

A dark, atmospheric scene from a video game. In the foreground, a woman with long blonde hair and a denim jacket looks directly at the viewer. Behind her, a diverse group of people are visible, some looking up and others looking around. The setting appears to be a密室逃脱 (escape room) or a similar confined space with graffiti on the walls.

# EVERY BREATH YOU TAKE

@Ch33r10

A CTI REVIEW OF STALKERWARE

\*not speaking on behalf of my employers

# **FOR THE LAWYERS**

**“The opinions expressed in this presentation are those of the presenter, in their individual capacity, and not necessarily those of my employers.”**

**@Ch33r10**

# **STALKERWARE**

- **WHAT IS IT?**
- **HOW DOES IT WORK?**
- **TARGETS/OPERATORS**
- **TRADECRAFT**
- **CTI HYPOTHESES**
- **CORPORATE AMERICA SOLUTIONS**

**@Ch33r10**

# **STALKERWARE**

**WHAT IS IT?**

**@Ch33r10**

TOP SECRET

# STALKERWARE



# SPY

@Ch33r10

# STALKERWARE

Software used to “facilitate intimate partner violence, abuse, or harassment, including pernicious intrusions into the targeted person's life by way of physical or digital actions”

~The Citizen Lab

STALKERWARE | SPYWARE | DUAL-USE APPS | mRAT

# INTIMATE PARTNER SURVEILLANCE TOOLS

- COMMODITY STALKERWARE/ SPYWARE
- DUAL-USE APPS
- mRAT
- SHARED ACCOUNTS
- OSINT, SOCIAL MEDIA, PEOPLE, RECEIPTS, ETC

# COMMODITY STALKERWARE

BASIC Active & Passive Data  
Collection

- Texts
- Call Logs
- Some Chat Apps
- Pics & Videos
- Browser History
- GPS Location



# TARGET

	Record/Access/Monitor											
	Keystrokes	Calendar	Contacts	GPS	Email	Web Traffic	Stored Media	Social Media	Phone Logs	Chat Apps	SMS	Phone Calls
<b>Cerberus</b>					X							X
<b>FlexiSPY</b>	X	X	X	X	X	X	X	X	X	X		X
<b>Highster Mobile</b>		X	X	X	X	X	X	X		X	X	X
<b>Hoverwatch</b>	X	X	X	X					X		X	X
<b>Mobistealth</b>	X	X	X			X	X	X	X	X		X
<b>mSpy</b>		X	X	X			X	X	X	X	X	X
<b>TeenSafe</b>		X	X	X					X	X		X
<b>TheTruthSpy</b>	X	X	X	X	X	X	X	X	X	X		

# **STALKERWARE**

**Mobistealth**

**mSpy**

**FlexiSpy**

**Highster Mobile**

**Hoverwatch**

**Spyzie**

**TheTruthSpy**

**TeenSafe**

**Cerberus**

**Xnspy**

**WebWatcher**

**& More!!!**

# STALKERWARE

HOW DOES IT WORK?

@Ch33r10

**COMMODITY**

# **STALKERWARE**

## **REQUIRED:**

- **PHYSICAL ACCESS TO DEVICE**
- **INTERNET ACCESS**



**INSTALL APPS FROM UNKNOWN SOURCES  
& DISABLE GOOGLE PLAY PROTECT**



**JAILBROKEN iPHONE (SPY W iCLOUD ACCT ACCESS)**

# RWDEICA

LHM KILL CHAIN

COMMODITY STALKERWARE



**COMMODITY**

# **STALKERWARE**

**EASY TO USE, LEGAL-ISH\*, CHEAP,  
READILY AVAILABLE, SIMILAR  
CAPABILITIES TO mRAT/SPYWARE, NO  
USER INTERACTION, NO TECHNICAL SKILL**

**DRAWBACK: PHYSICAL ACCESS TO DEVICE**

\*intercepting private communication is generally illegal (potential wiretapping crime) unless person doing it is a parent, employer, LE with warrant. Stalkerware vendors suggest getting consent.

**mRAT**

# **STALKERWARE**

**CHEAP-ISH, REMOTE INSTALLATION  
REQUIRES: SPECIFIC KNOWLEDGE TO  
OBTAIN, USER INTERACTION,  
TECHNICAL SKILL!!!**

**DRAWBACK: ILLEGAL**

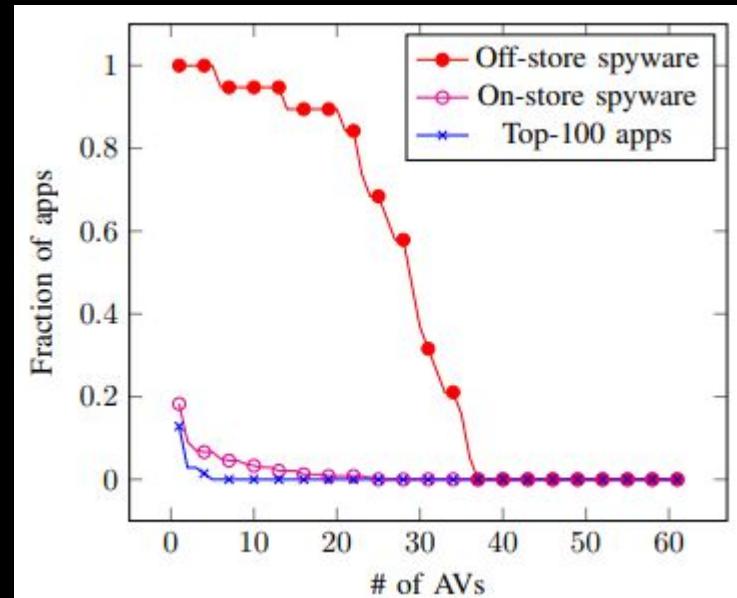
# MITRE ATT&CK

TACTIC	TECHNIQUE	PROCEDURE
Initial Access	T1461: Lockscreen Bypass	Dental molding kit or playdough to lift fingerprints
Initial Access	T1475: Deliver Malicious App via Authorized App Store	Install spyware from Google Play Store
Collection, Credential Access	T1412: Capture SMS Messages	Use Spyware to receive SMS
Remote Service Effects	T1468: Remotely Track Device without Authorization	Use Spyware to Track User

# EXISTING AV & ANTI-SPYWARE TOOLS INEFFECTIVE AT DETECTING & REMEDIATING STALKERWARE

Product	Filename	APK Version	Positive Count	Engines Used	% Positives
Cerberus	Cerberus_disguised.apk	3.5.2	6	63	9.5%
FlexiSPY	flexispy_5002_3.0.1.apk	3.0.1	34	63	54.0%
Hoverwatch	hoverwatch-setup-fovmf.apk	6.3.260	22	59	37.3%
mSpy	mspy_android.apk	5.3.0	20	63	31.7%
TheTruthSpy	TheTruthSpy.apk	N/A	0	0	0.0%
TheTruthSpy	TheTruthSpy-2.apk	N/A	0	0	0.0%
					<b>MEAN</b> 22.1%

Table 6: Overall Antivirus Detection of Stalkerware Applications



THE CITIZEN LAB | THE PREDATOR IN YOUR POCKET P 40 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>

2018 IEEE SYMPOSIUM ON SECURITY & PRIVACY | THE SPYWARE USED IN INTIMATE PARTNER VIOLENCE P 452 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618>

# **STALKERWARE**

**TARGETS**

**“THE VICTIMS ARE EVERYDAY PEOPLE”**

**~Morgan Marquis-Boire**

**@Ch33r10**

# RELATIONSHIPS

@Ch33r10

**SIMILAR SURVEILLANCE  
CAPABILITIES AS STALKERWARE**

**TARGETS**

@Ch33r10

# CHILDREN



@Ch33r10

# EMPLOYEES

@Ch33r10

# TARGETED WITH PEGASUS: JOURNALISTS & CIVIC MEDIA



Targeted by  
Mexican  
Gov-linked  
Operator



Targeted by  
Saudi  
Gov-linked  
Operator



**STOPPING THE PRESS:** New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator

CITIZEN LAB 2020

**DISSIDENTS**

**ACTIVISTS** BLM

**CITIZENS** WeChat | Hong Kong

**RELIGIOUS LEADERS** Tibetans | Muslims

# CRIMINALS

@Ch33r10

# TERRORISTS

An aerial photograph of the Pentagon building in Washington, D.C., following a terrorist attack. The left side of the building is severely damaged, with large sections of the facade and roof missing, revealing the interior framework. Debris is scattered across the ground in front of the building. A construction crane stands on the right side. An American flag flies from a pole on the far right. The surrounding area appears to be a mix of construction and office buildings.

WHATSAPP- "YOU'VE BEEN HACKED"  
EUROPEAN LE- OOOPSY

@Ch33r10



# MILITARY GOVERNMENTS GOV OFFICIALS LAW ENFORCEMENT

TikTok=BAN

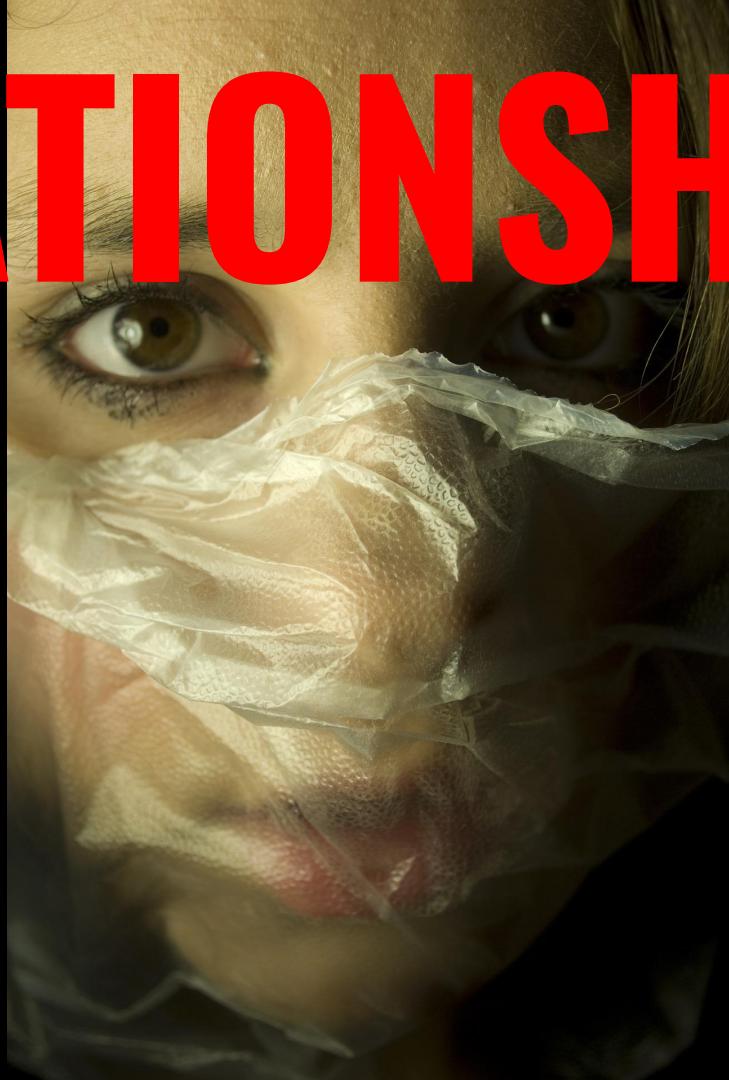
LOOKOUT | STEALTH MANGO | MIDDLE EAST |  
INDIRECT COMPROMISE USA/UK/AUS/IRAN

# STALKERWARE

## OPERATORS

@Ch33r10

# RELATIONSHIPS



@Ch33r10

# **STALKERWARE VENDOR BREACHES**



**FlexiSpy: Metropolitan Police**

**Mobistealth: Military, FBI, ICE,  
DHS, TSA**

**SIMILAR SURVEILLANCE  
CAPABILITIES AS STALKERWARE**

**OPERATORS**

@Ch33r10

# PARENTS SCHOOLS

A dark, textured background featuring a large, weathered metal drum or barrel. The drum has some faint markings, possibly "1000" and "L". The lighting is dramatic, highlighting the texture of the metal and the surrounding environment.

Seattle

@Ch33r10

# COMPANIES

@Ch33r10

# CYBERCRIME HACKTIVISTS



@Ch33r10

# CRIMINALS TERRORISTS

El Chapo

@Ch33r10

# LAW ENFORCEMENT



MIAMI PEN-LINK  
SWEDEN MARCH 2020  
CITYLAB | CELLEBRITE  
MOTHERBOARD METROPOLITAN POLICE

# NATION-STATE

JAVIER VALDEZ CARDENAS RECKLESS-1  
PAKISTANI MILITARY | STEALTH MANGO

# **STALKERWARE**

## **HOSTILE ACTOR TRADECRAFT**

**@Ch33r10**

# KIMBER

**SHARED ACCTS | DUAL-USE APPS | UNILATERAL  
MANIPULATE FRIENDS/FAMILY  
EMOTIONAL & PSYCHOLOGICAL ABUSE**

# SUKI WYNN

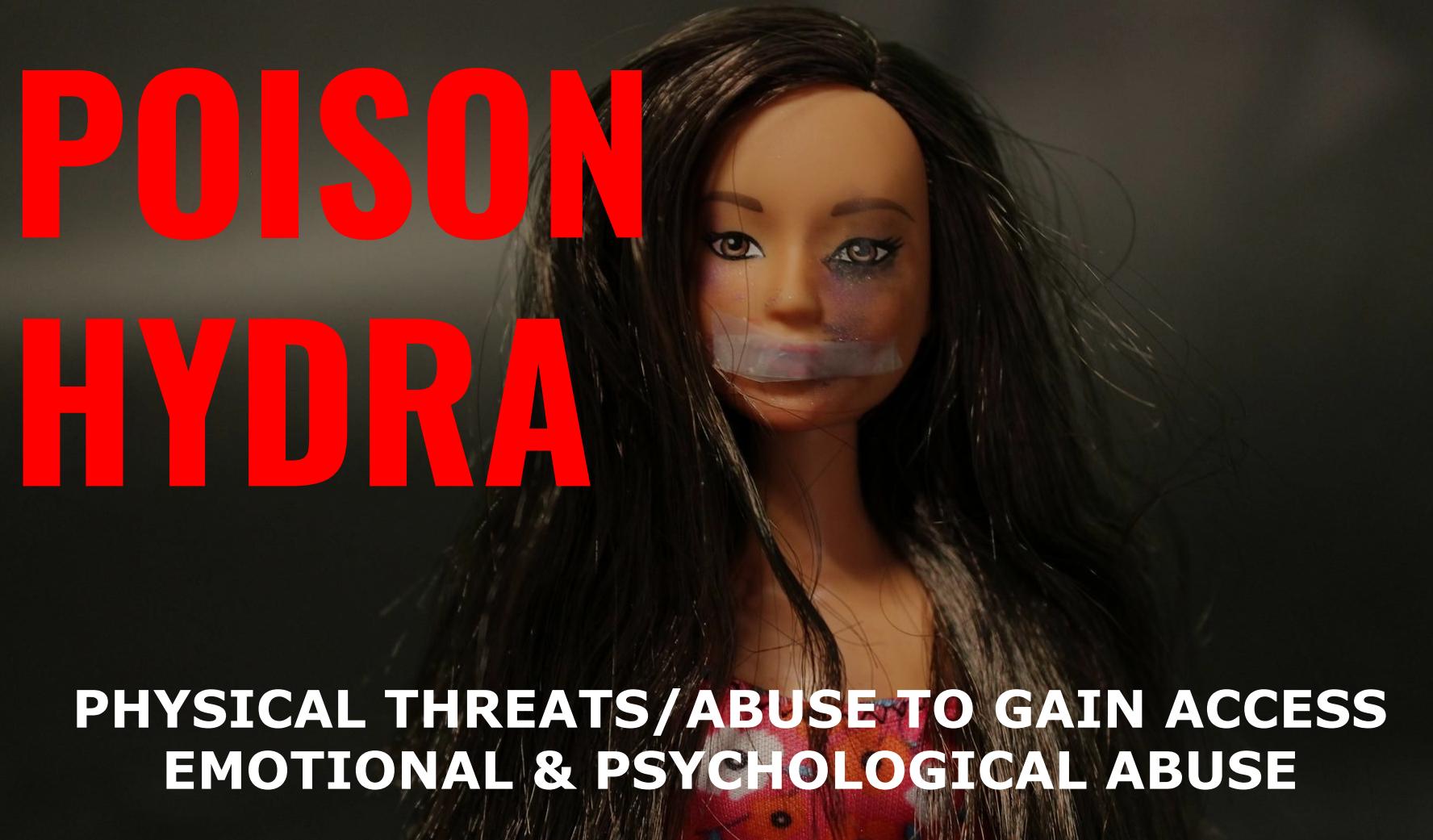


**COMMODITY STALKERWARE OR SPYWARE  
EMOTIONAL & PSYCHOLOGICAL ABUSE**

# ELECTRA

**mRAT | TECHNICAL | SOCIAL ENGINEERING  
EMOTIONAL & PSYCHOLOGICAL ABUSE**

# **POISON HYDRA**



**PHYSICAL THREATS/ABUSE TO GAIN ACCESS  
EMOTIONAL & PSYCHOLOGICAL ABUSE**

# **STALKERWARE**

**CTI HYPOTHESES**

**NORMAL USE OF  
COMMODITY STALKERWARE**



# RTFM CORPORATE AMERICA

@Ch33r10

# CORPORATE MOBILE DEVICE MANAGEMENT/ BYOD

@Ch33r10

# CORPORATE STALKERWARE VENDORS

- POOR SECURITY PRACTICES
- MISCONFIGS SPYFONE S3/API & KidsGuard
- BREACHES
- UNENCRYPTED  
TRANSMISSION/MITM?

# STALKERWARE VENDOR BREACHES

Retina-X (2x)  
Flexispy  
Mobistealth  
Spy Master Pro  
SpyHuman  
Spyfone  
HelloSpy

TheTruthSpy  
Family Orbit  
mSpy  
Copy9  
Xnore

# CORPORATE

## HOW MANY EMPLOYEES IMPACTED BY STALKERWARE?

WOMEN ((20K\*50%)\*33%)= **3,333**

MEN ((20K\*50%)\*16%)= **1,667**

5K (25%) Employees experience IPV sometime in their lifetime  
x 54% IPV Survivors Tracked w Stalkerware =

**2.7K (13.5%)** Employees impacted by stalkerware at one point in their lives

# APAV-PORTUGUESE ASSOCIATION FOR VICTIM SUPPORT

REPORTED ITEM	#
STALKING	580
DEFAMATION	315
BREACH OF HOME OR DISTURBANCE OF PRIVATE LIFE	113
PRIVATE LIFE DEBAUCHERY/ILLEGAL RECORDINGS & PICS	93
VIOLATION OF CORRESPONDENCE OR TELECOM	37
CYBERCRIME	84
BULLYING	150
COMPUTER SECURITY	24

## 2019 APAV Annual Report

29,816 Total Cases

1,396 Possible Stalkerware Related

4.7% Reported Cases in 2019 involved items that could be related to Stalkerware

# **STALKERWARE**

## **CTI HYPOTHESES**

### **REPURPOSED USE OF STALKERWARE**

# CORPORATE INSIDER THREAT

@Ch33r10

# CORPORATE

EXECUTIVES  
EMPLOYEES

@Ch33r10

# CORPORATE COMPETITORS



@Ch33r10

# CORPORATE INDUSTRIAL ESPIONAGE

@ch33r10

# STALKERWARE

## CORPORATE AMERICA SOLUTIONS

@Ch33r10

# CORPORATE

## CTI

**THE CITIZEN LAB  
THE PREDATOR IN  
YOUR POCKET P 37-38**

[https://citizenlab.ca/docs/stalker\\_ware-holistic.pdf](https://citizenlab.ca/docs/stalker_ware-holistic.pdf)

App	Domain	IP	Country	ASN Name	ASN #
Cerberus	www.cerberusapp.com	66.228.35.203	United States	Linode, LLC	63949
FlexiSPY	admin.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
FlexiSPY	admin.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
FlexiSPY	api.flexispy.com	180.150.144.84	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	blog.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
FlexiSPY	blog.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
FlexiSPY	client.mobilefonex.com	180.150.156.198	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	community.flexispy.com	104.25.91.115 <sup>90</sup>	United States	Cloudflare, Inc.	13335
FlexiSPY	community.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335

**BAD=**  
**JAILBREAK**  
**WECHAT/TIKTOK**

# CORPORATE



## TABLE TOP

MONETIZE | TAKE-DOWN

# AWAWARENESS

A close-up photograph of a woman's face. Her eyes are the central focus, looking directly at the viewer. She has dark hair and is wearing dark eyeliner. A smartphone is held in front of her face, with its screen displaying a close-up of her own eyes. Her fingers, with dark red-painted fingernails, are visible holding the phone. The background is dark and out of focus.

CHRIS COX | OPERATION SAFE ESCAPE

# RESOURCES

A dramatic, high-contrast image showing a woman's face and hands reflected in shards of broken glass. The shards are scattered across a dark, textured background, creating a jagged, fragmented effect. The lighting highlights the edges of the glass and the woman's features, conveying a sense of vulnerability and碎裂 (fragility or destruction).

TALL POPPY | SAFE ESCAPE | NCADV | NNEDV |  
CORNELL TECH | STOPSTALKERWARE

# **STALKERWARE**

- **Stalkerware, Spyware, mRAT, Dual-use Apps**
- **Data Access varies by vendor/type**
- **Target/Operators: Relationships**
- **Sub-optimal AV detection**
- **Org Specific Threat Modeling**



*Jimmy's Some Sugar*

 APKTOOL  
 DEX2JAR  
 JD-GUI

VS

 VIRUSTOTAL  
 HYBRID  
ANALYSIS  
 DECOMPILER

@chmodxx\_

*Jimmy's*

```
"com.android.browser.permission.READ_HISTORY_BOOKMARKS" />
"android.permission.READ_CALENDAR" />
"android.permission.CAMERA" />
"android.permission.READ_CONTACTS" />
"android.permission.GET_ACCOUNTS" />
"android.permission.ACCESS_COARSE_LOCATION" />
"android.permission.ACCESS_FINE_LOCATION" />
"android.permission.ACCESS_BACKGROUND_LOCATION" />
"android.permission.RECORD_AUDIO" />
"android.permission.MODIFY_AUDIO_SETTINGS" />
"android.permission.READ_PHONE_STATE" />
"android.permission.READ_PHONE_NUMBERS" />
"android.permission.READ_CALL_LOG" />
"android.permission.PROCESS_OUTGOING_CALLS" />
"android.permission.CALL_PHONE" />
"android.permission.READ_SMS" />
"android.permission.RECEIVE_SMS" />
"android.permission.RECEIVE_MMS" />
"android.permission.SEND_SMS" />
"android.permission.WRITE_EXTERNAL_STORAGE" />
"android.permission.READ_EXTERNAL_STORAGE" />
"android.permission.INTERNET" />
"android.permission.ACCESS_NETWORK_STATE" />
"android.permission.ACCESS_WIFI_STATE" />
"android.permission.CHANGE_WIFI_STATE" />
"android.permission.CHANGE_NETWORK_STATE" />
```



Ginger Some Sugar

```
stalkerware@ubuntu:~/Desktop/Sta
AndroidManifest.xml
assets
classes.dex
classes-dex2jar.jar
fabric
```

 DEX2JAR



```
arrayList1.add(" ");
ArrayList<String> arrayList2 = new ArrayList();
this();
arrayList2.add(e.d(paramContext));
arrayList2.add(e.b());
arrayList2.add("AD");
String str = a.a("http://protocol-a.thetruthspy.com/protocols/getsetting.aspx", arrayList1, arrayList2);
Logger logger = this.c;
StringBuilder stringBuilder = new StringBuilder();
this();
```



```
com.android.browser.permission.READ_HISTORY_BOOKMARKS"/>
    android.permission.READ_CALENDAR"/>
    android.permission.CAMERA"/>
    android.permission.READ_CONTACTS"/>
    android.permission.GET_ACCOUNTS"/>
    android.permission.ACCESS_COARSE_LOCATION"/>
    android.permission.ACCESS_FINE_LOCATION"/>
    android.permission.ACCESS_BACKGROUND_LOCATION"/>
    android.permission.RECORD_AUDIO"/>
    android.permission.MODIFY_AUDIO_SETTINGS"/>
    android.permission.READ_PHONE_STATE"/>
    android.permission.READ_PHONE_NUMBERS"/>
    android.permission.READ_CALL_LOG"/>
    android.permission.PROCESS_OUTGOING_CALLS"/>
    android.permission.CALL_PHONE"/>
    android.permission.READ_SMS"/>
    android.permission.RECEIVE_SMS"/>
    android.permission.RECEIVE_MMS"/>
    android.permission.SEND_SMS"/>
    android.permission.WRITE_EXTERNAL_STORAGE"/>
    android.permission.READ_EXTERNAL_STORAGE"/>
    android.permission.INTERNET"/>
    android.permission.ACCESS_NETWORK_STATE"/>
    android.permission.ACCESS_WIFI_STATE"/>
    android.permission.CHANGE_WIFI_STATE"/>
    android.permission.CHANGE_NETWORK_STATE"/>
```



**DECOMPILER.COM**

① 11 engines detected this file

23bf97b170e152e63ab738e40746556fa66491d12870d93702b87672483a506a  
TheTruthSpy.apk

3.77 MB | 2020-06-08 17:37:53 UTC  
Size | 1 day ago

apk | APK

DETECTION	DETAILS	RELATIONS	COMMUNITY
AhnLab-V3	① PUP/Android.Malct.517091	Avira (no cloud)	① PUA/ANDR.Monitor.FGBA.Gen
CAT-QuickHeal	① Android.Nidb.GEN33124 (PUP)	DrWeb	① Program Spyoo 4 origin
ESET-NOD32	① A Variant Of Android/Monitor.Spyoo.U	F-Secure	① PotentialRisk.PUA/ANDR.Monitor
K7GW	① Trojan ( 005668d81 )	Kaspersky	① Not-a-virus:HEUR:Monitor.AndroidOS.Ni...
Sophos AV	① Andr/TruthSpy-A	Symantec Mobile Insight	① Other:Android.Reputation.2
ZoneAlarm by Check Point	① Not-a-virus:HEUR:Monitor.AndroidOS.Ni...	Ad-Aware	② Undetected



VIRUSTOTAL

## Permissions

- ⚠ android.permission.ACCESS\_COARSE\_LOCATION
- ⚠ android.permission.ACCESS\_FINE\_LOCATION
- ⚠ android.permission.CALL\_PHONE
- ⚠ android.permission.CAMERA
- ⚠ android.permission.CHANGE\_WIFI\_STATE
- ⚠ android.permission.INTERNET
- ⚠ android.permission.PROCESS\_OUTG
- ⚠ android.permission.READ\_CALENDAR
- ⚠ android.permission.READ\_CALL\_LOG
- ⚠ android.permission.READ\_CONTACTS
- ⚠ android.permission.READ\_PHONE\_ST
- ⚠ android.permission.READ\_SMS
- ⚠ android.permission.RECEIVE\_MMS
- ⚠ android.permission.RECEIVE\_SMS
- ⚠ android.permission.RECORD\_AUDIO
- ⚠ android.permission.SEND\_SMS
- ⚠ android.permission.SYSTEM\_ALERT\_WINDOW
- ⚠ android.permission.WRITE\_EXTERNAL\_STORAGE

