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 may use the compromised service as a means 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 of [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 subscriber.

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’s network. Open source software may be an attractive target for supply chain attacks, as detection, reporting, and patch availability timelines can provide a greater window of opportunity for vulnerabilities to be exploited.

Labelling:

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

Metadata:

* Architecture Segment: MEC, OA&M, Virtualization
* Platform(s): 5G
* Access type required: N/A
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| HW supply chain | Hardware used in service may be compromised in its build and delivery supply chain |
| SW supply chain | Software used in service may be compromised in its build and delivery supply chain |
| OA&M tools | OA&M tools in service has greater access to network elements, compromise of such tools provide adversary access to network providing the service |
| Malicious Service provider | Service provider management may have nefarious intent for data collection or providing assistance to other nefarious actors |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| Supplier Evaluation | 5G Operators should evaluate suppliers of services for their technical and administrative controls to ensure that it meets minimum standards for assured services. These evaluations may include SW, HD supply chain, personnel and process used for service creation. |
| Integrate Performance and Change Management | 5G operators should integrate performance and change management from their suppliers into their own OA&M tools to have complete visibility into service |

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. |
| Transport network | Distributed deployment models may require third party transport service |
| MEC | Distributed deployment models may require third party MEC service |
| RAN | RAN as a Service or Shared RAN |
| MVNO Core and RAN infrastructure | Mobile Virtual Network Operators may complete rely on third party provided services for their subscriber |

Detection

|  |  |
| --- | --- |
| **ID** | **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 “System architecture for the 5G System (5GS); Stage 2 (Release 17)” | https://www.3gpp.org/DynaReport/23501.htm |
| 3GPP TS 23.558: “  Architecture for enabling Edge Applications” | https://www.3gpp.org/DynaReport/23558.htm |
| 3GPP TS 23.548: “5G System Enhancements for Edge Computing; Stage 2” | 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