T1437 Control plane signaling disguise for C2

Description: An adversary may use Control Plane signaling between Network Functions (NFs) of the Service Based Architecture to disguise adversary’s C2 communication.

The 5G NFs may implement TLS and HTTP/2 for their communications (e.g. via Service Based Interfaces), which means the traffic will be encrypted. This type of communication between authorized NFs may be used to avoid detection by using legitimate protocols and port numbers and encrypting that data. Encryption makes it difficult to employ detection techniques to identify suspicious traffic patterns. In addition, HTTP/2 optional parameters may be used to communicate between a core NF and an external application function via NEF or between an NF in visited PLMN and an NF in home PLMN via SEPP.

In the same fashion, an adversary may use encrypted channels between authenticated NFs to disguise C2 communication.

Labelling:

* Sub-techniques: None
* Applicable Tactics: command-and-control

Metadata:

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

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Third party app (AF) to Network Exposure Function (NEF) to Core NF used as a data exfiltration channel | The signaling AF to NEF to UDM and back from UDM to NEF to AF is used in several procedures ([1]). Example: NIDD (non-IP data delivery) (see clause 4.25 of [2]), or VN (Virtual Network) group management. See clause 4.15.6 of [2]. |
| An NF in vPLMN to an NF in hPLMN via SEPP | AMF in vPLMN communicates to AUSF in hPLMN during UE authentication. This channel can be used to disguise C2 communication. |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGM5501 | Employ TLS proxies with DPI firewalls. TLS proxy/firewall can employ DPI to decrypt the packets and send them off to their destination, but only after logging what the packet contains.  The firewalls/proxies connect to a SIEM whose data is being kept up to date with current threats. Service communication proxy (SCP) can be also used for this purpose. |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Operator resource identifiers and signaling | IP addresses. FQDNs and TLS connections of core NFs are used for nefarious purposes |

Detection

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

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 |
| 3rd Generation Partnership Project (3GPP) TS 23.502, “Procedures for the 5G System (5GS); Stage 2 (Release 17)”, Technical Specification, v17.4.0, March 2022. | https://www.3gpp.org/DynaReport/23502.htm |