



"Watching The Watchers, the Stalkerware Surveillance Ecosystem"

Security BSides London 2019

"While we focus on nation states' and corporation's role in steadily eroding our privacy and expanding omnipresent surveillance, an entire niche industry that caters to regular consumers who want similar spying capabilities has slipped largely under the radar."



Cian Heasley



@nscrutables



@nscrutables



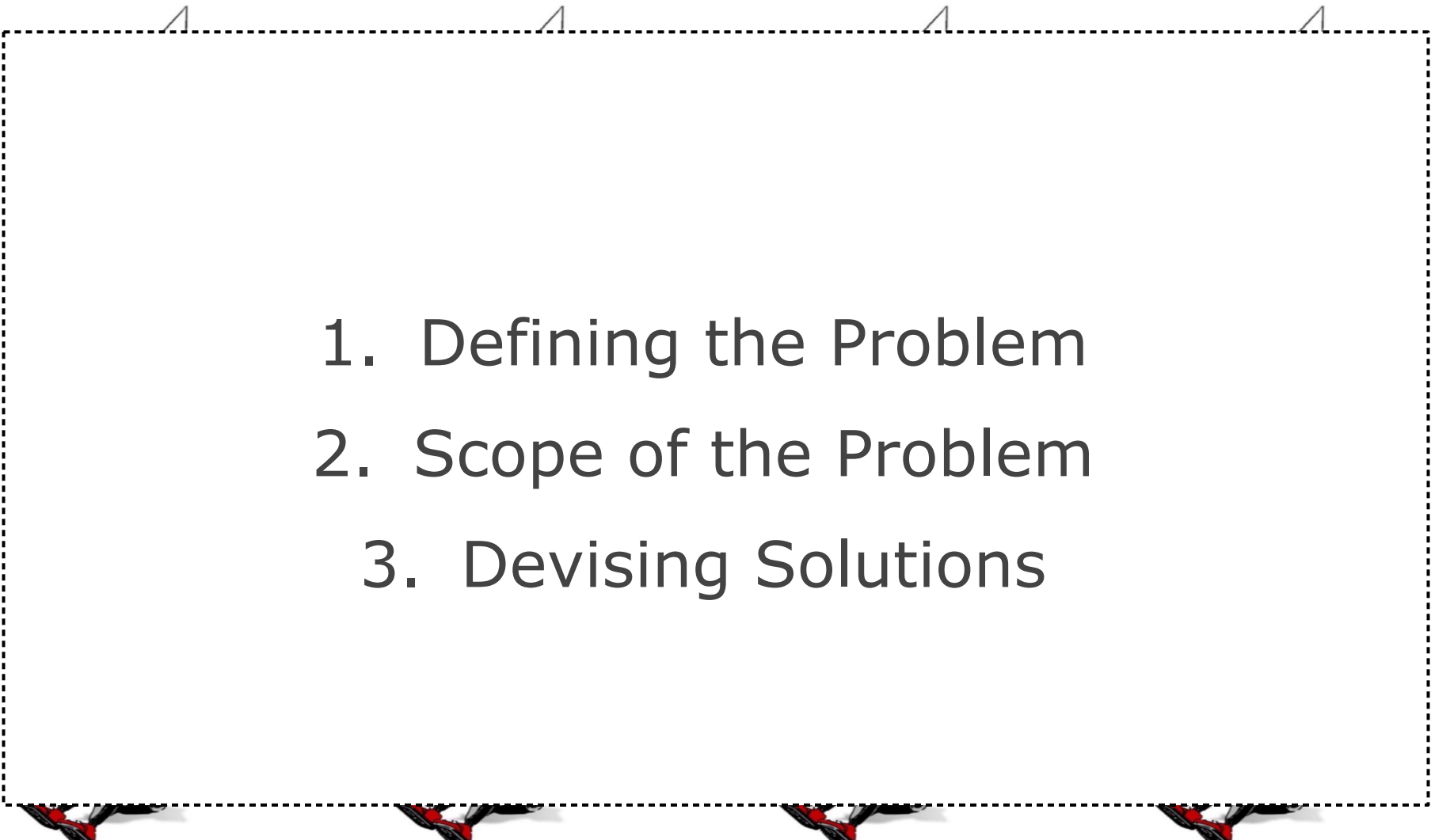
@diskurse

“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

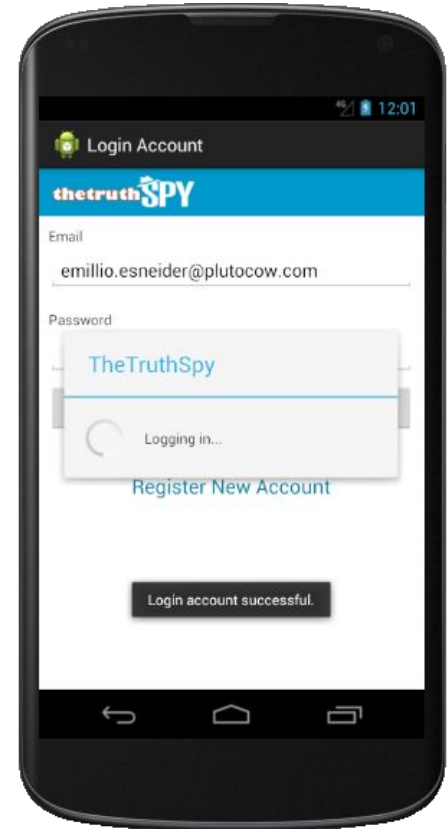
- 
- A large rectangular area defined by a dashed black border. At each of the four corners, there is a small, light gray tab-like shape pointing outwards. Along the bottom edge of the dashed border, there are four small, stylized penguin icons, each facing left. The penguins are black and white with red accents on their chests and feet.
1. Defining the Problem
 2. Scope of the Problem
 3. Devising Solutions

1. Defining the Problem

Defining the Problem

Stalkerware basics

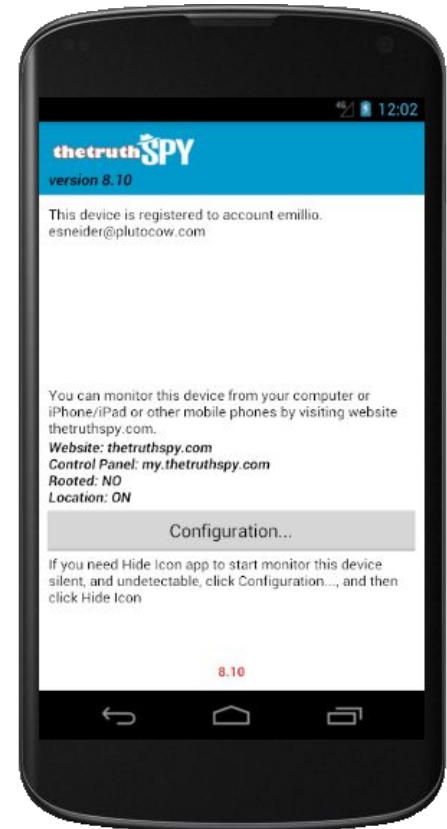
- Physical access to device needed
- Changes to device security settings
- Collects, monitors, exfiltrates data
- Exfiltrated data stored on server
- Basic functionality similar in all apps



Defining the Problem

Stalkerware is
variously described
as

- Mobile RAT
- Spouseware
- Spyware
- Intimate Partner Surveillance



Defining the problem

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



Source: Catwatchful

Defining the Problem

Promotional material from stalkerware provider "Hellospy". Imagery and language that evokes paranoia or depicts domestic violence or implies adultery is often used for marketing purposes.



The screenshot shows a web browser displaying the HelloSpy website. The URL in the address bar is hellospy.com/hellospy-for-personal-catch-cheating-spouses.aspx?lang=en. The page title is "Mobile Spy App for Personal Catch Cheating Spouses". Below the title is a navigation bar with three tabs: "Home", "Uses", and "HelloSpy for Bussiness". The main content area features the heading "Cheating by the numbers..." followed by a paragraph of text. To the right of the text is a photograph of a man and a woman in a tense interaction. Below the photograph is another paragraph of text. At the bottom of the page is a final line of text.

Home Uses HelloSpy for Bussiness

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.

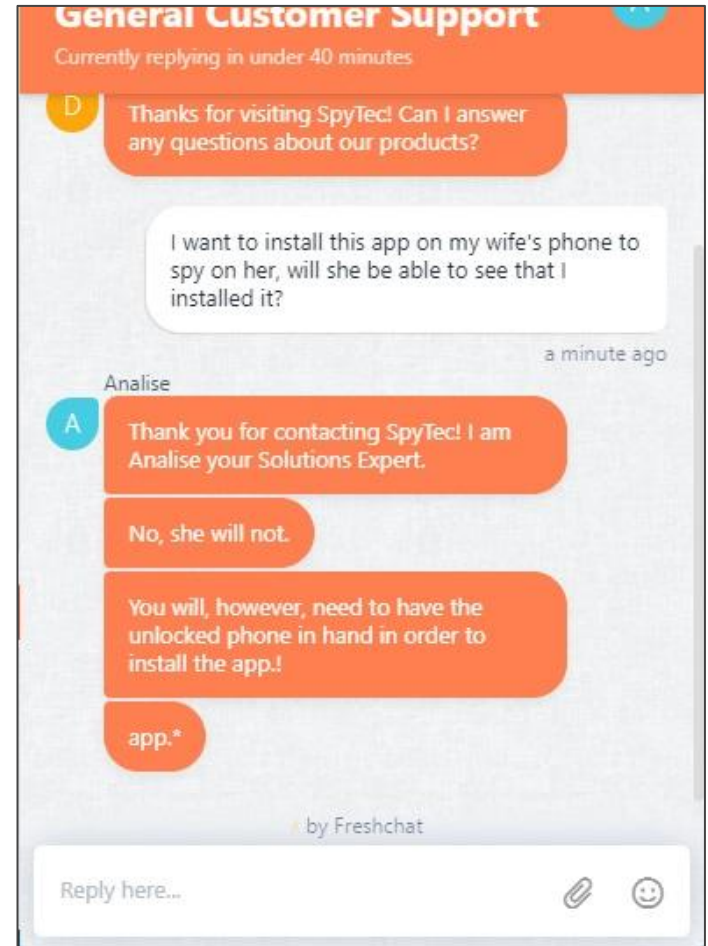
Good news is that technology can also be used to detect & reveal infidelity.

Defining the Problem

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

A review on their site says:

"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.**"



Defining the Problem

MOTHERBOARD

TECH BY VICE

| By Lorenzo Franceschi-Bicchieri | Mar 26 2019, 3:32pm

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.

2. Scope of the Problem

Scope of the Problem

Stalkerware is a global phenomenon but with often highly localized companies and franchises targeting specific customer bases, whether these be linguistic, national or cultural.

Many companies market similar apps to different markets.

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.

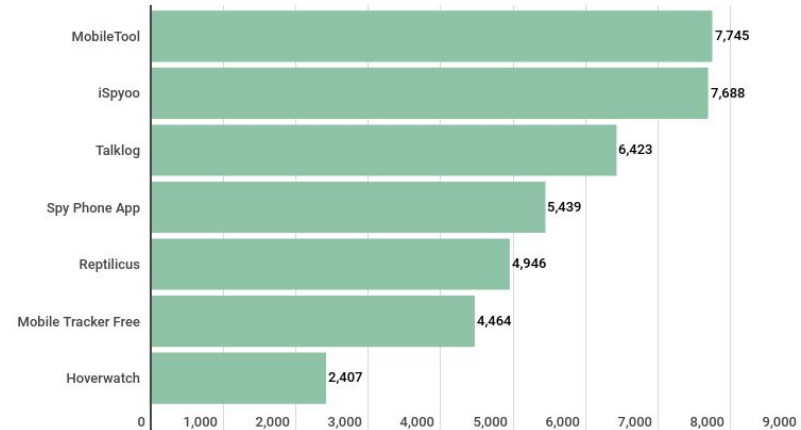
Zwracamy uwagę, że kontrola telefonu bez wiedzy i zgody jego użytkownika jest niezgodna z polskim prawem. Jeżeli używasz oprogramowania Let Me Spy na telefonie, z którego korzysta osoba trzecia - zawsze poinformuj go o ograniczeniu prywatności.

