T1014 Unauthorized software in NFVI

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

Description: An adversary may implant rootkits in the Network Function Virtualization Infrastructure (NFVI) that will hide the presence of programs, files, network connections, services, drivers, and other system components.

Rootkits are a special type of malware designed to remain hidden on a target computer. These Rootkits can be created for hardware and firmware for CMOS and other chips, Kernel, Memory, and Applications.

Adversaries may implant rootkits during device manufacturing process, use compromised CI/CD pipeline, direct access to device to implant rootkits in the Cloud, MEC, RAN, UE components.

Adversaries may use rootkit compromise for other actions such as credential dumping, configuration changes, or attack other components in the network. Rootkits are hard to detect and may not be easily identified by end point protection software. Host suspected of rootkit infection may need to be quarantined and rebuilt from scratch with known good software.

Labelling:

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

Metadata:

* Architecture Segment: Virtualization, 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 |
| M1047 | System audits can reveal anomalous behavior that may be caused by rootkits. |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Physical, Virtual, and cloud native functions | NFVI components that support virtualization and network connecting the virtual functions. |
| Hosts | Any compute entity that supports data processing functions, including Linux/Windows hosts, VMs, and or specialty equipment that has address and interacts with other NFVI elements. |

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 |