

# Cyber-violences in Intimate-Partner Violence

Digital Defender Partnership - July 2023

Etienne for Echap - [etienne@maynier.eu](mailto:etienne@maynier.eu) <https://echap.eu.org/>



# Context for this talk

- Started as a discussion among friends about how gender-based violence was a non-existing conversation in hacker / free software groups
- We created a non-profit organization called Echap to help women shelters and organizations working with survivors
- Our work / experience focused on domestic violences for people being supported by women shelters



# Today

- Let's talk about cyber-violences in intimate partner violences
- Different types of cyber-violences
- How to disconnect from your ex
- Checking online accounts
- Checking devices with some forensic

# How-to

- We have shared pads for notes / questions. Feel free to add notes and questions in English or Spanish
- You can ask questions in the chat
- Not a lot of space for interactive learning, but there is a learning exercise for after the session in the pad
- There are lots of resources for after this talk + slides will be shared
- Get in touch!



# Disclaimer

/!\ This is a collective work, I am sharing here work done by Echap and many other people



# Content Warning

We will talk about domestic violence, abuse and I will share some real-life examples of online domestic abuse

# Cyber-violences

# Cyberviolences

## Harassment

- Mostly on social media
- Can be group harassment (e.g. Gamergate)
- In domestic violence, often one person harassment
- Fake accounts on social media

## Cyber-control

- Using technology to increase control on the survivor's life
- Extend control outside of the house
- Asking for regular message, photos, videos
- Control of interactions online

## Cyber-surveillance

- Intrusion in smartphones, emails etc.
- Stalkerware
- Tracking geolocation
- Intrusion in administrative accounts
- Using kids devices



# Cyber-control

- Control is a key part of domestic abuse
- Technology allows to extend this control outside of the house
- Ex: In France, 90% of domestic violence survivors declared that their partner required them to be reachable all the time (Hubertine Auclert 2018)

# Online Harassment

- Harassment can take very different forms depending on the context
- We generally think of harassment as online mobs (e.g. Gamer Gate)
- In intimate partner violence, harassment is generally done by few people:
  - Fake accounts in the name of the survivor
  - Non consensual publication of photos
  - Messages
  - Threats (80% in France - HA 2018)

# Digital surveillance

- Very common when a large part of digital life is shared with the abuser
- Passwords can be shared and reused, hard to know what the abuser has access to
- Very little space for privacy in abusive relations
- Most common cases are: password stolen, phone connected to the account
- Smartphones allow to share geolocation through standard apps

# Administrative violences

- Confiscation of administrative documents
- Control of most online accounts: bank, social services, taxes, phone plan etc.
- Bank details can be modified after separation to steal money
- Administrative surveillance: medical information, list of calls etc.

# Stalkerware



[HOME](#) [FEATURES](#) [PRICES](#) [DOWNLOAD NOW](#) [LOGIN](#) [Q](#)



## Easiest Steps to Install Android Spy App (Remote Installation)

### Easiest Steps to Install Android Spy App (Remote Installation)

THETRUTHSPY EDITOR - JULY 4, 2023

### 3 Easiest Ways to Spy My Wife's Phone for Free Without Her Knowing

THETRUTHSPY EDITOR - JUNE 29, 2023

### 3 Easiest Ways to Track Someone's Snapchat Messages

THETRUTHSPY EDITOR - JUNE 20, 2023

### 3 Easiest Ways to Track Other's Facebook Messages

THETRUTHSPY EDITOR - JUNE 11, 2023

### 3 Easiest Ways to Track Someone's Text Messages Without Their Phone

THETRUTHSPY EDITOR - MAY 30, 2023



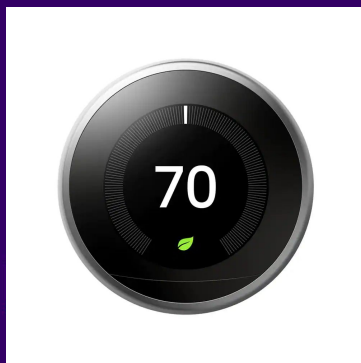
# Stalkerware

- Spyware products used on intimate partner violence
- Cost between 10\$ and 30\$ / month
- It is awful

# But

- Stalkerware is the “cool tech topic” for media while it’s probably a small minority of cases
- A lot of digital surveillance techniques exist that are easier and cheaper
- We won’t solve the stalkerware issue without solving the violence issue
- We need to be careful with techno-solutionism

# Internet of Things



ECH/P

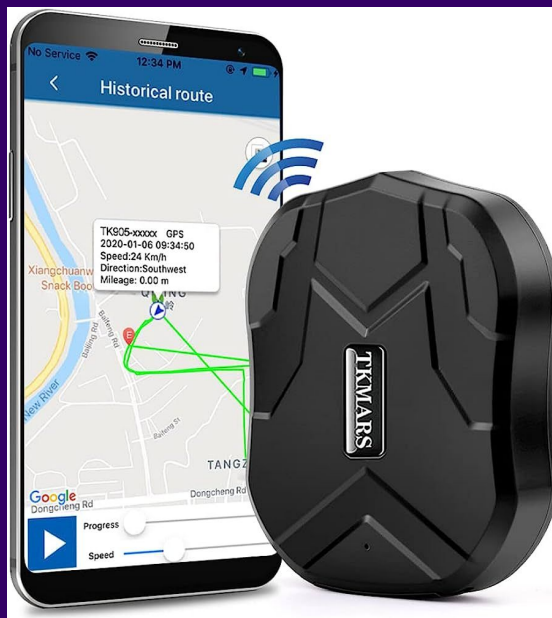


# IoT

Context	Category	Device	Discussed Strategies		Abuse Vectors
			Spy	Harass	
Shared-use devices	Home control	Smart speaker	-	-	- U R -
		Control tablet	- -	- - -	- U R -
	Smart appliances	TV	- -	- -	- U R I
		Thermostat	- -  -	-	- U R -
		Lights	- -  -	- -	- U - I
		Router	- - -	- -	- - R I
		Plug	- -  -	- -	- - R I
		Kettle	- - - -	- -	- - - I
		Smoke alarm	- - - -	- -	- - R -
		Fridge	- -  -	- - -	- - R -
		Mattress	- - -	- - -	- - R -
	Security systems	Doorbell		- -	- U - I
		Security camera	-  -	- - -	- U - I
		General camera	- -	- - -	C U - I
		Baby monitor	- -	- - -	C - - I
		Lock	- -  -	-	- U - I
		Motion sensor	- -  -	- - -	C - - I
		Presence sensor	- -  -	- - -	C - - I
	Vehicles	Garage door opener	- - - -	-  -	- - R I
		Car	- -  -	-	- - - I
		Car accessory	- -  -	- -	C - R -
Personal-use devices	Tracking devices	Watch		- - -	- - R -
		Item tracker	- -  -	- - -	C - - -
	Entertainment	Bluetooth headphones	-  -	- - -	C U R -
		Smart toy	- - -	- - -	- - R -
	Covert spying technologies	Hidden camera	- -	- - -	C - - -
		Spy drone	-   -	- - -	C - - -
		Thermal camera	-  - -	- - -	C - - -
		Listening device	- - -	- - -	C - - -
		Landline recorder	- - -	- - -	C - - -
		GPS tracker	- -  -	- - -	C - - -
		USB keylogger	- - -	- - -	C - - -

Source: Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse

# Airtags, cameras, GPS trackers



# Clinical Computer Security for Victims of Intimate Partner Violence

Sam Havron\*,<sup>1</sup>

Diana Freed\*,<sup>1</sup>

Rahul Chatterjee<sup>1</sup>

Damon McCoy<sup>2</sup>

Nicola Dell<sup>1</sup>

Thomas Ristenpart<sup>1</sup>

<sup>1</sup> *Cornell Tech*

<sup>2</sup> *New York University*

## Clients & Devices

Clients seen	44
Consultations performed	46
Devices seen	105
Devices manually inspected	97
Devices scanned w/ ISDi	75
Median devices per client	2
Max devices per client	7
Median apps per scanned device	170

## Chief Concerns

Worried about tech abuse/tracking/spyware	18
Abuser hacked accounts or knows secrets	20
Worried abuser was tracking their location	10
Phone is glitchy	10
Abuser calls from unknown numbers	9
Unrecognized app on child's phone	1
Money missing from bank account	1
Curious and want to learn about privacy	4

## Detected Issues

Clients w/ vulnerabilities	23
Clients w/ unsolved problems	2
Clients w/ no problems detected	19
Potential spyware detected	3
Potential password compromise	14
Presence of unknown "trusted" devices	12
Shared family/phone plan	4
Rooted device	1

and tested a range of new technical and non-technical tools that systematize the discovery and investigation of the complicated, multimodal digital attacks seen in IPV. An initial field study with 44 IPV survivors showed how our procedures and tools help victims discover account compromise, exploitable misconfigurations, and potential spyware.

shown how abusers exploit technology to harass, impersonate, threaten, monitor, intimidate, and otherwise harm their victims [8, 14, 19, 20, 27, 35, 43]. Prevalent attacks include account compromise, installation of spyware, and harassment on social media [20, 27]. In many cases digital attacks can lead to physical violence, including even murder [34]. Unfortu-



# Activity!

**Share in the pad some forms of cyber-violences you have encountered in your work that are missing in this list**

# Disconnect from your ex



## Shared life

Living with an abusive partner who physically control and monitor how technology is used.

Limited possibilities for privacy and high risk of reprisal.

Key aspect is to secure communications with the survivor without adding more risks to the situation.

## Leaving

Attempt to leave the perpetrator.

Need privacy to prepare departure and have physical protection in new place.

Often a key moment to stay safe and disconnect from the abuser

## Separated Life

Continue life without the abuser, both online and offline.

Need to stay connected with close people to have support.

Sometime need to stay in touch with the abuser and manage that securely.

Risk of harassment



# How to disconnect

## Tech Disconnect Short Form

Compiled by the Clinic to End Tech Abuse

Last Updated: July 2, 2020

### What is this?

We have created a checklist of ways you may still be connected with your ex-partner online or on your devices. These connections may let them continue to get information about your life.

If you are concerned that any of the actions we suggest below will increase any risks to your safety, we strongly recommend that you consult with a case worker at a domestic violence organization -- or other appropriate support organization -- beforehand.

### Checklist



# How to disconnect

- List online accounts
  - Email, social networks but also administrative accounts (social services, bank...)
- List devices
  - List connected accounts (Google, iCloud)
- Pick a solid password strategy
- Change passwords
- Do specific checks on email and social media accounts
- Secure the devices

# Checking Online Accounts

# Key part of disconnecting / digital security

- Changing passwords is good, but not enough for social media / email accounts
- Different ways to keep access to the account exist
  - Phones connected to the account
  - App passwords
  - Auto forward
  - Apps etc.

# Ex Google

## Activity on this account

This feature provides information about the last activity on this mail account and any concurrent activity. [Learn more](#)

This account is open in 2 other locations.

(Location may refer to a different session on the same computer.)

### Concurrent session information:


Access Type [ ? ] (Browser, mobile, etc.)	Location (IP address) [ ? ]
Authorised Application	France ( )
Browser	France ( )

Visit [Security Check-up](#) for more details


### Recent activity:

Access Type [ ? ] (Browser, mobile, POP3, etc.)	Location (IP address) [ ? ]	Date/Time (Displayed in your time zone)
Browser (Chrome) <a href="#">Show details</a>	* France ( )	02:19 (0 minutes ago)
Authorised Application () <a href="#">Show details</a>	France ( )	02:18 (0 minutes ago)
Browser (Chrome) <a href="#">Show details</a>	France ( )	02:16 (2 minutes ago)
Authorised Application () <a href="#">Show details</a>	France ( )	02:15 (3 minutes ago)
Browser (Chrome) <a href="#">Show details</a>	France ( )	01:00 (1 hour ago)
Browser (Chrome) <a href="#">Show details</a>	France ( )	00:35 (1.5 hours ago)
Mobile	France ( )	23:51 (2 hours ago)
Mobile	France ( )	21:57 (4 hours ago)
Mobile	France ( )	15:30 (10 hours ago)
Mobile	France ( )	13 Jul (12 hours ago)

# Ex: Google

 Your devices


You're signed in on these devices or have been in the last 28 days. There might be multiple activity sessions from the same device. [Learn more](#)





1 session on Linux computer

[What's this?](#)

Linux  
France  
Google Chrome

 Your current session







1 session on Android phone

[What's this?](#)

Fairphone3  
France  
1 hour ago  
Android device, Turo






1 session on unknown device

[What's this?](#)

Unknown device  
Debian Chromium



# Ex: Google

## Settings

Fr ▾

[General](#) [Labels](#) [Inbox](#) [Accounts and Import](#) [Filters and blocked addresses](#) [Forwarding and POP/IMAP](#) [Add-ons](#) [Chat and Meet](#) [Advanced](#) [Offline](#) [Themes](#)

### Forwarding:

[Learn more](#)

[Add a forwarding address](#)

Tip: You can also forward only some of your mail by [creating a filter!](#)

### POP download:

[Learn more](#)

#### 1. Status: POP is disabled

- ☐ Enable POP for **all mail**
- ☐ Enable POP for **mail that arrives from now on**

#### 2. When messages are accessed with POP

keep Gmail's copy in the Inbox ▾

#### 3. Configure your email client (e.g. Outlook, Eudora, Netscape Mail)

[Configuration instructions](#)

### IMAP access:

(access Gmail from other clients using IMAP)

[Learn more](#)

#### Status: IMAP is enabled

- ☒ Enable IMAP
- ☐ Disable IMAP

#### When I mark a message in IMAP as deleted:

- ☒ Auto-Expunge on - Immediately update the server. (default)
- ☐ Auto-Expunge off - Wait for the client to update the server.

