T1499.002 Base Station flood with fictitious access requests

Description: An adversary may transmit an overwhelming number of access requests to a gNB to degrade the ability of legitimate UE to obtain access.

An adversary transmits large number of access requests over Random Access CHannel (RACH) to degrade the ability of legitimate UE to obtain access from the gNB. May be done via a compromised UE or a fake UE.

Labelling:

* Sub-technique(s): N/A
* Applicable Tactics: Impact

Metadata:

* Architecture segment: RAN, UE
* Platforms: 5G RAN
* Access type required: Radio access
* Data Sources: access requests
* Theoretical/Proof of Concept/Observed: Observed

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Access request flooding | Adversary transmits an overwhelming number of access requests over Random Access CHannel (RACH) to degrade the ability of legitimate UE to obtain access. May be done via a compromised UE or a SDR running OAI-5G modified software. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Use** |
| FGM1502 | Increase RACH resources. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Transmit to gNB with sufficient power to succeed in flooding. | Adversary must be able to transmit to gNB with sufficient power to be received. |
|  |  |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| RACH | Adversary targets access requests in Random Access CHannel (RACH) |
|  |  |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5007 | Excessive number of access requests received at gNB. |
|  |  |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Less service for legitimate UEs | Legitimate UEs have low probability of successfully requesting access |

References:

|  |  |
| --- | --- |
| **Name** | **URL** |
| European Union Agency for Cybersecurity (ENISA): “ENISA Threat Landscape for 5G Networks” Report, December 2020. | https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks |