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.”

“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 online. They still haven't taken it down.

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.
Spyware company leaves private customer data on the internet

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

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.
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.
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.

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
Source: Spyera leak
Der er registreret malware

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

SystemUpdate

..::..::..

SystemUpdate

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

OK
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
مجان للجميع
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
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.

<table>
<thead>
<tr>
<th>Email Address</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:nalhadira@moh.gov.sa">nalhadira@moh.gov.sa</a></td>
<td><a href="mailto:hahlmubarak@rca.gov.om">hahlmubarak@rca.gov.om</a></td>
</tr>
<tr>
<td><a href="mailto:aalamer@tvtc.gov.sa">aalamer@tvtc.gov.sa</a></td>
<td><a href="mailto:Msada@pp.gov.qa">Msada@pp.gov.qa</a></td>
</tr>
<tr>
<td><a href="mailto:aalamer@tvtc.gov.sa">aalamer@tvtc.gov.sa</a></td>
<td><a href="mailto:salsulaiman@tvtc.gov.sa">salsulaiman@tvtc.gov.sa</a></td>
</tr>
<tr>
<td><a href="mailto:thakfans@scta.gov.sa">thakfans@scta.gov.sa</a></td>
<td><a href="mailto:khadija.almemari@duaibed.gov.ae">khadija.almemari@duaibed.gov.ae</a></td>
</tr>
<tr>
<td><a href="mailto:bolkhima@dzit.gov.sa">bolkhima@dzit.gov.sa</a></td>
<td><a href="mailto:ymmhathrami@rca.gov.om">ymmhathrami@rca.gov.om</a></td>
</tr>
<tr>
<td><a href="mailto:asadeeq@moh.gov.sa">asadeeq@moh.gov.sa</a></td>
<td><a href="mailto:salsulaiman@tvtc.gov.sa">salsulaiman@tvtc.gov.sa</a></td>
</tr>
<tr>
<td><a href="mailto:badreyeh.alhantoubi@mopw.gov.ae">badreyeh.alhantoubi@mopw.gov.ae</a></td>
<td><a href="mailto:ghazouania@scta.gov.sa">ghazouania@scta.gov.sa</a></td>
</tr>
<tr>
<td><a href="mailto:helaziz@mcit.gov.eg">helaziz@mcit.gov.eg</a></td>
<td><a href="mailto:isglmic.cur@mo.gov.xsd">isglmic.cur@mo.gov.xsd</a></td>
</tr>
<tr>
<td><a href="mailto:info@curriculum.gov.sl">info@curriculum.gov.sl</a></td>
<td><a href="mailto:akjhfl@moh.gov.sa">akjhfl@moh.gov.sa</a></td>
</tr>
<tr>
<td><a href="mailto:info@curriculum.gov.ll">info@curriculum.gov.ll</a></td>
<td><a href="mailto:abalalrashedi@moh.gov.sa">abalalrashedi@moh.gov.sa</a></td>
</tr>
<tr>
<td><a href="mailto:halsiddiqi@mot.gov.qa">halsiddiqi@mot.gov.qa</a></td>
<td><a href="mailto:mohd_khalifa@stc.gov.ae">mohd_khalifa@stc.gov.ae</a></td>
</tr>
<tr>
<td><a href="mailto:halsiddiqi@mot.gov.qa">halsiddiqi@mot.gov.qa</a></td>
<td><a href="mailto:TMBayah@sfda.gov.sa">TMBayah@sfda.gov.sa</a></td>
</tr>
<tr>
<td><a href="mailto:nalaedi@coh.gov.sa">nalaedi@coh.gov.sa</a></td>
<td><a href="mailto:malajmi@kkia.gov.sa">malajmi@kkia.gov.sa</a></td>
</tr>
<tr>
<td><a href="mailto:Mohammad.sh@mopsd.gov.jo">Mohammad.sh@mopsd.gov.jo</a></td>
<td><a href="mailto:npc.drug@sfda.gov.sa">npc.drug@sfda.gov.sa</a></td>
</tr>
</tbody>
</table>
Data from Hellospy database leak
Data from Hellospy database leak
Data from Hellospy database leak
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
“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
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 forSpying on colleagues and families are in great demand, which is universally known to breed supply.
Eva @evacode • Aug 7
Safety for victims of domestic abuse should not be a premium feature.
@Trendmicro.