# Risks of Social Networks

- Hacking or access to the account: shared or stolen password etc.
- Control: stalking, gathering personal information etc.
- Harassment: messages, threats, fake accounts...

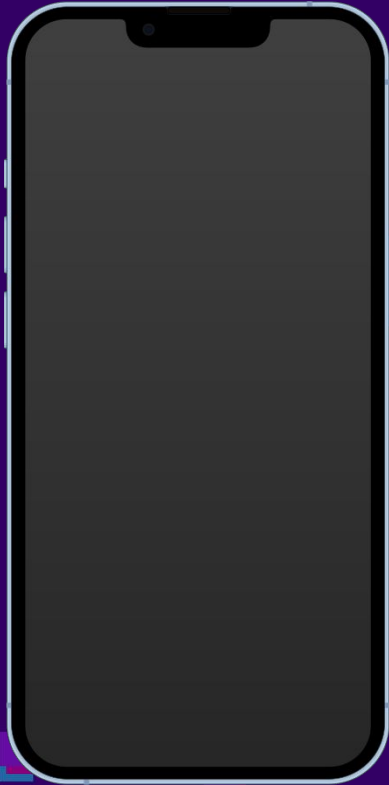
**Break - 10 minutes**



# Securing Devices

# iPhones

# iPhones



- There are many ways to share data on an iPhone, that can be used by an abusive partner
- Stalkerware apps are quite rare, they actually use access to iCloud data and backups

# Share Geolocation

<https://support.apple.com/en-us/HT210514>

## Find people and share your location with Find My

Learn how to use the Find My app to share your location with friends and family members. You can even set up location-based notifications, so that you know if someone left a location or just arrived home.



The Find My app combines Find My iPhone and Find My Friends into a single app. If you need help finding it, [use Search on your iPhone, iPad, or iPod touch](#) or [use Spotlight on your Mac](#).


## Share your location

When Share My Location is turned on, you can share your location with friends, family, and contacts from your iPhone, iPad, or iPod touch with Find My. You can also share your location in the Find People app on watchOS 6 or later with Apple Watch models that have GPS and cellular and are paired with your iPhone.

If you already [set up Family Sharing](#) and use Location Sharing, your family members automatically appear in Find My.

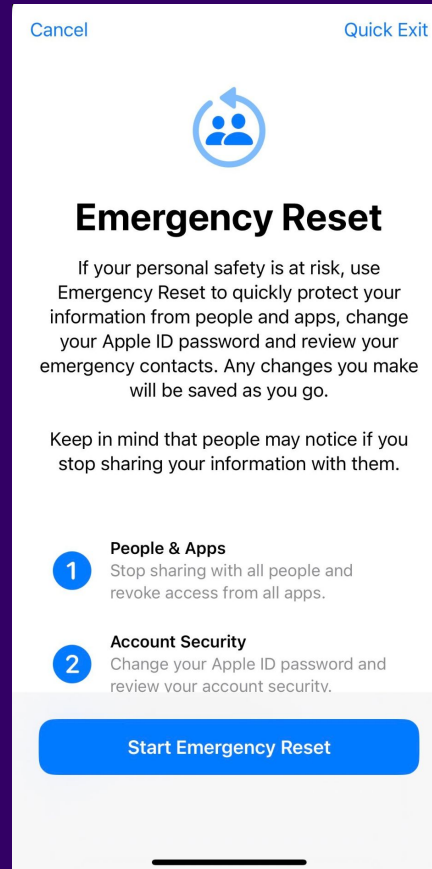
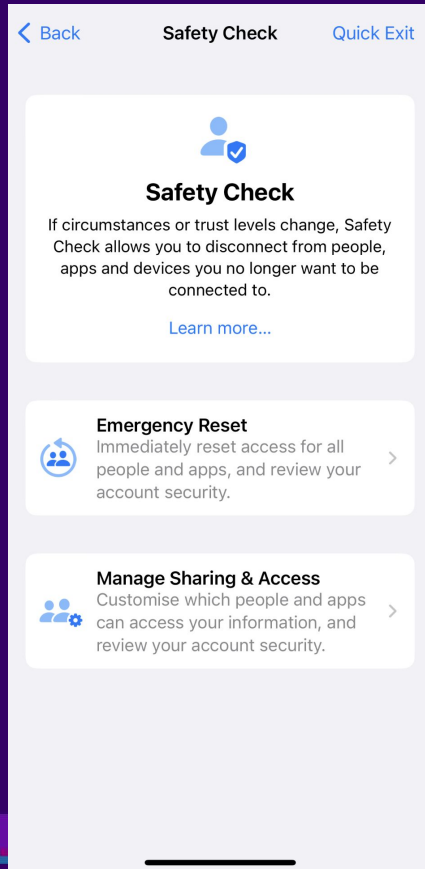
[You can also share your location in Messages](#) 😊

## Share with people

1. Open the Find My app and select the People tab.
2. Tap the Add button .



# iPhone : Safety Check





# Personal Safety User Guide

Keep yourself safe and your data private



# Need to secure the iCloud account!

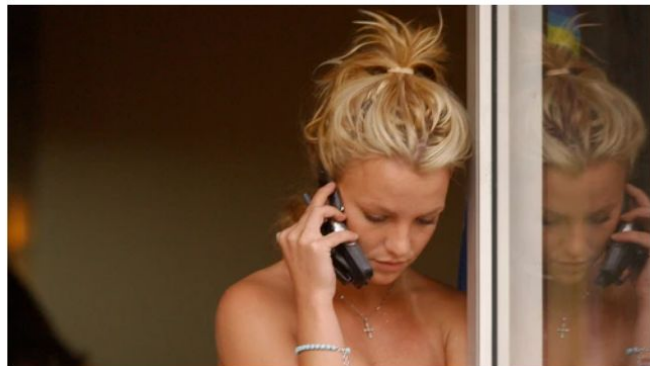
## How Jamie Spears Spied on Britney Spears Through iCloud

A security firm spied on Britney Spears through her iCloud account. Here's how to figure out if someone is doing that to you, and how to stop it.



By Lorenzo Franceschi-  
Bicchieri

October 1, 2021, 3:00pm [Share](#) [Tweet](#) [Snap](#)



# Stalkerware

## Spyzie Setup Guide for iPhone

Step by Step Guide to Setup Spyzie for iOS Devices.

Learn [how to track an Android phone](#) instead.

Spyzie's iOS tracker works like magic to track any iPhone or iPad remotely from any corner of the world. All that happens without the need to access the target iPhone or install any app on it. Here's how:

### Part One: Things You Will Need to Track an iPhone/iPad

#### **Spyzie Account with Subscription**

Allows you access to Spyzie's dashboard to use all of its features

#### **iCloud credentials of the target device**

With the iCloud credentials, you can track any iPhone or iPad without touching it.

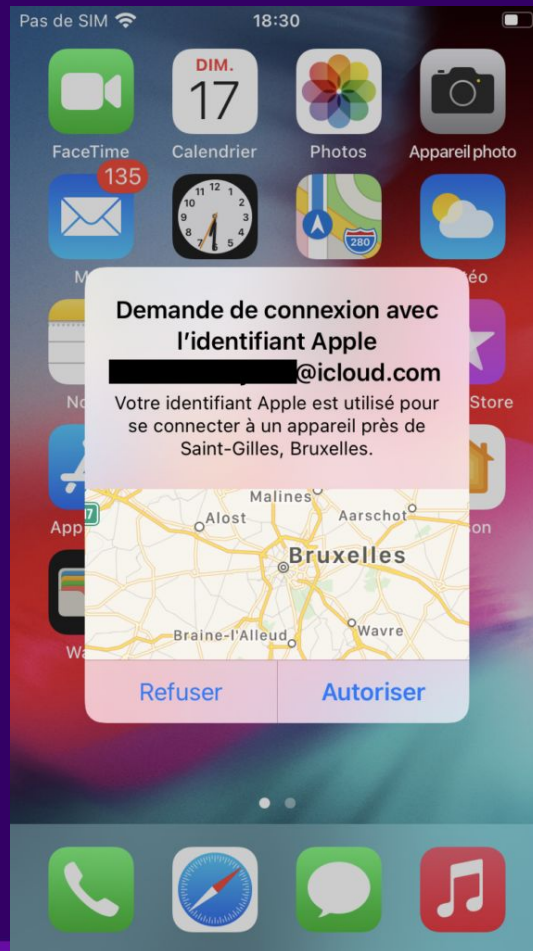
### Part Two: Steps to Spy on an iPhone in Secret

Read from  
<https://spyzie.io/how-to-track-someone-iphone-location.html>





# iCloud 2FA



# Some stalkerware

<https://xnspy.zohodesk.com/portal/en/kb/articles/iphone-in-stallation-guide-15-12-2014>

## iPhone Installation Guide



---

### — On this page

All done! Now you can start monitoring target iPhone or iPad remotely by logging into your XNSPY Control Panel online.

---

**Step 1:** Tap on Cydia icon on your iPhone home screen.

**Step 2:** Tap on Sources at the bottom of the screen.

**Step 3:** Tap Edit on the right side of the screen.

**Step 4:** Tap Add on the left side of the screen.

**Step 5:** You will see a prompt to enter the download URL.

**Step 6:** Enter the URL, <http://mydwnd.com> and tap Add Source.

**Step 7:** Wait for the phone to verify the URL.

**Step 8:** Wait for the system to Update Sources.

**Step 9:** As the download gets complete, tap Return to Cydia.

**Step 10:** Tap MonitoringApp repo icon in the list you see.

# Check the list of apps from the backup

- Do an iPhone backup with iTunes / libimobiledevice (see <https://docs.mvt.re/>)
- Analyze the backup with MVT
- List of apps is contained in Info.plist file

```
> mvt-ios check-backup -o results decrypted8
```

```
MVT - Mobile Verification Toolkit
```

```
https://mvt.re
```

```
Version: 2.3.0
```

```
Indicators updates checked recently, next automatic check in 12 hours
```

```
23:24:57 INFO
```

```
[mvt.ios.cmd_check_backup] Parsing STIX2 indicators file at path
```

```
/home/etienne/.local/share/mvt/indicators/raw.githubusercontent.com_AsoEchap_stalkerware-indicators._stalkerware.stix2
```

# Check the list of apps from the backup

```
{
  "name": "net.whatsapp.WhatsApp",
  "DeviceBasedVPP": false,
  "artistName": "WhatsApp Inc.",
  "bundleShortVersionString": "23.5.78",
  "bundleVersion": "456738319",
  "com.apple.iTunesStore.downloadInfo": {
    "accountInfo": {
      "AltDSID": "000519-08-e1320e5c-2188-4bac-b18b-120067e4fba5",
      "AppleID": "          @icloud.com",
      "DSPersonID": 16813981945,
      "DownloaderID": 0,
      "FamilyID": 0,
      "PurchaserID": 16813981945
    },
    "purchaseDate": "2019-08-29T23:26:54Z"
  },
  "gameCenterEnabled": false,
  "gameCenterEverEnabled": false,
  "genre": "Social Networking",
  "genreId": 6005,
  "hasMessagesExtension": false,
```



# Check the list of apps from the backup

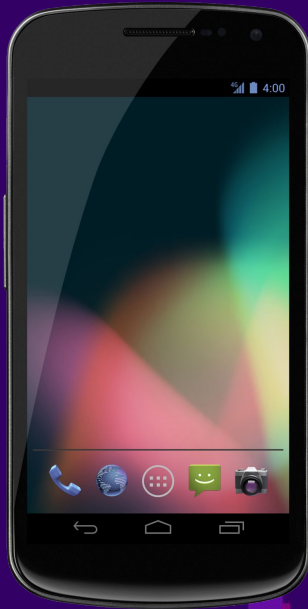
```
"itemName": "WhatsApp Messenger",
"kind": "software",
"launchProhibited": false,
"rating": {
  "label": "12+",
  "rank": 300
},
"redownload-params": "productType=C&price=0&salableAdamId=310633997&pricingParameters=SWUPD",
"releaseDate": "2009-05-04T02:43:49Z",
"s": 143442,
"sideLoadedDeviceBasedVPP": false,
"softwareVersionBundleId": "net.whatsapp.WhatsApp",
"softwareVersionExternalIdentifier": 855575888,
"sourceApp": "com.apple.AppStore",
"storeConort": "/|date=1567119600000&sf=143442&pgtp=Software&pgid=310633997&prpg=Software_310633997",
"subgenres": [],
"variantID": "1:iPhone9,3:13",
"isodate": "2019-08-29 21:26:54.000000",
"icon_sha256": "cb575af8eebf548dfce840c247c7b163e67fa49c73008c967bc45a060485ff73"
},
```

# Demo



# Android

# Android Devices



- Many embedded options to share sensitive information such as geolocation
- Need to secure the related Google account
- Android Stalkerware exist



# Sharing on Google Maps

On some creepy websites :

## How to track Someone on Google maps without them knowing

By Barbara Thompson ⓘ Updated June 30, 2023

As parents, you always worry about your kids and prefer being able to track their cell phone location to know where they are. You sometimes also want to track the activity of your partner or spouse.

There are many techniques that allows you to keep an eye on your child or loved one who may be out of communication. These methods also let you determine where they are, what they're doing, and whether any potential danger is involved.

Here are some most used methods to track Someone on Google maps without them knowing:

### Method 3: Using on Google Maps Location Sharing

How to track Someone using Location Sharing within the Google Maps app:

#### What is Location Sharing?

Location Sharing is an essential feature in Google Maps which enables users to share their GPS location with a specific contact. Friends or family mainly use it to share real-time Map of the locations.

#### What are things you need to Enable Location Sharing?

- Physical access to the Cell phone.
- You need a Pin or Password to unlock the phone device.
- Pre-installed Google Maps app.
- The user should be logged into their Google account.

#### How You can Enable Location Sharing in Google Maps

Here are steps for enabling Location Sharing using the Google Maps app:

**Step 1)** First, Open the Settings option and check that ensure location tracking features are enabled

**Step 2)** Open the Google Maps app Maps on the target Android phone.

**Step 3)** Tap your right corner with the user's profile picture

and select the Location Sharing option

**Step 4)** Tap On the "Share Location" option.

**Step 5)** Then, tap "Until you turn this off"

**Step 6)** Next, select your phone device

# Checking shared features

- No one place to check everything, need to check manually
- Geolocation: in Google maps or in the Google account “People and sharing tab”
- Pictures shared in Google Photos
- + Checks for apps with a lot of access

# Android Stalkerware

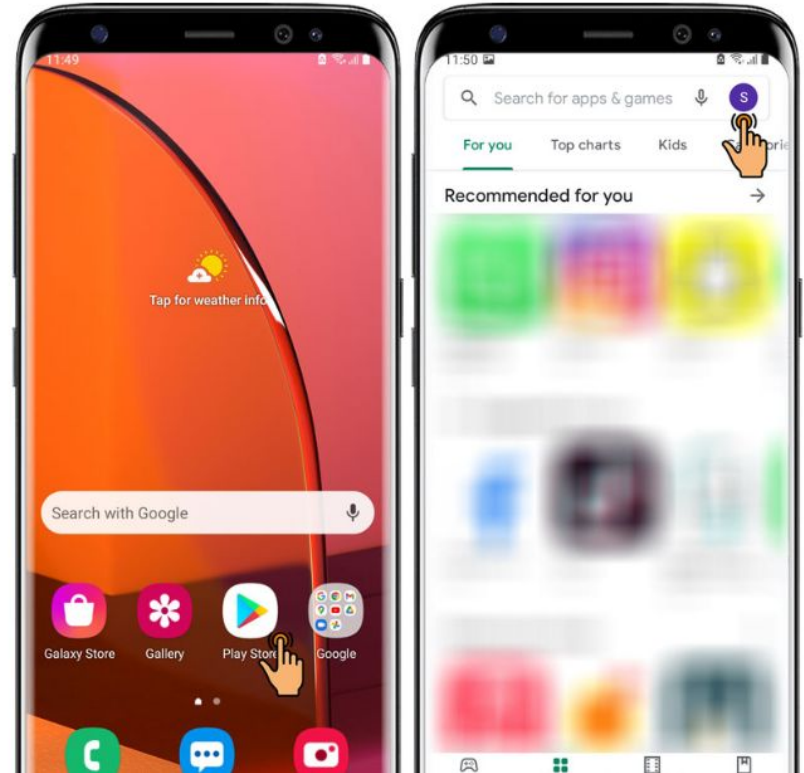
Let's see how it works

<https://support.hoverwatch.com/hc/en-us/articles/207595389-How-to-Install-Hoverwatch-for-Android>

## 1. Prepare the Device you Wish to Monitor

Prevent Android from asking questions about the activity of the monitoring program:

1. Tap the Google **Play Store** app.
2. Tap Menu > **Play Protect** > **Settings**.
3. Turn OFF **Scan apps with Play Protect**.



# Stalkerware Features

Category	Capabilities	mSPY	Mobile-tracker-free	Cleanguard	HoverWatch	Flexispy	Spyic	Spyhuman	TheTruthSpy	iKeyMonitor	Cerberus	Spy24	Spapp	Meuspy	Highstermobile
Basic Capabilities (§ 3.2)	Ambient Recording		★			★		★	★	★	★	★	★	★	
	Calendar	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Call Logs	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Clipboard		★						★	★		★			
	Contacts	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Info of Other Applications	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Location	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Network Info	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Phone Info	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	SMS or MMS	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Shared Media Files	★	★	★	★	★	★	★	★	★	★	★	★	★	★
Data Gathering (§ 3.3)	Invisible camera access		★	★	★	★		★	★	★	★	★	★	★	★
	Invisible microphone access		★	★	★	★		★	★	★		★	★	★	
	Accessing protected data	★	★	★	★	★	★	★	★	★	★	★	★	★	★
	Taking screenshots	★	★	★	★			★		★		★	★	★	
Hiding the App (§ 3.4)	Hiding app icon	★	★	★	★	★	★	★	★	★	★	★	★	★	
	Launching a hidden app		★		★	★	★	★	★	★	★	★	★	★	
	Hide from recents screen	★	★	★	★	★	★	★		★	★	★		★	★
Persistence (§ 3.5)	Obscuring the uninstallation process	★	★	★		★		★	★	★	★	★	★	★	
	Creating "diehard" services	★	★	★	★	★	★	★	★	★	★	★	★	★	★



Source: “No Privacy Among Spies” (PETS 2023)

# IOCs

<https://github.com/AssoEchap/stalkerware-indicators/>

jvoisin Updating generated indicator files and README		8c70e6f on May 31	🕒 717 commits
📁 generated	Updating generated indicator files and README	2 months ago	
📁 tools	Adds tools	6 months ago	
📁 vendors	Updating generated indicator files and README	7 months ago	
📄 .flake8	Flake8 checks in scripts	last year	
📄 .gitignore	Update generation script and add linter	last year	
📄 README.md	Updating generated indicator files and README	2 months ago	
📄 ioc.yaml	Updating generated indicator files and README	2 months ago	
📄 quad9_blocklist.txt	Update readme and blocklist	last year	
📄 rules.yar	Updating generated indicator files and README	6 months ago	
📄 samples.csv	Updating generated indicator files and README	2 months ago	

☰ README.md

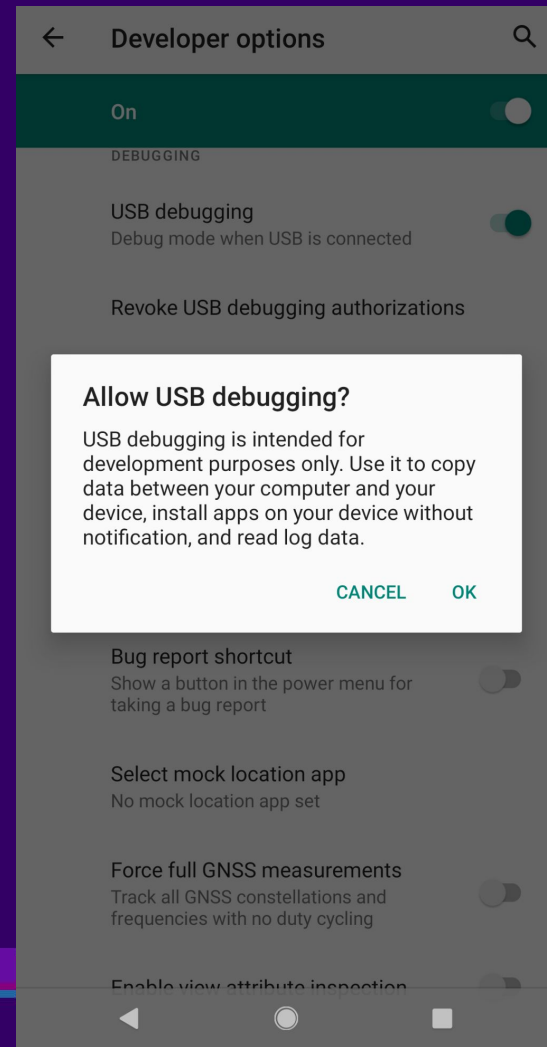
## Stalkerware Indicators of Compromise

Indicators of compromise (IOC) for Stalkerware and Watchware applications for Android and iOS

*Warning: these indicators are not providing a complete detection of stalkerware applications. They are based on research from a few people on their free time and many apps are likely missing. Use it carefully. No detection based*

# Checking with MVT

Allow USB debugging first





# Checking with MVT

```
> mvt-android check-adb -o test_mvt_adb
```

```
MVT - Mobile Verification Toolkit
```

```
https://mvt.re
```

```
Version: 2.3.0
```

```
Indicators updates checked recently, next automatic check in 12 hours
```

```
00:38:10 INFO [mvt.android.cmd_check_adb] Parsing STIX2 indicators file at path
/home/etienne/.local/share/mvt/indicators/raw.githubusercontent.com_AsoEchap_stalkerware-indicators_master_generated
_stalkerware.stix2
00:38:11 INFO [mvt.android.cmd_check_adb] Extracted 758 indicators for collection with name "TheTruthSpy"
INFO [mvt.android.cmd_check_adb] Extracted 178 indicators for collection with name "HelloSpy"
INFO [mvt.android.cmd_check_adb] Extracted 5 indicators for collection with name "SpyAdvice"
INFO [mvt.android.cmd_check_adb] Extracted 91 indicators for collection with name "Reptilicus"
INFO [mvt.android.cmd_check_adb] Extracted 21 indicators for collection with name "PhoneSheriff"
INFO [mvt.android.cmd_check_adb] Extracted 15 indicators for collection with name "OwnSpy"
INFO [mvt.android.cmd_check_adb] Extracted 186 indicators for collection with name "Cocospy"
INFO [mvt.android.cmd_check_adb] Extracted 8 indicators for collection with name "VIPTrack"
INFO [mvt.android.cmd_check_adb] Extracted 74 indicators for collection with name "EasyLogger"
INFO [mvt.android.cmd_check_adb] Extracted 106 indicators for collection with name "Hoverwatch"
INFO [mvt.android.cmd_check_adb] Extracted 28 indicators for collection with name "LetMeSpy"
INFO [mvt.android.cmd_check_adb] Extracted 41 indicators for collection with name "Snoopza"
INFO [mvt.android.cmd_check_adb] Extracted 31 indicators for collection with name "TrackMyPhones"
```

```
00:39:08 INFO [mvt.android.modules.adb.settings] Running module Settings...
WARNING [mvt.android.modules.adb.settings] Found suspicious setting "samsung_errorlog_agree = 0" (disabled sharing of crash
logs with manufacturer)
WARNING [mvt.android.modules.adb.settings] Found suspicious setting "install_non_market_apps = 1" (enabled installation of
non Google Play apps)
WARNING [mvt.android.modules.adb.settings] Found suspicious setting "package_verifier_user_consent = -1" (disabled Google
Play Protect)
```

```
00:39:14 INFO [mvt.android.modules.adb.dumpsys_accessibility] Running module DumpsysAccessibility...
INFO [mvt.android.modules.adb.dumpsys_accessibility] Found installed accessibility service
"com.android.settings/com.samsung.android.settings.development.gpuwatch.GPUWatchInterceptor"
INFO [mvt.android.modules.adb.dumpsys_accessibility] Found installed accessibility service
"com.samsung.accessibility/.universalswitch.UniversalSwitchService"
INFO [mvt.android.modules.adb.dumpsys_accessibility] Found installed accessibility service
"com.samsung.accessibility/com.samsung.android.app.talkback.TalkBackService"
INFO [mvt.android.modules.adb.dumpsys_accessibility] Found installed accessibility service
"com.sec.android.app.camera/com.samsung.android.glview.AccessibilityGestureHandler"
INFO [mvt.android.modules.adb.dumpsys_accessibility] Found installed accessibility service
"com.dy.spyzie.v4/com.dy.services.NeNotificationService02"
INFO [mvt.android.modules.adb.dumpsys_accessibility] Found installed accessibility service
"com.kms.free/com.kaspersky.components.accessibility.KasperskyAccessibility"
INFO [mvt.android.modules.adb.dumpsys_accessibility] Identified a total of 6 accessibility services
WARNING [mvt.android.modules.adb.dumpsys_accessibility] Found a known suspicious app with ID "com.dy.spyzie.v4" matching
indicators from "Cocospy"
```

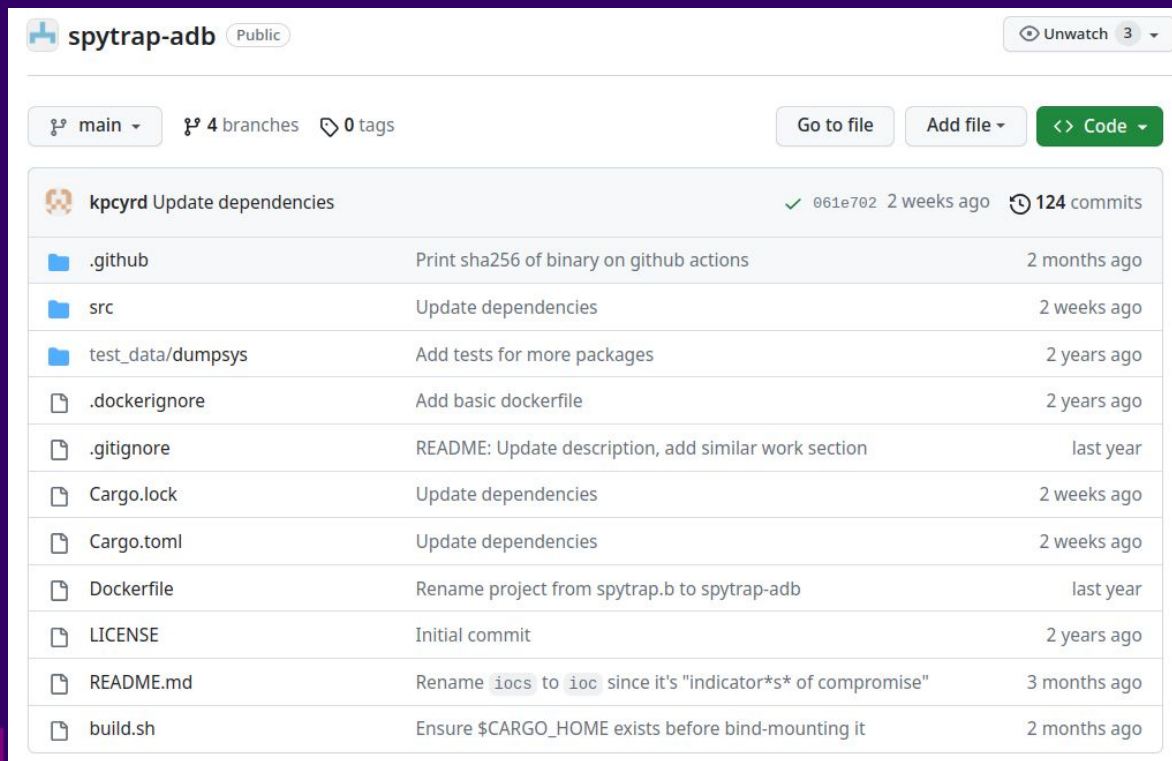
```
00:43:42 INFO [mvt.android.modules.adb.packages] Extracted at total of 348 installed package names
WARNING [mvt.android.modules.adb.packages] Found a known suspicious app with ID "com.dy.spyzie.v4" matching indicators from
"Cocospy"
INFO [mvt.android.modules.adb.logcat] Running module Logcat...
00:43:44 INFO [mvt.android.modules.adb.logcat] Current logcat logs stored at test_mvt_adb/logcat.txt
INFO [mvt.android.modules.adb.logcat] Logcat logs prior to last reboot stored at test_mvt_adb/logcat_last.txt
```



# Demo



# spytrap-adb



spytrap-adb Public

Unwatch 3

main 4 branches 0 tags

Go to file Add file > Code >

kpcyrd Update dependencies ✓ 061e702 2 weeks ago 124 commits

github	Print sha256 of binary on github actions	2 months ago
src	Update dependencies	2 weeks ago
test_data/dumpsys	Add tests for more packages	2 years ago
.dockerignore	Add basic dockerfile	2 years ago
.gitignore	README: Update description, add similar work section	last year
Cargo.lock	Update dependencies	2 weeks ago
Cargo.toml	Update dependencies	2 weeks ago
Dockerfile	Rename project from spytrap.b to spytrap-adb	last year
LICENSE	Initial commit	2 years ago
README.md	Rename <code>iocs</code> to <code>ioc</code> since it's "indicator*s* of compromise"	3 months ago
build.sh	Ensure \$CARGO_HOME exists before bind-mounting it	2 months ago

<https://github.com/spytrap-org/spytrap-adb>



# Our Android Checklist

- Check Android account (and secure it)
- Check shared geolocation in Google Maps
- Check shared photo albums
- Check apps that are device admin
- Look for stalkerware
  - Check if Play Protect is disabled
  - Check if the phone is rooted with Root Verifier
  - If needed: check with MVT / antivirus

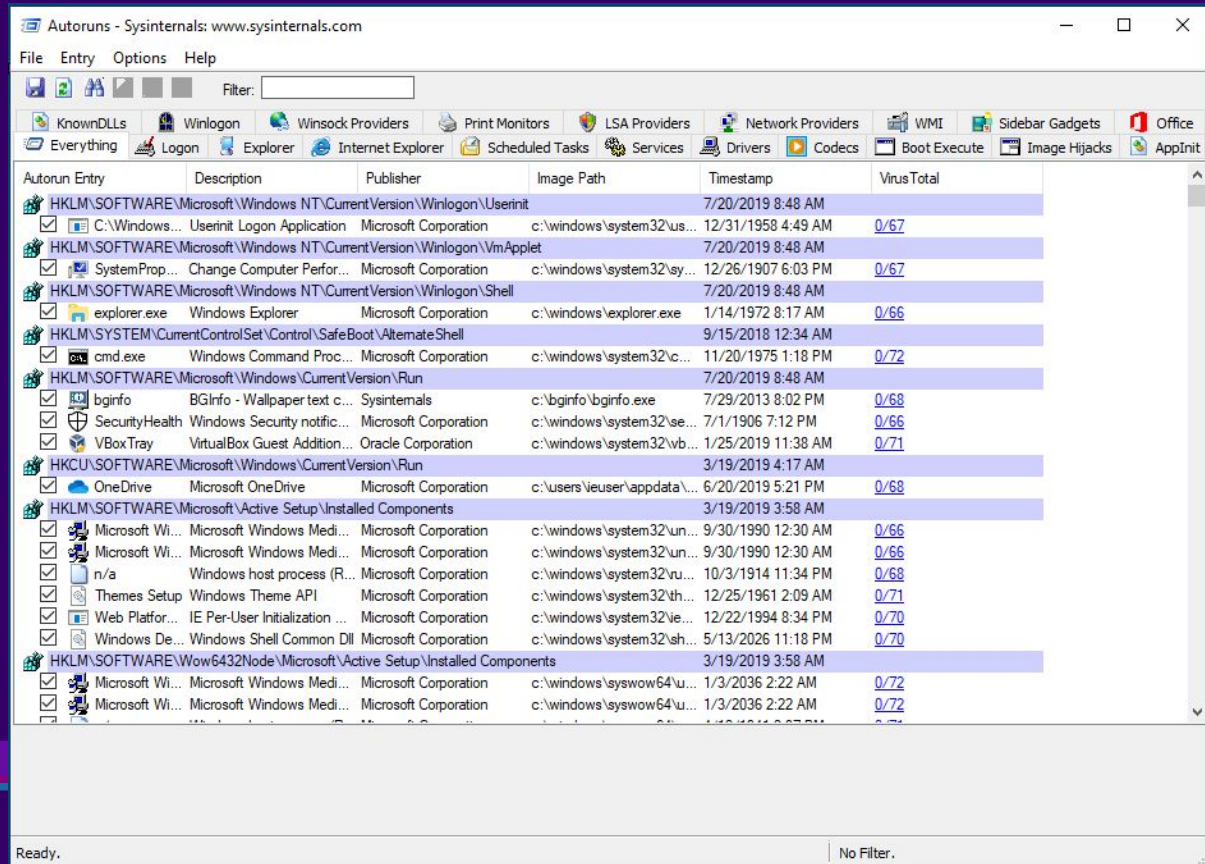
# Computers

# Computers



- Several stalkerware have a Windows version
- AFAIK not possible to share geolocation through standard interface
- Some simple tools to look for suspicious programs

# Autoruns



# Running Processes

Process Explorer - Sysinternals: www.sysinternals.com

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
Registry		1,792 K	71,428 K	68			
System Idle Process	62.77	56 K	8 K	0			
System	2.52	192 K	156 K	4			
Interrupts	18.50	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		488 K	1,020 K	288			
Memory Compression		244 K	36,276 K	1500			
csrss.exe		1,620 K	5,224 K	384			
wininit.exe		1,316 K	6,084 K	452			
services.exe		4,836 K	8,640 K	544			
svchost.exe		908 K	3,592 K	652	Host Process for Windows S...	Microsoft Corporation	0/71
svchost.exe		11,656 K	29,484 K	740	Host Process for Windows S...	Microsoft Corporation	0/71
ShellExperienceHost.exe	Susp...	27,488 K	79,956 K	4976	Windows Shell Experience H...	Microsoft Corporation	0/71
SearchUI.exe	Susp...	90,696 K	163,976 K	3988	Search and Cortana applicati...	Microsoft Corporation	0/64
RuntimeBroker.exe		11,640 K	35,300 K	3300	Runtime Broker	Microsoft Corporation	0/71
ApplicationFrameHost.exe		14,868 K	33,640 K	4652	Application Frame Host	Microsoft Corporation	0/72
SkypeApp.exe	Susp...	12,844 K	6,516 K	5264	SkypeApp	Microsoft Corporation	0/65
YourPhone.exe	Susp...	10,060 K	5,212 K	5272			0/66
SkypeBackgroundHost.exe	Susp...	1,988 K	1,220 K	5288	Microsoft Skype	Microsoft Corporation	0/71
RuntimeBroker.exe		3,052 K	14,216 K	5412	Runtime Broker	Microsoft Corporation	0/71
MicrosoftEdgeSH.exe	Susp...	4,084 K	13,928 K	8860	Microsoft Edge Web Platform	Microsoft Corporation	0/20
RuntimeBroker.exe		2,628 K	12,680 K	5744	Runtime Broker	Microsoft Corporation	0/71
RuntimeBroker.exe		6,176 K	25,260 K	5872	Runtime Broker	Microsoft Corporation	0/71
RuntimeBroker.exe		2,220 K	10,720 K	6036	Runtime Broker	Microsoft Corporation	0/71
RuntimeBroker.exe		2,136 K	8,624 K	6076	Runtime Broker	Microsoft Corporation	0/71
smartscreen.exe		12,172 K	25,476 K	100	Windows Defender SmartScr...	Microsoft Corporation	0/66
WindowsInternal.Com...	Susp...	14,388 K	42,292 K	6424	WindowsInternal.Composabl...	Microsoft Corporation	0/65
WinStore.App.exe	Susp...	15,172 K	324 K	2260	Store	Microsoft Corporation	0/66
RuntimeBroker.exe		1,488 K	6,800 K	5580	Runtime Broker	Microsoft Corporation	0/71
dihost.exe		3,276 K	11,076 K	2768	COM Surrogate	Microsoft Corporation	0/68
WmiPrvSE.exe		2,568 K	8,180 K	2960			
Microsoft.Photos.exe	Susp...	47,240 K	472 K	5160			0/72
RuntimeBroker.exe		8,832 K	27,960 K	1932	Runtime Broker	Microsoft Corporation	0/71
MicrosoftEdge.exe	Susp...	21,640 K	62,872 K	8716	Microsoft Edge	Microsoft Corporation	0/68
browser_broker.exe		1,600 K	8,100 K	8608	Browser_Broker	Microsoft Corporation	0/67
MicrosoftEdgeCP.exe	Susp...	19,508 K	47,724 K	8780	Microsoft Edge Content Proc...	Microsoft Corporation	0/70
SystemSettings.exe	Susp...	15,172 K	572 K	8404	Settings	Microsoft Corporation	0/69
RuntimeBroker.exe	1.66	8,044 K	28,424 K	8028	Runtime Broker	Microsoft Corporation	0/71
WmiPrvSE.exe		3,116 K	9,588 K	1964			

CPU Usage: 37.23% Commit Charge: 34.91% Processes: 140 Physical Usage: 46.39%



# Review network connections

TCPView - Sysinternals: www.sysinternals.com

File Options Process View Help

Process	PID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
[System Proc...	0	TCP	msedgewin10.phub.net.cable.rogers.com	57458	4.27.248.254	http	TIME_WAIT
[System Proc...	0	TCP	msedgewin10.phub.net.cable.rogers.com	57473	64.4.54.18	https	TIME_WAIT
dasHost.exe	1016	UDP	MSEDGEWIN10	ws-discovery	*	*	
dasHost.exe	1016	UDP	MSEDGEWIN10	ws-discovery	*	*	
dasHost.exe	1016	UDP	MSEDGEWIN10	50239	*	*	
dasHost.exe	1016	UDPv6	msedgewin10	3702	*	*	
dasHost.exe	1016	UDPv6	msedgewin10	3702	*	*	
dasHost.exe	1016	UDPv6	msedgewin10	50240	*	*	
lsass.exe	552	TCP	MSEDGEWIN10	49669	MSEDGEWIN10	0	LISTEN
lsass.exe	552	TCPv6	msedgewin10	49669	msedgewin10	0	LISTEN
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57202	209.148.170.136	https	CLOSE
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57203	13.107.21.200	https	ESTAB
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57204	104.43.203.255	https	ESTAB
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57205	104.43.203.255	https	ESTAB
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57206	104.43.203.255	https	ESTAB
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57207	a-0001.a-msedge...	https	ESTAB
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57208	104.43.203.255	https	ESTAB
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57209	104.43.203.255	https	ESTAB
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57210	104.43.203.255	https	ESTAB
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57217	chi.outbrain.com	https	CLOSE
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57218	a23-213-190-147...	https	CLOSE
MicrosoftEdg...	8780	TCP	msedgewin10.phub.net.cable.rogers.com	57228	72.21.91.29	http	CLOSE
SearchUI.exe	3988	TCP	msedgewin10.phub.net.cable.rogers.com	57219	13.107.21.200	https	ESTAB
SearchUI.exe	3988	TCP	msedgewin10.phub.net.cable.rogers.com	57220	13.107.21.200	https	ESTAB
SearchUI.exe	3988	TCP	msedgewin10.phub.net.cable.rogers.com	57225	13.107.18.254	https	ESTAB
services.exe	544	TCP	MSEDGEWIN10	49668	MSEDGEWIN10	0	LISTEN
services.exe	544	TCPv6	msedgewin10	49668	msedgewin10	0	LISTEN
spoolsv.exe	1880	TCP	MSEDGEWIN10	49667	MSEDGEWIN10	0	LISTEN
spoolsv.exe	1880	TCPv6	msedgewin10	49667	msedgewin10	0	LISTEN
svchost.exe	772	TCP	MSEDGEWIN10	epmap	MSEDGEWIN10	0	LISTEN
svchost.exe	2412	TCP	MSEDGEWIN10	5040	MSEDGEWIN10	0	LISTEN
svchost.exe	1036	TCP	MSEDGEWIN10	49665	MSEDGEWIN10	0	LISTEN

Endpoints: 87 Established: 21 Listening: 26 Time Wait: 2 Close Wait: 4



# Conclusion

# Thanks

- Echap : <https://echap.eu.org/>
- IPV Tech bibliography : <https://ipvtechbib.randhome.io/>
- Email : [etienne@maynier.eu](mailto:etienne@maynier.eu)

