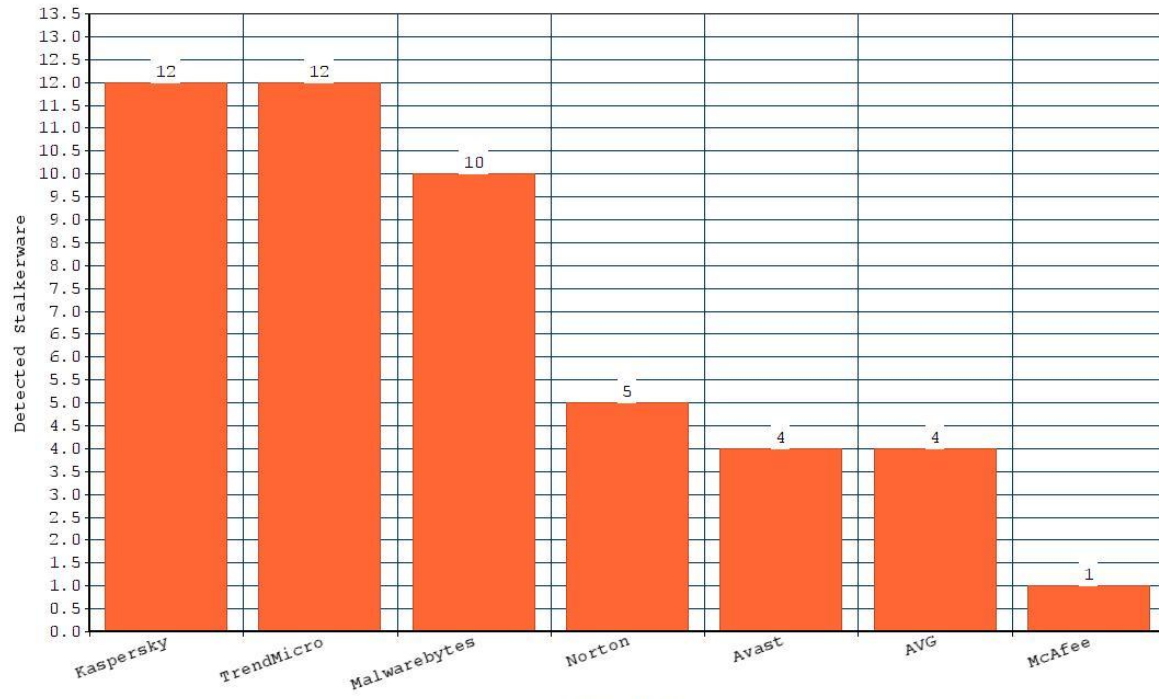


## Free Android AV Installed

- Kaspersky
- MalwareBytes
- Trend Micro
- McAfee
- Avast
- AVG
- Norton



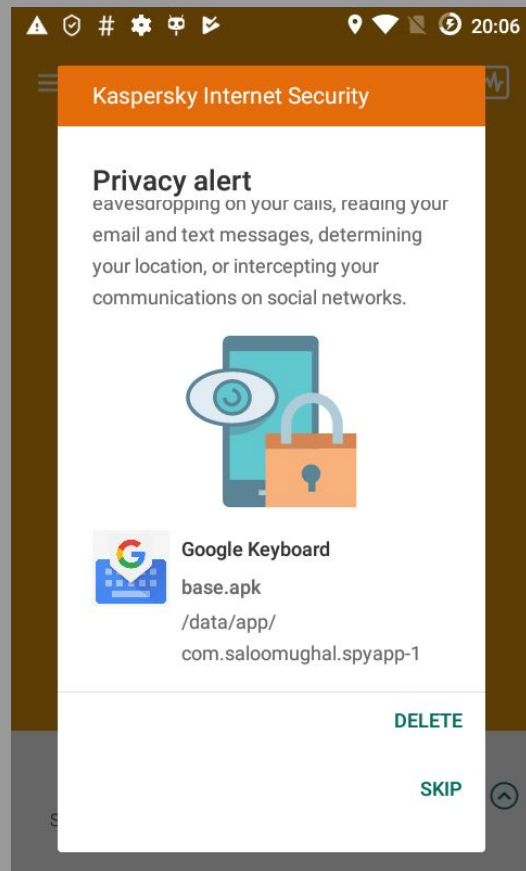
### Stalkerware Detection



Android AV  
Cian Heasley

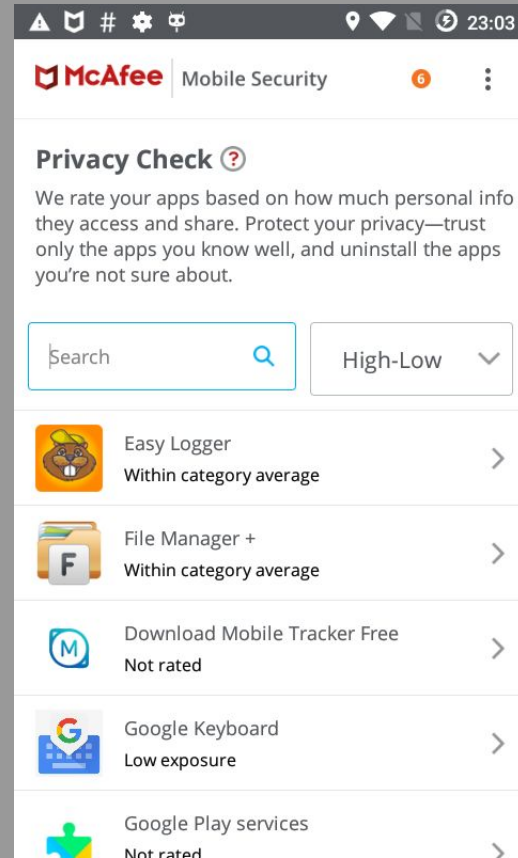
When it comes to antivirus we have to worry about not just whether the various stalkerware apps are detected but also whether the antivirus solution is explaining the significance of that detection.

Some companies do a better job of this than others, though many have promised to do take the problem more seriously.



When it comes to antivirus we have to worry about not just whether the various stalkerware apps are detected but also whether the antivirus solution is explaining the significance of that detection.

Some companies do a better job of this than others, though many have promised to do take the problem more seriously.



“..this industry doesn't exist in a vacuum. Instead, various tech and financial giants process payments or push adverts to customers for these companies. Now, **Motherboard has found that PayPal has been allowing various spyware companies that specifically market to people who want to abusively spy on their spouse to sell its products.**”

- Joseph Cox and Lorenzo Franceschi-Bicchierai

**MOTHERBOARD**  
TECH BY VICE

By Joseph Cox and Lorenzo Franceschi-Bicchierai | Feb 20 2019, 4:46pm

## PayPal Processes Payments for 'Stalkerware' Software Sold to Abusive Partners

The booming industry of spyware to spy on romantic partners doesn't exist in a vacuum: Companies need financial and tech giants to process their payments and advertise their wares.

