T1499.501 Consume data allocation to deny or degrade service

Description: A malicious app consumes subscriber data allocation so as to deny or degrade service to that UE.

A malicious application might consume a UE's limited data plan, denying or throttling service.

Labelling:

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

Metadata:

* Architecture segment: UE
* Platforms: 5G UE
* Access Type required: Application on UE
* Data Sources:
* Theoretical/Observed: Theoretical

Procedure Examples:

|  |  |
| --- | --- |
| **Name** | **Description** |
| Malicious data consumption application | Convince user to download or maliciously introduce application that consumes excessive data |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Name** |
| FGM5007 | Unlimited data plan. Attack is mitigated with a true unlimited data plan |
| FGM5008 | Monitor installed applications for data usage. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| A malicious app or set of apps have to have been installed on the UE | There are several methods to achieve this |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| Assured user communications | Communications is denied until additional data usage is purchased. |

Detection

|  |  |
| --- | --- |
| **ID** | **Detects** |
| FGDS5006 | Excessive data usage reported by UE or service provider. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Sustained degraded communication until additional data is purchased. | Sustained degraded communication until additional data is purchased. |

References

|  |  |
| --- | --- |
| Name | URL |
| Android devices ensnared in DDoS botnet, Feb. 2021 | https://www.zdnet.com/article/android-devices-ensnared-in-ddos-botnet/ |
| Massive Android DDoS Botnet Derailed, Aug. 2017 | https://www.darkreading.com/attacks-breaches/massive-android-ddos-botnet-derailed |