Source: LetMeSpy

Scope of the Problem

“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



KASPERSKY Lab

Scope of the Problem

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)**

Scope of the Problem

- 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

Scope of the problem



wtspy



Scope of the problem

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

Scope of the problem

Taking the code 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

Data from WtSpy database leak

Scope of the problem

HelloSpy

[Login](#)[Forgot password](#)[g](#)[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](#)

Scope of the problem



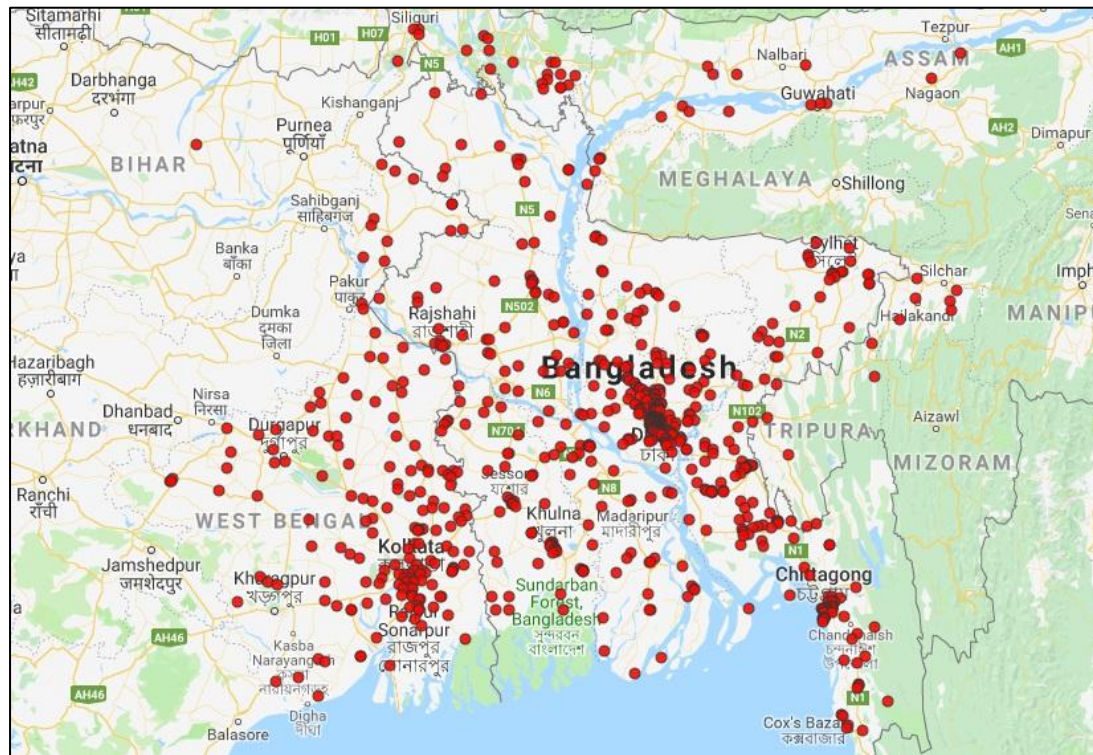
Data from Hellospy database leak

Scope of the problem



Data from Hellospy database leak

Scope of the problem



Data from HelloSpy database leak

3. Devising Solutions

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

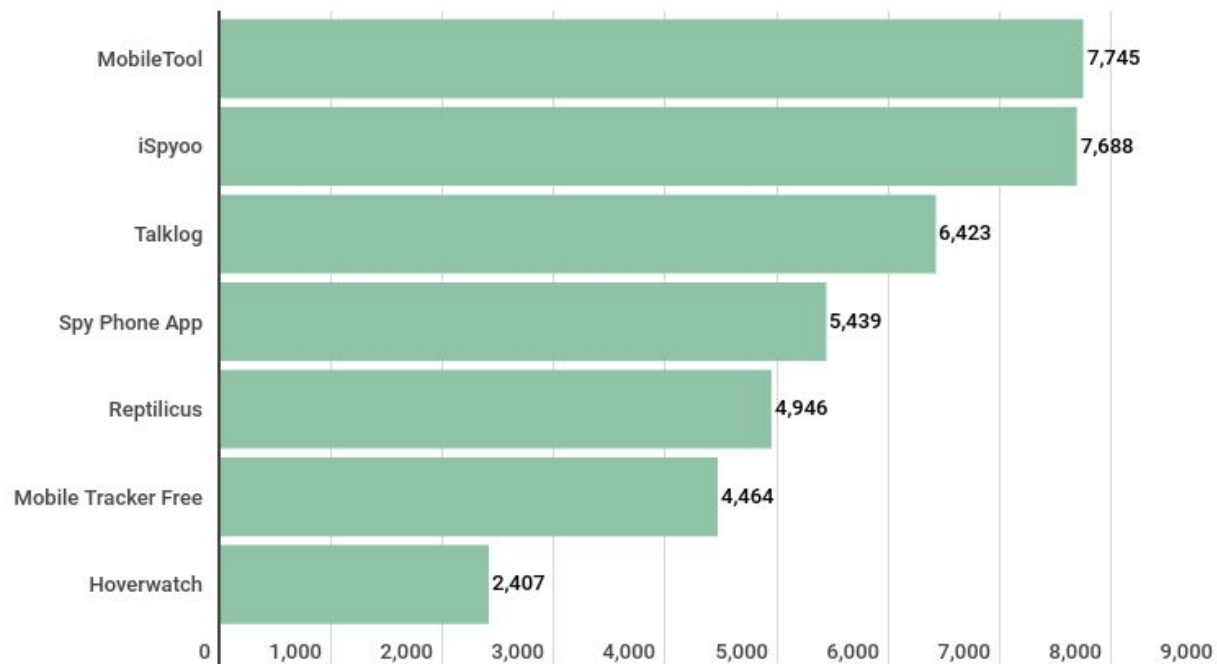


NYU

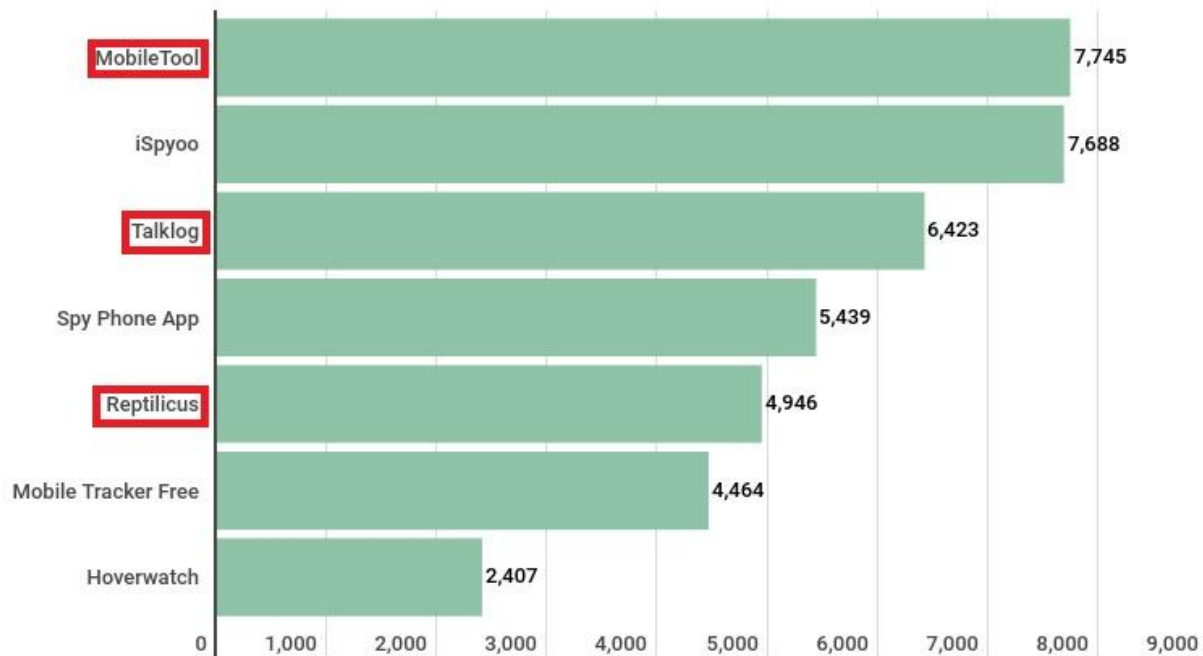
TANDON SCHOOL
OF ENGINEERING



Devising Solutions



Devising Solutions



Devising Solutions

“..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

Source: Vice Motherboard

Devising Solutions

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 LIDWIN 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 in Mobile Devices

Jessica Amery

An overview of mobile stalkerware,
specifically on the Android platform.

13:25 - 13:40

Branch: master New pull request Find File Clone or download

diskurse Update QUBS-LINCS-text.txt Latest commit 575f357 19 days 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

Stalkerware Github repo:

