Mobile Threat Intelligence Framework (MoTIF) Principles
Version 1.0
21 March 2024

Security Classification: Non-Confidential

Copyright Notice

Disclaimer

Compliance Notice

The information contain herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document is classified by GSMA as an Industry Specification, as such it has been developed and is maintained by GSMA in accordance with the provisions set out GSMA AA.35 - Procedures for Industry Specifications.

Table of Contents

1 Introduction

1.1 Overview

This document provides an overview of the GSMA Mobile Threat Intelligence Framework (MoTIF) and describes the principles of that framework.

The framework will enable adversaries' attacks against mobile networks and adversaries' use of mobile networks to be described in a structured way, based on the tactics, techniques and procedures (TTPs) that they employ.

1.2 Scope

The scope of GSMA MoTIF includes mobile network related attacks that are not already covered by existing public frameworks like the MITRE ATT&CK® Matrix for Enterprise [1] and the ATT&CK® Matrices for Mobile [2]. In scope are 2G, 3G, 4G, 5G, including all kind of telecommunication service enablers (e.g., roaming, SMS, VoIP) and future mobile technology evolutions. Fraud attacks against mobile networks and their customers are also included.

1.3 Abbreviations

Term	Description
AIR	Authentication Information Request
AS	Access Stratum
ATT&CK®	Adversarial Tactics, Techniques, and Common Knowledge
AuC	Authentication Centre
DEA	Diameter Edge Agent
FiGHT™	5G Hierarchy of Threats
FFS	For further study
GT	Global Title
HLS	High-Level Strategy
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
IMSI	International Mobile Subscriber Identity
MISP	Malware Information Sharing Platform
MNO	Mobile Network Operator
MoTIF	Mobile Threat Intelligence Framework
MSISDN	Mobile Station International Subscriber Directory Number
NF	Network Function
NAS	Non-Access Stratum
PRD	Permanent Reference Document
RAN	Radio Access Network
RAT	Radio Access Technology
SDO	STIX Domain Object
SIB	System Information Block

Term	Description
STIX™	Structured Threat Information Expression
SMS	Short Message Service
T-ISAC	Telecommunication Information Sharing and Analysis Centre
TAC	Tracking Area Code
TAU	Tracking Area Update
TTP	Tactics, Techniques and Procedures
UE	User Equipment
VPLMN	Visited Public Land Mobile Network

1.4 References

Ref	Doc Number	Title
[1]	MITRE ATT&CK® Enterprise Matrix	MITRE ATT&CK® Enterprise Matrix https://attack.mitre.org/matrices/enterprise/
[2]	MITRE ATT&CK® Mobile Matrix	MITRE ATT&CK® Mobile Matrix https://attack.mitre.org/matrices/mobile/
[3]	MITRE FiGHT™ 5G Hierarchy of Threats	https://fight.mitre.org/
[4]	PRD FS.58	Mobile Threat Intelligence Framework (MoTIF) Examples
[5]	PRD AA.35	Procedures for Industry Specifications
[6]	RFC2119	“Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. http://www.ietf.org/rfc/rfc2119.txt
[7]	RFC8174	Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words https://www.rfc-editor.org/info/rfc8174
[8]	CIS-CDM	Center for Internet Security (CIS) Community Defense Model (CDM) v2.0 https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0
[9]	Intel TARA	Prioritizing Information Security Risks with Threat Agent Risk Assessment https://media10.connectedsocialmedia.com/intel/10/5725/Intel_IT_Business_Value_Prioritizing_Info_Security_Risks_with_TARA.pdf
[10]	ENISA Threat Landscape 2021	https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[11]	STIX for MITRE ATT&CK	https://github.com/mitre-attack/attack-stix-data/blob/master/USAGE.md

1.5 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be

interpreted as described in RFC 2119 [6] and clarified by RFC8174 [7], when, and only when, they appear in all capitals, as shown here.

2 Principles of MoTIF Tactic/Technique Re-use, Naming and Descriptions

In GSMA MoTIF, adversaries' attack details are described according to industry practice which include tactics, techniques and sub-techniques. This information forms the MoTIF attack pattern, which is defined in this document in a way that is compatible with the MITRE ATT&CK® Enterprise and ATT&CK® Mobile matrices.

2.1 MoTIF Tactics

In GSMA MoTIF the same tactic names and general principles as the ATT&CK Enterprise matrix are used. The descriptions are also the same, except in the case where the ATT&CK Enterprise tactic description is obviously unsuitable or limiting for mobile networks. In this case the ATT&CK Mobile description is be used instead, or if that is not suitable either, a new, but closely aligned description is used.

An example of this is the *Credential Access* tactic, which is described in ATT&CK Enterprise as: *"The adversary is trying to steal account names and passwords"*. In this case this description is limiting when it comes to mobile networks as capturing authentication vectors would also count as a *Credential Access* vector, although strictly speaking it is not an account name or password. MoTIF instead uses the more appropriate description of this tactic from the ATT&CK Mobile matrix, which is: *"The adversary is trying to steal account names, passwords, or other secrets that enable access to resources"*.

MoTIF tactics are the same as those defined for the ATT&CK Enterprise Matrix v14.1, i.e.:

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defence Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact

Note: MITRE FiGHT [3] as of version 2.1.0 is using ATT&CK Enterprise Matrix v14.

2.2 MoTIF Techniques

Unlike tactics, MoTIF technique (and sub-technique) naming is based on the principle of extendibility and correctness via a new technique if required, rather than always preserving

the ATT&CK or FiGHT technique name and attempting to redefine it. Attempting to preserve and re-use existing ATT&CK techniques and sub-techniques would lead to issues when using MoTIF, as the existing ATT&CK Enterprise (and Mobile) techniques/sub-techniques are in many cases not suitable and difficult to accurately apply to mobile network adversaries.

For example, in the case where an adversary wished to do 4G cellular interception, part of the attack chain involves the attacker sending multiple Diameter AIR requests with different PLMN-IDs, to determine which ones would be allowed through in order to (later) retrieve the authentication vectors. This tactic would obviously be classified as *Reconnaissance: "The adversary is trying to gather information they can use to plan future operations".*

However, the technique or sub-technique to use to categorise this adversary activity needs to diverge from what is defined in ATT&CK to be precise. If MoTIF re-used existing ATT&CK Enterprise or FiGHT techniques and sub-techniques, then one way would be to classify this activity by re-using the technique *Network Service Scanning: FGT1046.*

- *Network Service Scanning* is defined as: *"Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation."*

This technique description is accurate, but not precise. It would tell the MoTIF user nothing about the actual technique that was used. By re-using the ATT&CK Enterprise technique/sub-techniques names, precision has been lost.

