FGT5006.002 DNS Manipulation: Encapsulation

Description: An adversary can hide user traffic within DNS requests that are part of the data sessions and transmit data undetected.

An adversary can hide user data within DNS requests that are part of data sessions to access the Internet and transmit data undetected. This can be used to hide traffic for billing fraud, command and control of a bot or other device, or for any other task where moving data through a permitted channel is useful.

To move data, the adversary may simply encode data as a hostname query by placing the data in the names section of a DNS lookup. The receiving DNS server, controlled by the adversary, logs the query and decodes the data from the name. The reply to the query may or may not actually need to be sent.

Labelling:

* Sub-Technique(s): N/A
* Applicable Tactics: Fraud, Command and Control, Exfiltration

Metadata:

* Architecture segment: Arch-User plane
* Platforms: 5G
* Access type required: user
* Data Sources: Network Traffic
* Theoretical/Proof of Concept/Observed: Theoretical

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Free fake DNS loophole | Operators do not enforce free DNS service via the standard five-tuple flow ID (src IP, dest IP, src port, dest port, protocol). Instead, they use only the destination port (or plus protocol ID), thus exposing a vulnerability. |

Mitigations

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

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Unauthenticated DNS Services | The end user must not have the capability to validate whether it is communicating with a malicious DNS or a valid one. |

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. |

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) |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| Billing Fraud | Attacker will be able to route traffic through DNS channels to use the network free of charge. |
| Command and Control Network | Attacker can route command and control traffic through DNS to control botnets or other entities. |
| Exfiltration Route | Attacker has a route to exfiltrate stolen data disguised as DNS packets. |

References

|  |  |
| --- | --- |
| **Name** | **URL** |
| “Bhadhra Framework”: 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 |
| Merve Sahin, Aurelien Francillon, Payas Gupta, and Mustaque Ahamad. 2017.  “*Sok: Fraud in telephony networks*”. In 2017 IEEE European Symposium on Security  and Privacy (EuroS&P). IEEE, p235–250 | https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7961983&tag=1 |
| Kui Xu, Patrick Butler, Sudip Saha, Danfeng (Daphni) Yao in DNS CC Journal, “DNS for Massive-Scale Command and Control” | https://people.cs.vt.edu/~danfeng/papers/DNS-CC-JOURNAL.pdf |