SHARE



TWEET



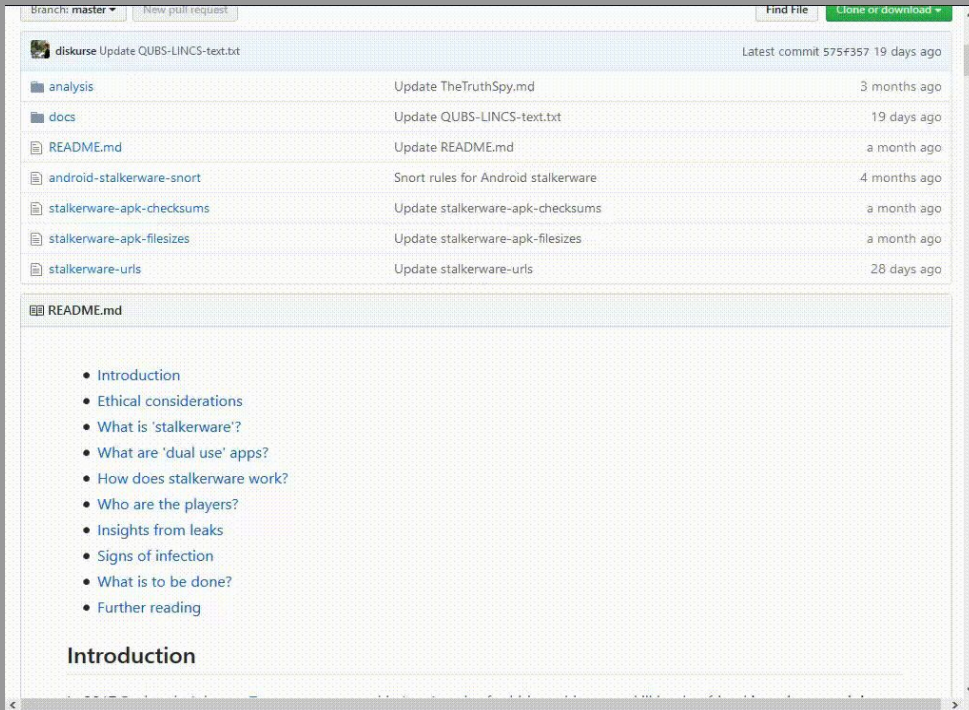
Image: Shutterstock



Company	Domain	PaymentService	Username
1TopSpy	1topspy.com	PayPal	
AppSpy			
GuestSpy	guestspy.com	PayProGlobal	Account suspended
Hellospy	hellospy.com	PayPal	LIXI CORPORATION
LetMeSpy	letmespy.com	PayPal	Rafal Lidwin LIDWN PL
MaxxSpy	maxxspy.com	PayPal	LIXI CORPORATION
mSpy	mspy.com	PayPal	
ShadowSpy	shadow-logs.com	PayPal	
Spy Phone App	spy-phone-app.com	PayPal & Bluesnap	
SpyApp247	spyapp247.com	PayPal	Account suspended
Spyera	spyera.com		
Spyfone	spyfone.com	PayPal	
Spyhuman	spyhuman.com	G2A Pay services	
SpyMasterPro	spymasterpro.com	PayPal	lokindra00kumar12@gmail.com
Spytec	spytec.com	PayPal	
SpyToMobile	spytomobile.com	PAYEER	G2S-PhoneSupport
Spyzie	spyzie.com	PayPal & APACPAY	
TheTruthSpy	thetruthspy.com	PayProGlobal	
Tispy	tispy.net	PayPal & PayProGlobal	Techinnovative Systems
Xnore	xnore.com	PayPal	
Xnspy	xnspy.com	CCBill	Serfolet Ltd

Source: @diskurse - Github

## Stalkerware Github repo:



The screenshot shows the GitHub repository for 'Stalkerware'. At the top, it indicates the current branch is 'master' and provides options for 'New pull request', 'Find file', and 'Clone or download'. Below this is a table of files and folders, each with a commit message and a timestamp. The 'README.md' file is selected, and its content is displayed below the table. The README includes a table of contents with links to various sections of the document.

File/Folder	Commit Message	Time Ago
analysis	Update TheTruthSpy.md	3 months ago
docs	Update QUBS-LINCS-text.txt	19 days ago
README.md	Update README.md	a month ago
android-stalkerware-snort	Snort rules for Android stalkerware	4 months ago
stalkerware-apk-checksums	Update stalkerware-apk-checksums	a month ago
stalkerware-apk-filesizes	Update stalkerware-apk-filesizes	a month ago
stalkerware-urls	Update stalkerware-urls	28 days ago

**README.md**

- [Introduction](#)
- [Ethical considerations](#)
- [What is 'stalkerware'?](#)
- [What are 'dual use' apps?](#)
- [How does stalkerware work?](#)
- [Who are the players?](#)
- [Insights from leaks](#)
- [Signs of infection](#)
- [What is to be done?](#)
- [Further reading](#)

### Introduction

