

IMSI-CATCHER

Found fake base station outside Høyres hus in the center of Oslo

This time Odd Helge Rosberg have no doubts about his findings.

Av [Marius Jørgenrud](#)

Published February 18th 2016 at 17:43 - Updated 18th of February at 17:44

HØYRES HUS (digi.no): The co-founder and CTO of the security company Rosberg System held a lecture for a full packed house at the HackCon conference.

He is one of IT experts Aftenposten used to go through the data in the much-publicized series of articles the newspaper had surrounding the disclosure of false base stations or IMSI catchers in the capital.

Rosberg strongly opposed PST when he last summer concluded that the so-called IMSI catchers "in all probability" was operating in the center of Oslo.

Now he has no doubt.

- Yesterday there was an incident. The alarm went off on my mobile phone. I discovered a fake base station here outside Conservatives house at 12.15. Unlike Aftenposten's data where we said in all probability, I can in this case, based on my data say that there certainly was a fake base station here, says Odd Helge Rosberg.

The signals were according to him visible for about five minutes Wednesday. In the two days the guy from Rogaland have been in town this is the only trace.

The discovery was made by a separate Android based mobile application, he calls it a test app, which reportedly can detect fake base stations.

The app is designed for internal use and not sold.

Meanwhile spent Rosberg ample time during the lecture to promote similar functionality that they sell commercially in collaboration with Evry.

Based on the experience they got working with Aftenposten; Rosberg System developed an IMSI catcher or Stingray discoverer.

- We have access to a list of all active mobile towers in Norway, both of Ice, Netcom and Telenor. This includes among other things a whitelist feature that is constantly updated, but you have to eliminate false positives, said Odd Helge Rosberg.

Several «unknown»

A screen he shared in a slide stems from the test app alarm. The picture describes a number of technical parameters the suspicious transmitter emits. With data the IT expert have never before come across.

After the lecture digi.no got a short talk with CTO Rosberg:

– It seems somewhat convenient tht you found an IMSI-catcher right here and now. Tell about the circumstances arund this finding.

- The circumstances are that I was in the middle of a phone call. Then the alarm started to sound. So I did not get a chance to look at it before the call was completed. When I checked afterwards, we first look at the possibility that there may be a false positive, things sometimes happen among the operators. But there were obvious signs that this was not normal operating behavior.

– Tens of thousands of measurements

According to him they have done several tens of thousand thousand measurements earlier. He has only once before found something indicating findings in Oslo, but the finding was not on par with yesterday.

He does not want to speculate on who may or may not be behind the false base station he believes to have uncovered.

- I must relate to the data I see. The data show that someone are doing something, but who is behind or why is not something the data can tell me anything about.

- What is the big difference between yesterday's findings and when you took a subject to Aftenposten last year?

- One of the things we criticized was that Aftenposten measurements were made over a relatively short time. That means you can not tell if this was a transmitter which came back again. Since I'm here, the measurements are now actually done over two days. And the transmitter was available for only about five minutes. Then it was gone. It was not seen again. The second point is in relation to speed, it says "unknown." We have performed tens of thousands of measurements, but it is the first time I've seen unknown as indicator. Transmitting speed is decided by the cell tower.

- It is your app does not recognize any pattern here?

- That's correct. We have some pretty advanced mechanisms to detect the transmitter behavior.

- *Will you give out this data, so it can be verifiable by others?*

- I will gladly work with agencies that wants to look at this, but I'm not sure I want to release it publicly.

Hard to uncover

Coverage director Bjørn Amundsen says it is impossible to comment Rosberg alleged findings.

- Telenor hires frequencies from Norwegian Post and Telecommunications Authority (Nkom). It is they who are responsible for what kind of communication is transmitted in the net. It may also be a legitimate matter, something the police do, and something I know nothing about.

There is no guarantee that we can see a fake base station just like that, says Amundsen.

Before he sends the ball on to Nkom Telenor's Director of Coverage points at another, very specific problem for mobile operators. Namely noise and disturbance from illegally set up repeaters.

- There is reason to believe that there are a high number of illegal repeaters in our network. They make noise back to our base stations. Nkom fines those who set this up. These are also very difficult to detect. False base stations are quite the same. It is impossible to say whether a disruption is caused by A or B, said Director of Coverage Amundsen of Telenor.

Nkom considers measuring equipment

John-Eivind Velure is frequency Director Nkom. Nor he can say anything specific about Rosberg's findings.

- Has there ever been proven to be false base stations in Norway, the way Nkom see it?

- Here I refer to the investigation last year. Eventually, we too are able to make our own investigations. But here must Nkom follow government rules for procurement, as this will take some time. We are now at the stage that we are considering suppliers of professional equipment, which can capture for example IMSI catchers, says Velure.

He confirmed however that illegal repeaters are a recurring problem they often face. Then the authorities go in and fines for illegal use of frequencies. That have, according to him, happened dozens of times in recent years.

Meanwhile, it seems unlikely that the data Rosberg captured may stem from an illegal repeater. It's just a dumb box that amplifies existing cellular signals.