1 Author: Stefan Ćertić https://www.certic.info

Utilizing social engineering in Mobile Location Services.

Despite technology development, social engineering is still used in combination with advanced technologies to discover and prevent crimes.

However, in wrong hands, it might be powerful tool to compromise your personal security. Especially today, when many hackers have access to SS7 network, with ability to execute GSM Map commands such as PSI (Provide Subscriber Information) and ATI (Any time interrogation) used to disclose your phone Cell ID location and similar data.

Let's cover the scenario of unsuccessful attempt to prevent locating.

- Subject decides to become invisible and prevent anyone from locating you.
- Subject throw away a mobile phone along with the SIM card and buy a new one or start using 'Burner' phones.
- Subject thrown away your laptop and buy a new one, making sure no username that connects to you is ever used.
- Subject even changes city and state.
- Subject get's found within a day :)

The behavior is not easy for subject to change. It's a spectrum of Social habits that might be used hand in hand with advanced technology to make perfect match of the location.

An Example:

- Subject's habit is to have a breakfast at restaurant at about 9am. He enjoys Mexican Food. Subject phone is likely to connect to a base station within the area of Mexican food restaurants.

- Subjects enjoy taking a long walk at the park after the breakfast. It is likely to find same IMSI at the park areas.

- Subject likes rock music having a habit of visiting gigs each Friday. Chances are IMSI could be isolated from the group of IMSI's collected within the other locations specific to known social behavior.

By collecting all the IMSI's connected at the base stations within the radius of Mexican Restaurants, Parks, Rock venues...making it more precise by limiting behavioral time, intersection could very easy lead towards one single match.

SS7 Connectivity could be very dangerous weapon in wrong hands.