Osservatorio Nessuno

Bugbane: Simplifying consensual Android forensics

FOSDEM 2026

Osservatorio Nessuno OdV - Intro

Osservatorio Nessuno OdV (`osservatorionessuno.org`) is an Italian non-profit, run entirely by volunteers, dedicated to defending privacy, anonymity, freedom of expression, and digital rights.

Osservatorio Nessuno OdV - Intro

Osservatorio Nessuno OdV (`osservatorionessuno.org`) is an Italian non-profit, run entirely by volunteers, dedicated to defending privacy, anonymity, freedom of expression, and digital rights.

Founded in 2021, the group operates Tor infrastructure, provides technical assistance to activists and journalists, develops open-source security tools, and conducts analysis and reverse engineering of surveillance technologies. It also engages in public advocacy and free educational outreach.

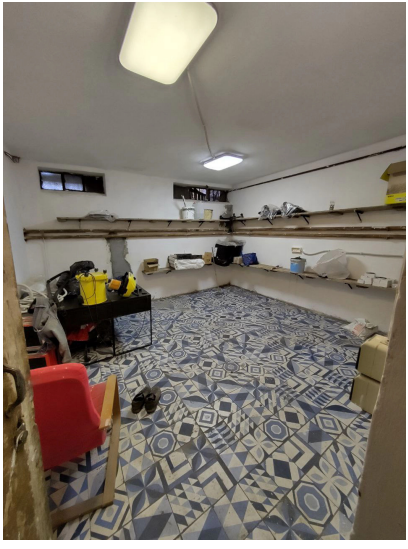
Osservatorio Nessuno OdV - Intro

Osservatorio Nessuno OdV (`osservatorionessuno.org`) is an Italian non-profit, run entirely by volunteers, dedicated to defending privacy, anonymity, freedom of expression, and digital rights.

Founded in 2021, the group operates Tor infrastructure, provides technical assistance to activists and journalists, develops open-source security tools, and conducts analysis and reverse engineering of surveillance technologies. It also engages in public advocacy and free educational outreach.

Born in hacklabs and self-organized spaces, we remain rooted in our grassroots foundations.

Osservatorio Nessuno OdV - HQ



When you think spyware...

WIRED

NEWSLETTERS SUBS

MORGAN MEAKER BUSINESS AUG 15, 2022 7:00 AM

Spyware Scandals Are Ripping Through Europe

The latest crisis that rocked the Greek government shows the bloc's surveillance problem goes beyond the notorious NSO Group.

Think Tank
European Parliament

MENU

Research / Advanced search / Greece's Predatorgate: The latest chapter in Europe's spyware scandal?

Greece's Predatorgate: The latest chapter in Europe's spyware scandal?

At a Glance – 08-09-2022

After Hungary, Poland and Spain, Greece is the latest Member State accused of spying on journalists and opposition politicians. While the opposition is seeking transparency and is steadily increasing the pressure, the Greek government has acknowledged select surveillance operations but insists on their legality and categorically denies purchasing or using the commercial Predator spyware. This EPRS paper synthesises the fast-paced and highly politicised developments at national level and contextualises the European Union's responses. It refers to the EPRS study 'Europe's PegasusGate' for more information and possible ways forward.

AP

CONTENT SOLUTIONS WHO WE SERVE INSIGHTS

Home — News Highlights — Spotlights — US-backed Israeli company's spyware

SPOTLIGHTS

US-backed Israeli company's spyware used to target European journalists, Citizen Lab finds

Europe is a spyware production and deployment hub

- **Spain & Italy** among the most **prolific producers** in the world

techcrunch.com

How Barcelona became an unlikely hub for spyware startups

Lorenzo Franceschi-Bicchierai

13–16 minutes

Toward the end of 2023, an Israeli security researcher from Tel Aviv said that he was approached on LinkedIn with an opportunity to work abroad with “good pay.” He said that the company’s HR department told him that it was a “legitimate” offensive security company that was starting from scratch in Barcelona, Spain.

Europe is a spyware production and deployment hub

techcrunch.com

How Barcelona became an unlikely hub for spyware startups

Lorenzo Franceschi-Bicchierai

13–16 minutes

Toward the end of 2023, an Israeli security researcher from Tel Aviv said that he was approached on LinkedIn with an opportunity to work abroad with "good pay." He said that the company's HR department told him that it was a "legitimate" offensive security company that was starting from scratch in Barcelona, Spain.

