

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

Hi, I'm Xena



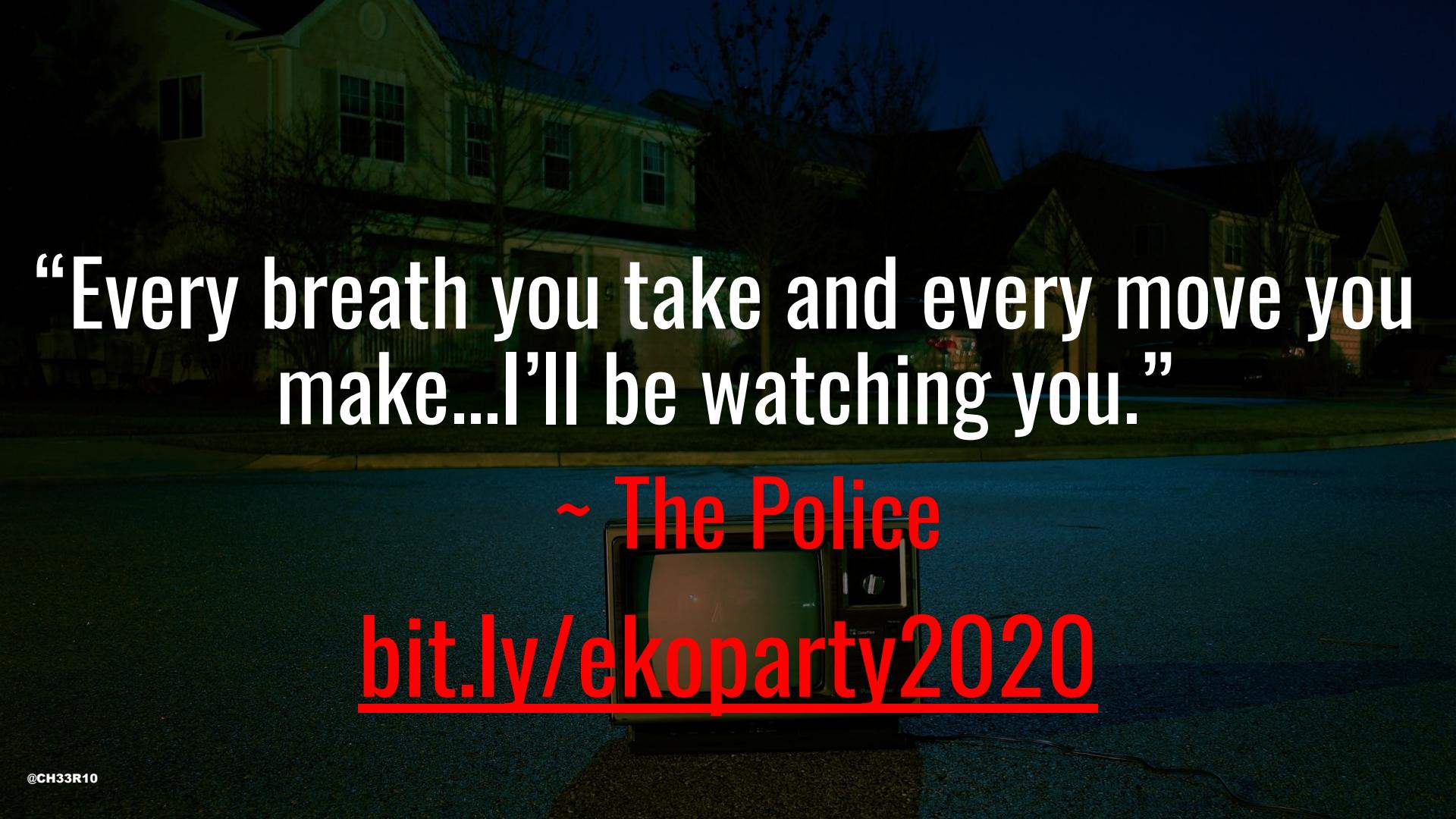
MARYMOUNT
UNIVERSITY

bit.ly/ekoparty2020

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.”

