T1592.501 Internal Resource Search

Description: An adversary may gain access to an operator's IR.21 related resources, which can reveal the critical network assets of both the operator and its partner MNOs.

International mobile network operators (MNOs) maintain information about their network infrastructure, roaming/interconnection configuration, and MNO partner billing agreements. This sensitive data is in a standardized format, under the name “IR.21”. GSMA administers databases of IR.21 for all international MNO and allowing all MNOs access to it. This type of sensitive information is intended to not be publicly accessible; however, data leaks and insider attacks have occurred, and thus this information can be and has been used by adversaries in their discovery tactics.

Labelling:

* Sub-technique #: None
* Applicable Tactics: Reconnaissance

Metadata:

* Architecture segment: OA&M
* Platforms: 5G Network
* Access Type Required: user or admin of GSMA
* Data Sources: IR.21 database files
* 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 |
| IR.21 accessible from the Internet | Claro Americas, and Vivo telecom, had their IR.21 database accessible from an internet in 2016 (References [2], [3] no longer accessible). |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| If known | Short description of potential mitigations. |
| FGM5500 | Control access to IR.21 files in GSMA. Host/application hosting this file should guard against such leak. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Access to GSMA account; in some cases, none. | Adversary needs to access the operator databases or GSMA repositories |

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. |
| Mobile network topology, interconnects. | Information on the IP addresses of the mobile network, along with those of the interconnect/roaming nodes. |
| IP addresses of core NFs | Hostnames and IP addresses of core network functions like subscriber databases and functions involved in roaming exchanges (e.g. Access and Mobility Function (AMF)). |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| If known | Short description of possible detection techniques such as logs or sensors. |
| FGDS5009 | Access to IR.21 file should be logged. |
| FGDS5008 | Leaking this information in the Internet is obvious |

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) |
| Discovered IP addresses | IP addresses of core network functions known |

References:

|  |  |
| --- | --- |
| Name | URL |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |
| Claro Americas IR.21 Data, Accessed 30-June-2016 | http://www.claro.com.br/sites/files/contratos/arquivos/orpa\_roam\_claro\_001-2015\_-\_anexo\_4-apend\_a-roaming\_nacional\_-\_ir\_21\_0.pdf |
| Vivo Brazil IR.21 Data, Accessed 30-June-2016. | https://www.vivo.com.br/portalweb/ShowPropertyServlet?nodeId=/UCMRepository/CONTRIB\_093689 |