T1048 Control plane signaling exfiltration

Description: An adversary may use Control Plane signaling between operator-internal Network Functions and externally-facing NFs or proxies to exfiltrate data to external endpoints.

The operator network uses edge functions that communicate to external parties: The Network Exposure Function (NEF) communicates with external Application Functions (AF), and the Security Edge Protection Proxy (SEPP) communicates with nodes on the IP Interchange (roaming/interconnect fabric). This channel can be used by an adversary to exfiltrate data originating at a compromised NF inside the operator network and ending up at the external node (AF, IPX node). For example, HTTP/2 optional parameters may be used to communicate between a core NF and an external server via NEF or SEPP.

Labelling:

* Sub-techniques: None
* Applicable Tactics: exfiltration

Metadata:

* Architecture Segment: Control-plane, Roaming
* Platforms: 5G Network
* Access type required: NF Service Account credentials
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| HTTP/2 optional parameters | HTTP/2 optional parameters may be used to communicate between a core NF and an external server (AF, IPX node) via NEF or SEPP. |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1037 | Filter and inspect network traffic coming out of SEPP and NEF |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Subscriber signaling data | Sensitive information in subscriber signaling data |
| Operator resource identifiers | Core NF identifiers (e.g. IP address, FQDN) such as AMF, SMF, UDM etc. |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0029 | Monitor and analyze traffic patterns and packet inspection over the SBI, especially to/from external functions. |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| 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 |