T1599 Network Boundary Bridging

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| Aug 2 | MV |  |  | Removed quotes. Red text added |
|  |  |  |  |  |

An adversary may compromise network separation controls to gain access to one or more of the 5G security zones or networks. 5G is a system of systems and may be composed of several network and security zones, and slices. A compromise of controls placed to maintain security zones or network segmentation based on IP networks, application groups or slices may allow adversary to gain unauthorized access to networks or services. This may occur at a Core, RAN, Cloud or Slice boundary.

Once the adversary has infiltrated the internals of the network, it has ample opportunities and a much broader attack surface to explore. The adversary can, e.g., conduct privilege escalation and process injection for gaining administrative rights, attempt password cracking of valid user accounts on the nodes, exploit vulnerabilities in databases and file systems, and take advantage of improper configurations of routers and switches.

Labelling:

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

Metadata:

* Platform(s): OA&M
* Access type required: User/NPE/Administrative access
* Data Sources:
* Theoretical/Proof of concept/Observed:
* Architecture Segment: Impl-OA&M, Impl-Virtualization, Arch-Slice

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1043 | Credential Access Protection |
| M1037 | Filter Network Traffic |
| M1026 | Privileged Account Management |
| M1032 | Multi-factor Authentication |
| M1027 | Password Policies - NIST Guidelines. This may also include token policies if security tokens are used. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Privileged access | Privileged access to device implementing the network separation controls |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Devices enforcing segmentation controls | Devices enforcing network segmentation and creating perimeter for applications may include firewalls, SDN controllers, or Proxies. |
|  |  |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0029 | Network Traffic should be monitored for traffic flows and messaging contents to determine abnormal activity. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Unusual network traffic flows | If network boundaries are breached, monitoring system may detect unusual network flow |
| Network mapping activity | Adversary may attempt to discover networks and live hosts on the networks |
| Connection attempts from unusual hosts | Adversary may attempt connect to hosts in the target network after profiling hosts and network mapping. |

References:

|  |  |
| --- | --- |
| Name | URL |
| S.P. Rao, S. Holtmanns, T. Aura: “Threat modeling framework for mobile communication systems”, May 2020 | https://arxiv.org/abs/2005.05110v1 |
| R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield, “Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK”, October 2021 | https://arxiv.org/abs/2108.11206 |