Rayhunter: Are “They” Listening

September 2, 2025

By Aaron Grothe

Introduction

If anybody has any questions or comments at any time please let me know.

If I start to mumble please let me know as well :-)

Slides will be on my website https://www.grothe.us in the presentations section in the next day or two. I also posted a link to the slide deck in the discord channel in the speaker-planning topic

Disclaimer

We're not going to be talking about making your own Stingray today. The information is out there and for about $200-500 you can make a pretty nice IMSI catcher

If you're in passive mode you're probably not doing anything illegal, but I am not a lawyer

Today we're mostly going to talk about a tool Rayhunter for detecting Stingray like snooping

You're messing with hardware and while unlikely you might break your hardware doing this. You have been warned.

Overview of Talk

We will break down the talk into the following sections

- Intro/Overview (You are here)
- Terms/Definition
- How a Stingray works
- Why This Matters
- Crocodile Hunter - Older Cousin to Rayhunter

Overview of Talk (Cont)

We will break down the talk into the following sections

- Rayhunter
- Demo - Rayhunter
- Rayhunter - From Source
- One Thing You Need to Do
- Future Things
- Tips that Would have Helped

Terms We Should Know

- CSS - Cell-Site Simulators (aka Stingray, IMSI Catcher)
- IMSI - International Mobile Subscriber Identifier
    - Unique to each SIM card or hardware
- TMSI - Temporary Mobile Subscriber Identity
    - Generated to be used after IMSI handshake to reduce number of times IMSI is broadcast
- IMEI - International Mobile Equipment Identity
    - Unique to each device
- CSLI - Cell Site Location Information
    - Cell tower information authorities can get from phone company
    - Not as accurate as CSS, might need a warrant

How a Stingray Works

Note: StingRay is a trademark of Harris Corporation, Stingray is the term used for Cell Phone Simulators. Think of Xerox to Copy.

Cellphone continually pings cell towers looking for best connection

A Stingray device usually runs in one of two modes Active and Passive

Active impersonates a cell phone tower

Passive scoops up as much data as it can get

"an unconstitutional, all-you-can-eat data buffet" - EFF

Stingray Active Mode

How it works

- Forces a cell phone to connect to it instead of one of a local cell tower
  - Does this by providing a stronger signal or a signal that says it is stronger than the others
  - From this it can actually try and force a lower level of network of encryption.
  - Write protocol metadata to internal storage
  - Denial of Service

Stingray Active Mode

Does this by providing a stronger signal or a signal that says it is stronger than the others

How does it do this?

- Be closer to the target than the cell tower
  - Inverse Square Law - double the distance from a radio transmitter, the signal strength will be one-quarter (1/4) of what it was at the original distance
- Broadcast a stronger signal

Stingray Active Mode

From this it can actually try and force a lower level of network of encryption.

- E.g. It may attempt to force your phone to connect 2g, the 2g encryption protocols are breakable in real time
  - Lower quality encryption handshake A5/1 vs A5/2, A5/1 call encryption is a very breakable cipher and A5/2 is an export weakened version of that.

Stingray Active Mode

Write protocol metadata to internal storage

- Any time you can write to internal storage of a device it is not a good thing

Stingray Active Mode

Denial of Service

- Can be used as part of downgrade attempts
  - You block 5g/4g and can force system back into 3g/2g options

Stingray Passive Mode

Passive Mode is largely a really nice sniffer

You can get information from the phones connecting to local cell towers

Information that can be captured

- IMSI/EMSI identifiers
- Signal strength, used for triangulation

Why this Matters

Spy ring plotted to track ukrainians at US air base in Germany

https://www.theguardian.com/uk-news/2024/dec/03/spy-ring-plotted-to-obtain-details-from-phones-of-ukrainians-at-us-air-base-in-germany-uk-court-hears?ref=news.itsfoss.com

Russian Spy ring was planning on using Stingray device to find IMSI identifiers at German Air Force Base to be able to correlate them when the Ukrainian pilots returned home, to be able to target them

Why this Matters

2014 Protest in Chicago

https://www.cbsnews.com/chicago/news/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/

Part of a transcript of a conversation between the police at site.

Officer 2: "Yeah one of the girls, an organizer here, she's been on her phone a lot. You guys picking up any information, uh, where they're going, possibly?"
Officer 1: "Yeah we'll keep an eye on it, we'll let you know if we hear anything."

Why this Should Matter to Us

You might be in their data collection

- They tend to suck up large swaths of data, not very discerning
- What happens to the data, how long it hangs around, who has access are poorly defined
- How many people are using these, are they needing to get court orders, etc. Not really :-(

Crocodile Hunter

Crocodile Hunter - https://github.com/EFForg/crocodilehunter - was the predecessor to the Rayhunter

Required more hardware and technical skill

- Laptop or Raspberry Pi 4+
- GPS Dongle
- Software Defined Radio (Lime SDR, Blade RF)

Crocodile Hunter

Crocodile Hunter was designed differently than its successor

- Listen to broadcast messages from nearby 4G/LTE cell towers
- Compare those messages to open source databases of FCC known towers
- Compare data for differences between two data sources
- Tracks cell towers that “move” over time
- Tracks cell towers that are in places that don’t make sense
    - Site with extensive coverage gets a “new” cell tower
- Optionally shared this information with central server to aggregate information

Rayhunter

Rayhunter is a new project from the EFF

- Uses commodity hardware
  - Orbic RC400L, TP-Link M7350, TP-Link M7310
  - Tmobile TMOHS1, UZ801, Wingtech CT2MHS01
  - PinePhone and PinePhone Pro, Moxee Hotspot
- Doesn't overwrite the software on the system
  - Adds additional functionality to system while still working as hotspot