## Interesting Strings

```
http://  
http://docs.google.com/gview?embedded=true&url=  
http://protocol-a.thetruthspy.com/protocols/get_snx_now.aspx  
http://protocol-a.thetruthspy.com/protocols/getsetting.aspx
```



VIRUSTOTAL

malicious

Threat Score: 100/100

AV Detection: 17%

Labeled as:

Monitor.AndroidOS.Nidb

## File Permissions

android.permission.READ\_CALENDAR

Allows an application to read the user's calendar data.

android.permission.CAMERA

Required to be able to access the camera device.

android.permission.READ\_CONTACTS

Allows an application to read the user's contacts data.

android.permission.T\_ACCOUNTS

Allows access to the list of accounts in the Accounts Service.

android.permission.ACCESS\_COARSE\_LOCATION

Allows an app to access approximate location.

android.permission.ACCESS\_FINE\_LOCATION

Allows an app to access precise location.

android.permission.ACCESS\_BACKGROUND\_LOCATION

-

android.permission.RECORD\_AUDIO

Allows an application to record audio.

## MITRE ATT&CK™ Techniques Detection

### Effects

- Premium SMS Toll Fraud 1

### Persistence

- App Auto-Start at Device Boot 1

### Collection

- Access Call Log 1
- Email Collection 1
- Microphone or Camera Recordings 1



# HYBRID ANALYSIS

Loading language 'x86:LE:32:def...' 



016)ato 0

REAGAN



App	Domain	IP	Country	ASN Name	ASN #
Cerberus	www.cerberusapp.com	66.228.35.203	United States	Linode, LLC	63949
FlexiSPY	admin.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
FlexiSPY	admin.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
FlexiSPY	api.flexispy.com	180.150.144.84	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	blog.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335
FlexiSPY	blog.flexispy.com	104.25.91.115	United States	Cloudflare, Inc.	13335
FlexiSPY	client.mobilefonex.com	180.150.156.198	Hong Kong	Rackspace IT Hosting AS IT Hosting Provider Hong Kong	45187
FlexiSPY	community.flexispy.com	104.25.91.115 <sup>90</sup>	United States	Cloudflare, Inc.	13335
FlexiSPY	community.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335



CITIZENLAB



mspyonline.com



www.mspyonline.com	172.67.70.114	104.26.4.35	104.26.5.35	...
cp.mspyonline.com	172.67.70.114	104.26.4.35	104.26.5.35	...
my.mspyonline.com	104.26.4.35	104.26.5.35	104.25.85.24	...
maps.mspyonline.com	104.26.5.35	104.26.4.35		
debug.mspyonline.com	142.91.14.150	46.166.133.19	109.201.145.153	
api7.mspyonline.com	104.25.85.24	104.25.84.24		
ajax.mspyonline.com	104.25.84.24	104.25.85.24	104.24.12.36	...
tracking.mspyonline.com	94.23.161.19	54.38.226.140	46.105.88.234	...
repo.mspyonline.com	104.25.85.24	104.25.84.24		
help.mspyonline.com	104.25.85.24	104.25.84.24	104.24.12.36	...

...

#### Files Referring ①

Scanned	Detections	Type	Name
2020-06-09	29 / 69	Win32 DLL	b3de682abcd28f358ecf5677bbf91dc39df2c61a
2020-06-07	13 / 61	Android	classes.dex
2020-06-10	31 / 70	Win32 DLL	1cedc2cdf98049785212262cd56915ec.bin
2020-06-11	5 / 60	Android	MSpyAndroidApp_v5.1.0_build_547.apk



CITIZENLAB

The screenshot shows a VirusTotal analysis page for an APK file. The file hash is 49a4380a485809122953354e2d3ddb056e15c3386396fc07dab482c521fc1af1. It has been analyzed by 23 engines, indicated by a circular progress bar with the number 23. The file size is 4.90 MB and it was submitted on 2020-05-23 23:19:40 UTC, 18 days ago. The file is identified as MSpyAndroidApp-v5.6.0-555.apk. The analysis tab selected is BEHAVIOR, which lists behavior tags: checks-gps, reflection, and telephony. The COMMUNITY tab shows a community score of 63. A pink box highlights the 'HTTP Requests' section under Network Communication, which contains a single entry: + https://a.thd.cc/apiv4/register/login.

Σ 49a4380a485809122953354e2d3ddb056e15c3386396fc07dab482c521fc1af1

23 engines detected this file

49a4380a485809122953354e2d3ddb056e15c3386396fc07dab482c521fc1af1

4.90 MB  
Size 2020-05-23 23:19:40 UTC  
18 days ago

MSpyAndroidApp-v5.6.0-555.apk  
apk contains-elf

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

VirusTotal Droidy

Full report

Behavior Tags

checks-gps reflection telephony

Network Communication

HTTP Requests

+ https://a.thd.cc/apiv4/register/login



# STALKERWARE VENDOR BREACHES

Retina-X (2x)  
Flexispy  
Mobistealth  
Spy Master Pro  
SpyHuman  
Spyfone  
HelloSpy

TheTruthSpy  
Family Orbit  
mSpy  
Copy9  
Xnore  
Mobiispy  
WtSpy  
KidsGuard



# SPY ON MY WIFE

spy on my wife

spyier.com › mobile-spy › spy-my-wife ▾

## How to Spy on My Wife Without Her Knowing (100% Works!)

Dec 17, 2019 - Is your marriage in trouble? Do you believe your wife is cheating on you? Here's how to spy on your wife's phone without her knowing ...

Part 1: How to Spy on My ... · Spyier – The ... · How to Spy on My Wife ...

mobiespy.com › blog › 5-apps-for-spying-on-your-spo... ▾

## 5 Apps For Spying On Your Cheating Spouse | MobieSpy

Catch **your cheating spouse** with the help of cell phone **spying** apps like mSpy, Stealth, PhoneSheriff, Mobile **Spy** and Mobistealth and reveal the truth.

appmia.com › how-to-spy-on-my-wifes-text-messages-f... ▾

## How to spy on my wife's text messages free - Appmia

Get monitoring app for **your wife's** Android phone or iPhone and track everything that goes in and out of the cell, regardless of how far you are from **your wife**.

You visited this page on 6/11/20.

# ESPIONAR MINHA ESPOSA



"espiar minha esposa"

All

Videos

Shopping

News

Images

More

X



About 7,410 results (0.37 seconds)

[www.cocospy.com › blog › pt-br › e...](#) ▾ [Translate this page](#)

**Como Espionar o Celular da Minha Esposa Sem Ela Saber ...**

Mar 29, 2019 - Os mais populares sistemas operacionais presentes hoje são o Android e o iOS. Se você deseja espionar sua esposa, então com certeza este ...

[fonespy.net › spy-on-my-wifes-phon...](#) ▾ [Translate this page](#)

**Como espionar o telefone da minha esposa sem tocá-lo ...**

Posted in Traindo o cônjugeTagged espionar meu marido, espionar meu namorado, **espionar minha esposa**, espionar minha namorada, espionar o telefone da ...

[www.spymasterpro.com › blog › mo...](#) ▾ [Translate this page](#)

**É possível monitorar as atividades online da minha esposa ...**

Tag: Acompanhe minha esposaEspião na esposae**espionar minha esposa**Minha esposa está me traindo?monitorar as atividades online da sua esposa ...

[www.spymasterpro.com › blog › tag-](#) [tag](#) ▾ [Translate this page](#)

**espionar minha esposa Archives – SpyMaster - Spymaster Pro**

**espionar minha esposa.** É possível monitorar as atividades online da minha esposa infiel? batota cônjuge · celular espião android · como rastrear batota ...

[www.spyzie.com › spy › how-to-spy...](#) ▾ [Translate this page](#)

**Como Espionar Minha Esposa Infiel - FamiSafe**

**spyzie**

Search All results ▾

?

