FGT5024 SIM boxing

Description: Adversary uses SIM boxing to bypass charging record keeping for international calls.

Service fraud involves bypassing controls to gain access to services or resources which the adversary is not entitled to or charged for. This includes bypassing billing and charging fees for use of services provided by the MNO. In this attack the adversary uses IP networks and so called "SIM boxes" to avoid termination fees between interconnected MNOs (so that international calls appear to be local calls). SIM boxing can also be used to offer very cheap SMS rates to customers by private persons posing as legitimate MNOs. The adversary places the SIM box in a 5G cell but does not use the regular roaming (e.g. IP Exchange /IPX) interconnect, instead, tunnels voice data over the top- i.e. over the Internet.

(Note: SIM boxes have a legitimate use by operators. In fraudulent use, they are placed in the range of a given base station so they can act as that set of UEs connecting to the base station and can be physically moved periodically to avoid being detected).

Labelling:

* Sub-technique(s):
* Applicable Tactics: Fraud

Metadata:

* Architecture Segment: Control-plane
* Platforms: 5G
* Access Type Required: N/A
* Data Sources:
* Theoretical/Proof of Concept/Observed: Observed

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 |
| Adversary poses as legitimate carrier, to get to intercepts calls/ SMSs and re-route them. | Adversary/fraudster/SIM boxers are effectively acting as an unlicensed and unregulated telecommunications carrier (pretends to be a legitimate telecom provider). Adversary intercepts call and routes it via the Internet as a VoIP call, to the SIMbox (instead of via a regulated MNO interconnect). See [3], [5] |
| Adversary sells fraudulent international calling cards. | Adversary offers discounted call rates directly to end consumers, primarily through the sale of international calling cards. Such cards have a number that the user must dial before she can dial the recipient’s number; this number will route to a number provided by a VoIP provider that points to the SIMbox in the recipient’s country. See [3], [5] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| M1040 | Several tools exist to tag such SIM cards and reject calls from them.  Analyze and monitor call patterns, mobility patterns, and detect anomalies. See [4] |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| SIM box equipment | Adversary purchases a SIM box, SIM cards, and obtains an Internet connection |

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. |
| Operator revenue | Revenue loss from international calls appearing as if they are domestic (often subsidized) |
| Operator resources for SMS, voice calls’ quality of service is impacted | A lot of calls are redirected to under provisioned cells, causing bad quality calls for legitimate subscribers |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| DS0029 | There are several tools, some using analysis after the fact, others test calls to network probes. Some tools use real time analysis of voice call characteristic – to detect VoIP calls illicitly tunneled into the operator network. |
| DS0018 | Use firewall to restrict unwanted traffic |
| FGDS5004 | The audio received by the base station from a simboxed  call will contain losses, indicating that the audio signal  has traveled over an Internet connection, while the audio from a legitimate call will not contain these losses. See [3] |
| FGDS5005 | Keeping track of SIM cards with strange usage pattern (e.g. bought but only used 1 hour) they may be part of a SIM box, and then blocking those SIM cards. |

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** |
| ENISA “Threat Landscape for 5G Networks Report” Nov 2019, section 5.2. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |
| Masrub et. al.: “SIM boxing Problem: ALMADAR ALJADID Case Study” | https://ieeexplore.ieee.org/document/9249872 |
| Reaves et.al, “Boxed Out: Blocking Cellular Interconnect Bypass Fraud at the Network Edge” | https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-reaves-boxed.pdf |
| Anne Josiane Kouam, Aline Carneiro Viana, Alain Tchana. “SIMBox bypass frauds in cellular networks: Strategies, evolution, detection, and future directions. Communications Surveys and Tutorials” | https://hal.inria.fr/hal-03105845v4/document |
| Mobile Ecosystem Forum, “Business SMS, SIM Farms and the Data Protection Risk”, whitepaper, 2020. | https://mobileecosystemforum.com/business-sms-sim-farms-and-the-data-protection-risk/ |