



TinyCheck®



How can technology assist victims of digital stalking?

Stephan Gerling
Senior Security Researcher
ICS-CERT , Kaspersky

Bullet2022

ABOUT KASPERSKY



>400,000,000

users worldwide are protected by our technologies

kaspersky

2

Founded in 1997 and present on 6 continents in almost 200 countries and territories

Provides innovative IT security solutions and services for business and consumers

Works closely together with public and private stakeholders to ensure people's security and safety.



1. Basics: what is stalkerware
2. Background: what Kaspersky is doing
3. Overview: tools & tactics to detect stalkerware
4. Deep dive: TinyCheck
5. Q&A



1. **Basics: what is stalkerware**
2. Background: what Kaspersky is doing
3. Overview: tools & tactics to detect stalkerware
4. Deep dive: TinyCheck
5. Q&A



WHAT IS STALKERWARE?

5

Stalkerware enables a perpetrator to secretly spy on another person's private life via a smart device.

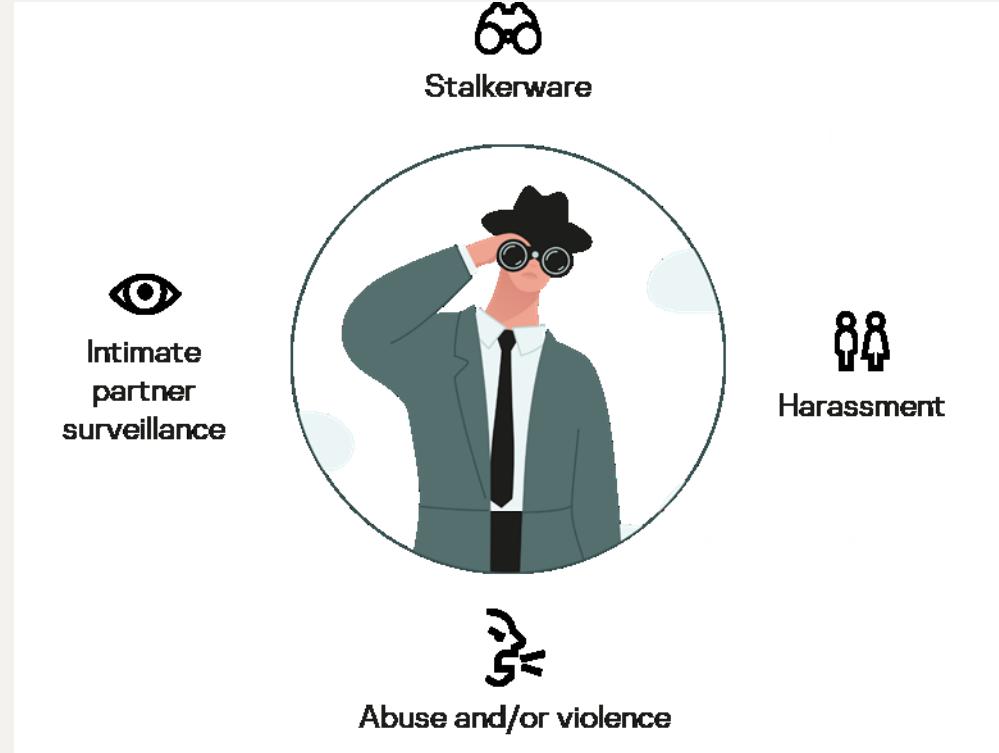


The software is commercially available and has access to an array of personal data, such as:

- device location,
- browser history,
- text messages,
- social media chats,
- photos and more.

THE CONTINUUM BETWEEN ONLINE & OFFLINE VIOLENCE

6



In Europe, **70% of women** who have experienced cyber stalking, have also experienced at least one form of physical or/and sexual violence from an intimate partner.

Source: EIGE (2017). Cyber violence against women and girls

32,694

mobile users were by
stalkerware globally in
2021*

4,236

in Europe

30%

People who see no issue
with monitoring their
partner under certain
circumstances

The Coalition Against
Stalkerware estimates
that stalkerware usage
likely exceeds **one million**
instances per year.

HOW DIFFICULT IS IT TO FIND IT?

8



The Best Phone Tracker for Parental Control

#1 CHOICE IN ITALY*

Know more. Worry less. That's the power that lets you find out what they're up to online. And they won't even know you're tracking them.

TRY NOW

view details



CELL-PHONE TRACKER, THAT:

Records calls, SMS, audio, contacts

Provides precise location

Monitors Facebook, WhatsApp, Snapchat, Instagram

Reveals all internet activity

1 month
FULL pack

from
€41,99
per month

Track 1 Device

All monitoring functions are available

- Facebook Spy App
- WhatsApp Spy App
- Instagram Spy App
- Keylogger
- GPS Location Tracker

12 months
FULL pack

from
€9,91
per month

Track 1 Device

All monitoring functions are available

- Facebook Spy App
- WhatsApp Spy App
- Instagram Spy App
- Keylogger
- GPS Location Tracker

3 months
FULL pack

from
€23,56
per month

Track 1 Device

All monitoring functions are available

- Facebook Spy App
- WhatsApp Spy App
- Instagram Spy App
- Keylogger
- GPS Location Tracker

WHAT CAN AN ABUSER MONITOR USING STALKERWARE?

This varies between apps, but it may include:

- Real-time location (through GPS)
- Text messages (including WhatsApp, etc.)
- Social media conversations
- Phone call recordings and call logs
- Live video and voice recordings
- Browser history

Sometimes allows abuser to send messages from victim's device



Call Data and Recording

Our android spy records all conversations on the device keeping a detailed log. You will be able to see both the contact's name and the duration of the conversation.



Stay invisible

Probably, the spy app's biggest advantage is its ability to remain completely hidden. Unless the owner of the phone knows exactly what to look for he or she won't be able to see the secret app. This also applies to instances when the device is unrooted.



Monitoring WhatsApp, Facebook, Viber, SMS and MMS

This spy mobile app stores all text messages, SMS and multimedia messages (MMS).



Front Camera Photos

This app can spy camera. You can view unlocked snapshots in the Reports section of your back-office



Location

The application allows you to track the location of the mobile with the Cell Spy installed. You don't need to worry about the battery draining quickly as the app's energy efficient algorithms will prevent this from happening.



Internet activity

The software saves all internet activity of the device it is installed on. This allows you to see the websites the owner of the mobile has visited.

PERPETRATOR'S PERSPECTIVE – REMOTE CONTROL

10

The screenshot shows a web-based remote control interface for a Samsung Galaxy S10. The left sidebar lists various monitoring features: Demo's Galaxy S10, Dashboard, Phone Files, Call Logs, Messages, Contacts, Browser History, Photos, Video Preview, App Activities, Keylogger (which is selected), Calendar, Location Tracking, Social Apps, Remote Control, and Data Export. The main area displays a list of keylogger entries for the 'Keylogger' feature. Each entry includes the app icon, app name, and the captured text. The interface also features a sync button, an update timestamp, a search bar, and a monitor now button.

| App | Captured Text | Date |
|------------|-------------------------------|---------------------|
| Chrome | tips for a first date | 2021-01-25 18:30:46 |
| Memo | Alisa's party at 6pm tonight. | 2021-01-25 15:30:46 |
| AnyConnect | | |
| Chrome | | |
| Memo | | |
| AnyConnect | | |
| Chrome | vruv@si.com | 2021-01-25 12:05:00 |
| Memo | | |
| AnyConnect | | |

PERPETRATOR'S PERSPECTIVE – REMOTE CONTROL

Dashboard > Samsung SM-G930F (IT-SA_Demo)

SMS History

Display last 10 messages

| Type | Person | To/From | Content |
|------|--------|-------------|---|
| ↓ | - | TamamFin-AD | ، ويسري هذا العرض حتى 30 نوفمبر 2022 احصل على تمويل الشخصي الآن من تمام بموافقة فورية وبدون مستندات! حمل التطبيق الآن documents ! Download the app now https://app.tamam.life/jdF1 APR starts at 8.83%, and this offer is valid until November 30, |
| ↓ | - | ZainKSA | Dear Customer, We wish you a pleasant stay in Germany Now, you can subscribe, re-subscribe, manage roaming services, read offer code to 959 from the following: 1 day 1GB for 59 SAR, send RD1 3 days 2GB for 99 SAR, send RD3 7 days 10GB for 199 SAR with 100 minutes for 179 SAR, send DV3 7 days 12GB with 150 minutes for 299 SAR, send DV7 15 days 18GB with 200 minutes 50 SAR send V50 7 days 120 minutes for 100 SAR send V120 30 days 200 minutes for 150 SAR send V200 have a Zain day ! |
| ↓ | - | Tawakkalna | Dear STEPHAN Please use the verification code 3091 to login to Tawakkalna |

