FGT5006 DNS Manipulation

Description: An adversary can manipulate DNS requests to redirect network traffic and potentially reveal end user activity.

DNS Manipulation encompasses a series of techniques relating to modifying DNS packets/configurations to redirect network traffic or unmask the identities and activities of end users.

Labelling:

* Sub-Technique(s): FGT5006.001, FGT5006.002
* Applicable Tactics: Collection, Defense Evasion, Fraud, Command and Control, Persistence, Exfiltration

Metadata:

* Architecture segment: User plane
* Platforms: 5G
* Access type required: privileged
* Data Sources: Network Traffic, Application Log
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples:

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

Mitigations

|  |  |
| --- | --- |
| **Name** | **Description** |
| FGM1557 | Use strong data integrity protection algorithms |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Unauthenticated DNS Services | The end user does not have the capability to validate whether it is communicating with a malicious DNS or a valid one. |
| Unmonitored DNS Traffic | DNS traffic must be permitted to move through the network without verification that it is routed to valid DNS Servers and without checking to ensure that the contents of the packets are actually DNS requests. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| DNS Servers | Whoever controls the DNS Servers controls how and what end users connect to over the network, making DNS Servers a type of critical infrastructure. |
| Subscriber data | Data such as URL accessed |

Detection

|  |  |
| --- | --- |
| **Name** | **Description** |
| DS0029 | Data transmitted across a network (ex: Web, DNS, Mail, File, etc.), that is either summarized (ex: Netflow) and/or captured as raw data in an analyzable format (ex: PCAP) |
| DS0015 | Logs from DNS forwarders/servers can be used to detect changes in usage from endpoints |

Post-Conditions

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

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| D. Rupprecht, K. Kohls, T. Holtz, and C. Popper, “Breaking LTE on Layer Two” https://alter-attack.net | https://alter-attack.net/media/breaking\_lte\_on\_layer\_two.pdf |
| S.P. Rao, S. Holtmanns, T. Aura, “Threat modeling framework for mobile communication systems” | https://arxiv.org/pdf/2005.05110.pdf |
| Peng, C., Li, C., Tu, G., Lu, S., & Zhang, L. (2012). Mobile data charging: new attacks and countermeasures. Proceedings of the 2012 ACM conference on Computer and communications security. | https://dl.acm.org/doi/pdf/10.1145/2382196.2382220 |