T1525: Compromised image

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

Description: An adversary may install a compromised image in the image repository to achieve persistence.

The 5G VNF software is either developed in house or supplied by a product vendor. Typically, software is stored in a deployment repository for deployment or for an orchestrator to use as part of an automated workload deployment activity. An adversary may install a compromised image in the repository of 5G VNFs and or VM/Container images to later establish C2 connection and subsequent modification, discovery, and exfiltration operations.

Labelling:

* Sub-techniques: No sub-techniques
* Applicable Tactics: persistence

Metadata:

* Architecture Segment: Impl-Virtualization, Impl-CSP, Impl-OA&M, Supply Chain
* Platform(s): VM, Container, Azure/AWS, IaaS, SDN
* Access type required: User or Administrative access to repository
* Data Sources: Logs for repository
* 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

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1043 | Restricted Permissions to add images to repositories for person and non-person accounts |
| M1049 | Manual or automated image creation and storage must include image hash |
| FGM5090 | Logs from tools and repository must be corelated to ensure unauthorized activity is reported. |
| FGM5089 | In addition to image name, deployment tools must use hash and verify image during deployment |
| FGM5088 | Development and production repositories should be separated to avoid access and image slipovers. Production repositories should be access controlled for accounts responsible for deployments and operations accounts only. |
| M1035 | Access to repositories should be restricted to known networks from where any authorized actions need be executed. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Credential and Access to repository and or image creation tools (i.e. Docker) | An image can be manipulated, or a new image can be introduced to have same impact. Privileged Access to tool or repo is required. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Core, RAN, SDN, System tools | An adversary may target a particular network domain, CI/CD, or security and operations tools. |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGDS5012 | Analyze logs and other CI/CD events to detect unauthorized activity |
| FGDS5015 | An automated image hash verification should be performed |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| A Compromised Image is deployed in production | A compromised image deployed in the production can lead to variety of adversarial activities depending on what capabilities were added/deleted from the image. |

References:

|  |  |
| --- | --- |
| Name | URL |
| ENISA THREAT LANDSCAPE FOR 5G NETWORKS, December 2020, section 6.2. Accessed April 13, 2021 | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks/ |
| Docker Documentation, Security, Content in Trust | https://docs.docker.com/engine/security/trust/ |