FGT5001 Network-side SMS collection

Description: An adversary may compromise the operator's SMS Center (SMSC) to collect SMS messages to/from the UEs.

The SMSC is a server in 3G, 4G, and 5G networks, and it communicates in 5G with the SMS Function (SMSF) and IMS function IP-SM-GW, using MAP protocol.

An adversary can eavesdrop the SMS data to/from certain subscribers (identified by IMSI or MSISDN), by compromising the operator’s SMSC. Similar techniques can be applied to other operator functions such as IP-SM-GW or STF, SMSF, towards the same goal.

Labelling:

* Sub-technique(s) : None
* Applicable Tactics: collection

Metadata:

* Architecture segment: User plane
* Platforms: 5G Network
* Access Type Required:
* 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 |
| Malware loaded into a Linux running SMSC server | A data miner program may be loaded by an installation script. The script targets and saves SMS messages (the contents, the IMSI and the source and destination phone number). This is highly targeted to given IMSI numbers (e.g., proponents of movements against the Chinese gov’t). (note: Call Data Records (CDRs) were also targeted for certain IMSIs, the info therein is call metadata, i.e. time, duration, phone numbers). [1], [2]. |

Mitigations

|  |  |
| --- | --- |
| **ID** | **Description** |
| If known | Short description of potential mitigations. |
| M1049 | Check telecom servers for malware or use endpoint security solution. Implement the latest patches in Linux systems and use strong anti-virus software to detect malware. |

Pre-Conditions

|  |  |
| --- | --- |
| **Name** | **Description** |
| If known | Short description of conditions that must be present for technique to be used. |
| Malware developed | Adversary must first develop the malware to achieve the procedures herein. |

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. |
| User data | User data from SMS |

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** |
| Dynamic Ciso.com “New Malware Discovered by FireEye APT41, Infects SMS Servers Within Telecoms”, Nov 1, 2019, retrieved March 4, 2022. | https://dynamicciso.com/new-malware-discovered-by-fireeye-apt41infects-sms-servers-within-telecoms |
| Leong, Raymond, Perez, Dan & Dean, Tyler, “MESSAGETAP: Who’s Reading Your Text Messages” FireEye. 31 Oct 2019. | https://www.mandiant.com/resources/messagetap-who-is-reading-your-text-messages |