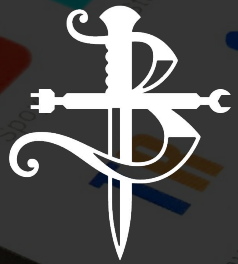

EVERY BREATH
YOU TAKE
A CTI REVIEW OF STALKERWARE
@Ch33r10
*not speaking on behalf of my employers

Hi, I'm Xena



MARYMOUNT
UNIVERSITY

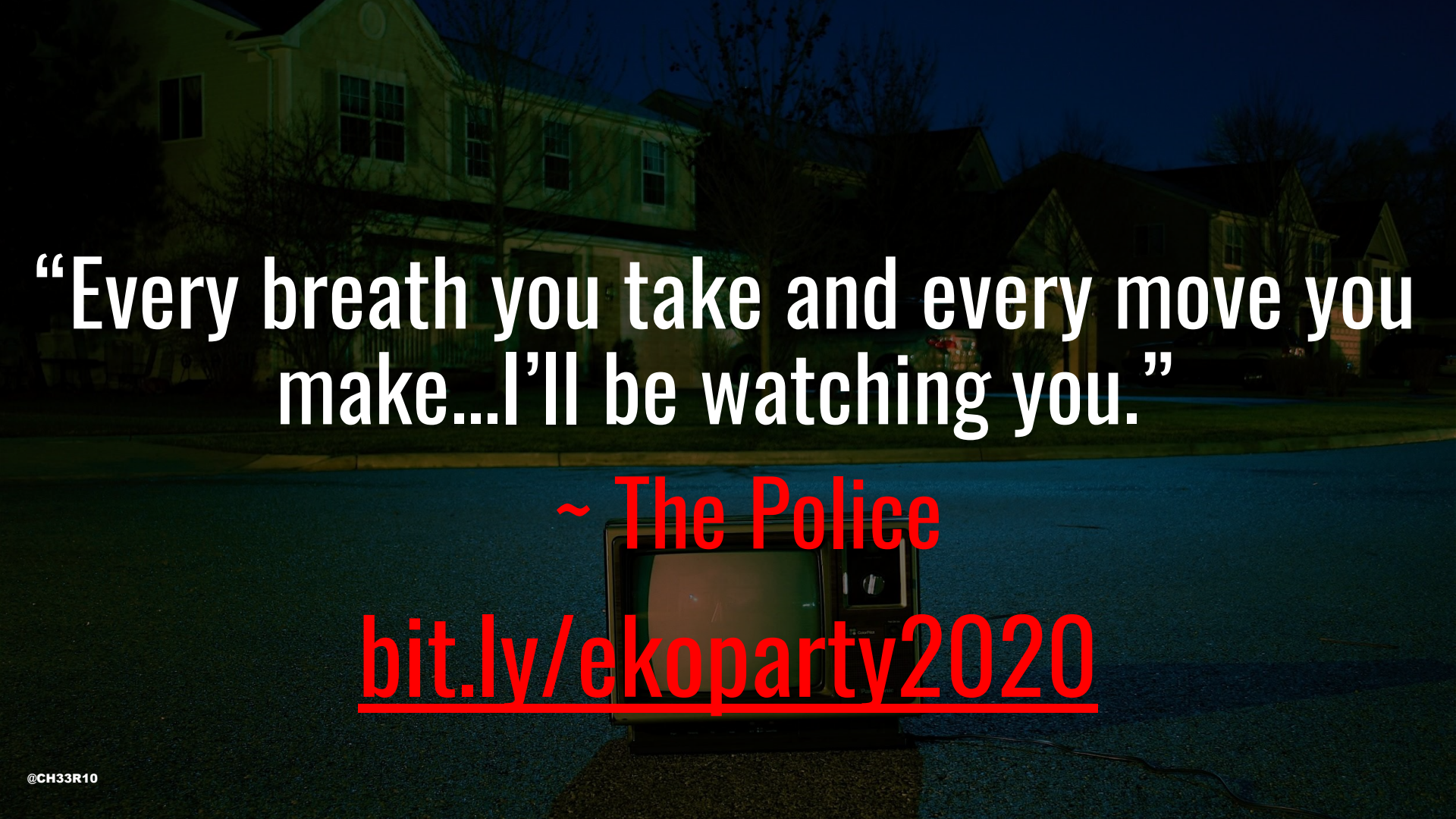
bit.ly/ekoparty2020

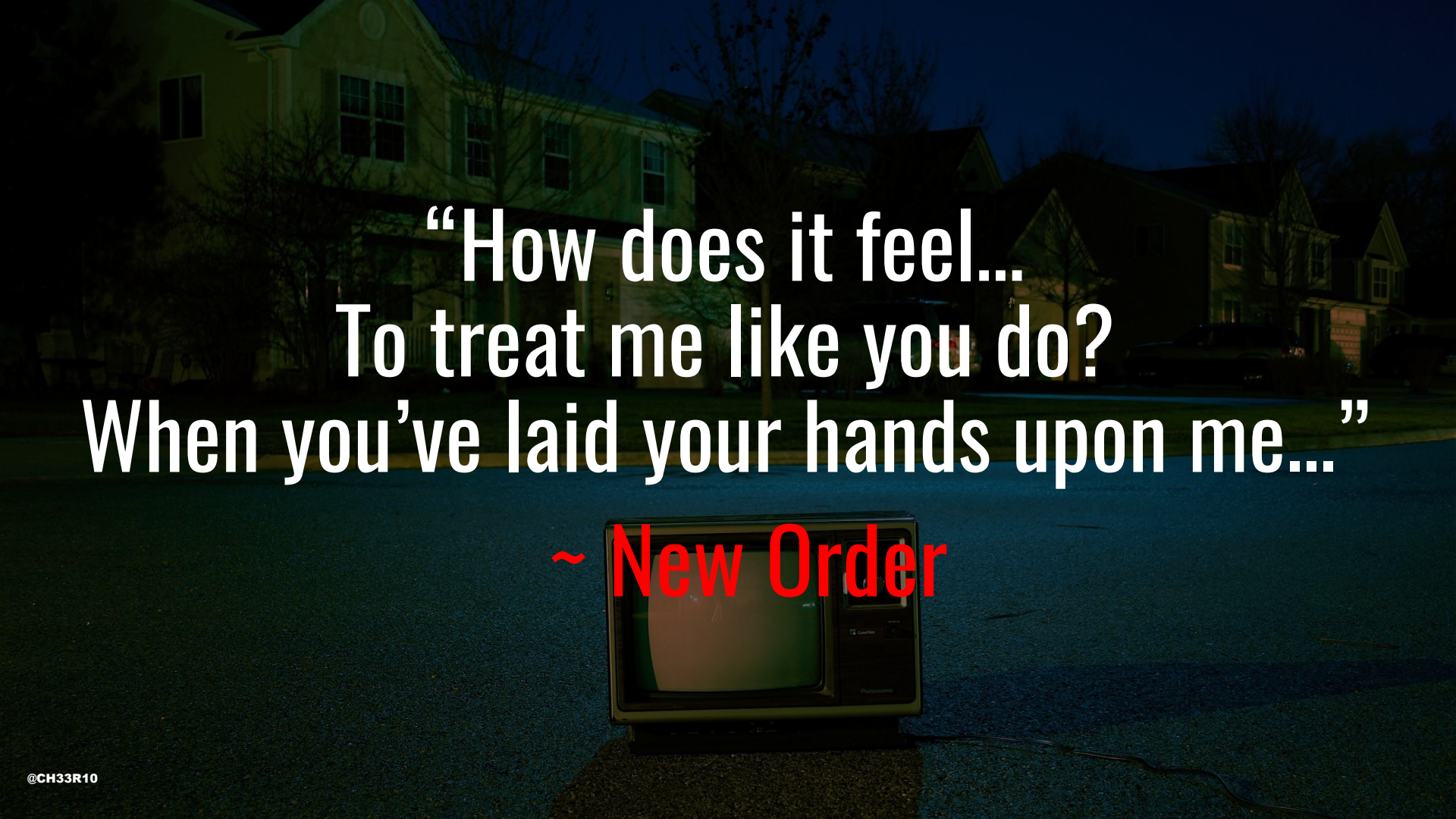
@CH33R10

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
@CH33R10


“How does it feel...
To treat me like you do?
When you’ve laid your hands upon me...”
~ New Order
@CH33R10

STALKERWARE

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

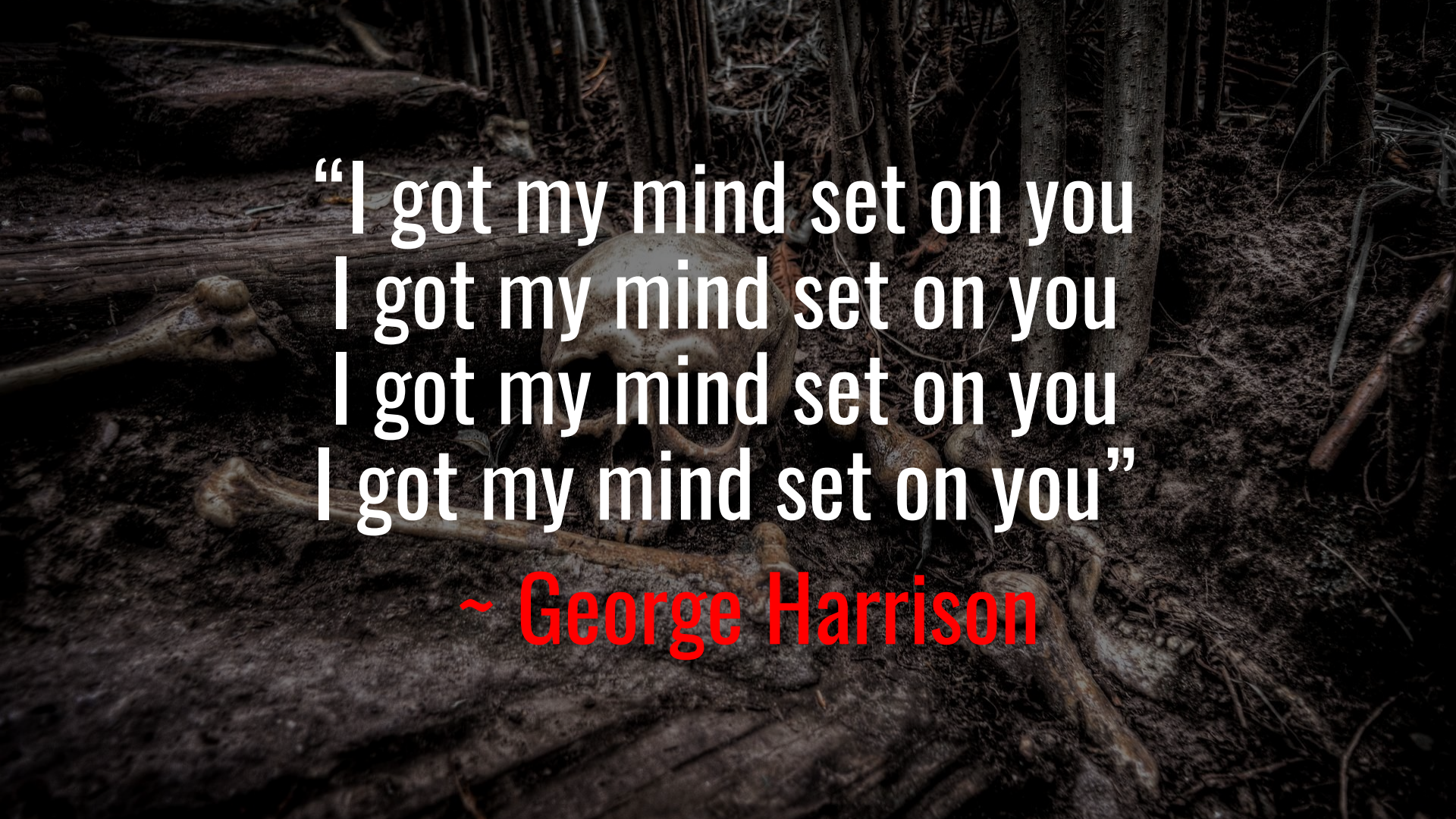
@Ch33r10

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
25

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

THE CITIZEN LAB | THE PREDATOR IN YOUR POCKET P 20 https://citizenlab.ca/docs/stalkerware-holistic.pdf

STALKERWARE

Mobistealth
mSpy
FlexiSpy
Highster Mobile
Hoverwatch
Spyzie
TheTruthSpy
TeenSafe
Cerberus
Xnspy
WebWatcher
& More!!!

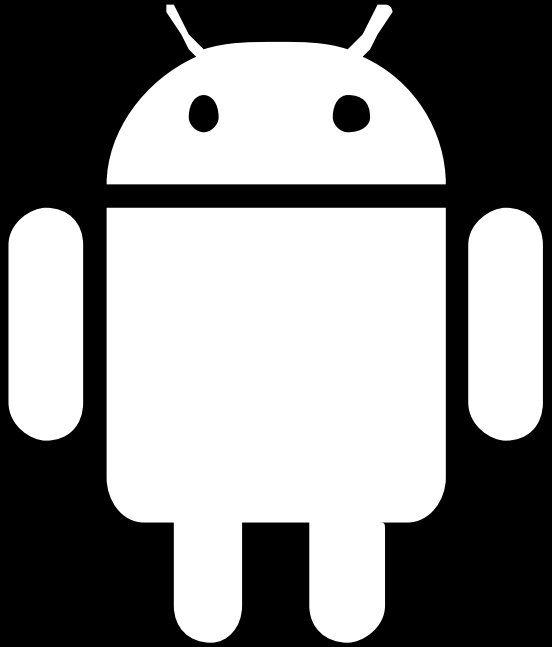
STALKERWARE

HOW DOES IT WORK?

@Ch33r10

COMMODITY

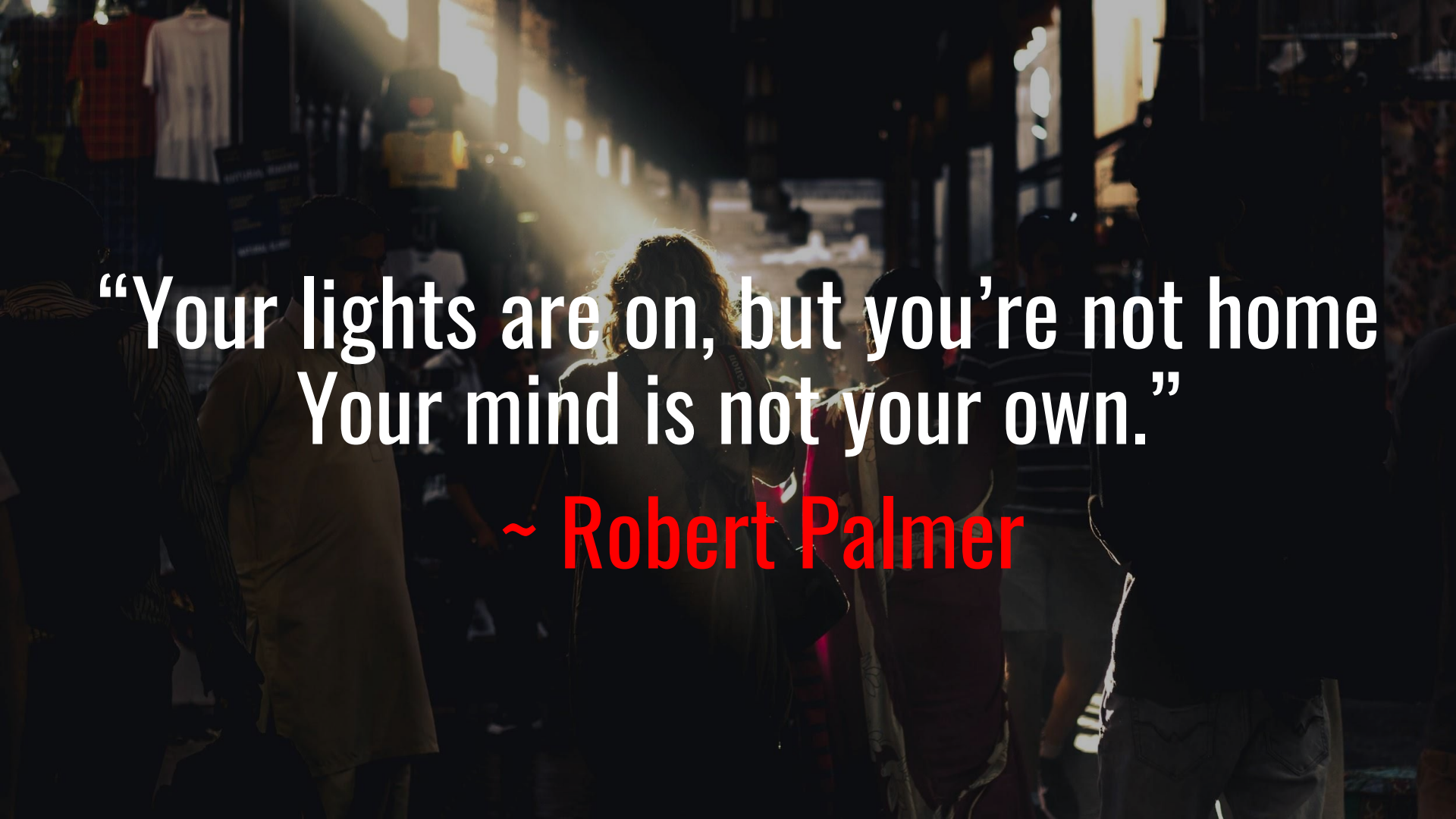
STALKERWARE



RWDEICA

LHM KILL CHAIN
COMMODITY STALKERWARE


“This TAINED LOVE you’ve given.”
~ Soft Cell
@CH33R10


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

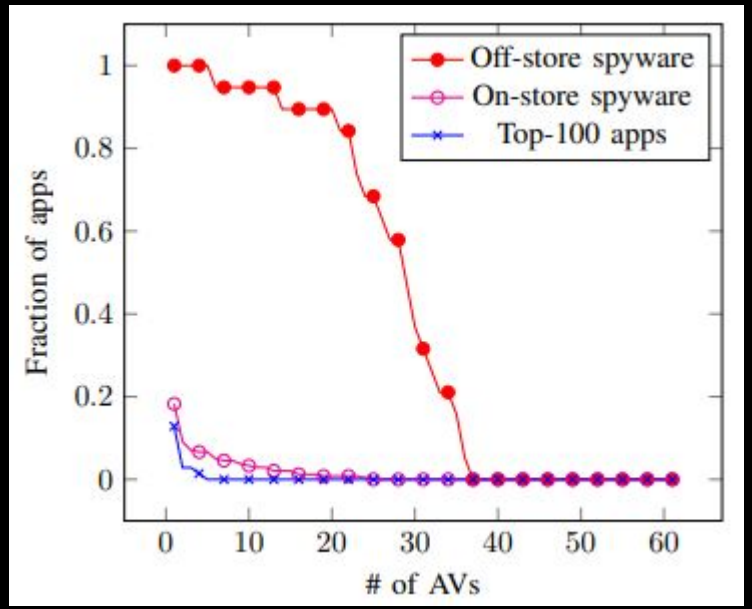
MITRE ATT&CK

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

Salvador Camarena

Daniel Lizárraga

Carmen Aristegui

Sebastián Barragán

Carlos Loret de Mola

Rafael Cabrera

Andrés Villarreal

Ismael Bojórquez

Griselda Triana

Targeted by Saudi Gov-linked Operator

Yahya Assiri

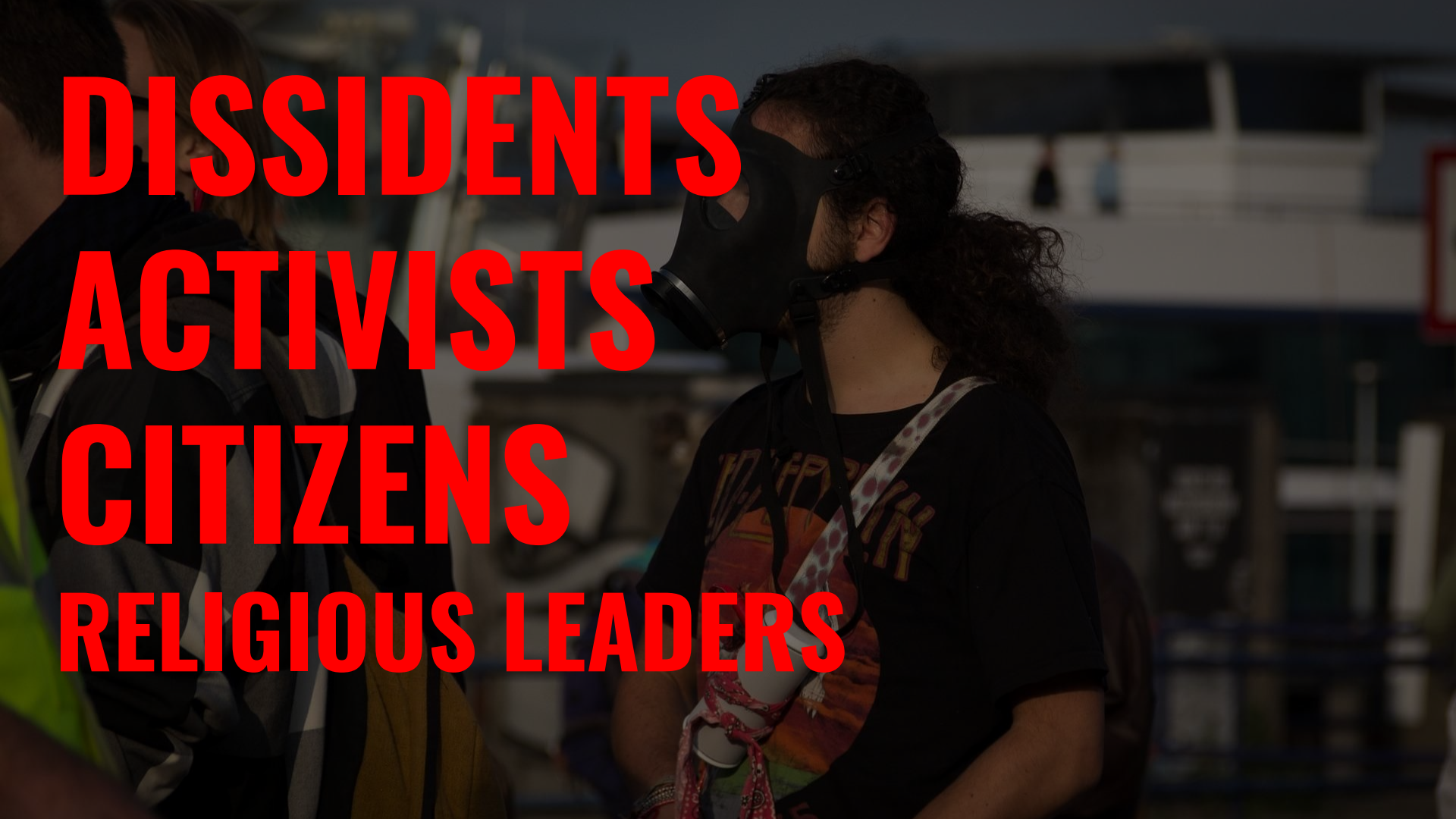
Omar Abdulaziz

Ghanem Al-Masarir

Ben Hubbard

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


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
STEVE IRWIN
77
@Ch33r10


LAW
ENFORCEMENT
POLISI
POLISI
POLISI
POLISI
POLISI
POLISI

NATION-STATE

STALKERWARE

HOSTILE ACTOR TRADECRAFT

@Ch33r10


KIMBER


SUKI WYNN


ELECTRA


POISON
HYDRA

STALKERWARE

CTI HYPOTHESES

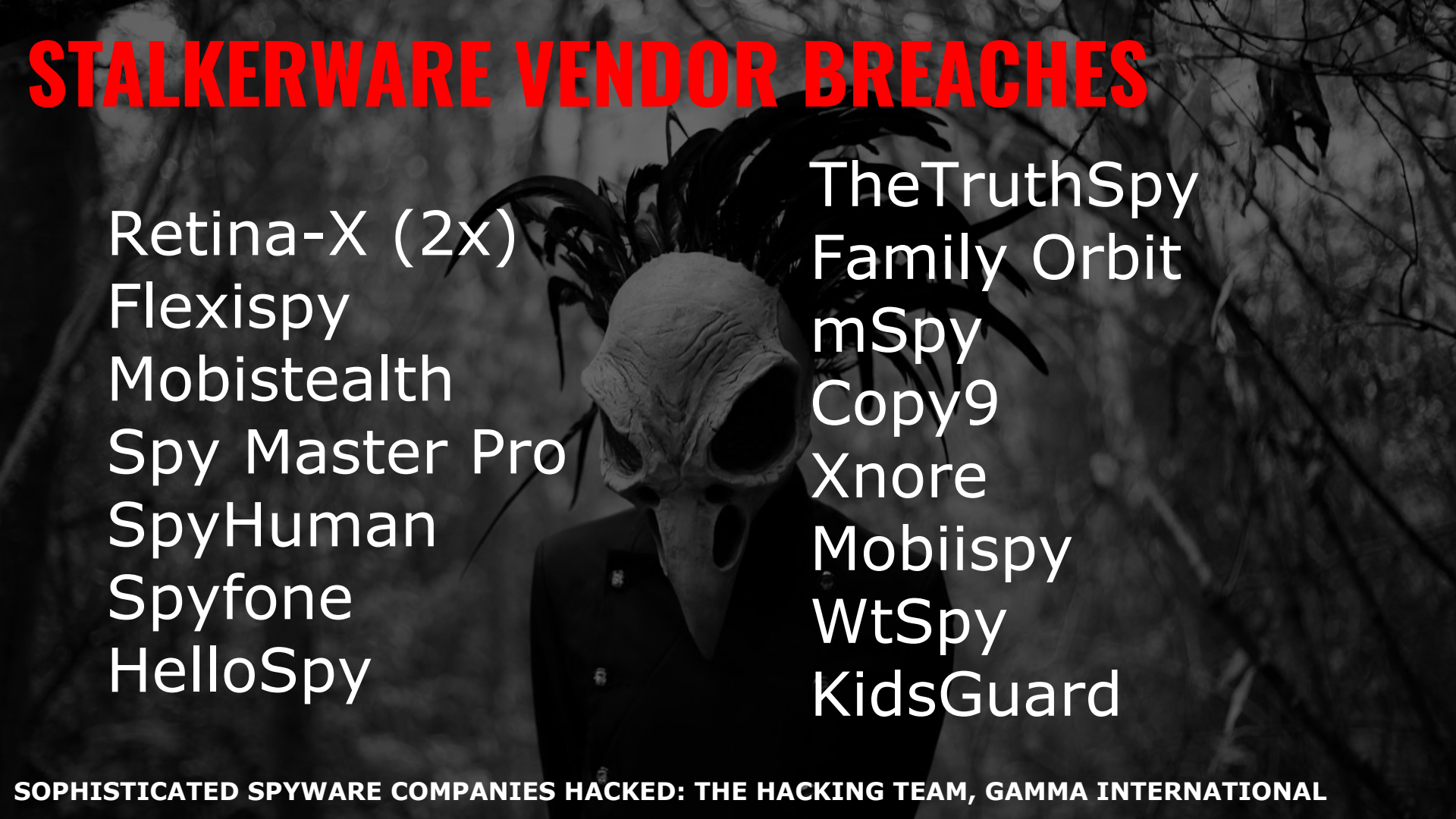
NORMAL USE OF COMMODITY STALKERWARE


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
Mobiispy
WtSpy
KidsGuard

SOPHISTICATED SPYWARE COMPANIES HACKED: THE HACKING TEAM, GAMMA INTERNATIONAL

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

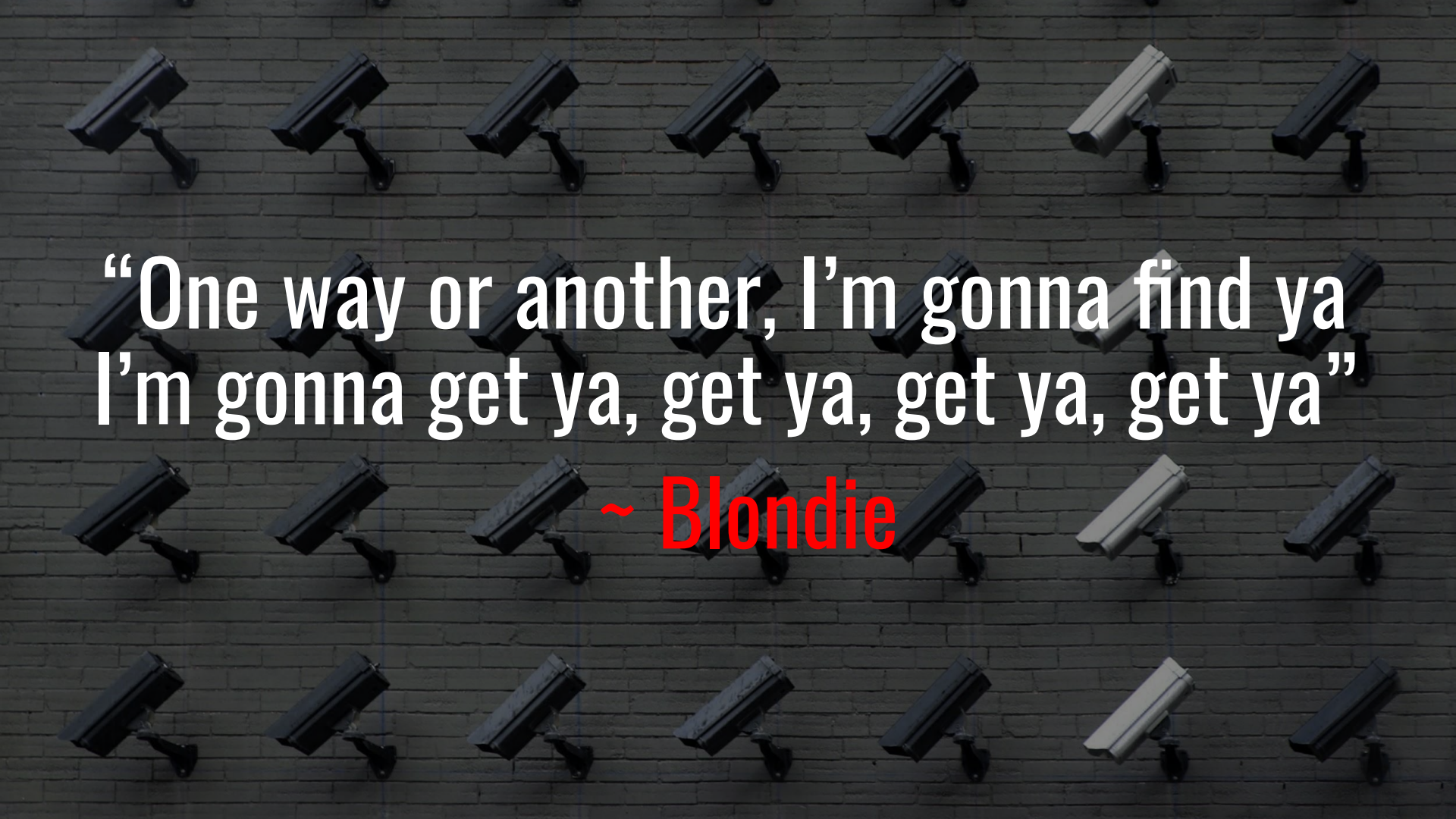
THE CITIZEN LAB | THE PREDATOR IN YOUR POCKET P 37-38 https://citizenlab.ca/docs/stalkerware-holistic.pdf

CORPORATE

TABLE TOP


AWARENESS

RESOURCES


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


AND ONE MORE
THING...


Gimme Some Sugar
APKTOOL
DEX2JAR
JD-GUI
VS
VIRUSTOTAL
HYBRID ANALYSIS
DECOMPILER
@chmodxx_


"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"/>
APKTOOL

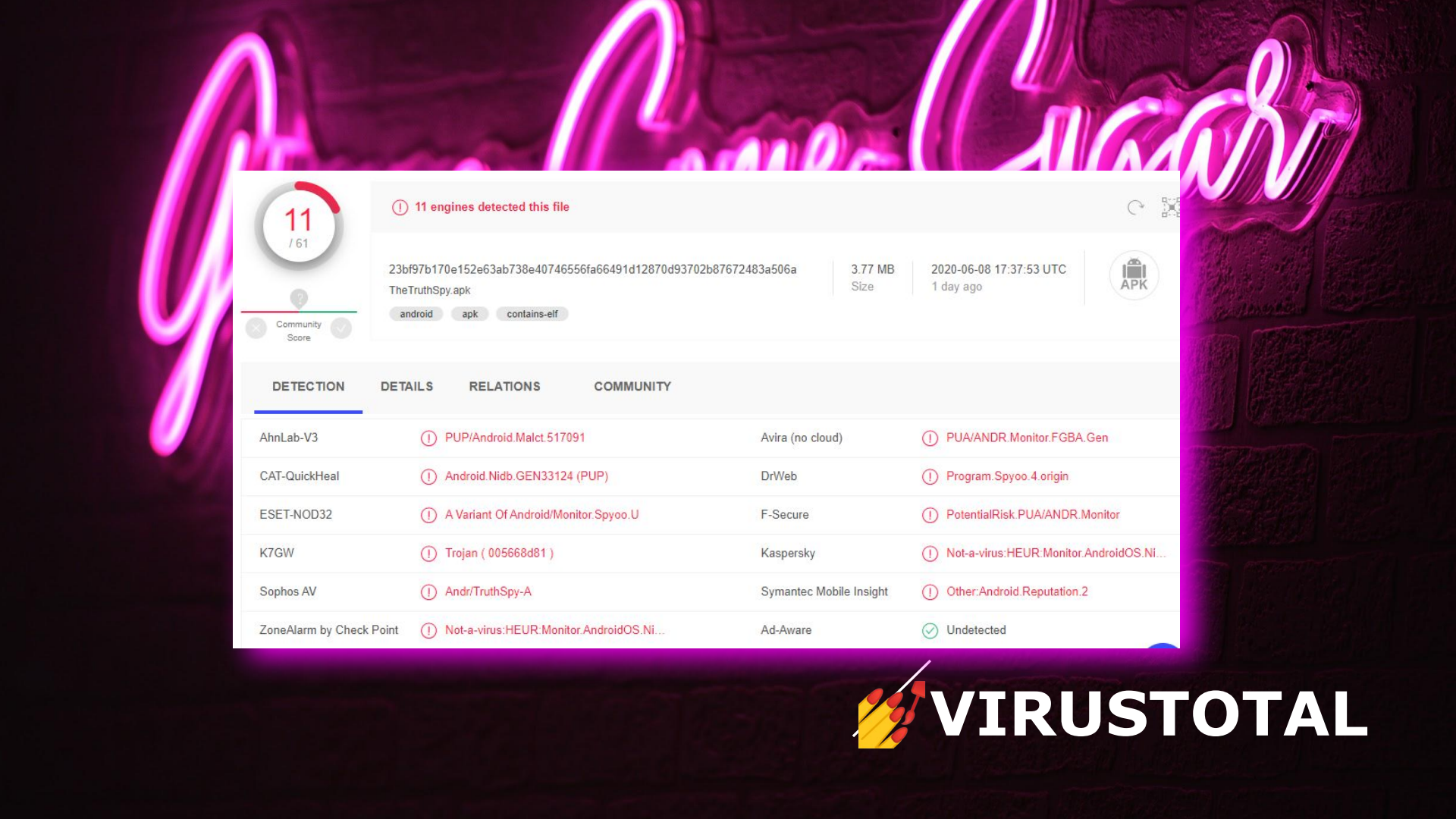

Gimme Some Sugar
stalkerware@ubuntu:~/Desktop/Sta
AndroidManifest.xml
assets
classes.dex
classes-dex2jar.jar
fabric
DEX2JAR

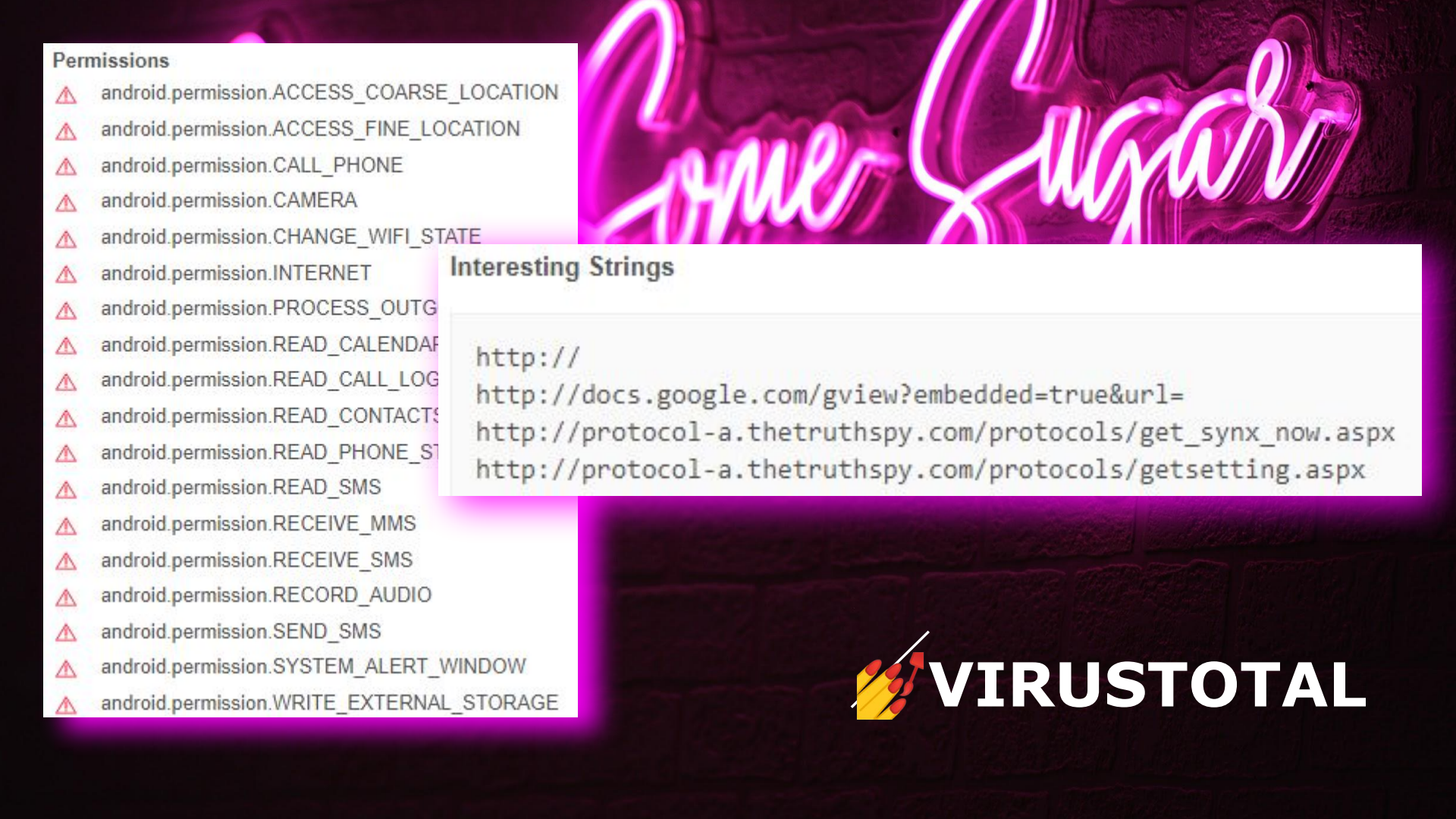

```
ArrayList<String> arrayList2 = new ArrayList();
this();
arrayList2.add(e.d(paramContext));
arrayList2.add(e.b());
arrayList2.add("AD");
String str = a.a("http://protocol-a.thetruthspy.com/protocols/getsetting.aspx", arrayList1, arrayList2);
Logger logger = this.c;
StringBuilder stringBuilder = new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

JD-GUI

```
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


11
/ 61
Community Score
11 engines detected this file
23bf97b170e152e63ab738e40746556fa66491d12870d93702b87672483a506a
TheTruthSpy.apk
android
apk
contains-elf
3.77 MB
Size
2020-06-08 17:37:53 UTC
1 day ago
APK
DETECTION
DETAILS
RELATIONS
COMMUNITY
AhnLab-V3
PUP/Android.Malct.517091
Avira (no cloud)
PUA/ANDR.Monitor.FGBA.Gen
CAT-QuickHeal
Android.Nidb.GEN33124 (PUP)
DrWeb
Program.Spyoo.4.origin
ESET-NOD32
A Variant Of Android/Monitor.Spyoo.U
F-Secure
PotentialRisk.PUA/ANDR.Monitor
K7GW
Trojan (005668d81)
Kaspersky
Not-a-virus:HEUR:Monitor.AndroidOS.Ni...
Sophos AV
Andr/TruthSpy-A
Symantec Mobile Insight
Other:Android.Reputation.2
ZoneAlarm by Check Point
Not-a-virus:HEUR:Monitor.AndroidOS.Ni...
Ad-Aware
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_synx_now.aspx
http://protocol-a.thetruthspy.com/protocols/getsetting.aspx
VIRUSTOTAL

malicious

Threat Score: 100/100
AV Detection: 17%
Labeled as:
Monitor.AndroidOS.Nidb

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

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.
AD_CONTACTS	Allows an application to read the user's contacts data.
T_ACCOUNTS	Allows access to the list of accounts in the Accounts Service.
CESS_COARSE_LOCATION	Allows an app to access approximate location.
CESS_FINE_LOCATION	Allows an app to access precise location.
CESS_BACKGROUND_LOCATION	-
CORD_AUDIO	Allows an application to record audio.

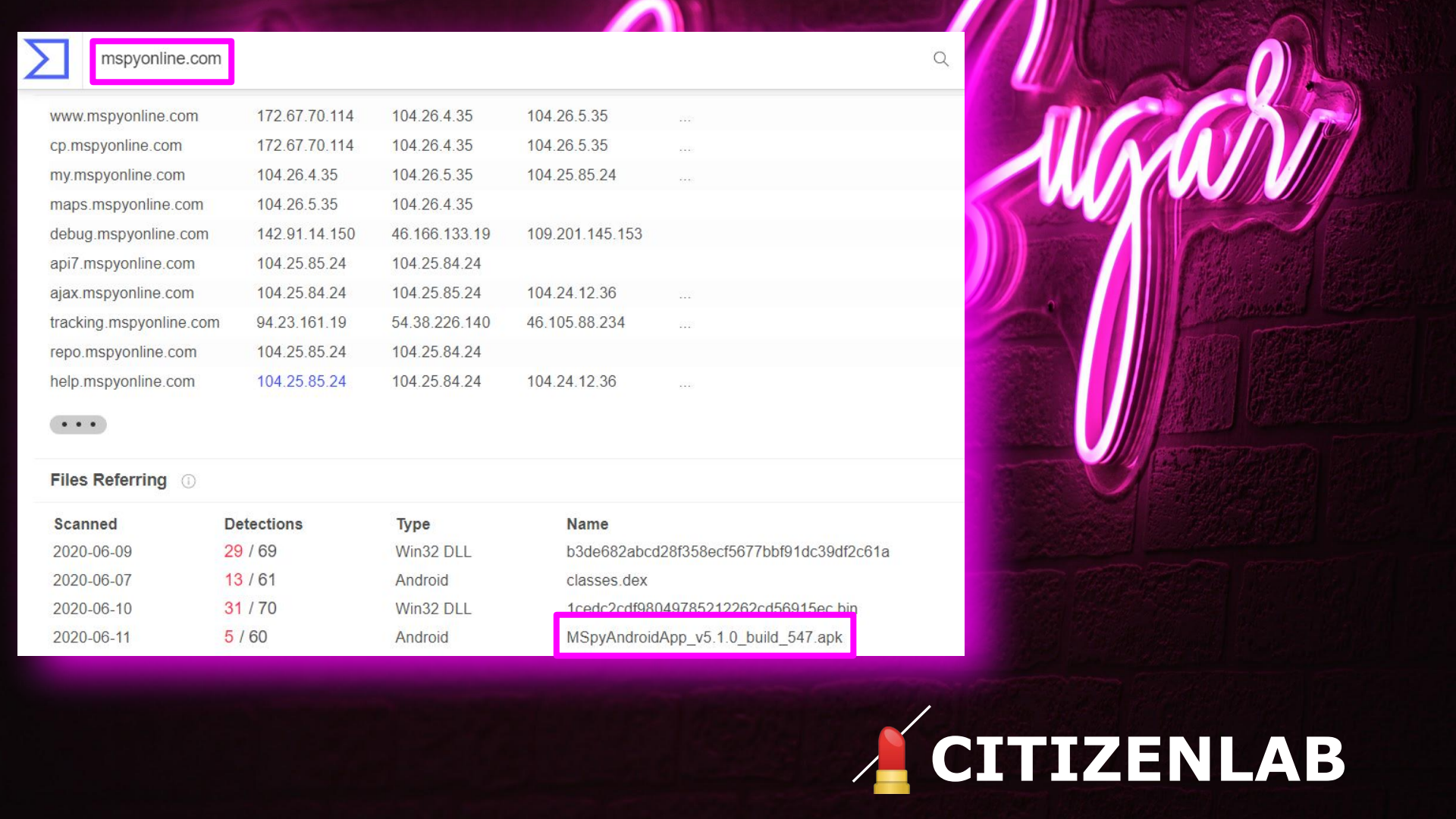
HYBRID ANALYSIS

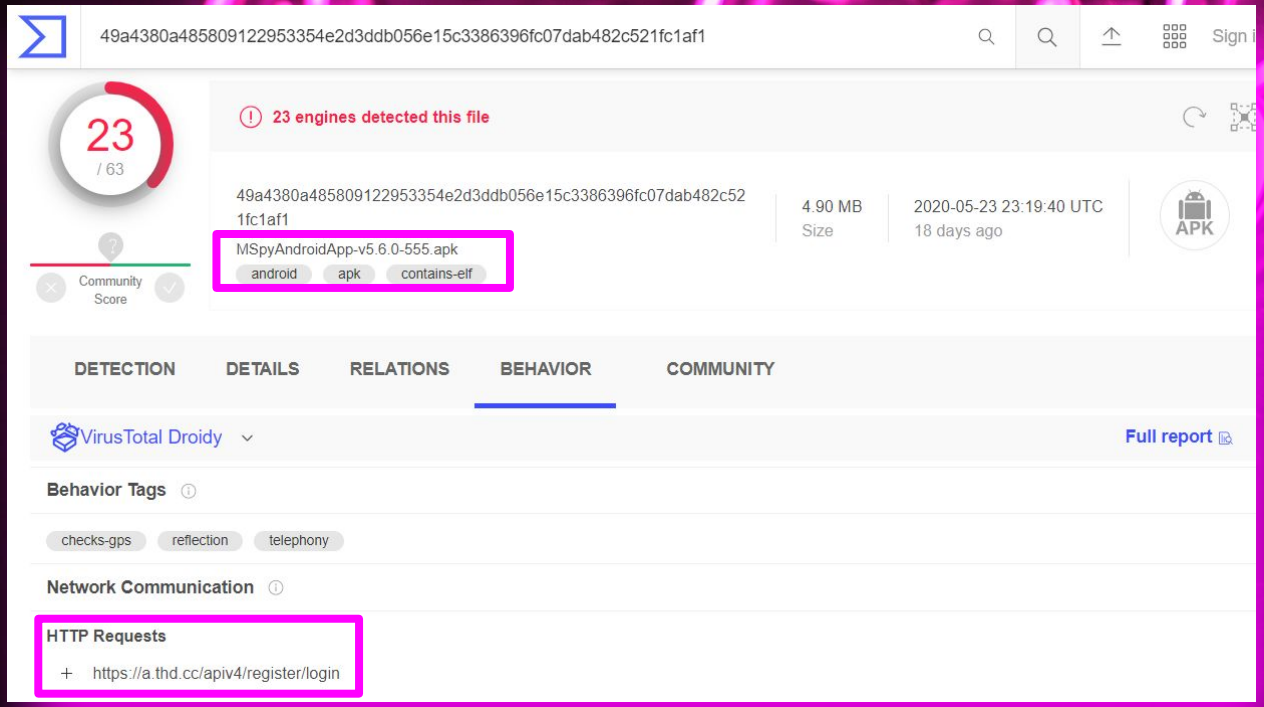
Loading language 'x86:LE:32:def...


BRAD

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
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
2020-06-11 5 / 60 Android MSpyAndroidApp_v5.1.0_build_547.apk
CITIZENLAB


49a4380a485809122953354e2d3ddb056e15c3386396fc07dab482c521fc1af1
Sign i
23
/ 63
23 engines detected this file
49a4380a485809122953354e2d3ddb056e15c3386396fc07dab482c52
1fc1af1
MSpyAndroidApp-v5.6.0-555.apk
android
apk
contains-elf
4.90 MB
Size
2020-05-23 23:19:40 UTC
18 days ago
APK
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

CITIZENLAB

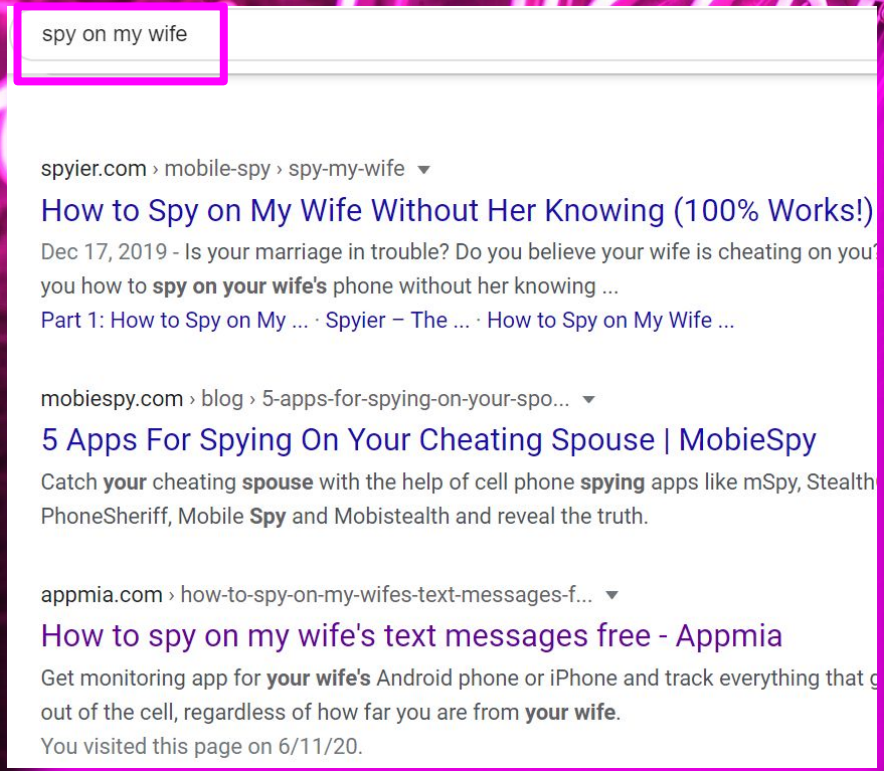
STALKERWARE VENDOR BREACHES

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

TheTruthSpy
Family Orbit
mSpy
Copy9
Xnore
Mobiispy
WtSpy
KidsGuard

SPY ON MY WIFE

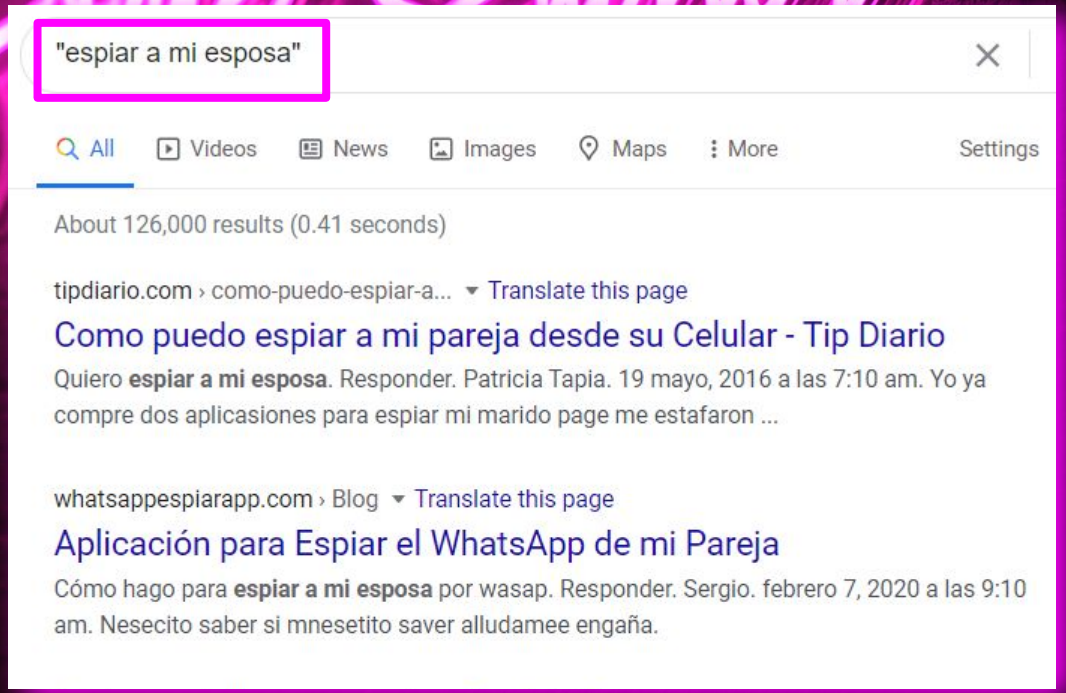
GOOGLE

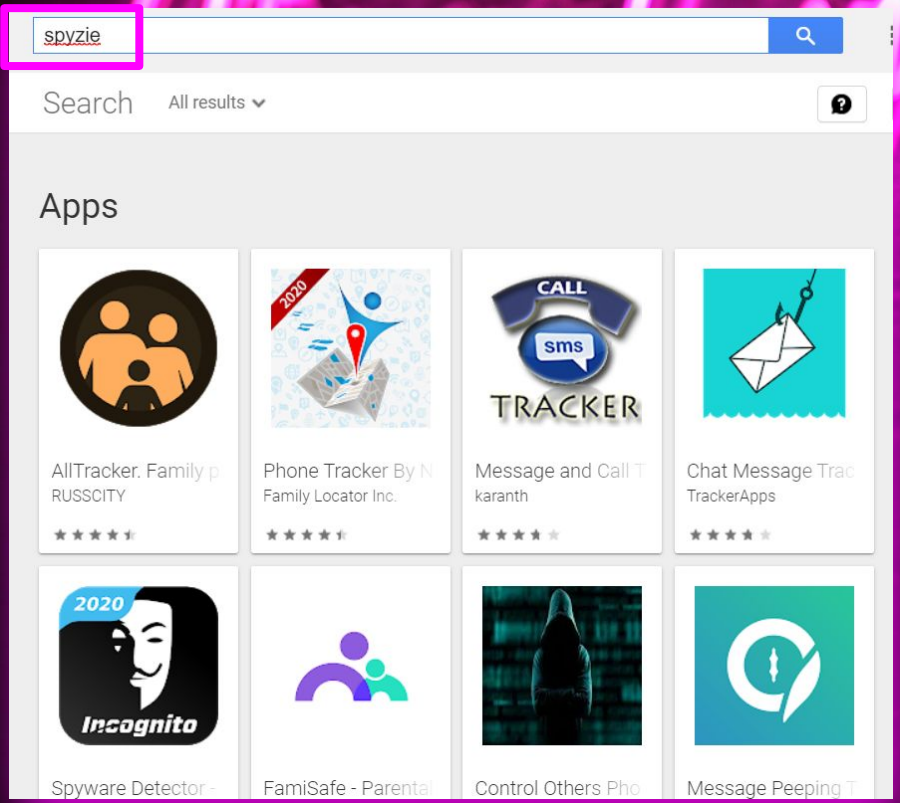


ESPIAR

A MI ESPOSA

GOOGLE

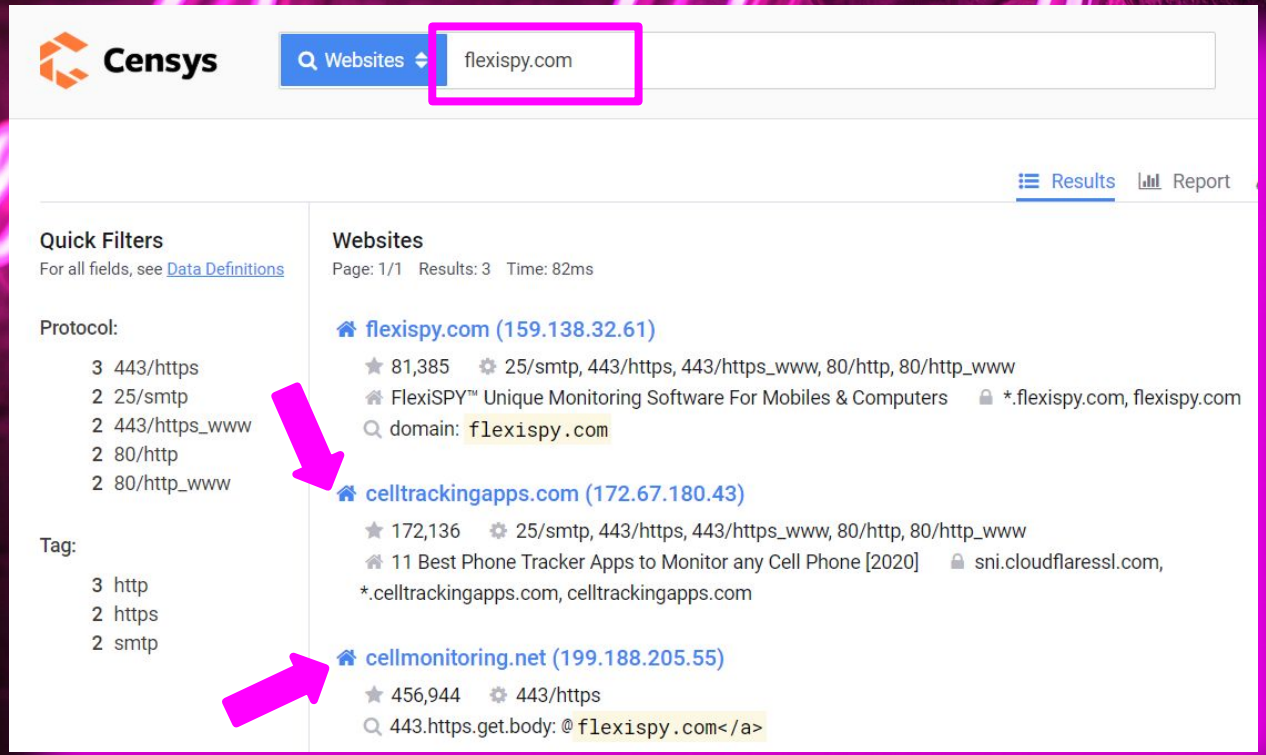




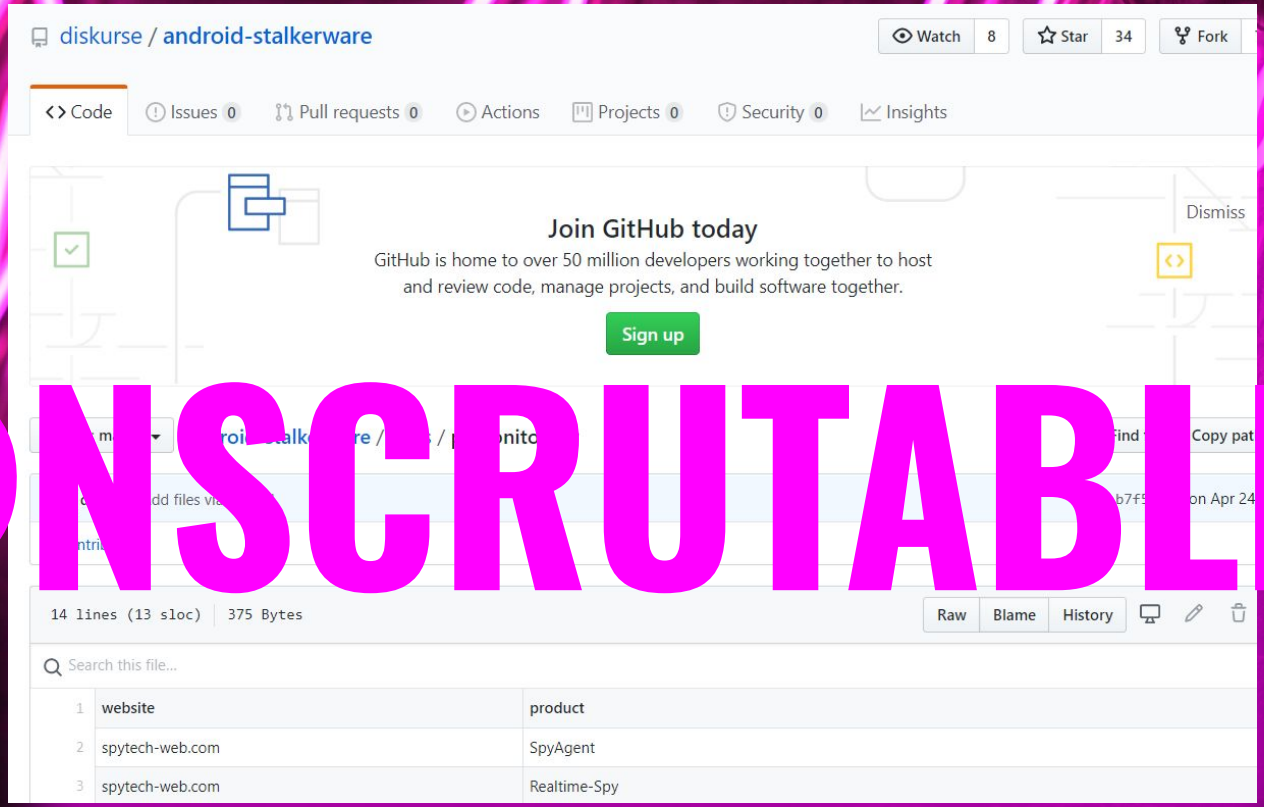
ADDITIONAL INFORMATION

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



SSL/TLS CERTS



@NSCRUTABLES

SECURITY RESEARCHERS

#stalkerware apk

Top | Latest | People | Photos | Videos

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.

3 10 16

@NSCRUTABLES

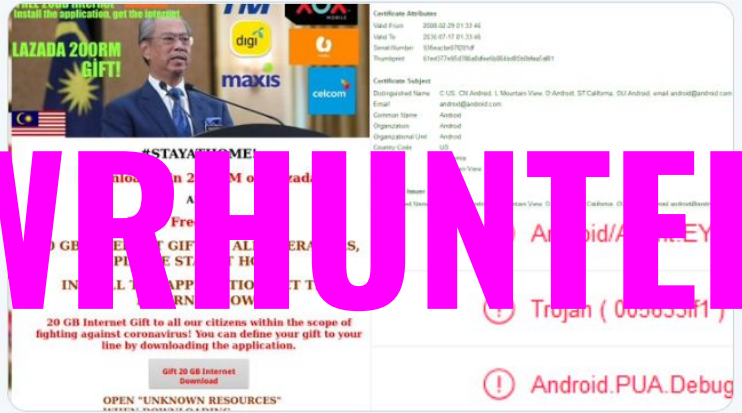
👑SECURITY RESEARCHERS

@malwrhunterteam apk

Top Latest People Photos Videos

MalwareHunterTeam @malwrhunterteam · 2h

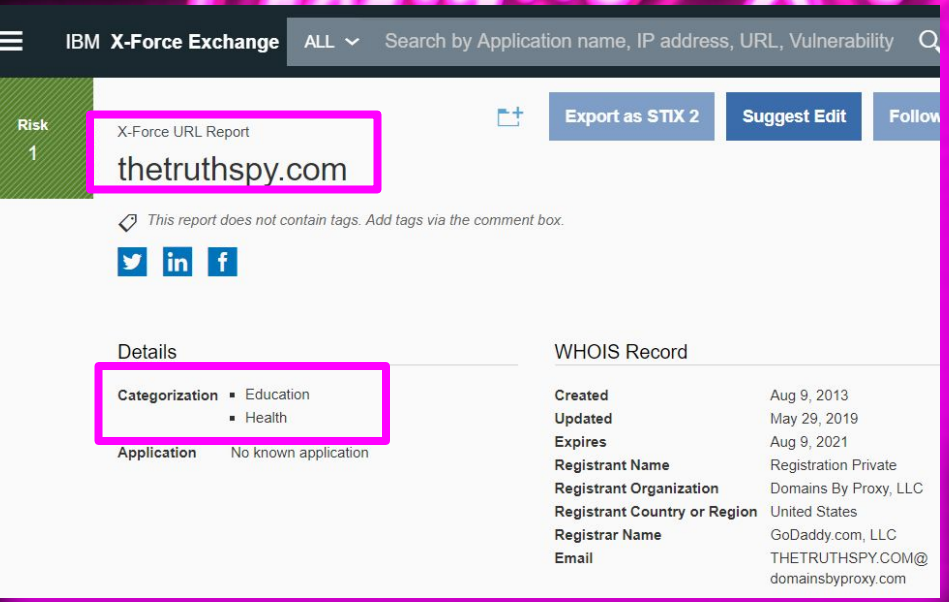
Not much detected "20GBGift.**apk**":
5386abd90497dc0b97537ae585addfa1772b10cd4353e41b413e90eb07a145f
e
From: https://20gbcampings[.]com/ ->
https://20gbcampings[.]com/**APK**/20GBGift.**apk**
cc @JAMESWT_MHT @douglasmun

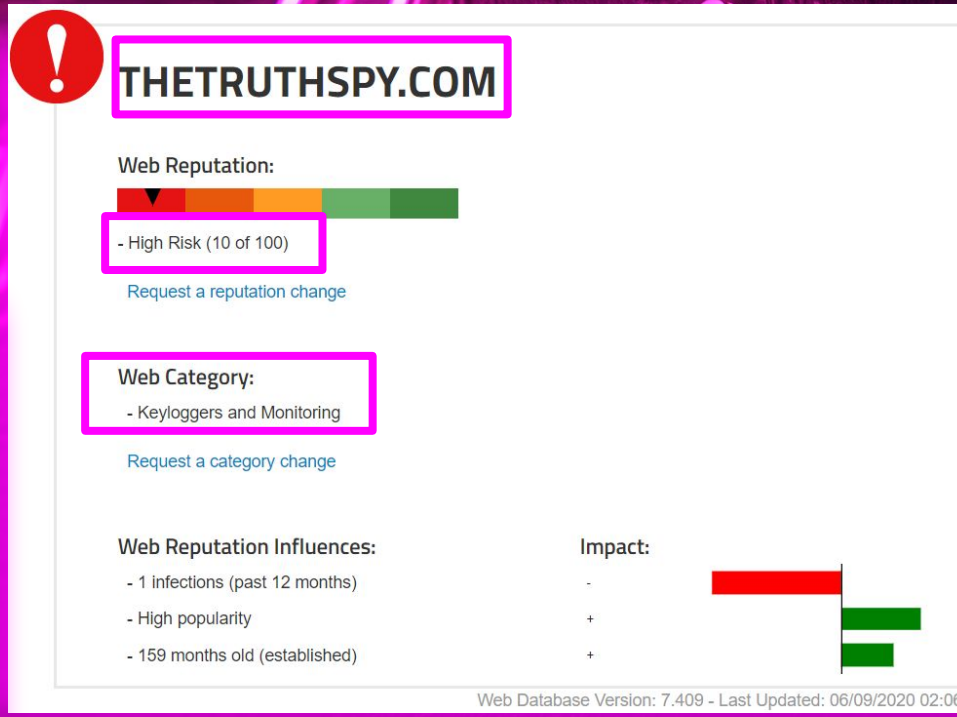


4 5

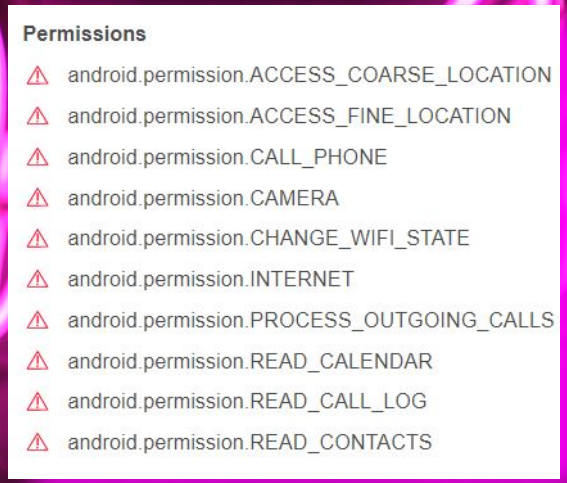
@MALWRHUNTERTEAM

SECURITY RESEARCHERS



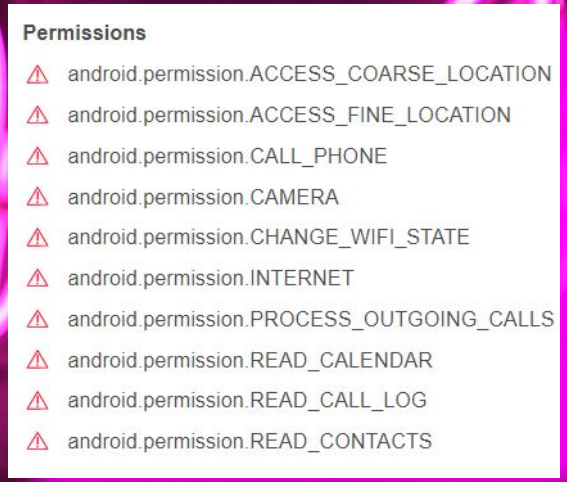


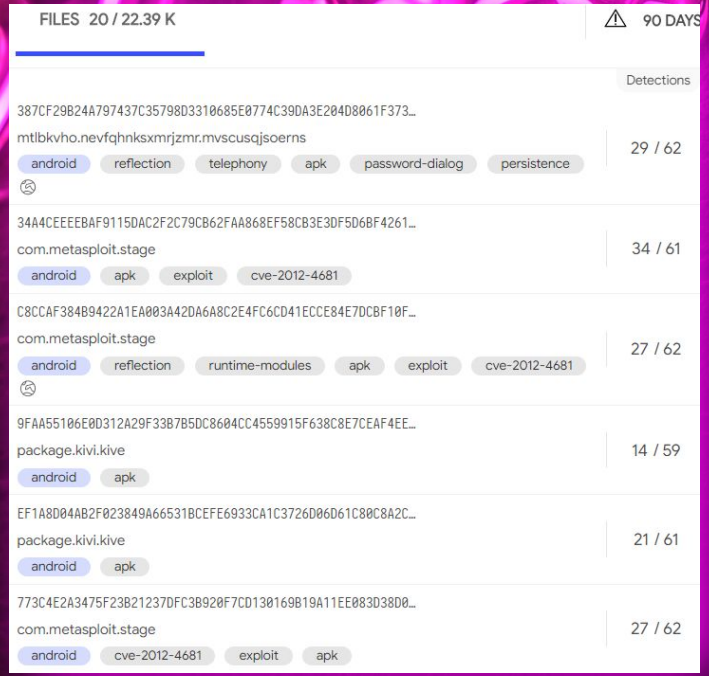
✨URL CATEGORY



submitter:AR
androguard:"android.permission.ACCESS_COARSE_LOCATION"
androguard:"android.permission.CAMERA"
androguard:"android.permission.READ_SMS" p:2+

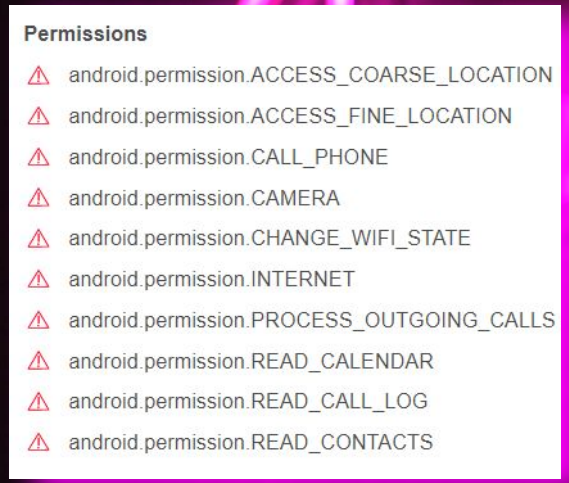
VIRUSTOTAL SEARCH

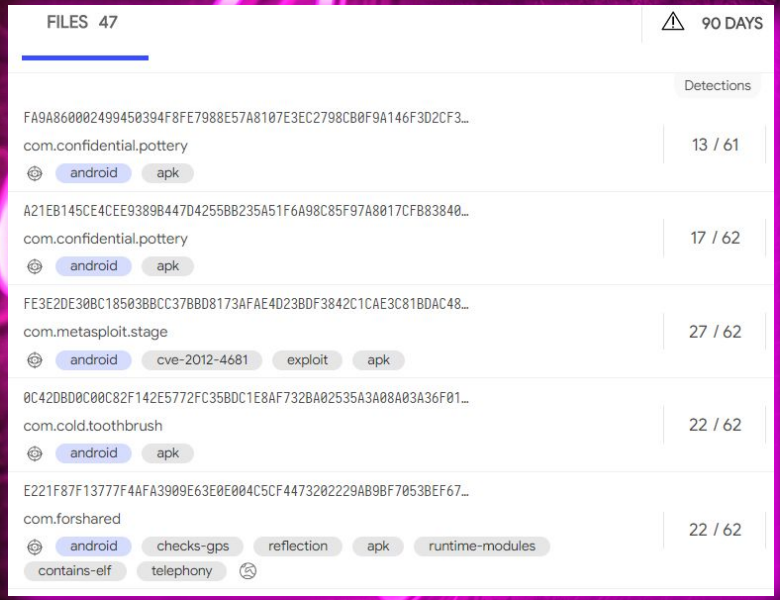




androguard:"android.permission.ACCESS_COARSE_LOCATION"
androguard:"android.permission.CAMERA"
androguard:"android.permission.READ_SMS" p:2+

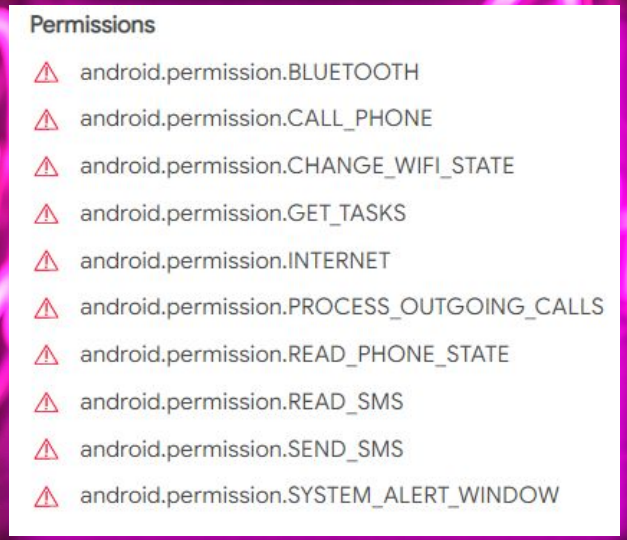
VIRUSTOTAL SEARCH

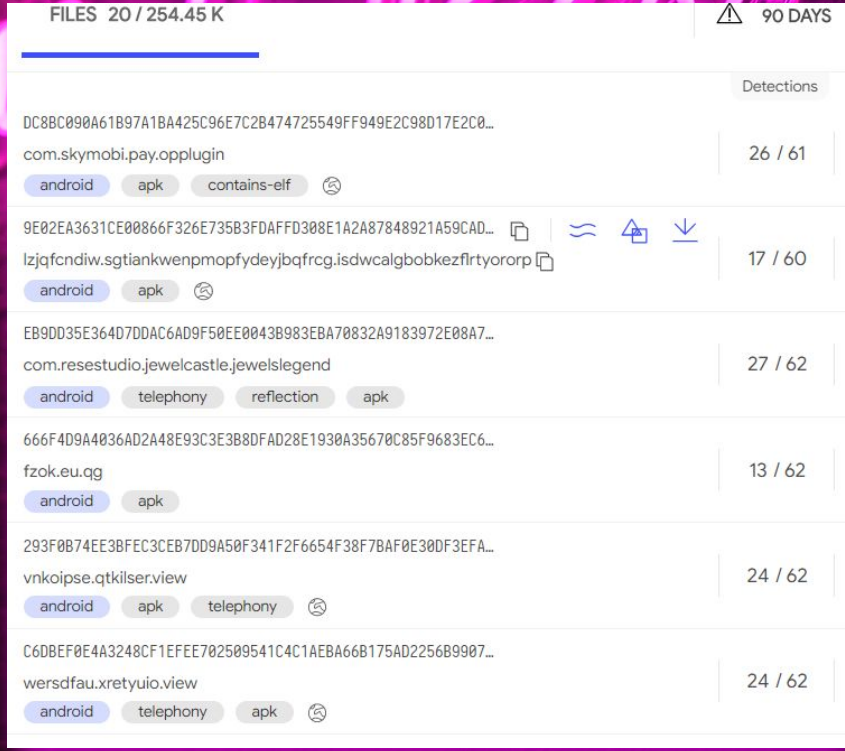




submitter:AR tag:android tag:apk
androguard:"android.permission.ACCESS_COARSE_LOCATION"
androguard:"android.permission.ACCESS_FINE_LOCATION"
androguard:"android.permission.INTERNET"
androguard:"android.permission.WRITE_EXTERNAL_STORAGE" p:13+

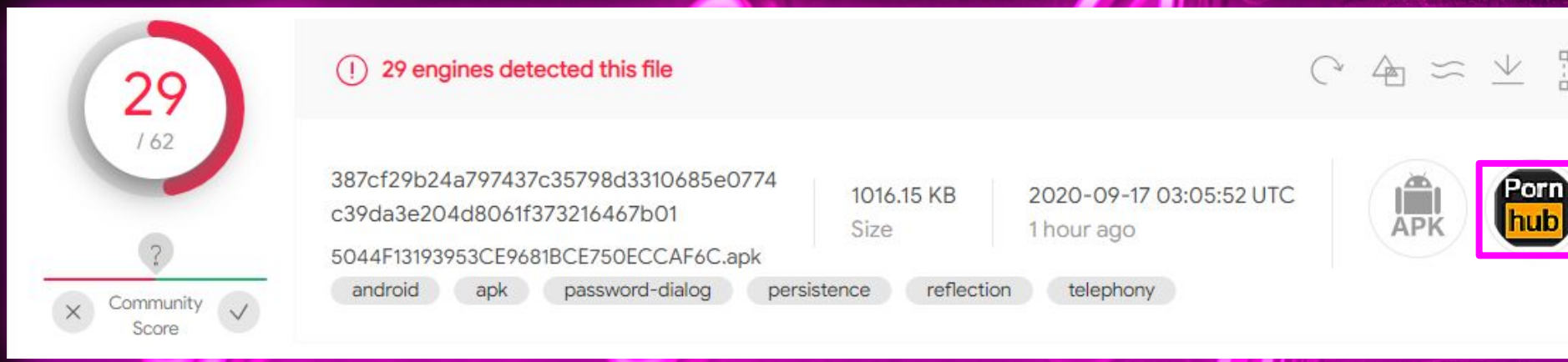
VIRUSTOTAL SEARCH

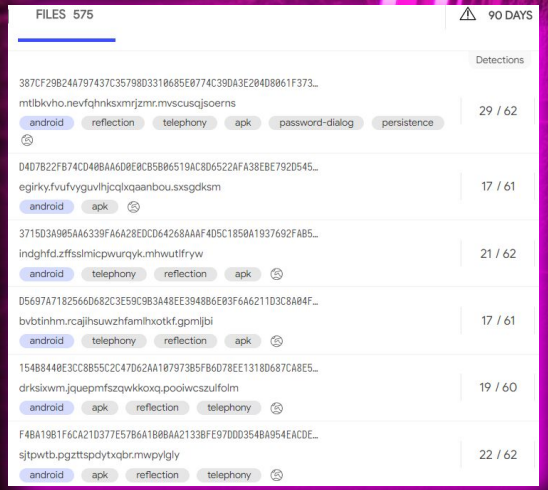




androguard:"android.permission.
READ_SMS" p:13+

VIRUSTOTAL SEARCH





main_icon_dhash:a6ccd2d8d0d4
ccd0 p:5+

VIRUSTOTAL SEARCH

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	celltrackingapps.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	ikeymonitor.com	stalkerware	@ch33r10
domain	letmespy.com	stalkerware	@ch33r10
domain	mobiespy.com	stalkerware	@ch33r10
domain	mobile-spy.com	stalkerware	@ch33r10
domain	mobispy.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.thetruthspy.com	stalkerware	@ch33r10
domain	protocol-a732.thetruthspy.com	stalkerware	@ch33r10
domain	spappmonitoring.com	stalkerware	@ch33r10
domain	spyfone.com	stalkerware	@ch33r10
domain	spymasterpro.com	stalkerware	@ch33r10
domain	theonespy.com	stalkerware	@ch33r10
domain	xnspy.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, 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

💋 bit.ly/ekoparty2020

THANK YOU <3

🦞 bit.ly/ekoparty2020