T1588 IMSI Catcher

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
|  |  |  |  |  |
|  |  |  |  |  |

Description: An adversary may buy, build, or steal International Mobile Subscriber Identity (IMSI) catcher to capture IMSI numbers from nearby phones in a target area.

IMSI catchers are very similar to fake base stations but may not have full capabilities of the base station. IMSI Catcher terms has been traditionally associated with UE identity catching or location identification. Adversary may buy an IMSI Catcher from legitimate vendors selling products or build one with open-source code and generic radio transceivers. Open-source code for software defined radio, or RAN test equipment, or simulators can be modified to create an IMSI catcher.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: Resource Development

Metadata:

* Architecture Segment: RAN, UE
* Platforms: RAN
* Access type required : N/A
* Data Sources:
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| M1056 | This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of the mobile network operator . |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of the assets that adversary wants to target or that are at risk such as data (system/user, access token, crypto key etc.), capability, service. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detection** |
| If known | Short description of possible detection techniques such as logs or sensors. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |
|  |  |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. IMSI-catch me if you can: IMSI-catcher-catchers. In Proceedings of the 30th annual computer security applications Conference, pages 246–255, 2014. | https://its-wiki.no/images/f/fb/Dabrowski\_ISMI\_Catch\_me\_Catchers.pdf |
| Ravishankar Borgaonkar, Altaf Shaik , 5G IMSI Catchers Mirage, Balckhat USA Conference 2021 | https://blackhat.com/us-21/briefings/schedule/#g-imsi-catchers-mirage-23538 |
| HOW COPS CAN SECRETLY TRACK YOUR PHONE, The Intercept, online article, July 31, 2021. Accessed 6/22/2022 | https://theintercept.com/2020/07/31/protests-surveillance-stingrays-dirtboxes-phone-tracking/ |
| A Knight, Brier & Thorn, Hacking GSM: Building a Rogue Base Station to Hack Cellular Devices, Online Article. Accessed 6/22/2022 | https://www.brierandthorn.com/post/hacking-gsm-building-a-rogue-base-station-to-hack-cellular-devices |