T1542.501 Unauthorized software in NFVI- malware

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

Description: An adversary may implant malware in the Network Function Virtualization Infrastructure that will load during the pre-boot sequence to achieve persistence.

An adversary may implant unauthorized software in the NFVI to persist in the boot sequence or launch malicious software. 5G VNF deployments rely on underlying NFVI (Kubernetes, Openstack) resources and do not offer any checks of their own to validate resources. Possibilities exist to add malware in deployment pipelines, image building and storage process and thru add on tools. Unless Hardware Mediated Execution Environment (HMEE) is used to validate host resources, malware inserted during boot process may not be easily detected.

Labelling:

* Sub-techniques: none
* Applicable Tactics: persistence, defense-evasion

Metadata:

* Architecture Segment: Impl-Virtualization, Impl-OA&M
* Platform(s): Infrastructure, PNF, VNF Hosts
* Access type required: Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1046 | Boot integrity |
| M1045 | Code Signing |
| M1051 | Update Software |
| M1018 | User Account Management, active monitoring of access attempts to CI/CD tools |
| M1047 | System audits can reveal anomalous behavior that may be caused by rootkits. Audits of software repositories |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Physical, Virtual, and Cloud Native Functions | Any network functions within NFVI sphere of responsibility |
| Hosts | Any hosts in NFVI within 5G security zone or in CI/CD pipeline, security and OSS tools |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0022 | File changes of any sort that cannot be traced back to authorized change. |
| DS0007 | Software image inconsistency. Signature and checksum mismatch |
| DS0008 | Kernel executing unknow processes or unauthorized processes not typical of the host. |
| DS0029 | Network traffic pattern may reveal remote C2 communication from rootkit |
| DS0009 | Active processes or process log may reveal unauthorized activity due to rootkits |
| DS0019 | Background services not typically associated with the host |
| Degraded performance | System may have reboots, or unexpected performance degradation, may be slow to respond to inputs. |

Post-Conditions

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

References:

|  |  |
| --- | --- |
| Name | URL |
| ETSI NFV SEC025, Secure E2E VNF & NS management spec (WIP) v006, retrieved April 26, 2021 | https://docbox.etsi.org/ISG/NFV/Open/Drafts/SEC025\_Secure\_E2E\_VNF\_%26\_NS\_management |