T1020.001 Network Traffic Duplication

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| July 27, 2022 | MV |  | Modified labeling/metadata | Other changes to bring in line with expected formats |
| July 18, 2023 | MV | Removed hyperlinks from Detections and Mitigations because they were not showing |  |  |

Description: An adversary may use compromised virtualized network elements to (vSwitch, vRouter, Virtual Firewalls) to span traffic to sniffing port for access to user plane and control plane data.

In a virtualized environment, access can be gained much more easily as the servers making up a function are more likely to be virtually distributed and the SDN vSwitch would allow an adversary to fork IP packets flowing much more easily between hosts remotely. Most network devices/software have capabilities for traffic duplication for troubleshooting or legal purposes (Lawful Interception). Such forking is very difficult to detect or prevent from within a 3GPP NF or VM. An adversary could read data in transit without being detected by application monitoring software.

Labelling:

* Sub-techniques: none
* Applicable Tactics: Discovery

Metadata:

* Architecture Segment: OA&M, Virtualization
* Platforms: 5G
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| M1041 | Encrypt sensitive data flows for Control plane and User plane traffic |
| M1026 | Manage accounts with privilege to make changes either in the device or its controller. |
|  |  |

Pre-Conditions

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

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Virtual elements | Virtual switch, Virtual Router, Virtual Firewalls, Virtual Load Balancers, SDN Controllers |
|  |  |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| DS0029 | Monitor network traffic for new traffic flows, analyze socket connections and protocol used to determine abnormal behavior. |
| DS0017 | Monitor Command executions on the devices |
| DS0022 | Network elements use active and start up configuration files, monitoring configuration drifts can reveal abnormal activity |
| DS0028 | Monitor log on sessions and escalation to higher privilege activity on the devices |
| DS0002 | Monitor all user accounts accessing network devices to detect abnormal activity |

Post-Conditions

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

References

|  |  |
| --- | --- |
| Name | URL |
| 3GPP TR 33.848 Security Impacts of Virtualization,  Section 5.15.2 | https://www.3gpp.org/DynaReport/33848.htm |