T1195.501 SIM credential theft

Description: An adversary may get access to several SIM credentials during transfer from a SIM card vendor to an operator.

Unauthorized actors use various means to intercept/steal SIM data in transit from SIM card vendors towards the HSM or the UDR/UDM in the operator's network in order to obtain customer credentials.

Labelling:

* Sub-technique: N/A
* Applicable Tactics: credential-access

Metadata:

* Architecture segment: UE
* Platforms: 5G
* Access type required: physical or malware insertion
* Data Sources:
* Theoretical/ Proof of concept/Observed: 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 |
| Infiltrate SIM vendor’s network. | Allegedly: the UK agency GCHQ planted malware on Gemalto servers to obtain SIM credentials. The number of keys obtained were in the order of millions. [1] |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| M1017 | Personnel security: Train personnel in SIM card OEMs to be wary of social engineering and other attempts of unauthorized parties to gain access to any relevant resource, and to report suspicious activities |
| M1030 | Physical and cyber security of IT systems, servers. |
| M1022 | Restrict access to files exchanged between SIM vendor and MNO |
| M1041 | Protect the files where SIM data is stored by encryption |
| FGM1557 | Protect the files where SIM data is stored by integrity protection |

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. |
| Privacy of subscriber data and voice traffic | Adversary is after getting the keys to decrypt cellular communications for those sets of SIMs whose credentials it captured. |

Detection

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of possible detection techniques such as logs or sensors. |
|  |  |

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** |
| Daily Mail.com, news article 20 Feb 2015, "US and UK spies hacked SIM card manufacturer to steal codes that allowed them to eavesdrop on mobile phones worldwide, according to bombshell documents leaked by Ed Snowden". | https://www.dailymail.co.uk/news/article-2961314/US-UK-hacked-SIM-card-manufacturer-steal-codes-allowed-eavesdrop-mobile-phones-worldwide-according-bombshell-documents-leaked-Ed-Snowden.html |
| GSMA FS.28 “Security Guidelines for Exchange of UICC Credentials”, Version 1.0, November 2020. | https://www.gsma.com/security/resources/fs-28-security-guidelines-for-exchange-of-uicc-credentials/ |

#doNotParse

*Background info*:

The SIM credentials enable actors to decrypt the voice, text and data communications of targeted mobile users in a passive way in order to evade detection.

Mitigations that were written but removed since they didn’t need a FiGHT -specific mitigation

* Secure SIM data by strong encryption
* Protect the files where data is stored by encryption and integrity protection
* Securely transfer those files between SIM vendor and MNO by physical or digital transmission

[2]