T1195.502 Compromise Service Supply Chain

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
|  |  |  |  |  |
|  |  |  |  |  |

Description: Adversaries may manipulate service or service delivery mechanisms prior to or while used by a mobile network operator (MNO) for the purpose of data or system compromise. The adversary will use the compromised service as a mean to apply additional techniques against interfaces exposed to the service provider such as the NEF. When the service provider hosts or provides core network functions, the adversary may attempt to compromise the 5G core components in the service provider environment, e.g. MEC hosted NFs, clause 5.13 in [1], or through the service provider environment, attempt compromise of other core NFs not hosted in the MEC. When service providers are used for providing service to customers, the adversary may be in a position to compromise information about the user. The adversary, as an example, may also compromise software and/or hardware used by the service provider, such as opensource, as a technique to gain initial access or achieve other tactics within the service provider to provide a position for initial access to the MNO.

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: initial-access

Metadata:

* Architecture Segment: MEC, OA&M, Virtualization
* Platform(s): None
* Access type required: N/A
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

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 |
|  |  |

Mitigations

|  |  |
| --- | --- |
| **MID** | **Use** |
| If known | Short description of potential mitigations. Preventive measures |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| NEF | Network Exposure Function is a likely target for adversaries in a MEC environment. |

Detection

|  |  |
| --- | --- |
| **DSID** | **Detects** |
| If known | Short description of possible detection techniques such as: analyze logs. |

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 |
| 3GPP TS 23.501 | https://www.3gpp.org/DynaReport/23501.htm |
| 3GPP TS 23.558 | https://www.3gpp.org/DynaReport/23558.htm |
| 3GPP TS 23.548 | https://www.3gpp.org/DynaReport/23548.htm |
| ETSI, White Paper No. 28, “MEC in 5G networks” | https://www.etsi.org/images/files/ETSIWhitePapers/etsi\_wp28\_mec\_in\_5G\_FINAL.pdf |

#doNotParse