T1195 Supply Chain Compromise

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

Description: Adversaries may manipulate products or product delivery mechanisms prior to deployment in an MNO’s production environment for the purpose of data or system compromise.

5G deployments are expected to have various deployment models comprise of vendor supplied VNF/CNFs, open-source software, and dedicated physical appliances from suppliers as well as white label hardware. It is also expected that 5G services to end consumer may include third party services to support resources required by 5G Core and RAN elements such as third party back haul, MEC or commercial Cloud data centers resources. Adversary may use a software or hardware supply chain to insert compromised components (binaries, FW, compromised processing chips) in the supply chain of a targeted MNO or taint entire supply chain first to have option to select a target from victims receiving compromised products. Opensource communities may be vulnerable to accidental or intentional compromise. These days a lot of reputable vendors also use open-source components in their license products, Opensource community can offer a conduit to a target victim.

Labelling:

* Sub-techniques: none
* Applicable Tactics: Initial Access
* Architecture Segment: Virtualization, OA&M
* Platform(s): Infrastructure, CI/CD & OA&M Tools, VNFs
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known |  |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1051 | Update Software regularly |
| M1016 | Vulnerability Scanning of software before it is brought into MNO environment as well as regular scans to detect abnormal behavior |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| CORE, RAN VNFs |  |
| OSS Tools |  |
| Security tools |  |
| CI/CD Tools |  |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0022 | Use verification of distributed binaries through hash checking or other integrity checking mechanisms. Scan downloads for malicious signatures and attempt to test software and updates prior to deployment while taking note of potential suspicious activity. |
| DS0013 | Perform physical inspection of hardware to look for potential tampering. Perform integrity checking on pre-OS boot mechanisms that can be manipulated for malicious purposes and compare against known good baseline behavior. |
|  |  |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC001, “Network Functions Virtualization (NFV); NFV Security; Problem Statement”, Jan. 2014, section 6.9 | https://www.etsi.org/deliver/etsi\_gs/nfv-sec/001\_099/001/01.01.01\_60/gs\_nfv-sec001v010101p.pdf |