

IMSI catcher



Cette page est presque vide

La rédaction du site se concentre pour le moment sur les tutoriels qui servent à réduire les risques des moyens d'enquête de la police.

La section menace sera complétée pour le mois de septembre.

Un IMSI-catcher est une fausse antenne relais mobile, utilisée par les services de police et de renseignement pour disposer d'informations sur les téléphones avoisinants qui s'y sont connectés.

Les IMSI-catchers sont utilisés pour savoir quels appareils et lignes mobiles une personne utilise, quels appareils sont présents dans une zone donnée - et par là même qui s'y trouve - et éventuellement intercepter des communications.

Ces dispositifs peuvent être installés dans une valise ou dans un véhicule.

Il n'existe pas de statistiques portant sur l'utilisation d'IMSI-catchers en judiciaire en France. Cependant, en renseignement, la CNCTR indique environ 600 recours par an à cette technique sur le territoire national (2021-2024), et 100 IMSI-catchers peuvent être utilisés de manière simultanée au maximum.

Conditions de mise en œuvre

L'IMSI-catcher simule une antenne relais. Son signal sera plus puissant que les antennes relais légitimes dans une faible zone autour de lui, ce qui va entraîner les téléphones dans cette zone à essayer de se connecter à lui.

Lorsqu'un téléphone tente de s'y connecter, l'IMSI-catcher peut demander au téléphone le numéro IMSI de sa carte SIM, ainsi que le numéro IMEI spécifique au téléphone.

Contrairement à certaines croyances, il n'y a pas besoin de rétrograder le réseau téléphonique en 2G pour que l'IMSI-catcher fonctionne. Même si des mesures de sécurité ont été rajoutées, des failles présentes dans les protocoles 4G et 5G-NSA permettent l'obtention des numéros IMSI et IMEI par un acteur malveillant.

Un IMSI-catcher peut intercepter le contenu des appels et SMS, mais en France, cette utilisation n'a pas été documentée à ce jour, ni en judiciaire ni en renseignement. Ceci peut

s'expliquer par la facilité avec laquelle il est possible d'intercepter les communications téléphoniques via la PNIJ.

Cependant, cette technique semble être très utilisée par des pirates pour l'envoi massif de SMS frauduleux, ces dispositifs sont souvent appelés également des SMS blaster.



Détails techniques du fonctionnement de l'IMSI-catcher