- **Spain & Italy** among the most **prolific producers** in the world
- **Israel** still partially leading the highly sophisticated market and **evidence of testing on Palestinians**[a]

Europe is a spyware production and deployment hub


techcrunch.com

How Barcelona became an unlikely hub for spyware startups

Lorenzo Franceschi-Bicchierai

13–16 minutes

Toward the end of 2023, an Israeli security researcher from Tel Aviv said that he was approached on LinkedIn with an opportunity to work abroad with "good pay." He said that the company's HR department told him that it was a "legitimate" offensive security company that was starting from scratch in Barcelona, Spain.

- **Spain & Italy** among the most **prolific producers** in the world
- **Israel** still partially leading the highly sophisticated market and **evidence of testing on Palestinians**[a]
- **EU** Countries with government-backed surveillance **scandals** include: **Greece**, **Spain**, **Italy**, **Serbia**, **Hungary**, **Estonia**, **Poland**, **Slovakia**, **Latvia**, ...

Europe is a spyware production and deployment hub


techcrunch.com

How Barcelona became an unlikely hub for spyware startups

Lorenzo Franceschi-Bicchierai

13–16 minutes

Toward the end of 2023, an Israeli security researcher from Tel Aviv said that he was approached on LinkedIn with an opportunity to work abroad with "good pay." He said that the company's HR department told him that it was a "legitimate" offensive security company that was starting from scratch in Barcelona, Spain.

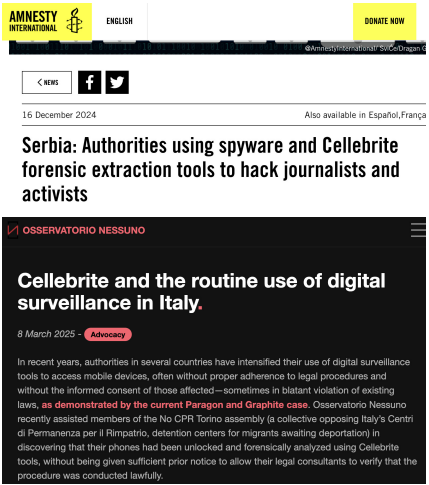
- **Spain & Italy** among the most **prolific producers** in the world
- **Israel** still partially leading the highly sophisticated market and **evidence of testing on Palestinians**[a]
- **EU** Countries with government-backed surveillance **scandals** include: **Greece**, **Spain**, **Italy**, **Serbia**, **Hungary**, **Estonia**, **Poland**, **Slovakia**, **Latvia**, ...
- Attribution is generally really hard, and **burden of proof always on victims**

[a] https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

You don't always need a million-dollar exploit chain

	$$$	**$$**	**$**
Installation	◦ 0-click ◦ 1-click + social	◦ social + privesc ◦ social + minor bugs	◦ social ◦ social + infra ◦ social + unlocking
Agent	memory	memory/app	app
Companies	◦ Paragon ◦ NSO ◦ Dataflow ◦ Cytrox	◦ RCS ◦ Memento	◦ SIO ◦ IPS Intelligence ◦ PC Tattletale ◦ InnovaSpy
Targets	◦ activists ◦ journalists ◦ dissidents ◦ politicians	◦ activists ◦ journalists ◦ dissidents	◦ activists ◦ employees ◦ partners
Complexity	high	medium	low

On the lower end



arachidi

2c. Intercettazione Telematica Attiva – SPYWARE

Disclaimer
I casi che abbiamo potuto analizzare si basano tutti su smartphone, ma potrebbero essere installati anche su pc con tecniche simili; inoltre le tecniche di attacco potrebbero essere oggi diverse e più sofisticate.

Op Sismi: avvenuta infenzione di un dispositivo tramite uno spyware di stato dal nome “Spyrtacus”.
Questa al momento è la terza volta che accade nel corso degli ultimi anni (da quel che ne sappiamo) e alcune parti dell’attacco accomunano tutti i casi che abbiamo potuto studiare.
Il costo nel 2023 è di 250€ (solo in caso di buon esito) per l’infezione, e di 170€ al giorno per il noleggio di una postazione pc con software di gestione.

Forensics vs live detection

- On **desktop**, the community have long focused on **live detection**

Forensics vs live detection

- On **desktop**, the community have long focused on **live detection**
- On **mobile**, it is not possible to **hook system APIs**, or **run privileged processes** (and maybe we shouldn't)

Forensics vs live detection

- On **desktop**, the community have long focused on **live detection**
- On **mobile**, it is not possible to **hook system APIs**, or **run privileged processes** (and maybe we shouldn't)
- Most efforts are either focused on **forensic methodology** (MVT) or **network-based detection** (PTS Project)

Forensics vs live detection

- On **desktop**, the community have long focused on **live detection**
- On **mobile**, it is not possible to **hook system APIs**, or **run privileged processes** (and maybe we shouldn't)
- Most efforts are either focused on **forensic methodology** (MVT) or **network-based detection** (PTS Project)
- Mostly **applicable only if spyware is known**, or there's deep suspicion of infection (with manual analysis)

Forensics vs live detection

- On **desktop**, the community have long focused on **live detection**
- On **mobile**, it is not possible to **hook system APIs**, or **run privileged processes** (and maybe we shouldn't)
- Most efforts are either focused on **forensic methodology** (MVT) or **network-based detection** (PTS Project)
- Mostly **applicable only if spyware is known**, or there's deep suspicion of infection (with manual analysis)
- Research: **static/dynamic analysis**, **anomaly detection**, difficult to do on device or without data collection

Lower-hanging fruits: easier detection and more threat intel

lower-hanging fruits

	$$$	**$$**	**$**
Installation	◦ 0-click ◦ 1-click + social	◦ social + privesc ◦ social + minor bugs	◦ social ◦ social + infra ◦ social + unlocking
Agent	memory	memory/app	app
Companies	◦ Paragon ◦ NSO ◦ Dataflow ◦ Cytrox	◦ RCS ◦ Memento	◦ SIO ◦ IPS Intelligence ◦ PC Tattletale ◦ InnovaSpy
Targets	◦ activists ◦ journalists ◦ dissidents ◦ politicians	◦ activists ◦ journalists ◦ dissidents	◦ activists ◦ employees ◦ partners
Complexity	high	medium	low

Consensual Forensics Methodology

Civil Society Helplines

A victim reach out through an helpline or via trusted grass-roots collectives.
To perform an acquisition of the (suspected) infected device:

Civil Society Helplines

A victim reach out through an helpline or via trusted grass-roots collectives.

To perform an acquisition of the (suspected) infected device:

- A technician travels on-site to the victim
- The victim performs an acquisition with remote support from a technician
- The victim sends their device to the technician for analysis

MVT

- MVT is the de facto standard tool for Consensual Mobile Forensics

MVT

- MVT is the de facto standard tool for Consensual Mobile Forensics
- It was developed by **Amnesty Tech Lab** in 2021 in the context of the "Pegasus Project" investigation

MVT

- MVT is the de facto standard tool for Consensual Mobile Forensics
- It was developed by **Amnesty Tech Lab** in 2021 in the context of the "Pegasus Project" investigation
- It is developed in Python as a command-line tool

MVT

- MVT is the de facto standard tool for Consensual Mobile Forensics
- It was developed by **Amnesty Tech Lab** in 2021 in the context of the "Pegasus Project" investigation
- It is developed in Python as a command-line tool
- Interpreting the results requires technical expertise

MVT

- MVT is the de facto standard tool for Consensual Mobile Forensics
- It was developed by **Amnesty Tech Lab** in 2021 in the context of the "Pegasus Project" investigation
- It is developed in Python as a command-line tool
- Interpreting the results requires technical expertise
- Uses ADB via USB to connect to the device and extract relevant artifacts

AndroidQF

- Developed to make the acquisition process easier for victims

AndroidQF

- Developed to make the acquisition process easier for victims
- More user-friendly than MVT

AndroidQF

- Developed to make the acquisition process easier for victims
- More user-friendly than MVT
- Written in Golang, compiled to a single binary

AndroidQF

- Developed to make the acquisition process easier for victims
- More user-friendly than MVT
- Written in Golang, compiled to a single binary
- Exports an encrypted MVT-compatible acquisition

AndroidQF

- Developed to make the acquisition process easier for victims
- More user-friendly than MVT
- Written in Golang, compiled to a single binary
- Exports an encrypted MVT-compatible acquisition
- The victim can share the export with a technician that uses MVT to analyse it

Bugbane

Bugbane

Our goals:

- Create a user-friendly on-device tool

Bugbane

Our goals:

- Create a user-friendly on-device tool
- Improve civil society threat intelligence by making widespread analysis possible

Bugbane

Our goals:

- Create a user-friendly on-device tool
- Improve civil society threat intelligence by making widespread analysis possible
- Scan acquisitions retroactively with updated Indicators of Compromise (IoC)

Bugbane

Our goals:

- Create a user-friendly on-device tool
- Improve civil society threat intelligence by making widespread analysis possible
- Scan acquisitions retroactively with updated Indicators of Compromise (IoC)
- Remain cross-compatible with other open-source tools such has MVT/AndroidQF

Bugbane

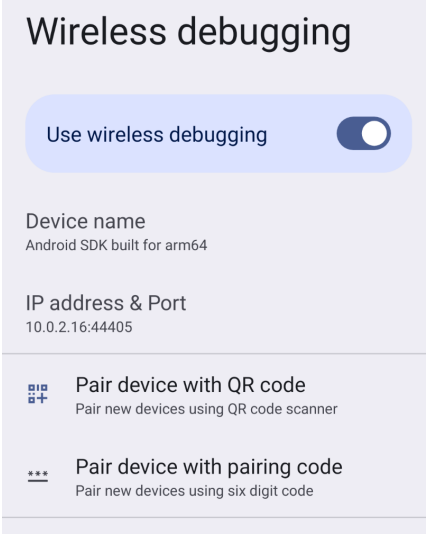
Our goals:

- Create a user-friendly on-device tool
- Improve civil society threat intelligence by making widespread analysis possible
- Scan acquisitions retroactively with updated Indicators of Compromise (IoC)
- Remain cross-compatible with other open-source tools such has MVT/AndroidQF

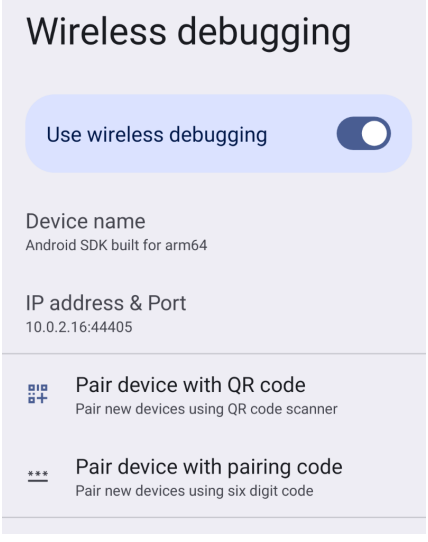
But mainly: perform acquisitions and analyses locally on the target device

Bugbane - Wireless ADB

- **Wireless ADB debugging!**

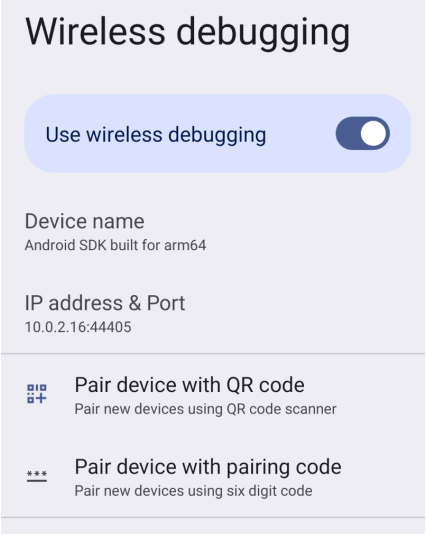


Bugbane - Wireless ADB



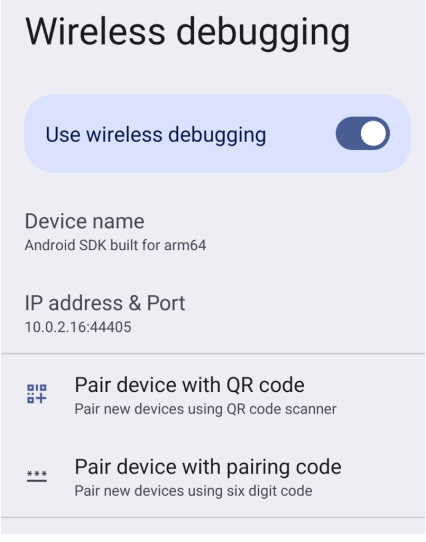
- **Wireless ADB debugging!**
- Available since Android 11+

Bugbane - Wireless ADB



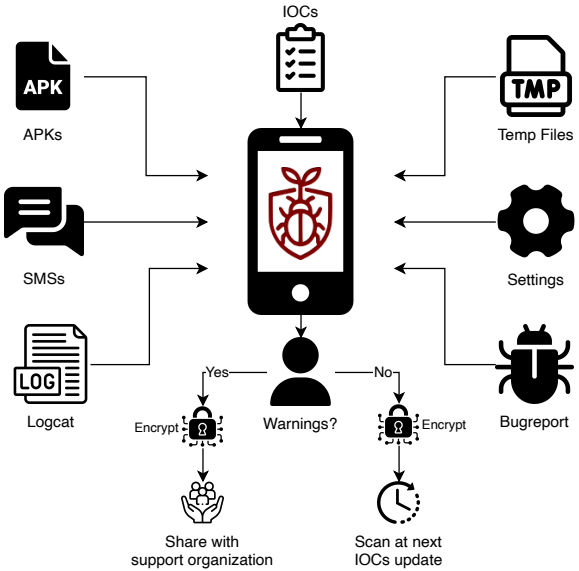
- **Wireless ADB debugging!**
- Available since Android 11+
- Grants the same privileges MVT requires, thus allowing 1:1 acquisitions

Bugbane - Wireless ADB

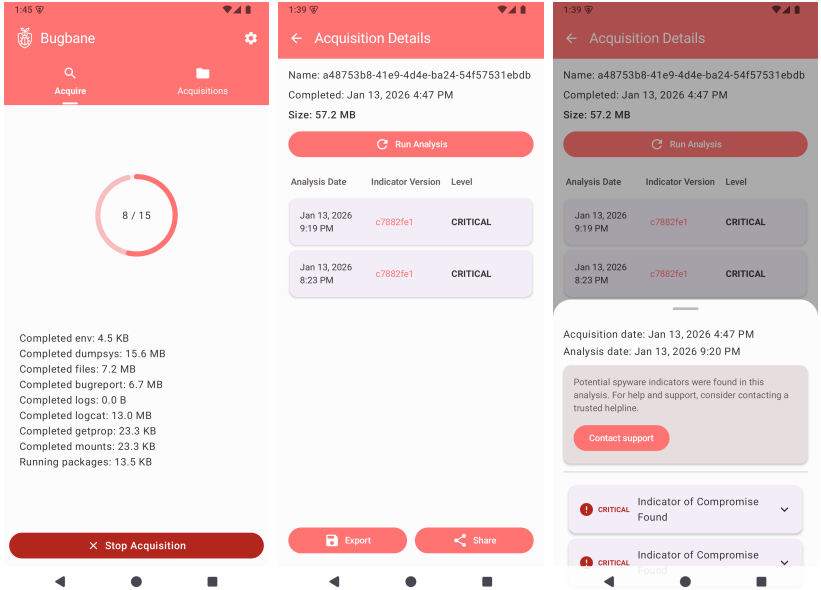


- **Wireless ADB debugging!**
- Available since Android 11+
- Grants the same privileges MVT requires, thus allowing 1:1 acquisitions
- Ironically, the same mechanism that low-end spyware use to escalate privileges

Bugbane - Architecture



Bugbane - UI


1:45
Bugbane
Acquire
Acquisitions
8 / 15
Completed env: 4.5 KB
Completed dumpsys: 15.6 MB
Completed files: 7.2 MB
Completed bugreport: 6.7 MB
Completed logs: 0.0 B
Completed logcat: 13.0 MB
Completed getprop: 23.3 KB
Completed mounts: 23.3 KB
Running packages: 13.5 KB
Stop Acquisition
1:39
Acquisition Details
Name: a48753b8-41e9-4d4e-ba24-54f57531ebdb
Completed: Jan 13, 2026 4:47 PM
Size: 57.2 MB
Run Analysis
Analysis Date
Indicator Version
Level
Jan 13, 2026 9:19 PM
c7882fe1
CRITICAL
Jan 13, 2026 8:23 PM
c7882fe1
CRITICAL
Export
Share
1:39
Acquisition Details
Name: a48753b8-41e9-4d4e-ba24-54f57531ebdb
Completed: Jan 13, 2026 4:47 PM
Size: 57.2 MB
Run Analysis
Analysis Date
Indicator Version
Level
Jan 13, 2026 9:19 PM
c7882fe1
CRITICAL
Jan 13, 2026 8:23 PM
c7882fe1
CRITICAL
Acquisition date: Jan 13, 2026 4:47 PM
Analysis date: Jan 13, 2026 9:20 PM
Potential spyware indicators were found in this analysis. For help and support, consider contacting a trusted helpline.
Contact support
CRITICAL
Indicator of Compromise Found
CRITICAL
Indicator of Compromise

Bugbane - Limitations

Research problems

- Can only catch known threats
- Threat actors can scrape public IOCs and update their obfuscation
- Saving artifacts on device can add evidences in case of seizures

Improvements under development

- Secure the app by encrypting local data
- Reproducible update infrastructure
- False positives detection/prevention
- UX

References

Bugbane

- Osservatorio Nessuno OdV - `https://osservatorionessuno.org`
- Rowen S - `https://rwn.sh`

Related projects

- MVT - `https://mvt.re`
- PTS - `https://pts-project.org`

Support

- CiviCERT - `https://civicert.org`

We have intentionally left out closed-source tools. Their lack of transparency, unclear data-collection practices, and weak integration with community processes make them unsuitable for community support.

Q&A

osservatorionessuno.org
bsky.app/profile/osservatorionessuno.org
mastodon.cisti.org/@0n_odv
github.com/osservatorionessuno