For this reason, the MoTIF approach in this case is to reuse the technique: *Network Service Scanning* and create a new sub-technique called *Scan Signalling Addresses.*

- The MoTIF technique name *Network Service Scanning* is based on *Network Service Scanning* as defined in MITRE FiGHT, but its description is expanded to include specific mobile network information and context.
- The sub-technique name *Scan Signalling Addresses* gives some further mobile - specific information on how exactly the scanning was undertaken. Other specific scanning sub-techniques could be *Scan IP Addresses* and *Obtain Subscriber Information*.

In general, the principle should be that unless the existing ATT&CK Enterprise/Mobile techniques/sub-techniques are relevant and relatively precise, then new techniques and sub-techniques SHALL be used, where the name chosen is mobile network related.

However, MoTIF users should be aware that sub-techniques should not be too precise, as this leads to duplication and an excessive number of techniques/sub-techniques. For example, in the above case, there is no need to define a sub-technique called: *Scan Diameter Signalling Addresses*, because the choice of protocol used can be indicated in

other tactics/techniques. A suggestion in this case would be *Initial Access* (tactic) -> *Exploit via Core Signalling Interface* (technique) -> *Diameter Protocol* (sub-technique).[1]

The re-use of a ATT&CK of FiGHT technique does not imply it will be used under the same tactic(s), nor that all the sub-techniques of the technique will be re-used.

2.2.1 ATT&CK / FiGHT technique/sub-technique tracking

As outlined in section 2.2, MoTIF reuses techniques/sub-techniques from MITRE ATT&CK. In addition, in some cases MoTIF is re-using MITRE FiGHT techniques and sub-techniques. The relevant version that these are based on are outlined in section 2.1

As ATT&CK changes/updates every 6 months, then where practical the MoTIF group should compare and inspect against any new ATT&CK version, to see if the re-use is still applicable (i.e. if there have been error corrections, or changes which make a technique or sub-technique reuse more or less useful). MITRE FiGHT updates less frequently, but the same inspection should occur as well.

2.3 Tactic/Technique Numbering

All MoTIF techniques, sub-techniques, software, mitigations, groups (procedure examples) and data sources (detection) SHALL have a unique MoTIF number regardless of whether they are new or re-used. A three- or four-letter prefix, in the format MO[Y] SHALL be used with each MoTIF number, where Y is the one or two-letter ATT&CK designation. Numbers SHALL be assigned in the range 3000 to 3999. This approach is illustrated in Table 1.

Term	ATT&CK	GSMA MoTIF
Tactics	TAxxx	MOTAxxx (3000->3999)
Techniques	Txxxx	MOTxxxx (3000->3999)
Software	Sxxxx	MOSxxxx (3000->3999)
Mitigations	Mxxxx	MOMxxxx (3000->3999)
Groups (Procedure Examples)	Gxxxx	MOGxxxx (3000->3999)
Data Sources (Detection)	DSxxxx	MODSxxxx (3000->3999)

Table 1 – MoTIF Tactic/Technique Numbering

Other additional designations (which may arise if a new Term was introduced) SHALL follow this logic.

In the case of re-used techniques, the same number SHALL be taken. For example, *Trusted Relationship* (defined as T1199 in ATT&CK Enterprise, is designated as MOT1199 in GSMA MoTIF. For new MoTIF techniques, procedures etc, the number chosen SHALL be in the range 3000->3999. This will allow new techniques to be identified easily.

[1] MITRE ATT&CK and 5G FiGHT techniques reused for MOTIF will adopt British English spelling e.g., *"signalling."*

For MoTIF sub-technique numbering, existing ATT&CK sub-techniques SHALL have their number re-used. Existing MITRE FiGHT sub-techniques SHALL have their number re-used. New MoTIF sub-techniques SHALL be assigned numbers in the range .300→.399, as these are unlikely to be used by ATT&CK in the foreseeable future.

The different potential sub-technique numbering scenarios are illustrated via the examples in Table 2.

Technique	Sub-technique	GSMA MoTIF
Re-used from ATT&CK (e.g. *T1593 Search Open Websites/Domains*	Re-used from ATT&CK (e.g. *T1593.001 Social Media*)	MOT1593.001
Re-used from ATT&CK (e.g. *T1557 Adversary-in-the-Middle*	New MoTIF sub-technique	MOT1557.301
Re-used from MITRE FiGHT (e.g. *FGT5019 Subscriber Profile Identifier Discovery)*	New MoTIF sub-technique	MOT5019.301
Re-used from MITRE FiGHT (e.g. *FGT5012 Locate UE*)	Re-used from MITRE FiGHT (e.g. *FGT5012.001 Passive radio signals observation*)	MOT5012.001
New MoTIF technique	New MoTIF sub-technique	MOT3001.301

Table 2 – MoTIF Sub-technique Numbering Examples

2.4 Technique/Sub-technique Labeling

As MoTIF will include techniques/sub-techniques that originate from research studies, it is important to distinguish the theoretical attack scenarios from the techniques observed in the wild. This will help the users of the framework in prioritization of the detections and mitigations. Each technique/sub-technique will have the label *Use* as part of its technique specification, with an optional status in case it has not been observed in the wild:

- Demonstrated – There is no public or non-public source of information stating that a behaviour is in use in the wild. This category may contain new offensive research which has been proven with a Proof of Concept or with detailed technical description, but in the wild use by adversary groups is unknown.
- Theoretical – There is no public or non-public source of information stating that a behaviour is in use. This category may contain new offensive research, but in the wild use by adversary groups is unknown.

The field can have different values for different generations, if needed. For example:

- 2G,3G,4G
- 5G-SA: Theoretical.

Many of the techniques specified in MOTIF are publicly reported, but some are confidential. To give the user a clear understanding of the confidentiality, each technique/sub- technique will have the label ‘Confidentiality’ as part of the technique specification:

- Public – The use of technique/sub-technique is reported in public sources.

- GSMA Confidential – The use of technique/sub-technique is reported only in GSMA documents which are classified as GSMA Confidential.

A *Public* technique can have sub-techniques that are *GSMA Confidential*. The references within each Technique/sub-technique can be used to determine the Confidentially status.

2.5 New Technique/Sub-technique Submission

In order for new techniques/sub-techniques or other MoTIF extensions to be considered for use they should be submitted to the GSMA MoTIF group as proposed changes to the relevant MoTIF PRD(s). This submission, review and approval should take place using the standard GSMA PRD change request (CR) process as described in PRD AA.35 [5], which involves the following steps:

- The CR author drafts proposed changes to the existing PRD. Proposed new techniques, sub-techniques or tactics should be defined and structured in a manner that follows the existing MoTIF principles and conventions.
- The CR author presents the proposed changes to the MoTIF group, highlighting the context and benefits of the changes.
    - Context may include information such as what attack is the draft CR based on, adversary information etc. Good supporting information will maximise the likelihood of MoTIF support for the CR.
- The CR author considers and incorporates feedback from the MoTIF group (including the PRD editor) into an updated draft of the CR.
- Review cycles of draft CR presentation and update continue as needed until the MoTIF group agrees with the CR.
- FASG formal review and approval is sought, as per AA.35.
- One the CR is formally approved, the PRD is updated and republished.

Here are some general recommendations to assist CR creation:

A tactic describes the outcome that an adversary wants in terms of specific goals and events. These goals and events might be narrower in scope than the English-language meaning of the tactic name might suggest.

For example: *Impact (TA0040)* is defined in ATT&CK as: *“The adversary is trying to manipulate, interrupt, or destroy your systems and data”*. Based on this tactic definition, techniques that involve the collection of information, or sending of spam or disinformation to a target, while impactful, would not fall under this definition of *Impact*. Sub-techniques that involve these methods of execution should be classified under other tactics instead. Submitters seeking to extend MoTIF should first review existing MoTIF tactics, their meaning, and the current techniques assigned to them, to gather a better understanding of the potential use and most relevant tactic linked to any new technique.

Techniques and sub-techniques should be precise enough to be useful, but not too precise. This approach minimises duplication, excessive numbers of techniques and sub-techniques, and information sensitivity.

2.6 MoTIF High-Level Strategy Overlay

MoTIF covers not only adversary tactics, techniques and sub-techniques that are compatible with industry practice, but also optionally includes high-level strategy information such as adversary goals, attack targets and attack surfaces. The high-level strategy information can be added to the framework to give a more complete picture of intended attacks and make it easier to generate reports on intended attacks and mitigation techniques.

2.6.1 Principles of MoTIF High-Level Strategy (HLS) Overlay

Capturing the purpose and goal of adversaries, highlighting the mobile network components that could be their intermediate and final targets, and outlining what adversary actions could be necessary to accomplish that purpose is important. Checking for possible vulnerabilities that could be exploited in the system and developing a profile on how to perform the attack on the intended target is also valuable.

The information above would provide a general description of adversary behaviour. In addition, key information elements like attack goal, attack surface, attack target and a series of attack actions in sequence are important for framework users to know when facing an attack case. Thus, in MoTIF, the High-Level Strategy (HLS) information may be added as an optional element of the model. This information may be extracted and normalised from known attack cases. This is in line with industry practices like ENISA 2021 [10] CIS-CDM 2.0 [8], Intel TARA [9] and so on.

The HLS is mainly targeted at strategic decision-makers (e.g. CXO) and policy-makers, but it is also useful for the technical cybersecurity community to build a full picture on specific attacks. The HLS can be developed and used throughout the mobile industry to communicate non-atomic information within threat intelligence, adversary emulation, detection, assessment and so on.

2.6.2 Strategy Numbering

The key elements of HLS, i.e. attack goal, attack surface and attack target, SHALL have their own MoTIF numbering. A four-letter code, starting with an MO prefix SHALL be used before each number as shown in the table below. For MoTIF attack patterns (actions), the numbering is as described in section 2.3.

HLS Term	GSMA MoTIF
Attack Goal	MOAGxxx
Attack Surface	MOASxxx
Attack Target	MOATxxx

Table 3 – MoTIF High-Level Strategy Numbering

3 Examples of Applying MoTIF Principles

See PRD FS.58 “Mobile Threat Intelligence Framework (MoTIF) Examples” [4] (confidential to GSMA members).

4 MoTIF Elements

A matrix of MoTIF techniques (in **bold**) and sub-techniques (indented) is provided below. See section 4.1 for more details.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defence Evasion
Monitor Radio Interface	**Acquire Infrastructure**	**Exploit Interconnection Link**		**Adversary-in-the-Middle**		**Masquerading**
Broadcast Channel	Core Signalling Infrastructure Access	International Direct Signalling Link		Radio Interface Authentication Relay*		Originating Entity Spoofing
Gather Victim Identity Information	Radio Interface Access	National Direct Signalling Link				**Disguise Signalling Messages**
Phone and Subscription Information	**Develop Capabilities**	**Exploit via Core Signalling Interface**				Unexpected Encoding
Search Closed Sources	Mobile Network Tool	SS7 Protocol				
Mobile Network Operator Sources		Diameter Protocol				
Search Open Websites/ Domains		HTTPS/2 Protocol				
Social Media		**Exploit via Radio Interface**				
		AS Signalling				
		NAS Signalling				
		Radio Broadcast Channel				
		Trusted Relationship				
		Exploit Interconnection Agreements				
		Supply Chain Compromise				
		Compromise Software Supply Chain				

continues

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Access Subscriber Data	**Network Service Scanning**		**Identify Subscriber**			**Data Manipulation**
Subscriber Authentication Data	Scan Signalling Addresses		Retrieve Subscriber Identity Information			Stored Data Manipulation
Exploitation for Credential Access	**Exploit via Radio Interface**		Retrieve Subscriber Network Information			
	NAS Signalling		**Access Subscriber Data**			
	Identify Subscriber		Subscriber Authentication Data			
	Trigger Subscriber Terminated Activity		**Network Sniffing**			
	Retrieve Subscriber Identity Information		Radio Interface			
	Retrieve Subscriber Network Information		**Locate Subscriber**			
	Network Function Service Discovery		Core Network Function Signalling			

Figure 1 - MoTIF Matrix

Note: Re-used MITRE ATT&CK techniques/sub-techniques are coloured light red, reused MITRE FiGHT techniques/sub-techniques are coloured light blue. As additional use-cases and MoTIF versions are progressed additional techniques and sub-techniques will be identified. An asterisk (*) indicates a re-used FiGHT technique/sub-technique with a different name.

4.1 Techniques and Sub-techniques Definition

The following is a detailed list of the techniques and sub-techniques that have been identified for use in MoTIF version 1. Future versions of GSMA MoTIF will have additional techniques and sub-techniques. Examples of how these are applied are provided in FS.58 "MoTIF Examples" [5] (confidential to GSMA members) for the identified MoTIF use cases. 'References' and 'Analogous technique in other frameworks' are public, externally available references and frameworks - GSMA members may has access to additional reference resources and frameworks in the GSMA Member Gateway. Mitigations and detections for the various techniques and sub-techniques are for further study (FFS), and will be covered in v2 of GSMA MoTIF.

Where ATT&CK or FiGHT techniques or sub-techniques are used, text taken from the ATT&CK or FiGHT technique or sub-technique description is shown in *grey italics*.

4.1.1 Monitor Radio Interface

Name:	Monitor Radio Interface
ID:	MOT3001
Source:	New MoTIF Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	MOT3001.301 Broadcast Channel
Tactic:	Reconnaissance
Description:	The adversaries may monitor radio interface traffic to passively collect information about the radio network configuration or about subscribers in close vicinity of the adversary. (1), (2), (3), (4).
Platform:	Mobile Network
Procedure Examples:	See sub-technique.
References:	(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (3) Kumar, P. et.al. (2021). Murat: Multi-RAT False Base Station Detector (Section IIB) (4) Rupprecht, D. et.al. (2018). On Security Research Towards Future Mobile Network Generations. (Section III D)
Analogous technique in other frameworks:	

4.1.1.1 Broadcast Channel

Name:	Broadcast Channel
ID:	MOT3001.301
Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Reconnaissance
Description:	In mobile networks the adversary needs to obtain information about the cell configuration parameters that will be used to prepare for the next phase of an attack that is utilizing the radio interface. Example of configuration could be the physical cell ID (PCI), neighbouring cells, frequencies used, Tracking Area Codes (TAC). (1), (2), (3), (4)
Platform:	Mobile network
Procedure Examples:	ID / Name / Description: Adversary uses radio passive sniffing to obtain the broadcasted cell configuration that is found in the network information (SIB) messages, e.g. Radio Access Technology (RAT), frequency, System Information Block (SIB) configuration, cell ID. (1), (3)
References:	(1) Li, Z. et al. (2017). FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild. (2) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (3) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (4) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.
Analogous technique in other frameworks:	

4.1.2 Gather Victim Identity Information

Name:	Gather Victim Identity Information
ID:	MOT1589
Source:	Re-used ATT&CK Technique
Use:	N/A

Confidentiality:	Public
Sub-Technique:	MOT1589.301 Phone and Subscription Information
Tactic:	Reconnaissance
Description:	*Adversaries may gather information about the victim's identity that can be used during targeting. Information about identities may include a variety of details, including personal data (ex: employee names, email addresses, etc.) as well as sensitive details such as credentials.* In mobile networks, the adversary wants to obtain information about subscriber and phone identities to conduct more targeted attacks. Subscriber identity can be, for example, MSISDN, IMSI, GUTI, TMSI.
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts
Analogous technique in other frameworks:	ATT&CK Enterprise: Gather Victim Identity Information (T1589)

4.1.2.1 Phone and Subscription Information

Name:	Phone and Subscription Information
ID:	MOT1589.301
Source:	Re-used ATT&CK Technique -> New MoTIF Sub-Technique
Use:	N/A
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Reconnaissance
Description:	In mobile networks, targeted attacks towards subscribers have to be done using the subscriber identity. Obtaining the identity would allow the attacker to gather more information or initiate more targeted attacks. The adversary gathers phone or subscription related information about subscriber(s). Examples are phone number (MSISDN), IMSI (International Mobile Subscriber Identity), home mobile network operator, S@T browser availability on the UICC, IMEI (International Mobile Equipment Identity). The data might be acquired through interconnection, social engineering, social media or otherwise. (1)
Platform:	Mobile network

Procedure Examples:	ID	Name	Description
			Adversary obtains the subscriber MSISDN. (1)
			Obtain subscriber MSISDN/SUPI
References:	(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts		
Analogous technique in other frameworks:	ATT&CK Enterprise: Gather Employee Names (T1589.003),		

4.1.3 Network Service Scanning

Name:	Network Service Scanning
ID:	MOT1046
Source:	Re-used ATT&CK/FiGHT Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	MOT1046.301 Scan Signalling Addresses
Tactic:	Discovery
Description:	An adversary may discover operator network related information (identifiers). *Adversaries may attempt to get a listing of services running on remote hosts and local network infrastructure devices, including those that may be vulnerable to remote software exploitation. Common methods to acquire this information include port and/or vulnerability scans using tools that are brought onto a system.* In mobile networks, the adversary wants to obtain information about subscriber, signalling addresses, supported service at a certain server. The scan may take place from the Internet or the interconnection network or the radio network. Often automated mass scanning events take place.
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) GSMA PRD IR.70 - SMS SS7 Fraud (Public)
Analogous technique in other frameworks:	ATT&CK Enterprise: Network Service Discovery (T1046), FiGHT: Network Service Scanning (FGT1046) *NOTE: These two MITRE techniques are actually the same, however due to an error the FiGHT technique was renamed.*

4.1.3.1 Scan Signalling Addresses

Name:	Scan Signalling Addresses

ID:	MOT1046.301
Source:	Re-used ATT&CK/FiGHT Technique -> New MoTIF Sub-Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Discovery
Description:	By sending signalling messages to the network, the adversary tries to check if mobile network nodes leak node or network related information, or bypasses defences ((1) (2) below). Using this sub-technique as a preparatory step, the adversary can then tune his further attack steps to send specific attack messages based on this scan. Examples are SS7 scans to evaluate if a Global Title is in use or not. The adversary may also probe which PLMN-ID values are accepted by the HPLMN in Diameter Authentication Information Request (AIR).
Platform:	Mobile network
Procedure Examples:	

ID	Name	Description
		The adversary checks if subscriber's HPLMN accepts different PLMN-IDs in Diameter AIR.
		Adversary does scanning attack to determine serving MME/AMF that subscriber is attached to (IDR, 5G:TBC)

References:	(1) Enea. (2017). Designated Attacker - Evolving SS7 Attack Tools (2) Enea. (2018). Diameter Signalling Security - Protecting 4G Networks
Analogous technique in other frameworks:	ATT&CK Enterprise: IP Block Scanning (T1595.001)

4.1.4 Search Closed Sources

Name:	Search Closed Sources
ID:	MOT1597
Source:	Re-used ATT&CK Technique
Use:	N/A
Confidentiality:	Public
Sub-Technique:	MOT1597.301 Mobile Network Operator Sources
Tactic:	Reconnaissance
Description:	*Adversaries may search and gather information about victims from closed sources that can be used during targeting. Information about victims may be available for purchase from reputable private sources and databases, such as paid*

	subscriptions to feeds of technical/threat intelligence data. Adversaries may also purchase information from less-reputable sources such as dark web or cybercrime black markets. Adversaries may search and collect information about the mobile network operator from closed or semi-closed sources. Typical examples are GSMA IR.21, IR.85, FS.30 or T-ISAC, information from insiders or partners. The information acquisition might be done legally or illegally.
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) The Intercept. (2014). Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide. (2) https://www.wikileaks.org/hackingteam/emails/emailid/72166
Analogous technique in other frameworks:	ATT&CK Enterprise: Search Closed Sources (T1597)

4.1.4.1 Mobile Network Operator Sources

Name:	Mobile Network Operator Sources
ID:	MOT1597.301
Source:	Re-used ATT&CK Technique -> New MoTIF Sub-Technique
Use:	N/A
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Reconnaissance
Description:	The adversary may gather information about the mobile network operator to be used in initial access or for preparation of the attack. This can be network architecture, protocols, ports, Global Titles, roaming partners, suppliers. The adversary may search in closed sources like GSMA roaming database RAEX IR.21 (1), IMEI database (2) or IR.85.
Platform:	Mobile network
Procedure Examples:	ID | Name | Description | | | The adversary uses GSMA IR.21 for obtaining the node addresses and other information that is “necessary for targeting and the exploitation” (1).
References:	(1) The Intercept. (2014). Operation AURORAGOLD: How the NSA Hacks Cellphone Networks Worldwide. (2) https://www.wikileaks.org/hackingteam/emails/emailid/72166

Analogous technique in other frameworks:	

4.1.5 Acquire Infrastructure

Name:	Acquire Infrastructure
ID:	MOT1583
Source:	Re-used ATT&CK Technique
Use:	2G,3G,4G
Confidentiality:	Public
Sub-Technique:	MOT1583.301 Core Signalling Infrastructure Access, MOT1583.302 Radio Interface Access
Tactic:	Resource Development
Description:	*Adversaries may buy, lease, or rent infrastructure that can be used during targeting.* For example, commercial service providers exist that offer access to signalling infrastructure or sell False Base Station solutions. *Use of these infrastructure solutions allows an adversary to stage, launch, and execute operations. Solutions may help adversary operations blend in with traffic that is seen as normal.*
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) TBIJ. (2020) Spy companies using Channel Islands to track phones around the world.
Analogous technique in other frameworks:	ATT&CK Enterprise: Acquire Infrastructure (T1583)

4.1.5.1 Core Signalling Infrastructure Access

Name:	Core Signalling Infrastructure Access
ID:	MOT1583.301
Source:	Re-used ATT&CK Technique -> New MoTIF Sub-Technique
Use:	2G, 3G, 4G 5G-SA: Theoretical
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Resource Development

<table>
<tr><td>Description:</td><td>Adversaries may buy, lease, or rent SS7, Diameter, GTP-C signalling infrastructure access or services that can be used during targeting (1), (2), (3). Targeted attacks to mobile network operators may use ‘surveillance as a service’ specialists to achieve their goals (2). Their attacks often blend in with normal traffic coming from partners of the victim mobile network operator and make attribution difficult. Fraudsters and spammers may use specific partner gateways or access to messaging servers for their purposes.</td></tr>
<tr><td>Platform:</td><td>Mobile network</td></tr>
<tr><td>Procedure Examples:</td><td>
<table>
<tr><th>ID</th><th>Name</th><th>Description</th></tr>
<tr><td></td><td></td><td>The adversary buys access to the signalling infrastructure in order to send Diameter AIR.(1)</td></tr>
<tr><td></td><td></td><td>The adversary buys access to the signalling infrastructure in order to send SS7, Diameter, HTTPS/2.
SS7 GT Leasing
Diameter Origin Realm leasing (2), (3)</td></tr>
<tr><td></td><td></td><td>MNO allows the onboarding of an NF instance controlled by the external entity. (4), (5)</td></tr>
</table>
</td></tr>
<tr><td>References:</td><td>(1) TBIJ. (2020) Spy companies using Channel Islands to track phones around the world.
(2) CitizenLab. (2020). Running in Circles Uncovering the Clients of Cyberespionage Firm Circles.
(3) TBIJ. (2021). Swiss tech company boss accused of selling mobile network access for spying.
(4) Enea (2021) 5G Network Slicing Security in 5G Core Networks
(5) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem</td></tr>
<tr><td>Analogous technique in other frameworks:</td><td></td></tr>
</table>

4.1.5.2 Radio Interface Access

Name:	Radio Interface Access
ID:	MOT1583.302
Source:	Re-used ATT&CK Technique -> New MoTIF Sub-Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Resource Development
Description:	Adversaries may buy, lease, or obtain physical access to a mobile operator network base station or use their own rogue cellular base (Stingray) station for launching an attack (2) (3). The adversary could set up a rogue cellular base station infrastructure and then use it to eavesdrop on or manipulate cellular device communication. A compromised cellular femtocell could be used to carry out this technique (1).
Platform:	Mobile network
Procedure Examples:	ID / Name / Description The adversary acquires access to a false base station/false network. (1), (2), (3)
References:	(1) DePerry, D. & Ritter T. (2013). I Can Hear You Now - Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell. Black Hat USA2013 (2) Wired (2016). Here's How Much a StingRay Cell Phone Surveillance Tool Costs (3) Alibaba.com. Wholesale imsi catcher 4g For Online Communication
Analogous technique in other frameworks:	

4.1.6 Develop Capabilities

Name:	Develop Capabilities
ID:	MOT1587
Source:	Re-used ATT&CK Technique
Use:	N/A
Confidentiality:	Public
Sub-Technique:	MOT1587.301 Mobile Network Tool
Tactic:	Resource Development

Description:	*Adversaries may build capabilities that can be used during targeting. Rather than purchasing, freely downloading, or stealing capabilities, adversaries may develop their own capabilities in-house. This is the process of identifying development requirements and building solutions such as malware, exploits, and self-signed certificates. Adversaries may develop capabilities to support their operations throughout numerous phases of the adversary lifecycle.* In mobile networks adversary may develop false base stations (1), mobile exploits, core signalling exploitation tools (2), SIM card exploits, radio exploitation tools and other tools to initiate attacks.
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) Motherboard. (2018). Here's How Easy It Is to Make Your Own IMSI-Catcher (2) Lighthouse Reports. (2022). Revealing Europe's NSO.
Analogous technique in other frameworks:	ATT&CK Enterprise: Develop Capabilities (T1587).

4.1.6.1 Mobile Network Tool

Name:	Mobile Network Tool
ID:	MOT1587.301
Source:	Re-used ATT&CK Technique -> New MoTIF Sub-Technique
Use:	N/A
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Resource Development
Description:	Adversary develops special tools for mobile networks that carry out and deliver mobile network targeted exploits. (1) (2)
Platform:	Mobile network
Procedure Examples:	

ID	Name	Description
		The adversary develops a tool to deliver silent SMS. (1)
		Develop/have access to a tool/stack to send SS7, Diameter, HTTPS/2 commands. (2)
		Build the capability to invoke various services to exposed interfaces.(3)

References:	(1) Motherboard. (2018). Here's How Easy It Is to Make Your Own IMSI-Catcher (2) Lighthouse Reports. (2022). Revealing Europe's NSO.

	(3) Mobileum. (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem
Analogous technique in other frameworks:	N/A

4.1.7 Exploit Interconnection Link

Name:	Exploit Interconnection Link
ID:	MOT3002
Source:	MoTIF Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	MOT3002.301 International Direct Signalling Link MOT3002.302 National Direct Signalling Link
Tactic:	Initial Access
Description:	The adversary may get access to the target network via the interconnection interface.
Platform:	Mobile network
Procedure Examples:	ID: Name: Description: Authentication Information Request (AIR) from VPLMN is routed via an international route (1).
References:	(1) P1 Security. (2021). All authentication vectors are not made equal.
Analogous technique in other frameworks:	

4.1.7.1 International Direct Signalling Link

Name:	International Direct Signalling Link
ID:	MOT3002.301
Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Initial Access
Description:	The adversary may get access to the target network via a direct signalling link connected to the international exchange.

Platform:	Mobile network
Procedure Examples:	ID / Name / Description Diameter AIR from VPLMN is routed via international route (2) SS7/Diameter/HTTPS is routed via international route (1)
References:	(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor (2) P1 Security. (2021). All authentication vectors are not made equal.
Analogous technique in other frameworks:	

4.1.7.2 National Direct Signalling Link

Name:	National Direct Signalling Link
ID:	MOT3002.302
Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	2G, 3G, 4G 5G-SA: Theoretical
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Initial Access
Description:	The adversary may get access to the target network via a direct signalling link connected to the national exchange.
Platform:	Mobile network
Procedure Examples:	ID / Name / Description SS7/Diameter/HTTPS is routed via national route (1)
References:	(1) P1 Security. (2014). SS7map: mapping vulnerability of the international mobile roaming infrastructure
Analogous technique in other frameworks:	

4.1.8 Exploit via Core Signalling Interface

Name:	Exploit via Core Signalling Interface
ID:	MOT3003

Source:	New MoTIF Technique
Use:	2G,3G,4G 5G-SA: Demonstrated
Confidentiality:	Public
Sub-Technique:	MOT3003.301 SS7 Protocol MOT3003.302 Diameter Protocol MOT3003.303 HTTPS/2 Protocol
Tactic:	Initial Access
Description:	The adversary may access the target network by exploiting signalling (i.e. control plane) protocols.
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) P1 Security. (2021). All authentication vectors are not made equal.
Analogous technique in other frameworks:	

4.1.8.1 SS7 Protocol

Name:	SS7 Protocol
ID:	MOT3003.301
Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	2G,3G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Initial Access
Description:	The adversary may access the target network by using SS7 protocol.
Platform:	Mobile network
Procedure Examples:	ID / Name / Description The attacks described in (1) & (2) exploit SS7 interface for obtaining location information The adversary sends SS7 SRI-SMs, ATIs, PSIs and PSLs (3)
References:	(1) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe.

	(2) Lighthouse Reports. (2022). Revealing Europe's NSO. (3) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020.
Analogous technique in other frameworks:	

4.1.8.2 Diameter Protocol

Name:	Diameter Protocol
ID:	MOT3003.302
Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Initial Access
Description:	The adversary may access the target network by using Diameter protocol.
Platform:	Mobile network
Procedure Examples:	ID / Name / Description The adversary sends Diameter Authentication Information Request (AIR) (1). The adversary sends Diameter IDR (2)
References:	(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020.
Analogous technique in other frameworks:	

4.1.8.3 HTTPS/2 Protocol

Name:	HTTPS/2 Protocol
ID:	MOT3003.303
Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	5G-SA: Demonstrated
Confidentiality:	Public
Sub-Technique:	N/A

Tactic:	Initial Access
Description:	The adversary may access the target network by using HTTPS/2 protocol.
Platform:	Mobile network
Procedure Examples:	ID / Name / Description The adversary sends HTTPS/2 Nlmf_DL, Nlmf_PPI, Ngmlc_PL (1)
References:	(1) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020..
Analogous technique in other frameworks:	

4.1.9 Trusted Relationship

Name:	Trusted Relationship
ID:	MOT1199
Source:	Reused ATT&CK Technique
Use:	2G,3G,4G
Confidentiality:	Public
Sub-Technique:	MOT1199.301 Exploit Interconnection Agreements
Tactic:	Initial Access
Description:	*Adversaries may breach or otherwise leverage organizations who have access to intended victims. Access through trusted third-party relationship exploits an existing connection that may not be protected or requires more complicated defence mechanisms to detect and prevent unauthorized access to a network.* (1) (2)
Platform:	Mobile network
Procedure Examples:	ID / Name / Description
References:	(1) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe. (2) Lighthouse Reports. (2022). Revealing Europe's NSO
Analogous technique in other frameworks:	ATT&CK Enterprise: Trusted Relationship (T1199)

4.1.9.1 Exploit Interconnection Agreements

<table>
<tr><td>Name:</td><td>Exploit Interconnection Agreements</td></tr>
<tr><td>ID:</td><td>MOT1199.301</td></tr>
<tr><td>Source:</td><td>Reused ATT&CK Technique -> New MoTIF Sub-Technique</td></tr>
<tr><td>Use:</td><td>2G,3G,4G</td></tr>
<tr><td>Confidentiality:</td><td>Public</td></tr>
<tr><td>Sub-Technique:</td><td>N/A</td></tr>
<tr><td>Tactic:</td><td>Initial Access</td></tr>
<tr><td>Description:</td><td>The technique can be conducted by malicious partner or adversaries with access to interconnection networks or roaming partner’s mobile network. The adversary can remotely conduct the attacks by launching signalling messages e.g. related to location tracking, communication interception, or subscriber identify retrieval. (1), (2), (3)</td></tr>
<tr><td>Platform:</td><td>Mobile network</td></tr>
<tr><td>Procedure Examples:</td><td>
<table>
<tr><th>ID</th><th>Name</th><th>Description</th></tr>
<tr><td></td><td></td><td>The adversary uses roaming partner to send the malicious Authentication Information Request (AIR) from roaming partner’s VPLMN to target’s HPLMN (1).</td></tr>
<tr><td></td><td></td><td>The adversary is sending from a GT and Diameter realm which is nominally within a roaming partners range, with which there is an interconnection agreement (4)</td></tr>
<tr><td></td><td></td><td>Compromised roaming partner or service partners or MNOs rent access to an adversary (3)</td></tr>
</table>
</td></tr>
<tr><td>References:</td><td>(1) P1 Security (2021). All authentication vectors are not made equal.
(2) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe.
(3) Lighthouse Reports. (2022). Revealing Europe's NSO
(4) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor</td></tr>
<tr><td>Analogous technique in other frameworks:</td><td></td></tr>
</table>

4.1.10 Exploit via Radio Interface

Name:	Exploit via Radio Interface
ID:	MOT3006

Source:	New MoTIF Technique
Use:	2G,3G,4G
Confidentiality:	Public
Sub-Technique:	MOT3006.301 AS Signalling MOT3006.302 NAS Signalling MOT3006.303 Radio Broadcast Channel
Tactic:	Initial Access, Discovery
Description:	Adversaries may use the radio access network to initiate attacks towards the UE or the mobile network.(1) (2) (3) The adversary may leverage vulnerabilities in the protocols that make up the signalling procedures in a radio network, for example network information (SIB1) messages, or the RRC protocol, or NAS protocols to initiate attacks towards the UE or the mobile network.
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks. (3) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.
Analogous technique in other frameworks:	ATT&CK Mobile: Exploit via Radio Interfaces (T1477). Note: Deprecated

4.1.10.1 AS Signalling

Name:	AS Signalling
ID:	MOT1477.301
Source:	Reused ATT&CK Technique -> New MoTIF Sub-Technique
Use:	2G,3G 4G: Demonstrated
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Initial Access
Description:	Adversaries may modify or trigger control plane procedures on the radio interface control plane using Access Stratum (AS) signalling that occurs between the UE and the base station.

Platform:	Mobile network		
Procedure Examples:	ID	Name	Description
			The adversary uses 3GPP access radio to attract the UE to attach to a false base station by broadcasting cell configuration with a higher signal strength than the legitimate cell..
References:	(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks		
Analogous technique in other frameworks:			

4.1.10.2 NAS Signalling

Name:	NAS Signalling		
ID:	MOT1477.302		
Source:	Reused ATT&CK Technique -> New MoTIF Sub-Technique		
Use:	2G,3G 4G: Demonstrated		
Confidentiality:	Public		
Sub-Technique:	N/A		
Tactic:	Initial Access, Discovery		
Description:	Adversaries may modify or trigger Non-Access-Stratum (NAS) signalling related procedures that is generated from a false base station infrastructure. The adversary may impersonate core network elements (such as MME) towards the UE or UE towards the core network elements.		
Platform:	Mobile network		
Procedure Examples:	ID	Name	Description
			Using a false base station infrastructure, adversary initiates Identification procedure by sending an “Identity-Request” message to UE using NAS signalling, in order to request subscriber’s IMSI (1), (2). Using a false base station infrastructure, adversary uses a captured IMSI to spoof a location update request towards the core network, impersonating as legitimate UE (2).
References:	(1) CableLabs: (2019). False Base Station or IMSI Catcher: What You Need to Know. (2) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks		

Analogous technique in other frameworks:	

4.1.10.3 Radio Broadcast Channel (SIB1)

Name:	Radio Broadcast Channel (SIB1)
ID:	MOT1477.303
Source:	Reused ATT&CK Technique -> New MoTIF Sub-Technique
Use:	2G,3G,4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Initial Access
Description:	The adversary leverages the radio broadcast System Information Block1 messages (SIB1) to advertise to the target UEs new cell configuration that in return forces the UE to initiate different procedures like for example, cell re-selection or Tracking Area Update.(1), (2), (3)
Platform:	Mobile network
Procedure Examples:	

ID	Name	Description
		The adversary uses a false base station/network with relatively better signal strength to force the UE to select the fake cell and attach to its network (1).
		The adversary uses an active false base station to trigger a Tracking Area Update (TAU) procedure from the UE by broadcasting a different Location Area Code/Tracking Area code (LAC/TAC) to force the target UE to initiate a TAU (2) (3).

References:	(1) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service. (2) CableLabs: (2019). False Base Station or IMSI Catcher: What You Need to Know. (3) Quintin, C. (2020). Detecting Fake 4G Base Stations in Real Time. Black Hat USA 2020.
Analogous technique in other frameworks:	

4.1.11 Identify Subscriber

Name:	Identify Subscriber

ID:	MOT5019
Source:	Reused FiGHT Technique*
Use:	2G,3G,4G
Confidentiality:	Public
Sub-Technique:	MOT5019.301 Trigger Subscriber Terminated Activity MOT5019.302 Retrieve Subscriber Identity Information MOT5019.303 Retrieve Subscriber Network Information
Tactic:	Discovery, Collection
Description:	*An adversary may obtain a* subscriber *permanent* or temporary *identifier via various means.* An adversary may obtain the subscriber identifier by using HLR Lookup, or by monitoring the radio interface. *An adversary may obtain identifying information from 5G UEs only after the UE has been bid down (downgraded) to a lower security protocol e.g. 4G, since in 4G and 3G it is possible for the network to ask the UE to send its IMSI (International Subscriber Identifier) in the clear over the radio interface. The 5G UE sends an encrypted permanent identifier (called Subscriber Concealed Identifier (SUCI)) over the radio interface as part of the initial registration to the 5G network. Some non-UE specific information is part of the Subscriber Permanent Identifier or SUPI and is not encrypted (e.g., home network name).*
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network
Analogous technique in other frameworks:	Subscriber Profile Identifier Discovery: Intercept bid-down SUPI | MITRE FiGHT™ **= This is the same Technique as MITRE FiGHT, however a different name is used, MITRE FiGHT may potentially update in the future*

4.1.11.1 Trigger Subscriber Terminated Activity

Name:	Trigger Subscriber Terminated Activity
ID:	MOT5019.301
Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	2G: Demonstrated, 3G: Demonstrated, 4G: Demonstrated,
Confidentiality:	Public

Sub-Technique:	N/A
Tactic:	Discovery
Description:	The adversary can trigger mobile terminating activity, such as making calls to the subscriber's profile (1), sending silent SMS (2), or trigger notifications from the instant messengers (1), to trigger paging of the subscriber. The technique can be made more stealthy by using silent phone calls or silent SMSs (2) (3), The adversary can monitor the paging activity in the radio network and use that information to correlate the paging with the for identifying the target subscriber identifier.
Platform:	Mobile network
Procedure Examples:	ID: MOG3xxx Name: Description: The TORPEDO attack (3) was validated by making multiple silent VoLTE calls, silent CSFB calls, SMSs and Tweets. After identifying the victim's PFI, the researchers carried out paging channel hijacking. Once the paging channel was hijacked, the researchers made two calls to the victim, where the latter call forced MME to broadcast paging_imsi message.(3)
References:	(1) Shaik, A. et al. (2016). Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. (2) Nohl, K. & Munaut, S. (2010) GSM Sniffing. 27th CCC. (3) Hussain, S. et al. (2019) Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information.
Analogous technique in other frameworks:	N/A

4.1.11.2 Retrieve Subscriber Identity Information

Name:	Retrieve Subscriber Identity Information
ID:	MOT5019.302
Source:	Reused FiGHT Technique -> New MoTIF Sub-Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Discovery, Collection
Description:	The adversary can retrieve subscriber information such as the IMSI, MSISDN, SUPI, SUCI etc

Platform:	Mobile network		
Procedure Examples:	ID	Name	Description
			Adversary gains IMSI information on the MSISDN via SS7 techniques (SRI-SM) (1)
References:	(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network		
Analogous technique in other frameworks:	N/A		

4.1.11.3 Retrieve Subscriber Network Information

Name:	Retrieve Subscriber Network Information		
ID:	MOT5019.303		
Source:	Reused FiGHT Technique -> New MoTIF Sub-Technique		
Use:	2G,3G,4G		
Confidentiality:	Public		
Sub-Technique:	N/A		
Tactic:	Discovery, Collection		
Description:	The adversary can retrieve subscriber network information such as the current serving network element(s)		
Platform:	Mobile network		
Procedure Examples:	ID	Name	Description
			Adversary gains MSC/VLR serving information on the MSISDN via SS7 techniques (SRI-SM) (1)
References:	(1) Enea. (2016). Tracking the Trackers: Advanced Rogue Systems Exploiting the SS7 Network		
Analogous technique in other frameworks:	N/A		

4.1.12 Masquerading

Name:	Masquerading
ID:	MOT1036
Source:	Reused ATT&CK Technique
Use:	2G, 3G, 4G

Confidentiality:	Public
Sub-Technique:	MOT1036.301 Originating Entity Spoofing
Tactic:	Defence Evasion
Description:	*Adversaries may attempt to manipulate* parameters in the control signalling *to make them appear legitimate or benign to* mobile subscribers, end nodes *and/or security tools. Masquerading occurs when the* parameter value *is manipulated or abused for the sake of evading defences*, or convincing the target to believe it is communicating with a spoofed entity. A typical masquerading operating is manipulation of the source node address.
Platform:	Mobile network
Procedure Examples:	See procedure example in sub-technique.
References:	(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service.
Analogous technique in other frameworks:	ATT&CK Enterprise: Masquerading (T1036),

4.1.12.1 Originating Entity Spoofing

Name:	Originating Entity Spoofing
ID:	MOT1036.301
Source:	Reused ATT&CK Technique -> New MoTIF Sub-Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Defence Evasion
Description:	The adversary may attempt to manipulate the originating address information, such as Global Title Address, Diameter Host or Realm information for the sake of evading defences. The adversary may attempt to manipulate the configured cell ID on the false base station to configure it to a known cell ID in the network to evade detection.
Platform:	Mobile network
Procedure Examples:	

ID	Name	Description
		The adversary used spoofed vPLMN-ID in Authentication Information Request (AIR) to bypass Diameter Edge Agents (DEA) checks (1).

				Adversary reuses the same cell ID of an existing cell in the false base station (2).
				In VPLMN, the adversary sends HPLMN-ID to the UE from the false base station (1).
				The adversary spoofs MAP and Diameter addresses (3)
References:	(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Aftenposten (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service. (3) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor			
Analogous technique in other frameworks:				

4.1.13 Disguise Signalling Messages

Name:	Disguise Signalling Messages
ID:	MOT3005
Source:	New MoTIF Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	MOT3005.301 Unexpected Encoding
Tactic:	Defence Evasion
Description:	The adversary can disguise its signalling messages in order to avoid detection and blocking of their attacks. Examples include using unexpected addresses, unexpected message format or unexpected message encoding.
Platform:	Mobile network
Procedure Examples:	See procedure example in sub-technique.
References:	(1) Symsoft & P1 Security. (2018). SS7 and Diameter: Exploit Delivery over signalling protocols. (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019
Analogous technique in other frameworks:	

4.1.13.1 Unexpected Encoding

Name:	Unexpected Encoding
ID:	MOT3005.301

Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	2G,3G,4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Defence Evasion
Description:	The adversary may use an unexpected encoding of the signalling message in order to bypass detection and any defences which may be in place.
Platform:	Mobile network
Procedure Examples:	ID / Name / Description: Adversary uses Global Opcode encoding of the TCAP Operation Code in order to bypass signalling defences (1)
References:	(1) Puzankov, K. (2019) Hidden Agendas: bypassing GSMA recommendations on SS7 networks. HITB AMS SecConf May 2019
Analogous technique in other frameworks:	

4.1.14 Access Subscriber Data

Name:	Access Subscriber Data
ID:	MOT3004
Source:	New MoTIF Technique
Use:	2G,3G,4G
Confidentiality:	Public
Sub-Technique:	MOT3004.301 Subscriber Authentication Data
Tactic:	Credential Access, Collection
Description:	The adversary can collect several types of user-specific data. Such data include, for instance, subscriber identities, subscribed services, subscriber location or status.
Platform:	Mobile network
Procedure Examples:	See procedure example in sub-technique.
References:	(1) P1 Security. (2021). All authentication vectors are not made equal. (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019
Analogous technique in other frameworks:	

4.1.14.1 Subscriber Authentication Data

Name:	Subscriber Authentication Data
ID:	MOT3004.301
Source:	New MoTIF Technique -> New MoTIF Sub-Technique
Use:	2G,3G,4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Credential Access, Collection
Description:	The adversary may acquire subscriber authentication information from mobile network registers, such as HLR/HSS/AuC or MSC/VLR, SGSN, MME. For example, the adversary may query subscriber keys, authentication vectors etc. and use this information to tailor further phases of the attack.
Platform:	Mobile network
Procedure Examples:	ID: Name: Description: Adversary gathers the 4G authentication vectors (RAND, AUTN, XRES) (1)
References:	(1) P1 Security. (2021). All authentication vectors are not made equal.
Analogous technique in other frameworks:	

4.1.15 Network Sniffing

Name:	Network Sniffing
ID:	MOT1040
Source:	Reused ATT&CK Technique
Use:	2G/3G 4G: Demonstrated
Confidentiality:	Public
Sub-Technique:	MOT1040.301 Radio Interface
Tactic:	Collection
Description:	*Adversaries may sniff network traffic to capture information about an environment, including authentication material,* base station configuration and user plane traffic *passed over the network*.
Platform:	Mobile network

Procedure Examples:	
References:	(1) Kotuliak, M. et al. (2022) LTrack : Stealthy Tracking of Mobile Phones in LTE
Analogous technique in other frameworks:	Network Sniffing, Technique T1040 - Enterprise | MITRE ATT&CK® Network Sniffing | MITRE FiGHT™ (FGT1040)

4.1.15.1 Radio Interface

Name:	Radio Interface
ID:	MOT1040.501
Source:	Reused ATT&CK Technique -> Reused FiGHT sub-Technique
Use:	2G, 3G, 4G: Demonstrated
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Collection
Description:	*An adversary may eavesdrop on unencrypted* or encrypted *traffic to capture information to and from a UE.* *An adversary may employ a back-to-back* false base station *to eavesdrop on the communication and relay communication between the intended recipient and the intended source, over the radio interface.* The adversary may also passively sniff the radio traffic and capture specific traffic that can be then, if possible, analyzed.(1) When operating a false base station the adversary needs to obtain information about the cell configuration parameters that will be used to prepare for the next phase of an attack that is utilizing the radio interface. