<Number> <FiGHT Name of Technique/Sub-Technique>

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

Description: <BLUF SENTENCE, ONE LINE ONLY.> <Following paragraphs: Information about the (sub-)technique, what it is, what it’s typically used for, how an adversary can take advantage of it, and variations on how it could be used. Include references to authoritative articles describing technical[1] information related to the technique as well as in the wild use references as appropriate. >

(Background info (not too longwinded) can be added here to help understand the description above. The background info paragraph(s) should be in the FiGHT spreadsheet)

Labelling:

* Sub-techniques: <list full number(s), if any. COMMA DELIMITED LIST ONLY. If none, “None”. If a subtechnique, use “N/A”>
* Applicable Tactics: <at least 1, as appropriate, COMMA DELIMITED LIST ONLY>

Metadata:

* Architecture Segment: <e.g. RAN, MEC, OA&M, User-plane etc.>
* Platform(s): <at least 1. COMMA DELIMITED LIST ONLY.>
* Access type required: <N/A or: user/subscriber, admin (service account (P or NP)), expanded privilege, token. COMMA DELIMITED LIST ONLY >
* Data Sources: <blank; or: what data is needed to do detections listed below, e.g. logs>
* Theoretical/Proof of concept/Observed: <ONLY ONE OF THESE VALUES: Theoretical / Proof of Concept / Observed>

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** |
| If known | Short description of potential mitigations. Preventive measures |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |

Critical Assets

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of the assets that adversary wants to target or that are at risk such as data (system/user, access token, crypto key etc.), capability, service. |

Detection

|  |  |
| --- | --- |
| **DSID** | **Detects** |
| If known | Short description of possible detection techniques such as: analyze logs. |

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 |
| The name that will appear on the website | The fully functional URL that will be the hyperlink for the text in the left hand column. |

#doNotParse