T1048.003 DNS Queries

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Who | Current text | Proposed text | Final text |
|  |  |  |  |  |
|  |  |  |  |  |

Description: Adversaries may steal data by exfiltrating from an MNO by sending it over allowed DNS queries to DNS servers outside the MNO. The data may be sent to an alternate network location from that used for command and control.

Adversaries may opt to obfuscate this data within the constraints of DNS record types. The adversary may also use custom or publicly available encoding/compression algorithms (such as base64) as well as embedding data within protocol headers and fields.

Labelling:

* Sub-techniques: N/A
* Applicable Tactics: Exfiltration

Metadata:

* Architecture Segment: Control Plane, Roaming
* Platform(s): NF, SEPP
* Access type required: N/A
* Data Sources: Application Logs, Network Logs
* Theoretical/Proof of concept/Observed: Theoretical

Procedure Examples

|  |  |
| --- | --- |
| **Name** | **Description** |
| Specific example if known | If there is a documented instance of this technique occurring in earlier generation or a notional example |

Mitigations

|  |  |
| --- | --- |
| **MID** | **Use** |
| M1037 | Filter public network lookups to limit exfiltration destinations. Potential use of protective DNS services. |
|  |  |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| External DNS Resolution | Operator environment must permit DNS queries either directly or recursively for domains the operator doesn’t directly control. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| DNS Resolvers | The configuration of DNS Resolvers is important to ensure ability to monitor DNS queries for adversary behavior. |

Detection

|  |  |
| --- | --- |
| **DSID** | **Detects** |
| DS0015 | Collect and analyze DNS lookup logs for unusual patterns and destinations |
| DS0029 | Analyze network destinations for DNS traffic for unusual destinations and volumes. |

Post-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of potential capabilities achieved by the technique (e.g. escape from container gives control of the host) |

References:

|  |  |
| --- | --- |
| Name | URL |
| “Bhadra framework”: S.P. Rao, S. Holtmanns, T. Aura, “Threat modeling framework for mobile communication systems,” Retrieved April 28, 2022 | https://arxiv.org/pdf/2005.05110.pdf |

#doNotParse

Interesting write up on edge DNS for UE - <https://www.lightreading.com/partner-perspectives-(sponsored-content)/super-charge-your-5g-network-by-moving-dns-to-edge/a/d-id/772494>

https://www.infoblox.com/dns-security-resource-center/dns-security-issues-threats/dns-security-threats-data-exfiltration/