Chris Cox™ @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

Trend Micro •
@TrendMicro
Replying to @evacode

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
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
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
<table>
<thead>
<tr>
<th>Company</th>
<th>Domain</th>
<th>Payment Service</th>
<th>Username</th>
</tr>
</thead>
<tbody>
<tr>
<td>1TopSpy</td>
<td>1topspy.com</td>
<td>PayPal</td>
<td></td>
</tr>
<tr>
<td>AppSpy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GuestSpy</td>
<td>guestspy.com</td>
<td>PayProGlobal</td>
<td>Account suspended</td>
</tr>
<tr>
<td>Hellospy</td>
<td>hellospy.com</td>
<td>PayPal</td>
<td>LIXI CORPORATION</td>
</tr>
<tr>
<td>LetMeSpy</td>
<td>letmespy.com</td>
<td>PayPal</td>
<td>Rafal Lidwin UDWN.PL</td>
</tr>
<tr>
<td>MaxxSpy</td>
<td>maxxspy.com</td>
<td>PayPal</td>
<td>LIXI CORPORATION</td>
</tr>
<tr>
<td>mSpy</td>
<td>mspy.com</td>
<td>PayPal</td>
<td></td>
</tr>
<tr>
<td>ShadowSpy</td>
<td>shadow-logs.com</td>
<td>PayPal</td>
<td></td>
</tr>
<tr>
<td>Spy Phone App</td>
<td>spy-phone-app.com</td>
<td>PayPal &amp; Bluesnap</td>
<td></td>
</tr>
<tr>
<td>SpyApp247</td>
<td>spyapp247.com</td>
<td>PayPal</td>
<td>Account suspended</td>
</tr>
<tr>
<td>Spyera</td>
<td>spyera.com</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spyfone</td>
<td>spyfone.com</td>
<td>PayPal</td>
<td></td>
</tr>
<tr>
<td>Spyhuman</td>
<td>spyhuman.com</td>
<td>G2A Pay services</td>
<td></td>
</tr>
<tr>
<td>SpyMasterPro</td>
<td>spymasterpro.com</td>
<td>PayPal</td>
<td><a href="mailto:lokindra00kumar12@gmail.com">lokindra00kumar12@gmail.com</a></td>
</tr>
<tr>
<td>Spytsec</td>
<td>spytsec.com</td>
<td>PayPal</td>
<td></td>
</tr>
<tr>
<td>SpyToMobile</td>
<td>spytomobile.com</td>
<td>PAYEER</td>
<td>G2S-PhoneSupport</td>
</tr>
<tr>
<td>Spyzie</td>
<td>spyzie.com</td>
<td>PayPal &amp; APACPAY</td>
<td></td>
</tr>
<tr>
<td>TheTruthSpy</td>
<td>thetruthspy.com</td>
<td>PayProGlobal</td>
<td></td>
</tr>
<tr>
<td>Tispy</td>
<td>tispy.net</td>
<td>PayPal &amp; PayProGlobal</td>
<td>Techinnovative Systems</td>
</tr>
<tr>
<td>Xnore</td>
<td>xnore.com</td>
<td>PayPal</td>
<td>Serfolet Ltd</td>
</tr>
<tr>
<td>Xnspy</td>
<td>xnspy.com</td>
<td>CCBill</td>
<td></td>
</tr>
</tbody>
</table>

Source: @diskurse - Github
Stalkerware Github repo:

- 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