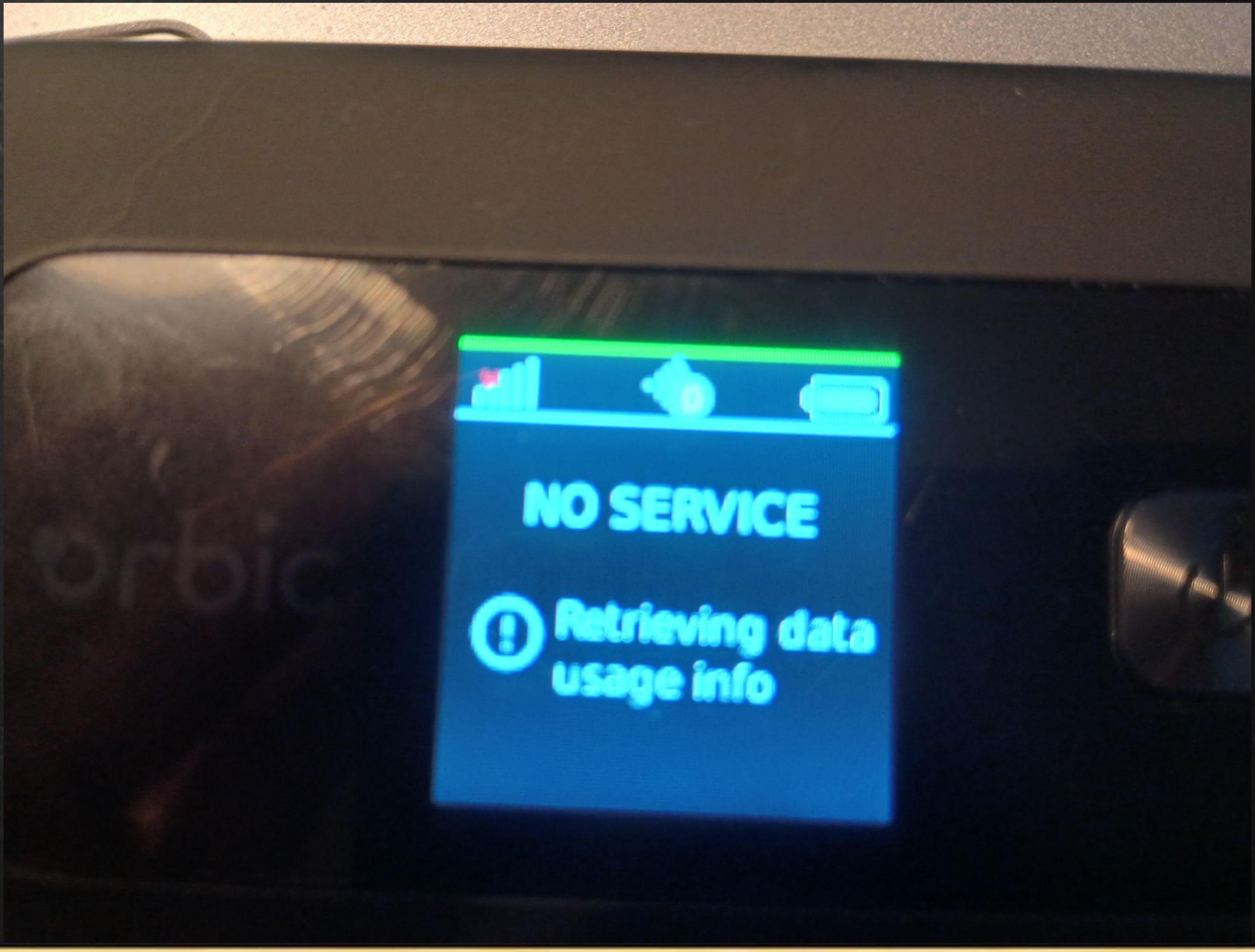
Rayhunter

Rayhunter goes by the behavior of the cell tower not location

Some of the things it detects

- Forced 2G downgrade
- Suspicious IMSI requests, once you're connected to a regular cell tower it will use the TMSI, Stingrays often request IMSI
- Null Cipher Use - bad handshake tries to use known weak encryption algorithms A5/2, Null, etc.

Rayhunter - Default Screen



NO SERVICE

Retrieving data usage info

Rayhunter - Default Screen

Note the Green Line at the Top, If this turns Red be concerned

Remember - “Green your data is probably unseen, Red your privacy may be dead”

There is also a GUI interface which we’ll take a look at in the demo section

Rayhunter - Demo

We'll open the Web GUI, and step through it a bit

Two ways to get to it you can connect to the wifi hotspot and hit port 8080 on it.

Or you can use the Android Debug Bridge (ADB) tools and hit it from your local machine

```
adb forward tcp:8080 tcp:8080
```

Rayhunter - From Source

We'll build the Rayhunter Software from source and go ahead and install it on the device

For this you'll need the following

nodejs/npm - required for building web front end
rustc - required for building module, recommend using rustup
adb - Android Debug Bridge, needed to push firmware

Rayhunter - From Source

We'll make one small change to the source code to make sure we know its our version

In the background image folder lets put the olug logo in there

```
cp olug.gif folder
```

```
# cargo build --bin rootshell --target
armv7-unknown-linux-musleabihf --profile firmware

# cargo run --bin installer orbic
```

Rayhunter - From Source

Let’s reboot and go to the web interface again

```
% adb forward tcp:8080 tcp:8080
```

In the background image should see option for olug, select that and reboot

And viola the olug logo

We’re running a very minor customization to the software

Rayhunter - From Source

Quite simply: EFF has done a stellar job with the Rayhunter software

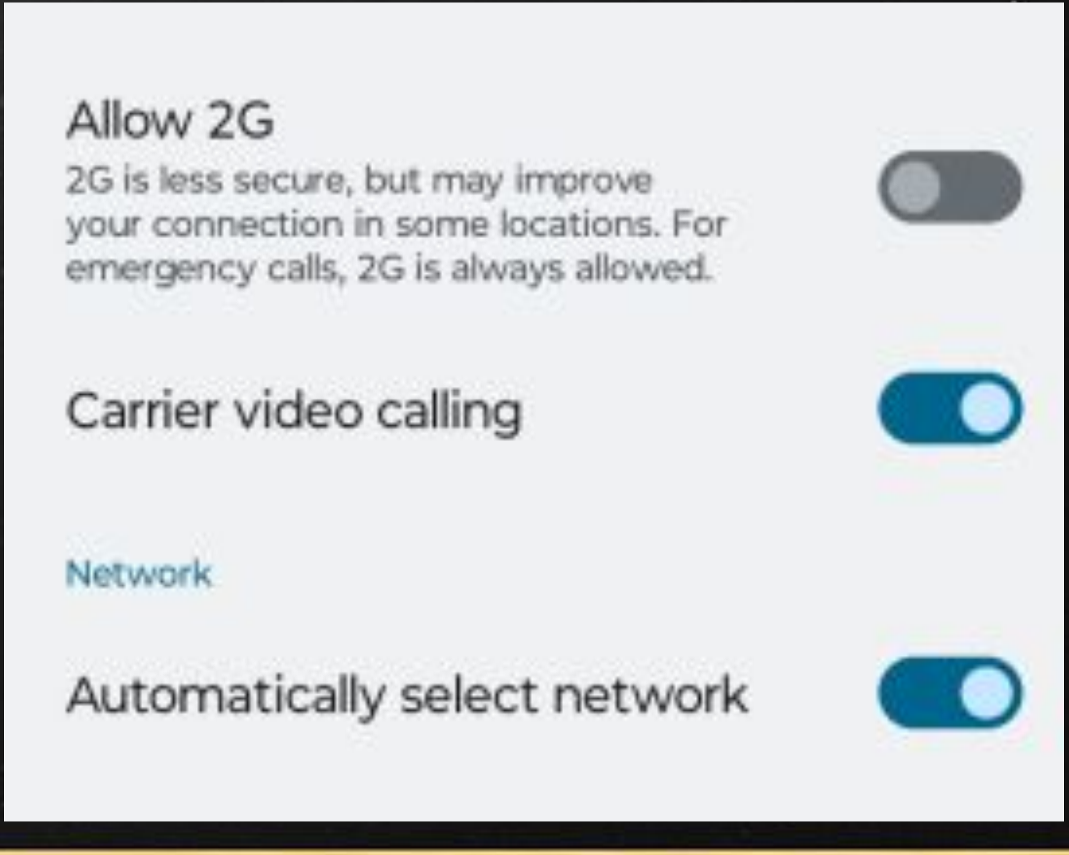
Usually when you flash firmware on a device it wipes the original functionality. This is additional functionality.

Source code is well documented. If you're interested in trying to create a wifi/imsi sniffer type of device the source code and hardware provide a pretty good starting point

One Thing You Need To Do

Check to see if your phone has 2G compatibility turned on.

Mine Was :-(



Allow 2G

2G is less secure, but may improve your connection in some locations. For emergency calls, 2G is always allowed.

Carrier video calling

Network

Automatically select network

Future Things

Android adding Security Features

- Android 12, added capability to disable 2g connections at modem
- Android 14, supported disabling of connections with null ciphers
- Anrdoid 15, notifies when cell tower requests identified repeatedly or tries to force new ciphering algorithm
- Android 17 is talking about possibly incorporating the response protocol of timing to better detect IMSI catchers, will require new hardware

Apple still needs to add the ability to disable 2g connection to user

Future Things

Cell Site Simulator Warrant Act 2023/2025

https://www.theregister.com/2025/08/04/infosec_in_brief/

Has been introduced at the end of July and is having some traction

Earlier version of this talk mentioned the Cell Site Simulator Warrant Act of 2023, had little chance of passing. This version seems to have some bi-partisan support

Tips that Would have Helped

Things I Wish I had Known

- Good USB-C Cable. Was fighting with this last night, picked up usb-c cable wouldn't recognize device, bad cable
- Kill adb bridge, when not using. When attempting to push updated firmware, failed over and over, adb bridge was running
- Start with a regular build. Start with regular release before trying git repo code.
- Git repo code may or may not work, if you've got issues fall back to regular release or previous git version

Tips that Would have Helped

Things I Wish I had Known

- The code is in two parts the front end which is svelte, typescript, etc. and the backend which is in rust. Make sure to build both of them
- If things lock up pull, the battery wait 30 seconds and reset
- You probably won't brick, but if you do and you only spent $12 is it a big deal??? :-)

Summary

You can get an Orbic RC400L on ebay right now for about $12.00.

You do need a valid SIM card to use it, but you can get those very cheaply as well.

You'll learn some interesting things in the process. Especially if you build from source and modify it a bit

Will be interesting to see how Rayhunter progresses and if it might start getting some of functionality that Crocodile Hunter, or if they will provide a mechanism or tool to submit suspicious information

Q & A and Thanks

That's all I've got for Tonight.

Any Questions?

Thanks for listening.

Links

Rayhunter

https://www.eff.org/deeplinks/2025/03/meet-rayhunter-new-open-source-tool-eff-detect-cellular-spying

https://github.com/EFForg/rayhunter

Crocodile Hunter

https://github.com/EFForg/crocodilehunter