## Apps

 AllTracker. Family protection RUSSCITY 	 Phone Tracker By N Family Locator Inc. 	 Message and Call Tracker karanth 	 Chat Message Tracker Apps TrackerApps 
 Spyware Detector - <b>Incognito</b> 	 FamiSafe - Parental Control Others Photo 	 Control Others Photo 	 Message Peeping T 

### ADDITIONAL INFORMATION

Updated	Size	Installs
June 6, 2020	7.2M	50,000,000+
Current Version	Requires Android	Content Rating
5.75	4.1 and up	Everyone <a href="#">Learn More</a>
Interactive Elements	In-app Products	Permissions
Users Interact, Shares Location	\$9.49 per item	<a href="#">View details</a>
Report	Offered By	<b>Developer</b>
<a href="#">Flag as inappropriate</a>	Family Locator Inc.	<a href="#">Visit website</a> devteam@onelocator.com <a href="#">Privacy Policy</a> 3 Albert alawal st, smouha, Alexandria

GOOGLE PLAY



Censys

Q Websites

flexispy.com

Results Report

#### Quick Filters

For all fields, see [Data Definitions](#)

#### Protocol:

- 3 443/https
- 2 25/smtp
- 2 443/https\_www
- 2 80/http
- 2 80/http\_www

#### Tag:

- 3 http
- 2 https
- 2 smtp

#### Websites

Page: 1/1 Results: 3 Time: 82ms

:flexispy.com (159.138.32.61)

- ★ 81,385 ⚒ 25/smtp, 443/https, 443/https\_www, 80/http, 80/http\_www
- HomeAs FlexiSPY™ Unique Monitoring Software For Mobiles & Computers ⚒ \*.flexispy.com, flexispy.com
- Q domain: flexispy.com

:flexispy.com (172.67.180.43)

- ★ 172,136 ⚒ 25/smtp, 443/https, 443/https\_www, 80/http, 80/http\_www
- HomeAs 11 Best Phone Tracker Apps to Monitor any Cell Phone [2020] ⚒ sni.cloudflaressl.com, \*.celltrackingapps.com, celltrackingapps.com

:flexispy.com (199.188.205.55)

- ★ 456,944 ⚒ 443/https
- Q 443.https.get.body: @ flexispy.com</a>

# @NSCRUTABLES

The GitHub repository page for 'diskurse / android-stalkerware' shows a code editor with a large redacted section. The redacted area contains the following table:

	website	product
1	spytech-web.com	SpyAgent
2	spytech-web.com	Realtime-Spy



# SECURITY RESEARCHERS

# @NSCRUTABLES

cian @nscrutables · 7h  
Was curious about the "Spyier" #stalkerware that appeared in a paid advertisement masquerading as an article in @TechTimes\_News & called out by @evacide and others.

Looking at the apk source, "Spyier" appears to be a reskinned version of "CocoSpy", with other named variants.

```
public class FlavorsConfig {  
    public static String account_auth_provider;  
    public static String account_auth_type;  
    public static String baseUrl;  
  
    public static void setUrls(String variant) {  
        baseUrl = "https://1.spyier.com/api/";  
        account_auth_type = "com.spyier.account_auth_type";  
        account_auth_provider = "com.spyier.account_auth_provider";  
    }  
    if ("spyier".equals(variant)) {  
        baseUrl = "https://1.spyier.com/api/";  
        account_auth_type = "com.spyier.account_auth_type";  
        account_auth_provider = "com.spyier.account_auth_provider";  
    }  
    if ("minspy".equals(variant)) {  
        baseUrl = "https://1.minspy.com/api/";  
        account_auth_type = "com.minspy.account_auth_type";  
        account_auth_provider = "com.minspy.account_auth_provider";  
    }  
    if ("spylne".equals(variant)) {  
        baseUrl = "https://1.spylne.com/api/";  
        account_auth_type = "com.spylne.account_auth_type";  
        account_auth_provider = "com.spylne.account_auth_provider";  
    }  
}
```

3 10 16



# SECURITY RESEARCHERS

# @MALWRHUNTERTEAM

Search: @malwrhuntereampk

Top Latest People Photos Videos

**MalwareHunterTeam** @malwrhuntereampk · 2h  
Not much detected "20GBGift.apk":  
5386abd90497dc0b97537ae585addfa1772b10cd4353e41b413e90eb07a145f  
e  
From: [https://20gbcampings\[.\]com/](https://20gbcampings[.]com/) ->  
[https://20gbcampings\[.\]com/APK/20GBGift.apk](https://20gbcampings[.]com/APK/20GBGift.apk)  
cc @JAMESWT\_MHT @douglasmun

The screenshot shows a social media post from the MalwareHunterTeam account. The post includes a link to a download page for a malicious APK file. The page features a banner with a man speaking at a podium and logos for Lazada, Maxis, Celcom, and Digi. Text on the page encourages users to download the app to support the fight against coronavirus. A warning message at the bottom states: "20 GB Internet Gift to all our citizens within the scope of fighting against coronavirus! You can define your gift to your line by downloading the application." Below this is a button labeled "Gift 20 GB Internet Download". Further down, there is a link "OPEN UNKNOWN RESOURCES". To the right of the download page, there is a detailed view of the APK's certificate attributes and subject information, which is heavily redacted. A red exclamation mark icon indicates that the APK is a "Trojan (0x5051f1)". The post has 4 likes and 5 comments.



# SECURITY RESEARCHERS

# URL CATEGORY

IBM X-Force Exchange ALL ▾ Search by Application name, IP address, URL, Vulnerability Q

Risk 1

X-Force URL Report

thetruthspy.com

This report does not contain tags. Add tags via the comment box.

[Twitter](#) [LinkedIn](#) [Facebook](#)

**Details**

**Categorization** • Education  
▪ Health

**Application** No known application

**WHOIS Record**

Created	Aug 9, 2013
Updated	May 29, 2019
Expires	Aug 9, 2021
Registrant Name	Registration Private
Registrant Organization	Domains By Proxy, LLC
Registrant Country or Region	United States
Registrar Name	GoDaddy.com, LLC
Email	THETRUTHSPY.COM@domainsbyproxy.com

# ! THETRUTHSPY.COM

Web Reputation:

- High Risk (10 of 100)

[Request a reputation change](#)

Web Category:

- Keyloggers and Monitoring

[Request a category change](#)

Web Reputation Influences:

- 1 infections (past 12 months)
- High popularity
- 159 months old (established)

Impact:

Web Database Version: 7.409 - Last Updated: 06/09/2020 02:00

#### Permissions

- ⚠ android.permission.ACCESS\_COARSE\_LOCATION
- ⚠ android.permission.ACCESS\_FINE\_LOCATION
- ⚠ android.permission.CALL\_PHONE
- ⚠ android.permission.CAMERA
- ⚠ android.permission.CHANGE\_WIFI\_STATE
- ⚠ android.permission.INTERNET
- ⚠ android.permission.PROCESS\_OUTGOING\_CALLS
- ⚠ android.permission.READ\_CALENDAR
- ⚠ android.permission.READ\_CALL\_LOG
- ⚠ android.permission.READ\_CONTACTS

**submitter:PT AND  
androguard:"android.permission.  
ACCESS\_COARSE\_LOCATION" AND  
androguard:"android.permission.  
CAMERA" AND  
androguard:"android.permission.  
READ\_SMS"**

#### FILES 4

4483AD81F45C02006BF1A9DA9A802029834B4C1F15C6C411C5402267EF2CD89D

com.metasploit.stage

android cve-2012-4681 exploit apk

2179162DEFAA17906E236221A5617A0CDFBEEECAB58C9EDA1B3A8BDB1208D036

com.metasploit.stage

android cve-2012-4681 exploit apk

6443A90C783B0FC365DCD8D86FA776CFFE4E3BBA5D7231F306AC88AB89990073

com.metasploit.stage

android cve-2012-4681 exploit apk

EF1E5983010B375431777EA04B226A136CF0D4ACBE99BEC30EF839F6B758C69B

com.metasploit.stage

android cve-2012-4681 exploit apk



**VIRUSTOTAL SEARCH**



# STALKERWARE & CORPORATE

 [sites.google.com/view/stalkerware](https://sites.google.com/view/stalkerware)



## THREAT SUMMARY REPORT

[CLICK HERE!](#)

## INDICATORS OF COMPROMISE - IOCs

[CLICK HERE!](#)



BSIDESPORTO 2020

## THREAT SUMMARY REPORT

STALKERWARE

07/23/20

### SUMMARY

On July 23rd, 2020, a presentation, "Every Breath You Take: A CTI Review of Stalkerware," at BSidesPorto provided insights into Stalkerware concerning what it is, how it works, who it targets, how stalkerware could impact Enterprise companies, and possible solutions to consider.

Stalkerware is software used to "facilitate intimate partner intimate partner violence, abuse, or harassment, including pernicious intrusions into the targeted person's life by way of physical or digital actions" [1]. Commodity stalkerware is a tool used for intimate partner surveillance along with commodity spyware, dual-use apps, shared accounts, IoT devices, home security services, mRATs, and more. Stalkerware could be considered spyware, stalkerware, dual-use apps, or mRATs based upon their respective usage.

### TECHNICAL SUMMARY

Capabilities of Commodity Stalkerware

- Basic: review text messages, various chat applications (WhatsApp, LINE), phone call logs, GPS location, browser history; stored media such as photos and videos [1].
- Varies by Stalkerware Vendor: access to email, social media, additional messaging apps, device settings, stored files, record phone calls, voicemails, calendar, contacts, record surroundings, keystrokes, take pictures [1].

Lockheed Martin Cyber Kill Chain of Commodity Stalkerware

- Reconnaissance
  - Information gathering on target
- Weaponization
  - Obtain url or other instructions for stalkerware installation through purchasing the service.
- Delivery
  - Obtain physical access to the targeted device.
- Exploitation
  - No technical exploits for commodity Stalkerware
  - Possible social engineering of target
  - Unlock screen, if locked.
  - Determine access to download apps from the App Store/Google Play Store, or modify settings of the phone.
    - Leverage remote support of stalkerware vendor to install stalkerware
- Installation
  - Install stalkerware via stalkerware vendor provided link, stalkerware vendor provided instructions, or via app store.
- Command and Control
  - Remote Access to device over Wifi or Cell and contents displayed on a web-based GUI for the operator



[sites.google.com/view/stalkerware](https://sites.google.com/view/stalkerware)



Contact me on Twitter:

[@Ch33r10](https://twitter.com/@Ch33r10)



*Give me some sugar*

 [github.com/ch33r10/stalkerware](https://github.com/ch33r10/stalkerware)



**MBA IT Management**  
**D.Sc. Cybersecurity Student at Marymount**  
**University**  
**GSEC, GCIH, GCFE, GMON, GDAT, GPEN,**  
**GCTI**

**@ch33r10**

## REFERENCES

- 1 <https://www.cbc.ca/news/opinion/opinion-stalkerware-abuse-covid-isolation-phones-1.5556379>
- 1 <https://www.zdnet.com/article/stalkerware-infections-grew-by-40-in-2019-says-kaspersky/>
- 6 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>
- 7 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>
- 8 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>
- 8 <https://assets.documentcloud.org/documents/4599753/NSO-Pegasus.pdf>
- 8 [https://www.vice.com/en\\_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x](https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x)
- 8 <https://youtu.be/EzMkqtNAo6A>
- 9 <https://assets.documentcloud.org/documents/4599753/NSO-Pegasus.pdf>
- 9 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>
- 11 <https://www.ft.com/content/263133ac-a28b-11e9-974c-ad1c6ab5efd1>
- 10 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>
- 13 <https://xnspy.com/install-spyware-on-android-remotely.html>
- 13 <https://www.defcon.org/images/defcon-20/dc-20-presentations/Robinson/DEFCON-20-Robinson-Spy-vs-Spy.pdf>
- 15 [https://www.vice.com/en\\_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x](https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x)
- 16 <https://www.helpnetsecurity.com/2014/10/21/delivering-malicious-android-apps-hidden-in-image-files/>
- 16 <https://www.blackhat.com/docs/eu-14/materials/eu-14-Apvrille-Hide-Android-Applications-In-Images-wp.pdf>
- 16 <https://thehackernews.com/2019/02/hack-android-with-image.html>
- 16 <https://blog.malwarebytes.com/mac/2019/08/unprecedented-new-iphone-malware-discovered/>
- 16 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618>
- 17 <https://attack.mitre.org>
- 18 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618>
- 18 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>
- 18 <https://www.cbc.ca/radio/day6/venezuela-s-would-be-presidents-alien-the-school-play-women-s-football-stalkerware-after-parkland-more-1.5116896/stalkerware-is-more-common-than-you-think-and-eva-galperin-has-a-plan-to-stop-it-1.5116916>
- 19 [https://www.vice.com/en\\_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x](https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x)
- 24 [https://www.vice.com/en\\_us/article/gyznng/how-nsa-group-helps-countries-hack-targets](https://www.vice.com/en_us/article/gyznng/how-nsa-group-helps-countries-hack-targets)
- 24 <https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html>
- 24 <https://www.ynetnews.com/articles/0,7340,L-5444998,00.html>
- 24 <https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/>
- 25 [https://www.vice.com/en\\_us/article/a357b5/hackers-tried-to-compromise-phones-of-tibetans-working-for-dalai-lama](https://www.vice.com/en_us/article/a357b5/hackers-tried-to-compromise-phones-of-tibetans-working-for-dalai-lama)
- 25 <https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284>
- 25 <https://www.citylab.com/equity/2017/02/cellphone-spy-tools-have-flooded-local-police-departments/512543/>
- 25 <https://thehackernews.com/2020/04/iphone-zero-day-exploit.html>
- 25 <https://thehackernews.com/2020/03/iphone-iOS-spyware.html>

## REFERENCES

- 26 <https://www.calcalistech.com/ctech/articles/0,7340,L-3774443,00.html>
- 27 <https://www.calcalistech.com/ctech/articles/0,7340,L-3774443,00.html>
- 27 <https://www.wsj.com/articles/police-tracked-a-terror-suspect-until-his-phone-went-dark-after-a-facebook-warning-11577996973>
- 28 <https://www.cyberscoop.com/u-s-army-bans-tiktok-amid-ongoing-scrutiny-chinese-made-video-app/>
- 28 <https://www.wsj.com/articles/police-tracked-a-terror-suspect-until-his-phone-went-dark-after-a-facebook-warning-11577996973>
- 28 <https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf>
- 31 [https://www.vice.com/en\\_us/article/zmwnm3/metropolitan-police-flexispy-legal-complaint](https://www.vice.com/en_us/article/zmwnm3/metropolitan-police-flexispy-legal-complaint)
- 31 [https://www.vice.com/en\\_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware](https://www.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware)
- 33 <https://www.cbsnews.com/news/610k-settlement-in-school-webcam-spy-case/>
- 33 <https://www.eff.org/wp/school-issued-devices-and-student-privacy>
- 34 <https://www.usatoday.com/story/tech/2019/10/08/is-the-boss-tracking-you-now/3901594002/>
- 34 [https://www.vice.com/en\\_us/article/7x5m5a/ftc-bans-retinax-from-selling-stalkerware](https://www.vice.com/en_us/article/7x5m5a/ftc-bans-retinax-from-selling-stalkerware)
- 34 <https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers>
- 36 <https://www.reuters.com/article/us-usa-mexico-el-chapo/el-chapo-aide-who-helped-fbi-tap-his-phones-takes-stand-idUSKCN1P32BQ>
- 37 <https://www.miamiherald.com/news/local/crime/article236013148.html>
- 37 <https://www.citylab.com/equity/2017/02/cellphone-spy-tools-have-flooded-local-police-departments/512543/>
- 37 <https://www.cpomagazine.com/cyber-security/swedish-police-given-green-light-for-spyware/>
- 37 [https://www.vice.com/en\\_us/article/zmwnm3/metropolitan-police-flexispy-legal-complaint](https://www.vice.com/en_us/article/zmwnm3/metropolitan-police-flexispy-legal-complaint)
- 37 [https://www.vice.com/en\\_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware](https://www.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware)
- 38 <https://threatpost.com/pegasus-spyware-targets-investigative-journalists-in-mexico/139424/>
- 38 [https://www.vice.com/en\\_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware](https://www.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware)
- 38 <https://info.lookout.com/rs/051-ESQ-475/images/lookout-stealth-mango-srr-us.pdf>
- 46 <https://www.usatoday.com/story/tech/2019/10/08/is-the-boss-tracking-you-now/3901594002/>
- 46 <https://threatpost.com/cerberus-trojan-major-spyware-targeted-attack/155415/>
- 47 <https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/>
- 47 <https://github.com/diskurse/android-stalkerware>
- 47 <https://twitter.com/lorenzofb/status/1057679550790934528>
- 47 [https://www.vice.com/en\\_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy](https://www.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy)
- 47 [https://www.vice.com/en\\_us/article/9kmj4v/spyware-company-spyfone-terabytes-data-exposed-online-leak](https://www.vice.com/en_us/article/9kmj4v/spyware-company-spyfone-terabytes-data-exposed-online-leak)
- 47 [https://www.vice.com/en\\_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x](https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x)
- 47 [https://www.vice.com/en\\_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked](https://www.vice.com/en_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked)
- 47 [https://www.vice.com/en\\_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher](https://www.vice.com/en_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher)

## REFERENCES

- 48 <https://github.com/diskurse/android-stalkerware>  
48 <https://twitter.com/lorenzofb/status/1057679550790934528>  
48 [https://www.vice.com/en\\_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy](https://www.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy)  
48 [https://www.vice.com/en\\_us/article/9kmj4v/spyware-company-spyfone-terabytes-data-exposed-online-leak](https://www.vice.com/en_us/article/9kmj4v/spyware-company-spyfone-terabytes-data-exposed-online-leak)  
48 [https://www.vice.com/en\\_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x](https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x)  
48 [https://www.vice.com/en\\_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked](https://www.vice.com/en_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked)  
48 [https://www.vice.com/en\\_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher](https://www.vice.com/en_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher)  
48 <https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/>  
49 <https://havron.dev/pubs/clinicalsec.pdf>  
49 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>  
50 [https://apav.pt/apav\\_v3/images/pdf/Estatisticas\\_APAV-Relatorio\\_Annual\\_2019.pdf](https://apav.pt/apav_v3/images/pdf/Estatisticas_APAV-Relatorio_Annual_2019.pdf)  
53 <https://www.nytimes.com/2020/01/22/technology/jeff-bezos-hack-iphone.html>  
55 <https://securityintelligence.com/articles/when-stalkerware-stalks-the-enterprise/>  
57 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>  
57 <https://blog.devolutions.net/2019/06/the-threat-stalkerware-poses-to-your-business>  
58 <https://threatpost.com/cerberus-trojan-major-spyware-targeted-attack/155415/>  
59 <https://github.com/diskurse/android-stalkerware/blob/master/README.md>  
59 <https://stopstalkerware.org/2019/10/06/the-stalkerware-threat/>  
59 Daniel Nash BSides Belfast 2018 The Terror of Tracking <https://www.youtube.com/watch?v=126s8hsuomM>  
59 <https://securityintelligence.com/articles/when-stalkerware-stalks-the-enterprise/>  
59 <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618>  
60 <https://TALLPOPPY.IO>  
60 <https://safeescape.org>  
60 <https://www.ncadv.org/>  
60 <https://nnedv.org/>  
60 <https://stopstalkerware.org>  
60 <https://www.ipvtechresearch.org/resources>  
60 <https://github.com/stopipv/isdi>  
60 <https://github.com/diskurse/android-stalkerware/blob/master/README.md>  
60 <https://stopstalkerware.org/2019/10/06/the-stalkerware-threat/>  
60 Usenix Security 2019 Clinical Computer Security for Victims of Intimate Partner Violence <https://youtu.be/YsFZ3OxwWN0>

## REFERENCES

- 63 Kristina Balaam Tools <https://www.youtube.com/watch?v=TbZI2bhchAM>
- 63 Kristina Balaam RE Apks <https://www.youtube.com/watch?v=7oj2YnyHh1g>
- 64 <https://ibotpeaches.github.io/Apktool/>
- 65 <https://github.com/pxb1988/dex2jar>
- 66 <http://jd.benow.ca/>
- 67 <http://www.decompiler.com/jar/250ac1190e6440c792401088dafd05d9/TheTruthSpy.apk/resources/AndroidManifest.xml>
- 68 <https://www.virustotal.com/gui/file/23bf97b170e152e63ab738e40746556fa66491d12870d93702b87672483a506a/details>
- 69 <https://www.virustotal.com/gui/file/23bf97b170e152e63ab738e40746556fa66491d12870d93702b87672483a506a/details>
- 70 <https://www.hybrid-analysis.com/sample/23bf97b170e152e63ab738e40746556fa66491d12870d93702b87672483a506a/5edef21d84b6396f6d37d741>
- 73 <https://citizenlab.ca/docs/stalkerware-holistic.pdf>
- 74 <https://www.virustotal.com/gui/domain/mspyonline.com/relations>
- 75 <https://www.virustotal.com/gui/file/49a4380a485809122953354e2d3ddb056e15c3386396fc07dab482c521fc1af1/detection>
- 76 <https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/>
- 76 <https://github.com/diskurse/android-stalkerware>
- 76 <https://twitter.com/lorenzofb/status/1057679550790934528>
- 76 [https://www.vice.com/en\\_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy](https://www.vice.com/en_us/article/7xnybe/hosting-provider-takes-down-spyware-mobiispy)
- 76 [https://www.vice.com/en\\_us/article/9kmj4v/spyware-company-spyfone-terabytes-data-exposed-online-leak](https://www.vice.com/en_us/article/9kmj4v/spyware-company-spyfone-terabytes-data-exposed-online-leak)
- 76 [https://www.vice.com/en\\_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x](https://www.vice.com/en_us/article/53vm7n/inside-stalkerware-surveillance-market-flexispy-retina-x)
- 76 [https://www.vice.com/en\\_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked](https://www.vice.com/en_us/article/gvye3m/spy-tech-company-hacking-team-gets-hacked)
- 76 [https://www.vice.com/en\\_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher](https://www.vice.com/en_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher)
- 77 [https://www.google.com/search?sxsrf=ALeKk01IwaKirOj0VOB8Q5-nNxG2LT5mmg%3A1591922557343&source=hp&ei=fc\\_iXr35EeOa\\_QaK3zg&q=SPY+ON+MY+WIFE&oq=SPY+ON+MY+WIFE&gs\\_lcp=CgZwc3ktYWIOAzIECCMQJzoFCAAQOzoFCAAAQkQI6BQgAEIMBOggIABCDARCRAjoHCAAQgwEOQzoFCAAQsQM6AggAOgQIAAKOgYIABAWEb5Q4wpYiB1gkyFoAHAAeACAAZ8BiAG\\_DZIBBDaUMTSYAOCgAQGgAQdnD3Mtd2l6&sclient=psy-ab&ved=0ahUKEwj9q6bUhfvpAhVjTdT8KHYovDgAQ4dUDCAk&uact=5](https://www.google.com/search?sxsrf=ALeKk01IwaKirOj0VOB8Q5-nNxG2LT5mmg%3A1591922557343&source=hp&ei=fc_iXr35EeOa_QaK3zg&q=SPY+ON+MY+WIFE&oq=SPY+ON+MY+WIFE&gs_lcp=CgZwc3ktYWIOAzIECCMQJzoFCAAQOzoFCAAAQkQI6BQgAEIMBOggIABCDARCRAjoHCAAQgwEOQzoFCAAQsQM6AggAOgQIAAKOgYIABAWEb5Q4wpYiB1gkyFoAHAAeACAAZ8BiAG_DZIBBDaUMTSYAOCgAQGgAQdnD3Mtd2l6&sclient=psy-ab&ved=0ahUKEwj9q6bUhfvpAhVjTdT8KHYovDgAQ4dUDCAk&uact=5)

## REFERENCES

79 <https://play.google.com/store/search?q=SPYZIE>

79 <https://play.google.com/store/apps/details?id=mg.locations.track5>

80 <https://censys.io/domain?q=flexispy.com>

81 <https://github.com/diskurse/android-stalkerware/blob/master/docs/pcmonitor.csv>

82 [https://twitter.com/search?q=%23stalkerware%20apk&src=typed\\_query](https://twitter.com/search?q=%23stalkerware%20apk&src=typed_query)

83 [https://twitter.com/search?q=%40malwrhunterteam%20apk&src=typed\\_query](https://twitter.com/search?q=%40malwrhunterteam%20apk&src=typed_query)

84 <https://zeltser.com/lookup-malicious-websites/>

84 <https://exchange.xforce.ibmcloud.com/url/thetruthspy.com>

84 <https://Brightcloud.com>

85

[https://www.virustotal.com/gui/search/submitter%253APT%2520and%2520androguard%253A%2522android.permission.ACCESS\\_COARSE\\_LOCATION%2522%2520AND%2520androguard%253A%2522android.permission.CAMERA%2522%2520AND%2520androguard%253AA%2522android.permission.READ\\_SMS%2522](https://www.virustotal.com/gui/search/submitter%253APT%2520and%2520androguard%253A%2522android.permission.ACCESS_COARSE_LOCATION%2522%2520AND%2520androguard%253A%2522android.permission.CAMERA%2522%2520AND%2520androguard%253AA%2522android.permission.READ_SMS%2522)

86 <https://sites.google.com/view/stalkerware>

87 <https://sites.google.com/view/stalkerware>

88 <https://sites.google.com/view/stalkerware>

89 <https://sites.google.com/view/stalkerware>

90 <https://github.com/ch33r10/Stalkerware>

## RESEARCH

- <https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>
- <https://www.ipvtechresearch.org/research>
- <https://www.zdnet.com/article/employee-safety-is-for-sale/>
- [https://www.vice.com/en\\_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware](https://www.vice.com/en_us/article/ywqqkw/military-fbi-and-ice-are-customers-of-controversial-stalkerware)
- <https://citizenlab.ca/docs/stalkerware-holistic.pdf>
- <https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/>
- Heather Mahalik <https://youtu.be/IEbLOvT4Fts>
- Eva Galperin <https://youtu.be/OvorPIKXrYA>
- <https://assets.documentcloud.org/documents/4599753/NSO-Pegasus.pdf>
- <https://www.nytimes.com/2019/12/22/us/politics/totok-app-uae.html>
- <https://www.nytimes.com/2019/11/06/opinion/whatsapp-nso-group-spy.html>
- <https://www.digitalbank.global/nso-group-competitors>
- <https://www.fastcompany.com/90369108/inside-the-shadowy-world-of-spyware-makers-that-target-activists-and-dissidents>
- [https://sii.transparencytoolkit.org/search?technology\\_sold\\_facet=Phone+Monitoring](https://sii.transparencytoolkit.org/search?technology_sold_facet=Phone+Monitoring)
- [https://www.calcalistech.com/ctech/articles/0\\_7340\\_1-3749924\\_00.html](https://www.calcalistech.com/ctech/articles/0_7340_1-3749924_00.html)
- <https://www.washingtonpost.com/opinions/2018/12/05/israel-is-selling-spy-software-dictators-betraying-its-own-ideals/>
- [https://www.vice.com/en\\_us/article/qvakb3/inside-nso-group-spyware-demo](https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo)
- [https://www.vice.com/en\\_us/article/3da5qj/government-hackers-iphone-hacking-jailbreak-nso-group](https://www.vice.com/en_us/article/3da5qj/government-hackers-iphone-hacking-jailbreak-nso-group)
- <https://www.welivesecurity.com/2018/06/07/invisimole-equipped-spyware-undercover/>
- <https://arsenalexperts.com/persistent/resources/pdf/Illicit%20Surveillance%20of%20Electronic%20Systems%20in%20Family%20Law%20Cases.pdf>
- [https://www.technologyreview.com/s/613915/stalkerware-apps-are-letting-abusive-partners-spy-on-their-victims/?utm\\_source=twitter&utm\\_campaign=site\\_visitor.unpaid.engagement&utm\\_medium=tr\\_social](https://www.technologyreview.com/s/613915/stalkerware-apps-are-letting-abusive-partners-spy-on-their-victims/?utm_source=twitter&utm_campaign=site_visitor.unpaid.engagement&utm_medium=tr_social)
- <https://www.zdnet.com/article/the-ultimate-guide-to-finding-and-killing-spyware-and-stalkerware/>
- How to Fake a Fingerprint <https://youtu.be/tj2Ty7WkGqk>
- <https://www.zdnet.com/article/google-cleans-out-stalker-apps-from-play-store/>
- <https://ivrodriguez.com/analyzing-ios-stalkerware-apps/>
- <https://blog.talosintelligence.com/2019/10/the-commoditization-of-mobile-espionage.html>
- <https://www.technologyreview.com/profile/patrick-howell-oneill/>
- [https://www.vice.com/en\\_us/contributor/lorenzo-franceschi-bicchieri](https://www.vice.com/en_us/contributor/lorenzo-franceschi-bicchieri)
- [http://www.structuredweb.com/sw/swchannel/CustomerCenter/documents/9353/25297/Lacoon\\_CP\\_Enterprise\\_mRAT\\_Research.pdf](http://www.structuredweb.com/sw/swchannel/CustomerCenter/documents/9353/25297/Lacoon_CP_Enterprise_mRAT_Research.pdf)

# RESEARCH

<https://blog.malwarebytes.com/malwarebytes-news/2019/11/malwarebytes-teams-up-with-security-vendors-and-advocacy-groups-to-launch-coalition-against-stalkerware/>

<https://www.ft.com/content/263133ac-a28b-11e9-974c-ad1c6ab5efd1>

[https://www.rsaconference.com/industry-topics/podcast/threats-of-surveillance-tools-spyware-and-stalkerware?utm\\_source=inhouse&utm\\_medium=email&utm\\_content=RSAC365-newsletter-edition2-text-ongoing-gen-dec2019-2&utm\\_campaign=Newsletter-Edition2-Text-Ongoing-Gen-Dec2019-RSAC365&spMailingID=41350779&spUserID=ODU5MDqxMzqxNzQ3S0&spJobID=1661540021&spReportId=MTY2MTU0MDAyMQS2](https://www.rsaconference.com/industry-topics/podcast/threats-of-surveillance-tools-spyware-and-stalkerware?utm_source=inhouse&utm_medium=email&utm_content=RSAC365-newsletter-edition2-text-ongoing-gen-dec2019-2&utm_campaign=Newsletter-Edition2-Text-Ongoing-Gen-Dec2019-RSAC365&spMailingID=41350779&spUserID=ODU5MDqxMzqxNzQ3S0&spJobID=1661540021&spReportId=MTY2MTU0MDAyMQS2)

<https://homeland.house.gov/preparing-for-the-future-an-assessment-of-emerging-cyber-threats>

[https://pages.cs.wisc.edu/~chatterjee/ppts/IPv\\_spyware.pdf](https://pages.cs.wisc.edu/~chatterjee/ppts/IPv_spyware.pdf)

<https://havron.dev/pubs/clinicalsec.pdf>

<https://havron.dev/pubs/freed-cscw19.pdf>

<http://nixdell.com/papers/stalkers-paradise-intimate.pdf>

<http://nixdell.com/papers/a046-freed.pdf>

<https://www.technologyreview.com/s/614168/nyc-hires-hackers-to-hit-back-at-stalkerware/>

<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8418618>

[http://damonmccoy.com/papers/Creepware\\_SP.pdf](http://damonmccoy.com/papers/Creepware_SP.pdf)

[https://www.vice.com/en\\_us/topic/when-spies-come-home](https://www.vice.com/en_us/topic/when-spies-come-home)

<https://citizenlab.ca/docs/stalkerware-legal.pdf>

<https://www.theguardian.com/world/2019/dec/20/cyprus-police-arrest-three-in-israeli-owned-spy-van-investigation>

<https://info.lookout.com/rs/051-ESQ-475/images/lookout-pegaus-technical-analysis.pdf>

Cian Heasley BSides London 2019 Watching the Watchers: The Stalkerware Surveillance Ecosystem <https://youtu.be/EzMkqtNAo6A>

<https://www.defcon.org/images/defcon-20/dc-20-presentations/Robinson/DEFCON-20-Robinson-Spy-vs-Spy.pdf>

[http://www.structuredweb.com/sw/swchannel/CustomerCenter/documents/9353/25297/Lacoon\\_CP\\_Enterprise\\_mRAT\\_Research.pdf](http://www.structuredweb.com/sw/swchannel/CustomerCenter/documents/9353/25297/Lacoon_CP_Enterprise_mRAT_Research.pdf)

Jessica Amery BSides London 2019 Stalkerware in Mobile Devices <https://youtu.be/TiUFxUChJcI>

<https://www.rsaconference.com/industry-topics/blog/tracking-every-move-from-location-based-apps-to-stalkerware-and-advanced-attacker>

<https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>

<https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html>

# RESEARCH

[https://www.researchgate.net/publication/340588456 Decomplied APK based malicious code classification](https://www.researchgate.net/publication/340588456)  
<https://www.blackhat.com/html/webcast/05072020-stalkerware-solutions-for-mitigating-its-impact-on-privacy-and-security.html>  
<https://threatpost.com/cerberus-trojan-major-spyware-targeted-attack/155415/>  
<https://www.cbc.ca/news/opinion/opinion-stalkerware-abuse-covid-isolation-phones-1.5556379>  
[https://www.vice.com/en\\_us/article/8899nz/nso-group-pitched-phone-hacking-tech-american-police](https://www.vice.com/en_us/article/8899nz/nso-group-pitched-phone-hacking-tech-american-police)  
[https://www.vice.com/en\\_us/article/n7wna7/lapd-phone-hacking-nso-group-westbridge](https://www.vice.com/en_us/article/n7wna7/lapd-phone-hacking-nso-group-westbridge)  
<https://thehackernews.com/2020/04/iphone-zero-day-exploit.html>  
<https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers>  
<https://thehackernews.com/2020/03/iphone-iOS-spyware.html>  
<https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2>  
<https://www.zdnet.com/article/stalkerware-infections-grew-by-40-in-2019-says-kaspersky/>  
<https://www.cnet.com/news/how-schools-may-use-kids-phones-to-track-and-surveil-them/>  
<https://techcrunch.com/2020/02/20/kidsguard-remove-stalkerware/>  
<https://techcrunch.com/2020/02/20/kidsguard-spyware-app-phones/>  
<https://blog.malwarebytes.com/stalkerware/2020/03/international-womens-day-awareness-of-stalkerware-monitoring-and-spyware-apps-on-the-rise/>  
<https://medium.com/@nickkshepard/the-continued-rise-of-stalkerware-eba471d851a4>  
<https://www.cnet.com/news/1-in-10-people-uses-stalkerware-to-track-partners-and-exes-poll-says/>  
<https://www.cnet.com/news/stalkerware-what-to-know-when-youre-the-target/>  
<https://threatpost.com/stalkerware-extra-creepy-features/153874/>  
<https://securityaffairs.co/wordpress/96295/malware/joker-malware-activity.html>  
<https://securityaffairs.co/wordpress/98279/malware/joker-malware-play-store.html>  
<https://www.techradar.com/news/stalkerware-poses-higher-privacy-risk-than-ever-heres-what-you-need-to-know>  
<https://www.refinery29.com/en-us/spyware-stalkerware-dangers>  
<https://wfhb.org/news/better-beware-stalkerware/>  
<https://blog.avast.com/the-stalkerware-threat-avast>  
<https://eandt.theiet.org/content/articles/2020/03/lurking-in-the-shadows-the-disturbing-rise-of-stalkerware/>  
<https://vpnoverview.com/news/monitoring-new-super-stalkerware/>  
<https://www.infosecurity-magazine.com/news/stalkerware-soared-91-in-uk-last/>  
<https://www.securityweek.com/rare-android-stalkerware-can-steal-data-control-devices>  
<https://the-parallax.com/2020/02/18/stopping-stalkerware-confounds-experts/>

## RESEARCH

- <https://the-parallax.com/2020/02/18/stopping-stalkerware-confounds-experts/>
- <https://www.techdirt.com/articles/20200220/14571543957/stalkerware-developer-found-leaking-sensitive-data-thousands-software-victims.shtml>
- <https://www.pcmag.com/news/ftc-blocks-us-company-from-selling-stalkerware-apps>
- <https://www.usenix.org/conference/enigma2020/presentation/galperin>
- <https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/>
- <https://www.nytimes.com/2020/01/22/technology/jeff-bezos-hack-iphone.html>
- <https://www.reuters.com/article/us-davos-meeting-saudi-arabia/saudi-foreign-minister-calls-claim-that-crown-prince-hacked-bezos-phone-absurd-idUSKBN1ZL1ED>