More Functions

- Browser History
- Browser Bookmarks
- Key Logger new
- Clipboard logs new
- Facebook Messages
- Messenger Lite new
- Documents new
- Wifi Networks new
- Sim Changes new

new

Model: SM-G930F
OS: Android

Export ▾ Table View Google Maps

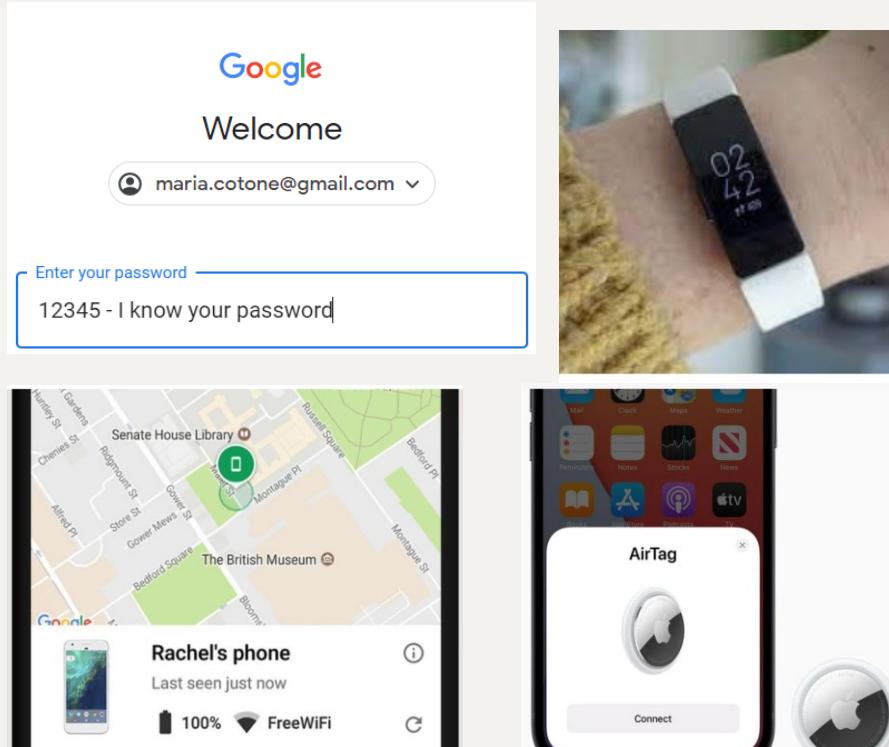
| | |
|--|--------|
| Browser History | \$1.99 |
| Browser Bookmarks | \$0.99 |
| Key Logger new | \$3.99 |
| Clipboard logs new | \$1.99 |
| Facebook Messages | \$3.99 |
| Messenger Lite new | \$3.99 |
| Documents new | \$1.99 |
| Wifi Networks new | \$0.99 |
| Sim Changes new | \$0.99 |
| Events Calendar | \$0.99 |
| Audio Files | \$0.99 |
| WhatsApp | \$3.99 |
| WhatsApp Calls new | \$2.99 |
| Viber Calls | \$1.99 |
| Viber Messages | \$1.99 |
| Skype Messages | \$2.99 |
| Skype Calls | \$2.99 |

REMEMBER! IT'S NOT JUST STALKERWARE!

12

Other ways of tech abuse (examples):

- Shared social media and/or email password
- Fitness trackers / sportwatches
- Find-my-device apps
- Regular access to a phone
- Tags (AirTag/Tile)



1. Basics: what is stalkerware
2. **Background: what Kaspersky is doing**
3. Overview: tools & tactics to detect stalkerware
4. Deep dive: TinyCheck
5. Q&A



Co-founder and driver of the Coalition Against Stalkerware



Project partner in the EU project „DeStalk“



Training by Kaspersky with INTERPOL



State of Stalkerware Report



The State of
Stalkerware
in 2021

TinyCheck®

CO-FOUNDER OF AN INTERNATIONAL ALLIANCE

15



**Coalition
Against
Stalkerware**

Founded in 2019 – today 40+ members from all over the world



Member organizations come from various fields:

1. Domestic violence victim support and perpetrator organizations
2. Digital rights advocacy
3. IT security companies
4. Academia/Security Research
5. Law enforcement



Supported by the Rights, Equality and Citizenship Programme of the European Union (2014-2020)

Project partners



Key output is an e-learning course on cyberviolence and stalkerware available in 5 languages. It is for professionals working in public authorities, victim support services and perpetrator programmes.

TRAINING FOR LAW ENFORCEMENT OFFICERS

17

Stalkerware

A basic technical training
October 25, 2021

WESNET
kaspersky

Welcoming words

Pei Ling Lee
Acting Assistant Director,
Cyber Strategy and Capabilities
Development

INTERPOL

INTERPOL_Cyber ✅ @INTERPOL_Cyber · 28. Okt.

Recognizing the rising threat of #stalkerware, INTERPOL provided an online training — developed by Coalition Against Stalkerware & @Kaspersky — to over 210 law enforcement officers worldwide to enhance their ability to investigate digital stalking 📱💻👀

 kaspersky.com
Kaspersky teams up with INTERPOL and civil socie...
In light of October being, in various countries across the globe, the month to raise awareness of ...

3 29 48



The State of
Stalkerware
in 2021

COALITION AGAINST
STALKERWARE



The State of
Stalkerware
in 2020

COALITION AGAINST
STALKERWARE



The State of
Stalkerware
in 2019

COALITION AGAINST
STALKERWARE

TinyCheck

kaspersky

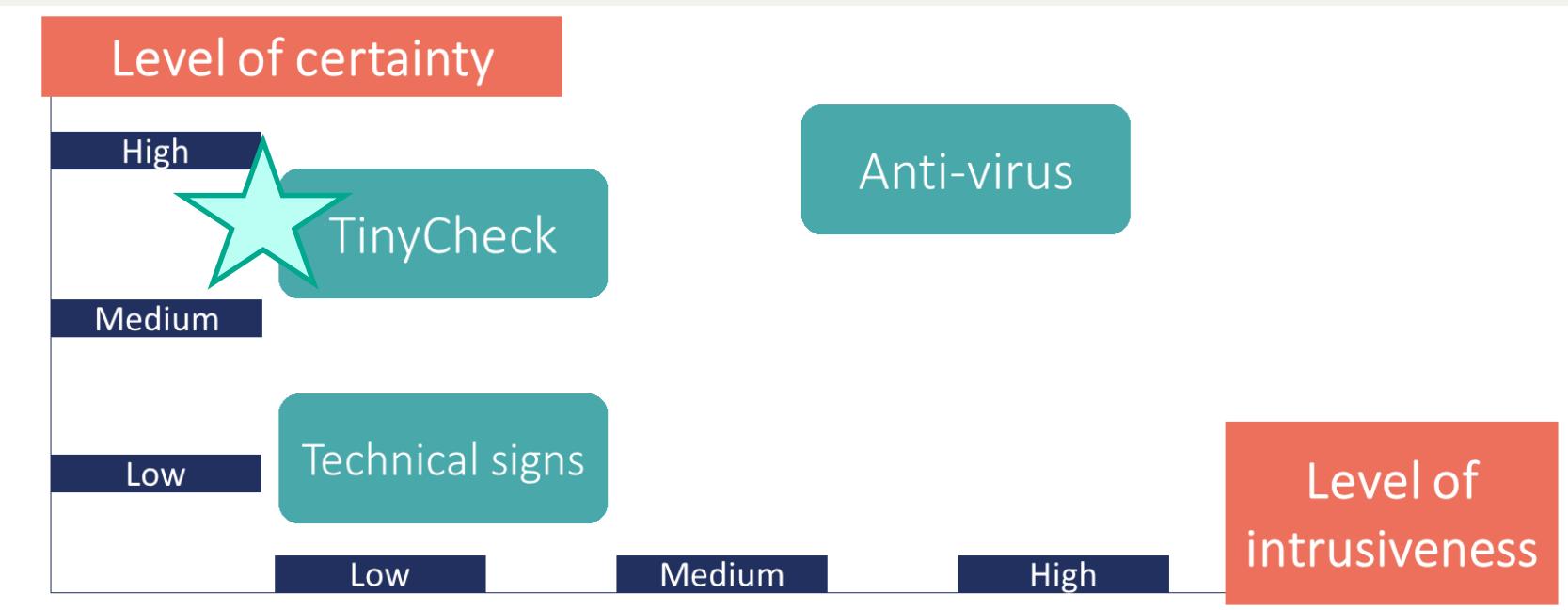
Every year Kaspersky analyzes the use of stalkerware around the world to better understand the threat it poses.

We partner with stakeholders across public and private sectors to raise awareness and find solutions to best tackle this important issue.

Find all State of the Stalkerware Reports & more here
<https://kas.pr/antistalkerware>

1. Basics: what is stalkerware
2. Background: what Kaspersky is doing
3. Overview: tools & tactics to detect stalkerware
4. Deep dive: TinyCheck
5. Q&A



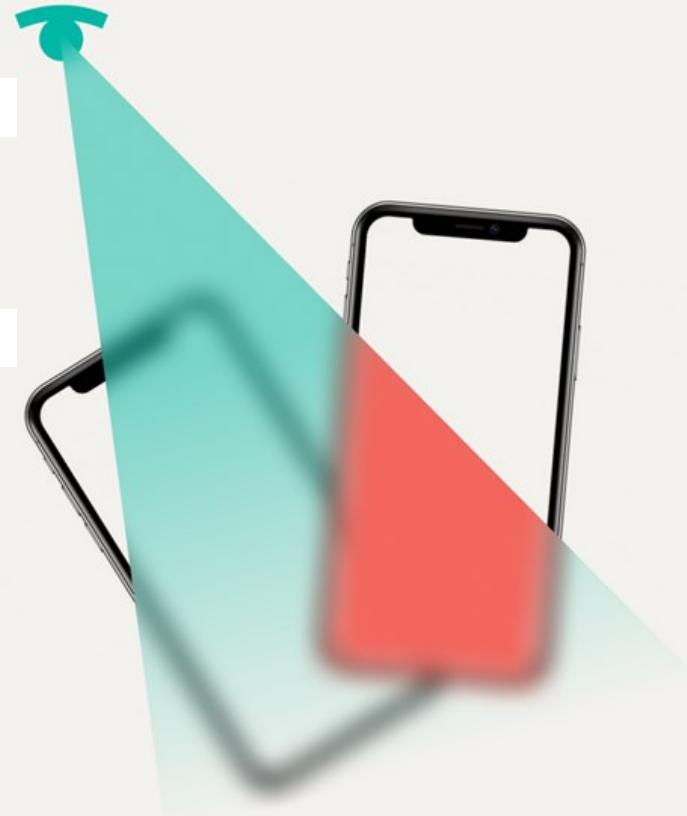


1. Basics: what is stalkerware
2. Background: what Kaspersky is doing
3. Overview: tools & tactics to detect stalkerware
4. Deep dive: **TinyCheck**
5. Q&A



INTRODUCING TINYCHECK

The goal of TinyCheck
is to help **non-profit**
organizations
supporting victims of
domestic violence and
protect their privacy.



TinyCheck®

22

1

Perpetrator will not be informed

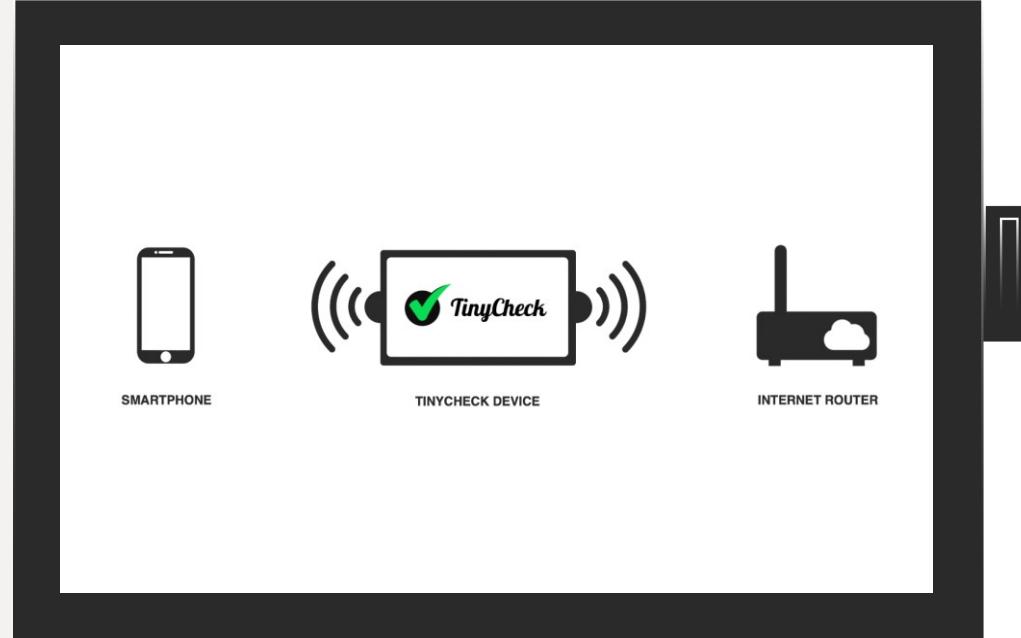
2

Check of all devices possible

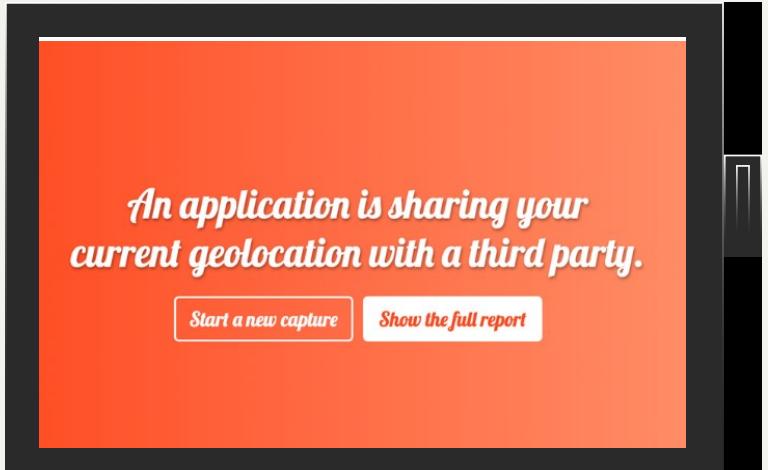
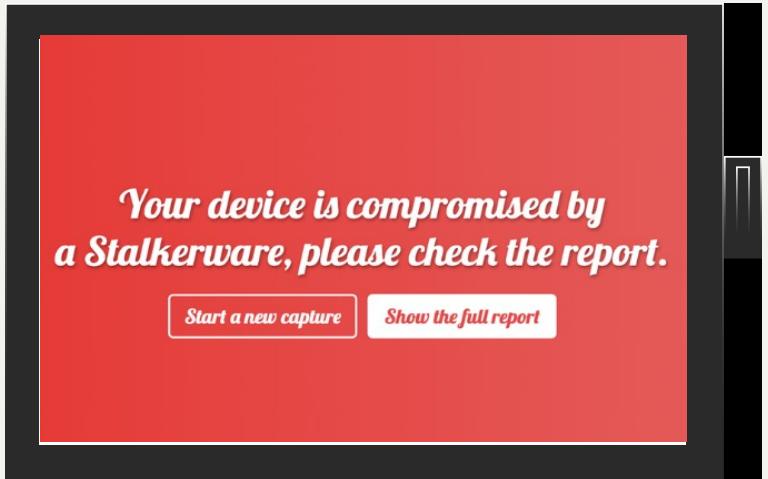
3

Affordable, open-source tool

How it works



Quick verdict



Detailed report

Report for iPhone
IP Address: 192.168.100.2
Mac Address: b8:53:ac:a3:10:a9

MODERATE IOC-03

A DNS request have been done to dmp.starbolt.io which is tagged as TRACKER.

The domain name dmp.starbolt.io seen in the capture has been explicitly tagged as a Tracker. This indicates that one of the active apps is geo-tracking your moves.

