T1599 Network Boundary Bridging

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
| Aug 2 2022 | MV |  |  | Removed quotes. Red text added |
| June 6 2023 | MV |  |  | Expanded mitigations. Added acronym disambiguation |
|  | MV | No procedures | Added 2 procedures |  |
| July 11, 2023 | MV | Description doesn’t show | Added word “Description” at the beginning of the file |  |

Description: 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, as well as slices. A compromise of controls placed to maintain security zones or network segmentation based on IP networks, application groups or slices may allow an 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.

The boundaries of a network and its security zones can exist between various technologies, such as 4G and 5G, or between different partners, such as private networks, mobile operators, or Mobile Virtual Network Operators (MVNOs). These boundaries can also exist between different network components, such as radio access, core, edge, and cloud, as well as between national or international links and operator cores, and service providers or operator cores.

In some cases, firewalls may be used to separate these zones, such as SS7 protocol, Diameter protocol, 5G APIs, enhanced SCP (Service Communication Proxy), IP (Internet Protocol), SIP (Session Initiation Protocol), and GTP (GPRS Tunneling Protocols) firewalls. Alternatively, an interworking function may be used to translate one protocol into another. However, it's important to note that privileged access is not always necessary to bypass a firewall or exploit an interworking function. Often, insufficient filtering may be the cause, or the filtering may not be sufficiently deep.

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** |
| Impersonate roaming partner/VAS (Value Added Service) provider | An adversary may impersonate a trusted source (roaming partner or VAS) to avoid filtering by firewall, and to transport data in and out of the targeted operator’s network. ([1]) |
| MANO abuse to change SDN (Software Defined Networking) configuration | An adversary may abuse the remote service offered for network MANO tools, to make configuration changes to SDN flow tables and cause packet filtering to not detect flow across boundaries. ([2]) |

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| M1043 | Protect credentials of management entities |
| M1037 | Filter Network Traffic, per protocol |
| M1026 | Manage accounts for privileged users for the security zones in the 5G network. |
| M1032 | Enable Multi-factor Authentication for privileged users |
| M1027 | Password Policies – follow 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 |