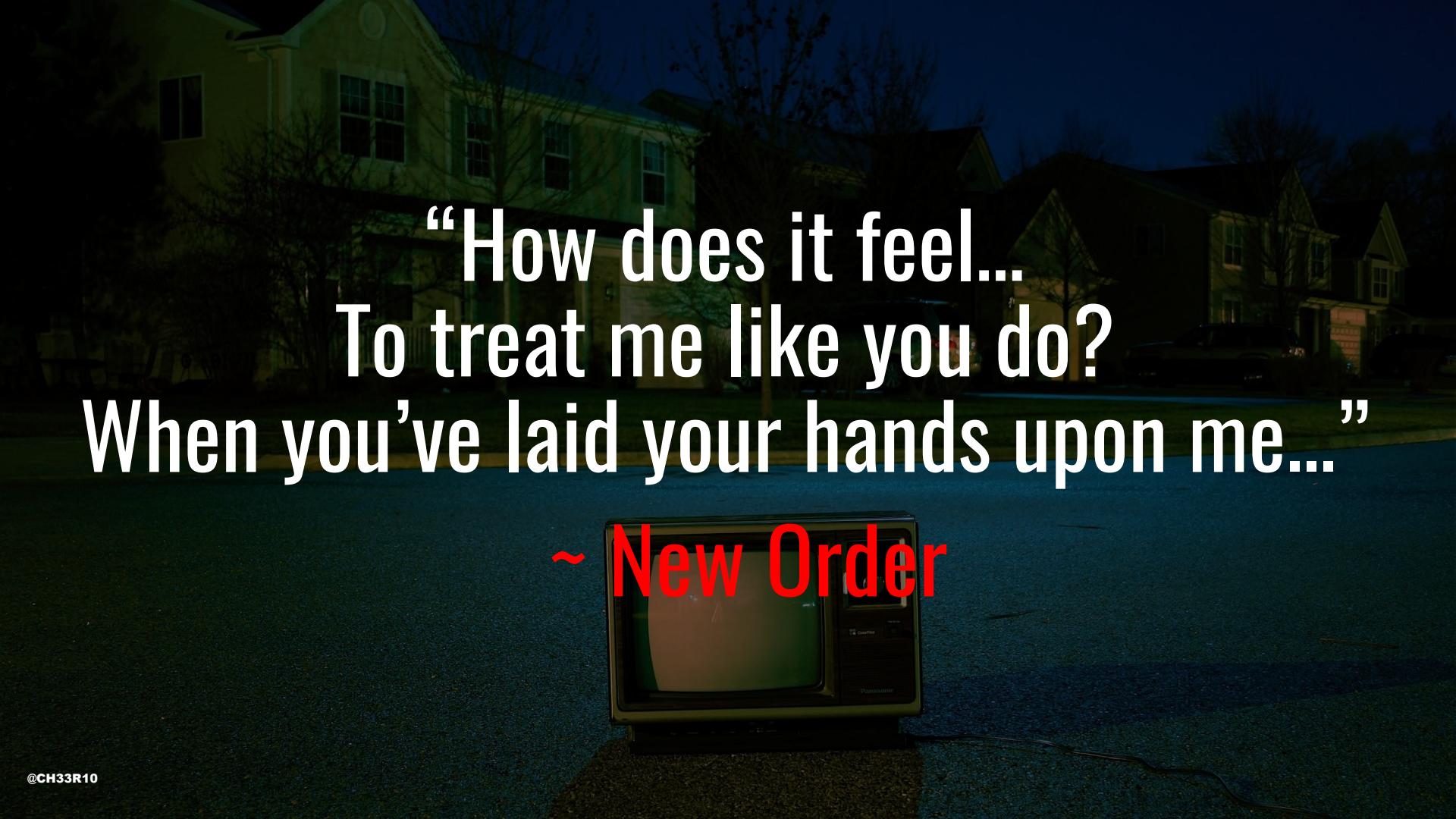
@Ch33r10



“Every breath you take and every move you
make...I'll be watching you.”

~ The Police

bit.ly/ekoparty2020



“How does it feel...
To treat me like you do?
When you've laid your hands upon me...”

~ New Order

STALKERWARE

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

@Ch33r10

STALKERWARE

WHAT IS IT?

@Ch33r10

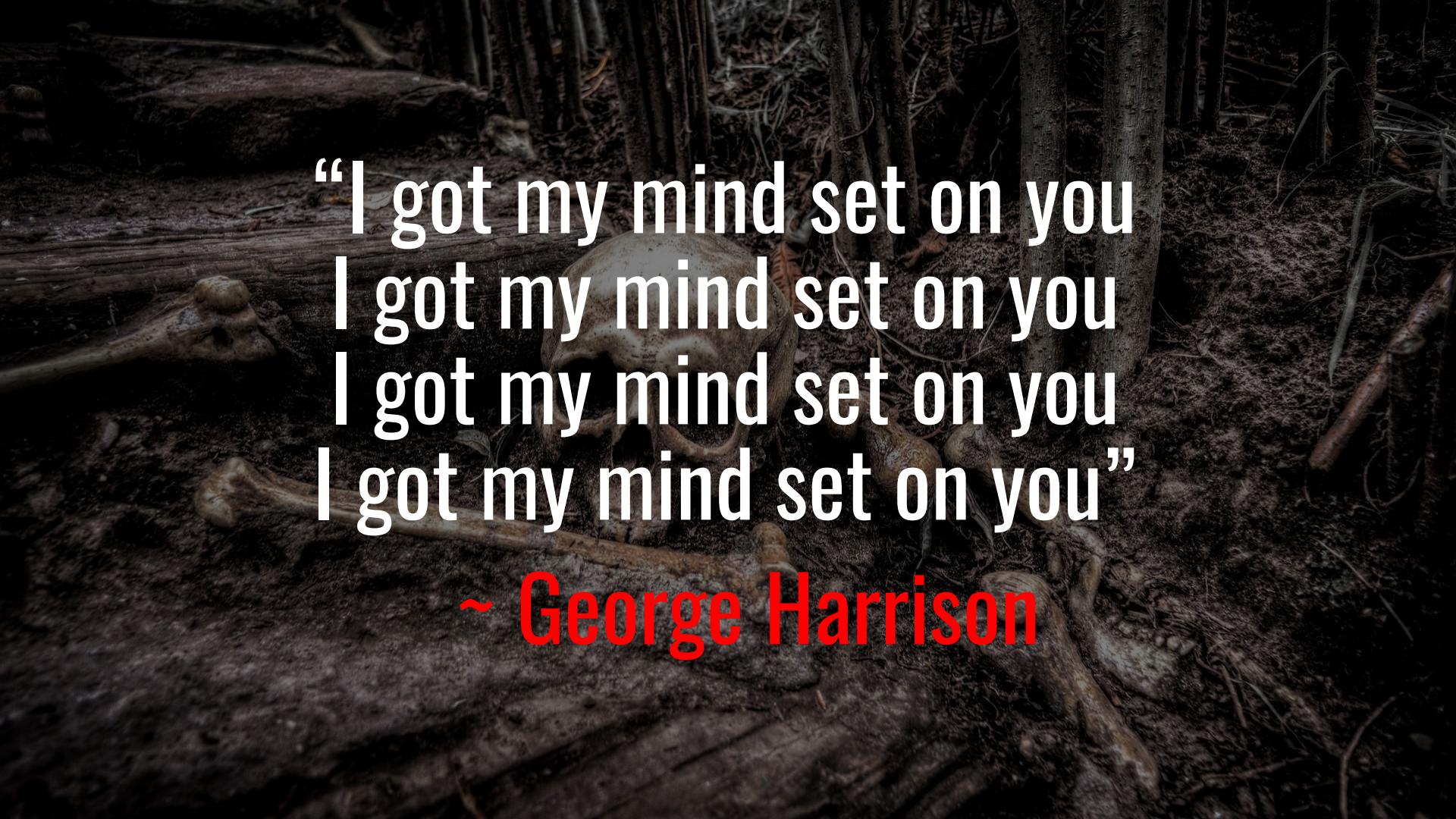
TOP SECRET

STALKERWARE



SPY

@Ch33r10



“I got my mind set on you
I got my mind set on you
I got my mind set on you
I got my mind set on you”

~ George Harrison

INTIMATE PARTNER SURVEILLANCE TOOLS

COMMODITY STALKERWARE

BASIC
Active &
Passive
Data Collection



TARGET

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

STALKERWARE

Mobistealth

mSpy

FlexiSpy

Highster Mobile

Hoverwatch

Spyzie

TheTruthSpy

TeenSafe

Cerberus

Xnspy

WebWatcher

& More!!!

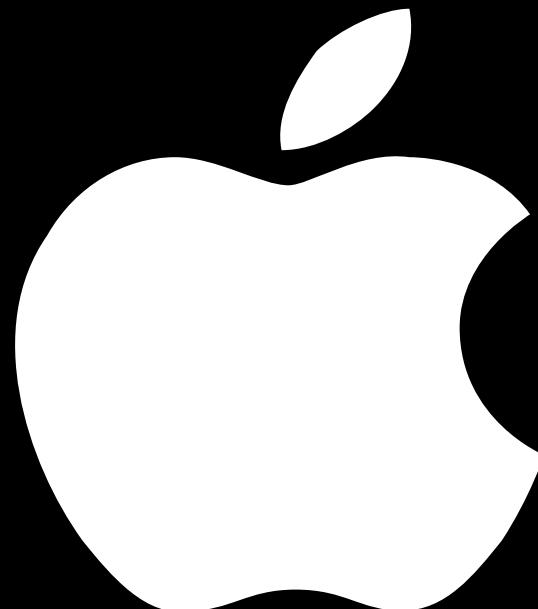
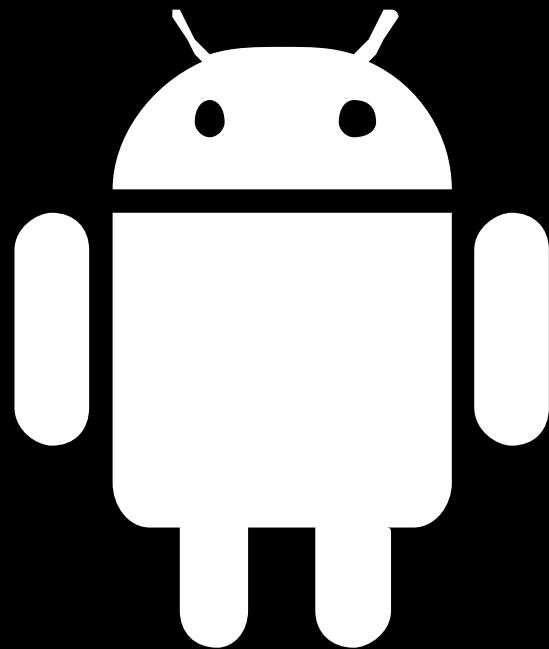
STALKERWARE

HOW DOES IT WORK?

@Ch33r10

COMMODITY

STALKERWARE



RWDEICA

LHM KILL CHAIN

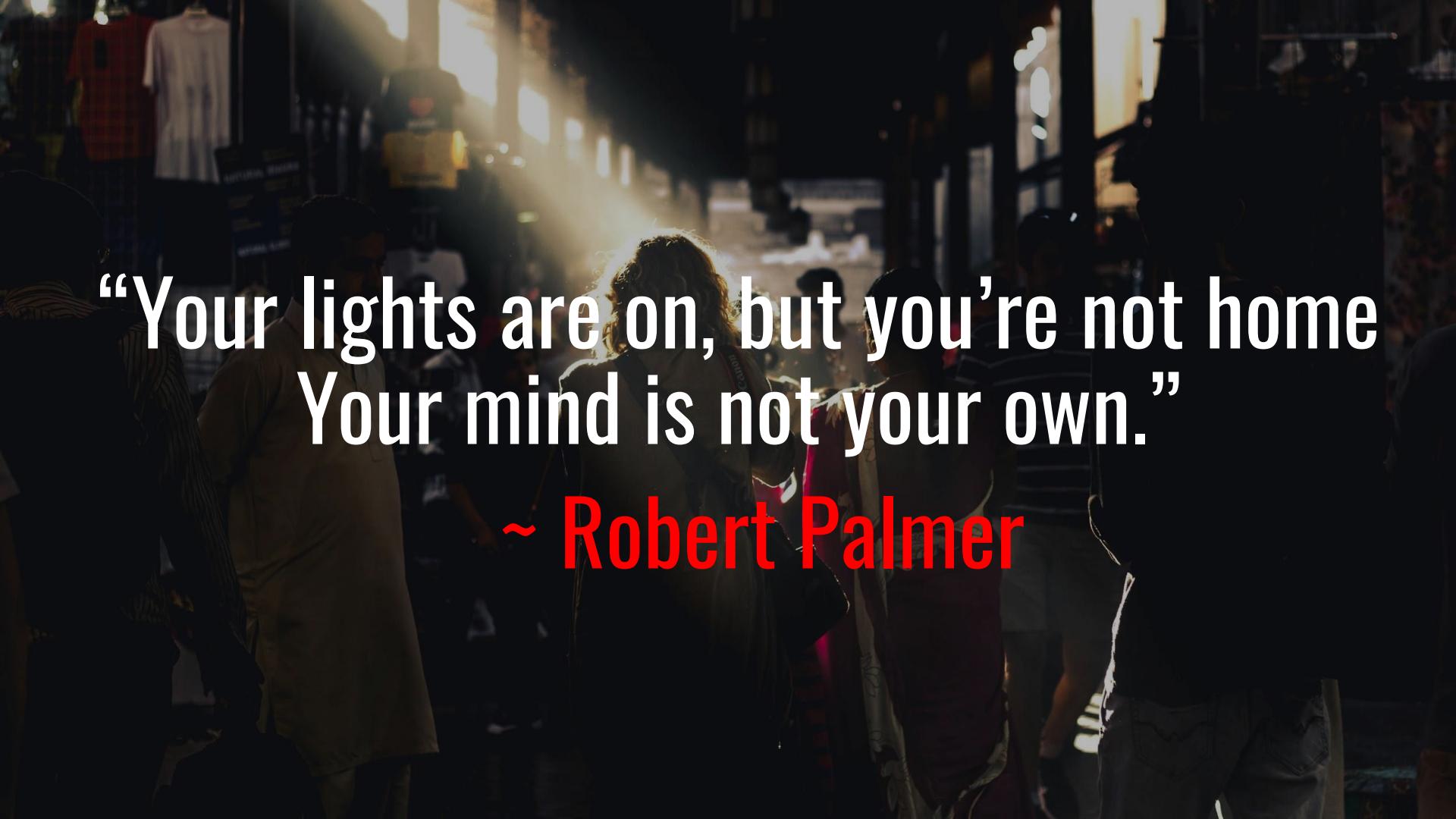
COMMODITY STALKERWARE





“This TAINED LOVE you've given.”

~ Soft Cell

A dark, grainy photograph of a crowded street at night. Bright lights from shop windows and street lamps create a hazy glow in the background, while the foreground is filled with the silhouettes and shapes of many people.

“Your lights are on, but you’re not home
Your mind is not your own.”

~ Robert Palmer

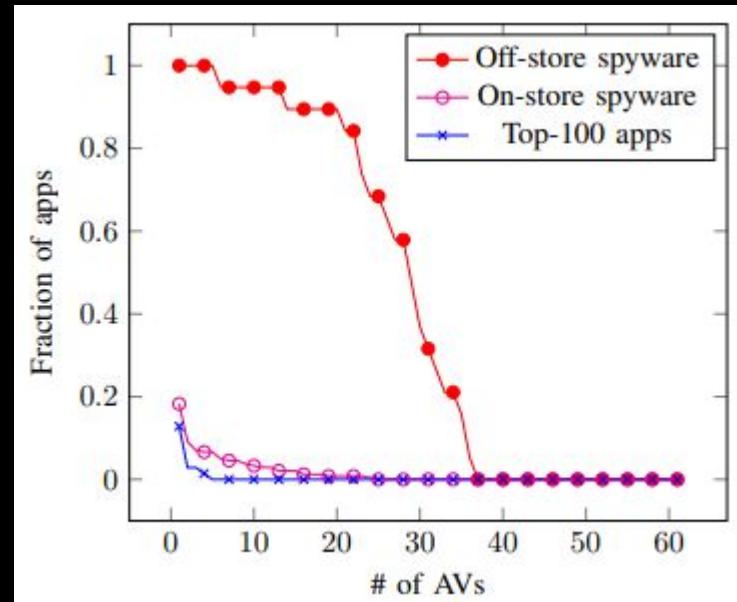
MITRE ATT&CK

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%
					MEAN 22.1%

Table 6: Overall Antivirus Detection of Stalkerware Applications



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



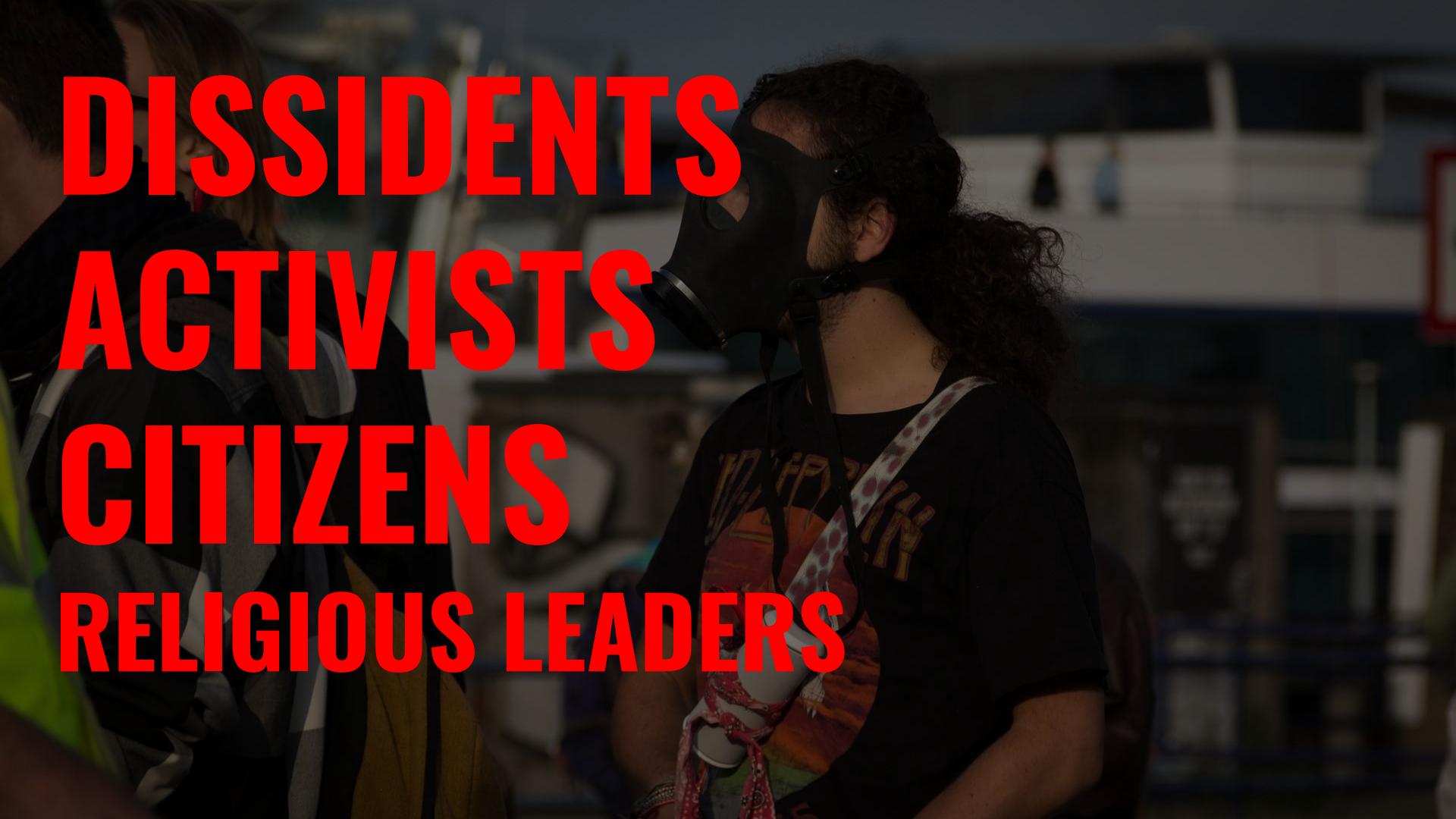
Targeted by
Saudi
Gov-linked
Operator



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

CITIZEN LAB 2020

**DISSIDENTS
ACTIVISTS
CITIZENS
RELIGIOUS LEADERS**



CRIMINALS

@Ch33r10

TERRORISTS



@Ch33r10

A black and white photograph of a military operation in a desert. In the foreground, several soldiers in camouflage uniforms and helmets are running across sand dunes. One soldier on the right is prominently featured, carrying a rifle and looking back over his shoulder. In the background, more soldiers are visible, some sitting on the ground and others standing in groups. The terrain is sandy and appears to be a coastal or island setting.

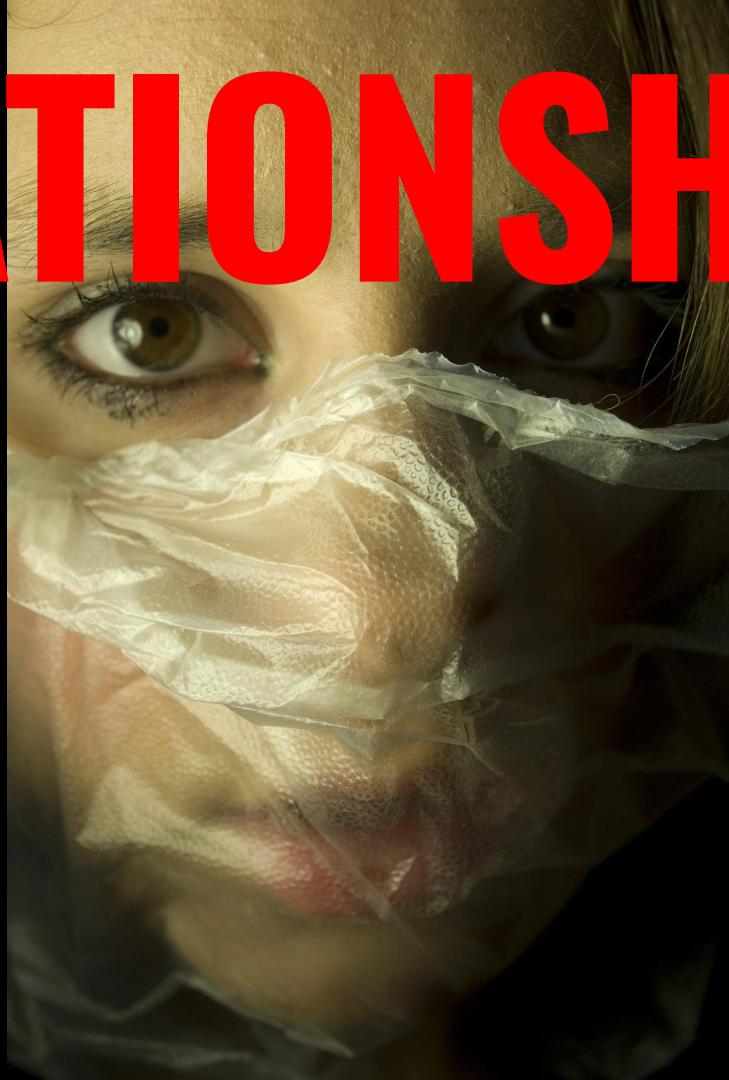
**MILITARY
GOVERNMENTS
GOV OFFICIALS
LAW ENFORCEMENT**

STALKERWARE

OPERATORS

@Ch33r10

RELATIONSHIPS



@Ch33r10

STALKERWARE VENDOR BREACHES



**SIMILAR SURVEILLANCE
CAPABILITIES AS STALKERWARE**

OPERATORS

@Ch33r10



PARENTS SCHOOLS

@Ch33r10

COMPANIES

@Ch33r10

CYBERCRIME HACKTIVISTS



@Ch33r10

CRIMINALS TERRORISTS

@Ch33r10

LAW ENFORCEMENT



NATION-STATE



STALKERWARE

HOSTILE ACTOR TRADECRAFT

@Ch33r10

KIMBER



SUKI WYNN



ELECTRA



POISON HYDRA



STALKERWARE

CTI HYPOTHESES

**NORMAL USE OF
COMMODITY STALKERWARE**



RTFM

CORPORATE AMERICA

@Ch33r10

CORPORATE MOBILE DEVICE MANAGEMENT/ BYOD

@Ch33r10

CORPORATE STALKERWARE VENDORS



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



ARGENTINA & DOMESTIC VIOLENCE

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

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 ⁹⁰	United States	Cloudflare, Inc.	13335
FlexiSPY	community.flexispy.com	104.25.92.115	United States	Cloudflare, Inc.	13335

CORPORATE

TABLE TOP

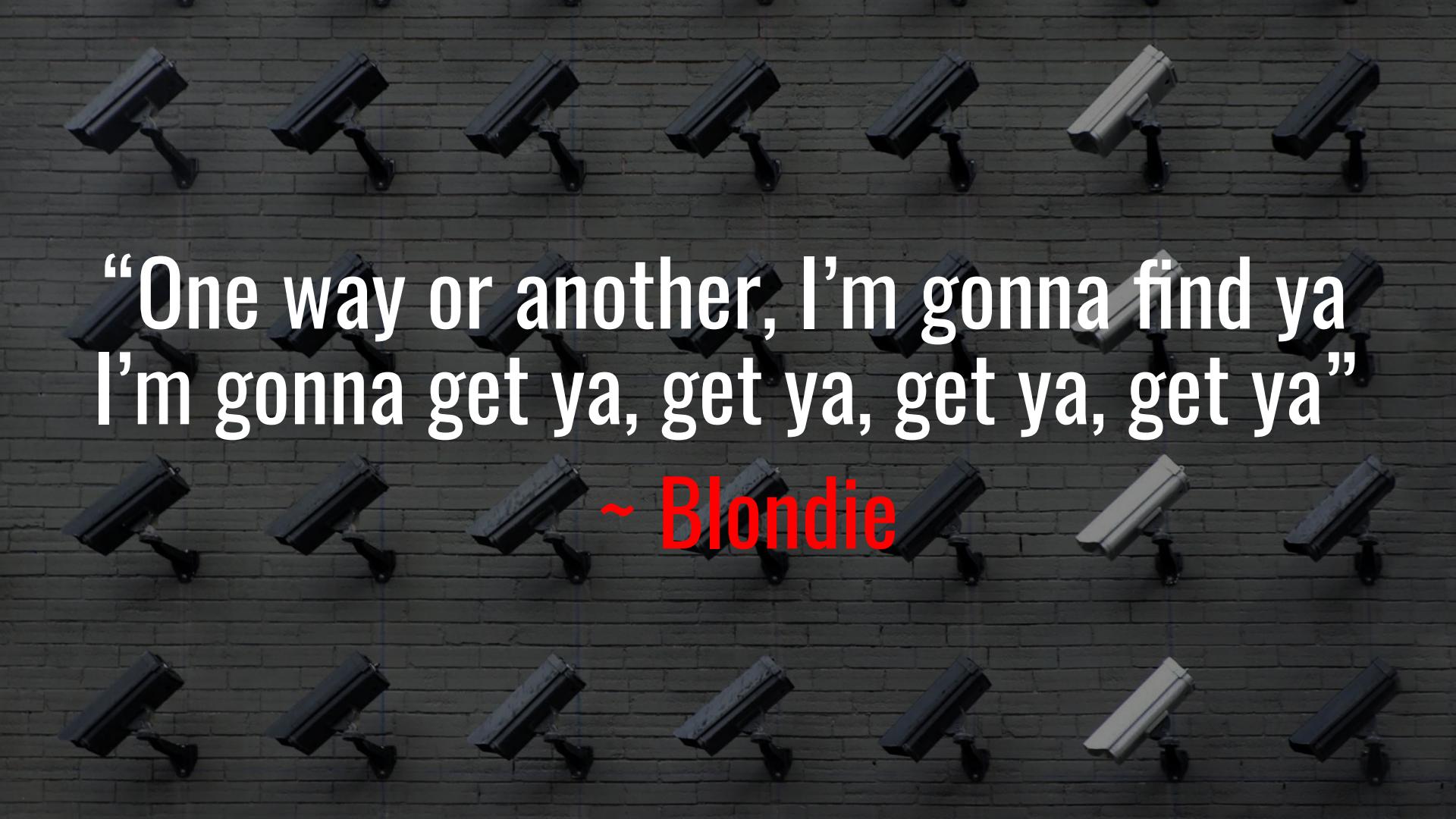


AWAWARENESS

A close-up photograph of a woman's face. She has dark hair and is looking directly at the camera with a neutral expression. Her eyes are brown. A large, bold, red text "AWAWARENESS" is overlaid across the upper portion of her face. The background is dark and out of focus.

RESOURCES

A dramatic, high-contrast photograph of a person lying face down on a dark surface covered in shards of broken glass. The person's head is turned to the side, showing a profile view of their face. The shards are sharp and jagged, reflecting light in a way that highlights their edges against the dark background. A large, solid red rectangular shape is overlaid on the upper left portion of the image, partially obscuring the scene below.



“One way or another, I’m gonna find ya
I’m gonna get ya, get ya, get ya, get ya”

~ Blondie

A black and white photograph of a dense forest. The scene is filled with tall, thin trees, their trunks reaching upwards towards a bright sky. In the foreground, several fallen tree trunks and branches are scattered across the ground, creating a sense of natural decay and movement. The lighting is dramatic, with strong highlights and shadows that emphasize the textures of the bark and the intricate patterns of the fallen logs.

**AND ONE MORE
THING...**

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 Size | 2020-06-08 17:37:53 UTC 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 ⁹⁰	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. At the top, a circular progress bar indicates 23 engines have detected the file, with 63 total. Below this, the file's SHA256 hash is listed as 49a4380a485809122953354e2d3ddb056e15c3386396fc07dab482c521fc1af1. The file size is 4.90 MB and it was uploaded on 2020-05-23 23:19:40 UTC, 18 days ago. The file is identified as MSpyAndroidApp-v5.6.0-555.apk and is categorized as an APK file containing ELF code.

DETECTION **DETAILS** **RELATIONS** **BEHAVIOR** **COMMUNITY**

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.

ESPIAR A MI ESPOSA



GOOGLE



"espiar a mi esposa"

All Videos News Images Maps More Settings

About 126,000 results (0.41 seconds)

[tipdiario.com > como-puedo-espiar-a... ▾ Translate this page](#)
Como puedo espiar a mi pareja desde su Celular - Tip Diario
Quiero **espiar a mi esposa**. Responder. Patricia Tapia. 19 mayo, 2016 a las 7:10 am. Yo ya compro dos aplicasiones para espiar mi marido page me estafaron ...

[whatsappespiaapp.com > Blog ▾ Translate this page](#)
Aplicación para Espiar el WhatsApp de mi Pareja
Cómo hago para **espiar a mi esposa** por wasap. Responder. Sergio. febrero 7, 2020 a las 9:10 am. Neseccito saber si mnesetito saver alludamee engaña.

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 - Incognito 	 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 Learn More
Interactive Elements	In-app Products	Permissions
Users Interact, Shares Location	\$9.49 per item	View details
Report	Offered By	Developer
Flag as inappropriate	Family Locator Inc.	Visit website devteam@onelocator.com Privacy Policy 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

@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 String[] auth_providers = {"com.cocospy.account.auth_provider", "com.mingspy.account.auth_provider", "com.spylne.account.auth_provider"};  
    public static String[] auth_types = {"com.cocospy.account.auth_type", "com.mingspy.account.auth_type", "com.spylne.account.auth_type"};  
  
    public static String getBaseUrl(String provider) {  
        if ("spyier".equals(provider)) {  
            baseUrl = "https://i.spyier.com/api/";  
            account_auth_type = "com.spyier.account_auth_type";  
            account_auth_provider = "com.spyier.account.auth_provider";  
        }  
        if ("mingspy".equals(provider)) {  
            baseUrl = "https://i.mingspy.com/api/";  
            account_auth_type = "com.mingspy.account.auth_type";  
            account_auth_provider = "com.mingspy.account.auth_provider";  
        }  
        if ("spylne".equals(provider)) {  
            baseUrl = "https://i.spylne.com/api/";  
            account_auth_type = "com.spylne.account.auth_type";  
            account_auth_provider = "com.spylne.account.auth_provider";  
        }  
        return baseUrl;  
    }  
}
```

3 10 16



SECURITY RESEARCHERS

@MALWRHUNTERTEAM

Search: @malwrhunterteam apk

Top Latest People Photos Videos

MalwareHunterTeam @malwrhunterteam · 2h
Not much detected "20BGift.apk":
5386abd90497dc0b97537ae585addfa1772b10cd4353e41b413e90eb07a145f
e
From: [https://20gbcampings\[.\]com/](https://20gbcampings[.]com/) ->
[https://20gbcampings\[.\]com/APK/20BGift.apk](https://20gbcampings[.]com/APK/20BGift.apk)
cc @JAMESWT_MHT @douglasmun

Certificate Attributes
Valid From: 2020-02-29 01:33:44
Valid To: 2026-01-17 01:33:44
Subject: CN=Android, O=Android, ST=California, C=US, email=admin@android.com
Common Name: admin@android.com
Organization: Android
Organizational Unit: Android
Locality: Mountain View
City: Mountain View
State: California
Country: US
Trojan (0x505f1)

Android.PUA.Debug



SECURITY RESEARCHERS

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

 **URL CATEGORY**

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:AR

**androguard:"android.permission.
ACCESS_COARSE_LOCATION"**

**androguard:"android.permission.
CAMERA"**

**androguard:"android.permission.
READ_SMS" p:2+**

FILES 10

FE3E2DE30BC18503B8CC37BBD8173AFAE4D23BDF3842C1CAE3C81BD..

com.metasploit.stage

android cve-2012-4681 exploit apk

353E623E1E207CA819C48689AA81C2A7849EE479D96D890ED1BB078..

com.metasploit.stage

android cve-2012-4681 exploit apk

557A5E486F10100A1AD6511B5F378F2E8FD0FE32789771CA59059D2..

com.metasploit.stage

android cve-2012-4681 exploit apk reflection
runtime-modules checks-gps

F74BA467FA1E5D8A39AAEA0BC623CF64AD74B4CB0E713E80A913A..

com.metasploit.stage

android cve-2012-4681 exploit apk

2186A0A0FC657CF2A73260A17B85ED67A1D3B8E889E19C4811F448E..

com.metasploit.stage

android cve-2012-4681 exploit apk

325BC1C9E23EFEE5608825975A835DF136BF3626B574BC697F90..

com.metasploit.stage

android cve-2012-4681 exploit apk

⚠ 90 DAYS

Detections

27 / 62

25 / 60

27 / 61

25 / 62

28 / 63

26 / 62



VIRUSTOTAL SEARCH

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

**androguard:"android.permission.
ACCESS_COARSE_LOCATION"**

**androguard:"android.permission.
CAMERA"**

**androguard:"android.permission.
READ_SMS" p:2+**

FILES 20 / 22.39 K

⚠ 90 DAYS

Detections

387CF29B24A797437C3579803310685E0774C39DA3E204D8061F373...

mtlibkvhonenvfqnksxmjzmr.mvscusqjoerns

android reflection telephony apk password-dialog persistence

29 / 62

34A4CEE6EBAF9115DAC2F2C79CB62FAA868EF58CB3E3DF5D6BF4261...

com.metasploit.stage

android apk exploit cve-2012-4681

34 / 61

C8CCAF384B9422A1EA003442DA6A8C2E4FC6CD41ECCE84E7DCBF10F...

com.metasploit.stage

android reflection runtime-modules apk exploit cve-2012-4681

27 / 62

9FAA55106E0D312A29F3387B5DC8604CC4559915F638C8E7CEAF4EE...

package.kivi.kive

android apk

14 / 59

EF1A8D04AB2F023849A66531BCEFE6933CA1C3726D86D61C80C8A2C...

package.kivi.kive

android apk

21 / 61

773C4E2A3475F23B21237DFC3B920F7CD130169B19A11EE083D38D0...

com.metasploit.stage

android cve-2012-4681 exploit apk

27 / 62



VIRUSTOTAL SEARCH

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

FILES 47

FA9A86002499450394F8FE7988E57A8107E3EC2798CB0F9A146F3D2CF3...

com.confidential.pottery

@ android apk

13 / 61

A21EB145CE4CCE9389B447D04255BB235A51F6A98C85F97A8017CFB83840...

com.confidential.pottery

@ android apk

17 / 62

FE3E2DE30BC18503BBC37BB08173AFAE4D023BDF3842C1CAE3C81BDAC48...

com.metasploit.stage

@ android cve-2012-4681 exploit apk

27 / 62

0C42DBD0C00C82F142E5772FC35BDC1E8AF732BA02535A3A08A03A36F01...

com.cold.toothbrush

@ android apk

22 / 62

E221F87F13777F4AFA3909E63E0E004C5CF4473202229AB9BF7053BEF67...

com.forshared

@ android checks-gps reflection apk runtime-modules
contains-elf telephony @

22 / 62

submitter:AR tag:android tag:apk
androguard:"android.permission.ACCESS_COARSE_LOCATION"
androguard:"android.permission.ACCESS_FINE_LOCATION"
androguard:"android.permission.INTERNET"
androguard:"android.permission.WRITE_EXTERNAL_STORAGE" p:13+

**VIRUSTOTAL SEARCH**

Permissions

- ⚠ android.permission.BLUETOOTH
- ⚠ android.permission.CALL_PHONE
- ⚠ android.permission.CHANGE_WIFI_STATE
- ⚠ android.permission.GET_TASKS
- ⚠ android.permission.INTERNET
- ⚠ android.permission.PROCESS_OUTGOING_CALLS
- ⚠ android.permission.READ_PHONE_STATE
- ⚠ android.permission.READ_SMS
- ⚠ android.permission.SEND_SMS
- ⚠ android.permission.SYSTEM_ALERT_WINDOW

androguard:"android.permission.
READ_SMS" p:13+

FILES 20 / 254.45 K

⚠ 90 DAYS

DC8BC090A61B97A1BA425C96E7C2B474725549FF949E2C98D17E2C0...

com.skymobi.pay.opplugin

android apk contains-elf

9E02EA3631CE00866F326E735B3FDAFFD308E1A2A87848921A59CAD...

Izjqfcndiw.sgtiankwenpmopfydeyjbqfrcg.isdwcalgbobkezflirtyororp

android apk

EB9DD35E364D7DDAC6AD9F50EE0043B983EBA70832A9183972E08A7...

com.resestudio.jewelcastle.jewelslegend

android telephony reflection apk

666F4D9A4036AD2A48E93C3E3B8DFAD28E1930A35670C85F9683EC6...

fzok.eu.qg

android apk

293F0B74EE3BFEC3CEB7DD9A50F341F2F6654F38F7BAF0E30DF3EFA...

vnkoipse.qlkilser.view

android apk telephony

C6DBEF0E4A3248CF1FEE702509541C4C1AEBA66B175AD2256B9907...

wersdfau.xretyuiuo.view

android telephony apk



VIRUSTOTAL SEARCH

! 29 engines detected this file

387cf29b24a797437c35798d3310685e0774
c39da3e204d8061f373216467b01

5044F13193953CE9681BCE750ECCAF6C.apk

1016.15 KB
Size

2020-09-17 03:05:52 UTC
1 hour ago

Community Score: 29 / 62

Tags: android, apk, password-dialog, persistence, reflection, telephony

Porn hub APK

main_icon_dhash:a6ccd2d8d0d4
ccd0 p:5+

FILES 575	90 DAYS
387cf29b24a797437c35798d3310685e0774... mnlbkvho.nevfqhnksxmijzmr.mvscusqjsjoerns android reflection telephony apk password-dialog persistence	29 / 62
D407822fb74cd488a6d8e8cb58b6519ac8d6522fa38eb7920545... egirkyfvuygvujhjcqlxqanbou.sxsgdksm android apk	17 / 61
371503a905aa6339fA6a28EDCD64268AAFA405C1850A1937692FAB5... indghfd.zffsllmicpvurqyk.mhwutlfryw android telephony reflection apk	21 / 62
05697a71825660682c3e59c983a48eE3948B6f03f6a621103c8a04f... bvbthnhm.rajihsuwzhfamihxotkf.gpmnljbi android telephony reflection apk	17 / 61
15488440E3CC8855C2C47062A18797385FB6078EE1318D687CA8E5... drisksxwm.jquepmfiszqwkkoqx.poolivcszuflom android apk reflection telephony	19 / 60
F4BA1981F6CA21D377E57B6A1B06AA2133BF97D00354BA954EACDE... sjtpwtb.pgztspdytxbr.mwpvlyglj android apk reflection telephony	22 / 62



VIRUSTOTAL SEARCH

EKOPARTY 2020 SPEAKERS



XENA OLSEN

"Every Breath You Take: A CTI Review of Stalkerware"



EVERY BREATH YOU TAKE: A CTI REVIEW OF STALKERWARE

[EKOPARTY 2020 Spotify Playlist](#)

Learn why stalkerware is an emerging threat to Enterprise & how it can lead to a breach. Poor AV detection combined with the stigma attached to stalkerware makes it a great tool to exfil data, steal credentials, breachstortion, & more!

Reverse engineer Android APKs & use OSINT to hunt stalkerware.

TYPE	INDICATOR	DESCRIPTION	CONTRIBUTOR
domain	account.refog.com	stalkerware	@ch33r10
domain	alltracker.org	stalkerware	@ch33r10
domain	appmia.com	stalkerware	@ch33r10
domain	calltruth.com	stalkerware	@ch33r10
domain	cellmonitoring.net	stalkerware	@ch33r10
domain	celctrackingapps.com	stalkerware	@ch33r10
domain	famisafe.wondershare.jp	stalkerware	@ch33r10
domain	hellospy.com	stalkerware	@ch33r10
domain	highstermobile.com	stalkerware	@ch33r10
domain	hoverwatch.com	stalkerware	@ch33r10
domain	keymonitor.com	stalkerware	@ch33r10
domain	letmespy.com	stalkerware	@ch33r10
domain	mobiespy.com	stalkerware	@ch33r10
domain	mobile-spy.com	stalkerware	@ch33r10
domain	mobisp.net	stalkerware	@ch33r10
domain	mobistealth.com	stalkerware	@ch33r10
domain	mspy.com	stalkerware	@ch33r10
domain	onelocator.com	stalkerware	@ch33r10
domain	onexsoftech.com	stalkerware	@ch33r10
domain	prospybubble.com	stalkerware	@ch33r10
domain	protocol-a.thetruthspyc.com	stalkerware	@ch33r10
domain	protocol-a732.thetruthspyc.com	stalkerware	@ch33r10
domain	spappmonitoring.com	stalkerware	@ch33r10
domain	spfone.com	stalkerware	@ch33r10
domain	spymasterpro.com	stalkerware	@ch33r10
domain	theonespy.com	stalkerware	@ch33r10
domain	xospy.com	stalkerware	@ch33r10

EKOPARTY #PWNDEMIC 2020

THREAT SUMMARY REPORT

STALKERWARE

09/26/20

SUMMARY

On September 26th, 2020, a presentation, "Every Breath You Take: A CTI Review of Stalkerware," at EKoparty 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, keystroke, 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

 bit.ly/ekoparty2020

THANK YOU <3

 **bit.ly/ekoparty2020**