T1199.501 MNO Roaming Partners

Description: An adversary may breach or otherwise leverage a mobile network operator’s (MNO’s) roaming partners or their service partners to gain access to subscriber’s services or obtain information about that subscriber from their home network. Since these relationships are of a more trusted nature, end-to-end security is not necessarily used.

An adversary may use the trusted relationship with other mobile network operators and their related service providers such as roaming hubs, roaming partners, national partners, SMS service providers, lookup services to gain access to subscriber information at the subscriber’s home MNO. An adversary may take advantage of potentially weaker security at a roaming partner of a targeted MNO. The roaming MNO or their service partners could also be adversaries themselves.

These trusted relationships expose more interfaces to the roaming partner and their service providers than described in the related technique [FGT5029](/techniques/FGT5029). The information an adversary can obtain or modify about a subscriber and the subscriber’s activity depends on the specific location and assets compromised and additional techniques used. Information such as location, call records, messages, etc. are potentially obtained. Adversary use of additional techniques to compromise the VPLMN UPF (N9 endpoint) may result in direct compromise of user plane data. The adversary may generate queries using specially crafted messages as described in [FGT5029](/techniques/FGT5029) or obtain credentials and operate as an apparently authorized partner would to collect information. Depending on the roaming partner’s configuration, core functions may be directly exposed to service providers used by the roaming partner.

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: Initial-Access, Collection

Metadata:

* Architecture Segment: Roaming, App-Layer, Supply-Chain
* Platforms: SEPP
* Access type required: service account, token, expanded privilege
* Data Sources: application logs, network connection logs
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Partner supply chain compromise | The service partner of the MNO targeted may themselves be targeted as part of an attack chain using that roaming partners supply chain |
| Partner insider | A roaming partner, may have an adversary with a privileged position in the roaming or service partners organization and can use that position to attempt additional techniques against the targeted MNO. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1030 | Minimize exposure of functions to only those partner functions that need to access. |
| M1018 | Management of credentials used by partners to be scoped to the least privilege can minimize potential abuse. Does not mitigate misuse within allowed privileges. |
| M1037 | Ensure communication with functions such as a SEPP is constrained to necessary addresses, ports, and protocols. |
| M1054 | Validation of credentials properly can mitigate some MITM attacks and ensure revoked/expired credentials are not allowed. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Compromised partner | An adversary must already have compromised a trusted ~~V~~PLMN or one of their service providers, e.g. IPX, VAS, etc. |
| Compromised credentials | An adversary may need compromised legitimate credentials that could be used to obtain information from the MNO |
| Identified vulnerability | An adversary may need to identify a vulnerability in an MNO network function to send specially crafted requests to obtain initial access. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| SEPP | An adversary would want to compromise the cSEPP as it is the VPLMN end-point for the N32c channel to the HPLMN |
| VPLMN UPF | An adversary would want to compromise the VPLMN UPF as it is used as an endpoint on the roaming network for the N9 user plane interface between UPFs |
| VAS | An adversary would want to compromise a trusted VAS with access to the MNO’s core functions |
|  |  |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0015 | Analysis of application logs on the HPLMN SEPP and PLMN NFs may indicate unusual control channel activity. |
| DS0029 | Analysis of network traffic from VAS, and/or IPX may indicate unexpected or unusual traffic. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
|  |  |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| 5GS Roaming Guidelines Version 5.0 (non-confidential), NG.113-v5.0, GSMA, December 2021 | https://www.gsma.com/newsroom/wp-content/uploads//NG.113-v5.0.pdf |
| 5G; Security Architecture and Procedures for 5G System, TS 33.501 v16.10.0 Release 16, Sections 9.9, 13.1, 13.2, 3GPP, March 2022 | https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 |
| ETSI White Paper No. 46 – MEC security: Status of standards support and future evolutions, 1st edition, ETSI, May 2021 | https://www.etsi.org/images/files/ETSIWhitePapers/ETSI\_WP\_46-\_MEC\_security.pdf |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”,  October 2021 | https://arxiv.org/abs/2108.11206 |