LOW PROTO-03

HTTP communications have been done to the host dmp.starbolt.io

Do the interception in a public place (library, restaurant...) or common place (office, home...);

Intercept the network communications of the device for at least 10 minutes;

Interact with the analysed device during the interception (reboot it, take a photo, send a message...);

SPYGUARD 1.0

- MANAGE DEVICE
 - Device config
 - Analysis engine
 - Network config
 - Manage database
- MANAGE IOCS
 - Manage IOCs
 - Search IOCs
- MANAGE WHITELIST
 - Manage elements
 - Search elements
- EXTERNAL SOURCES
 - Watchers Instances
 - MISP Instances
 - MISP Instances

Manage watchers instances

Add watcher Existing watchers

| Type | Name | Status | Action |
|-----------|------------------------------|----------|--------|
| IOCS | SpyGuard IOCs repository | ✓ ONLINE | Delete |
| IOCS | ECHAP stalkerware repository | ✓ ONLINE | Delete |
| WHITELIST | SpyGuard whitelist | ✓ ONLINE | Delete |

WHAT DO YOU NEED TO BUILD TINYCHECK?

28



We are currently working with WESNET, the Australian peak body for Women's Domestic and Family Violence Services, to further test and develop TinyCheck to fit it better to the needs of workers in victim support servi



1. Collaborate on TinyCheck source code on GitHub
<https://github.com/KasperskyLab/TinyCheck>



2. Support the Coalition Against Stalkerware



3. Educate yourself and others on the issue of tech facilitated abuse and how you might help to combat digital violence.





Félix Aimé
@felixaime

...

31

Two years ago, I published #TinyCheck. An application to passively detect signs of compromise by examining network flows. Today, I'm releasing a forked and enhanced version of it, dubbed #SpyGuard. Some evolutions in this thread 🚀(1/7)

[Tweet übersetzen](#)



[github.com
SpyGuard - Overview](https://github.com/SpyGuard)

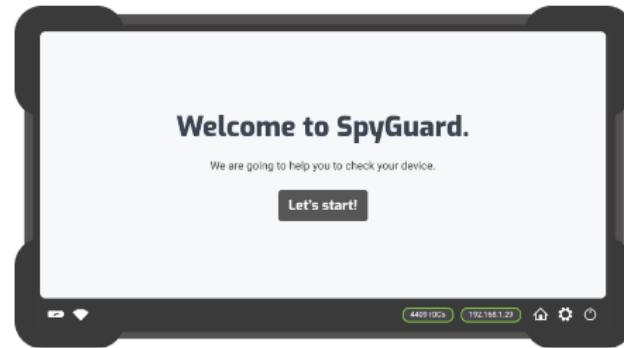
SpyGuard has one repository available. Follow their code on GitHub.

2:45 nachm. · 7. Nov. 2022 · Twitter Web App

<https://github.com/SpyGuard>

SPYGUARD

INTERCEPT DETECT REPORT



SPYGUARD

MANAGE DEVICE

MANAGE IOCS

MANAGE WHITELIST

EXTERNAL SOURCES

Getting started

SpyGuard is a forked and enhanced version of TinyCheck, an application developed by Kaspersky. SpyGuard's main objective is to detect signs of compromise by monitoring network flows transmitted by a device.

As it uses WiFi, SpyGuard can be used against a wide variety of devices, such as smartphones, laptops, IOTs or workstations. To do its job, the analysis engine of SpyGuard is using Indicators of Compromise (IOCs) and anomaly detection and is supported by Suricata.

This backend lets you configure your SpyGuard instance. You can push some IOCs for detection and whitelist elements which can be seen during legit communications in order to prevent false positives.

-

<http://localhost:8000>
<http://localhost:8443>

Frontend
Backend



Supported by the Rights, Equality
and Citizenship Programme of the
European Union (2014–2020)



DeStalk European replication event

"Tackling the digital dimension of violence against women"

Friday December 16

9:30 - 12:30 CET

Virtual event

Register at <https://tinyurl.com/destalkregistration>
Or scan the QR code



Registration link



TinyCheck®



Let's talk!

info@tiny-check.com

Any questions?

Check out

www.tiny-check.com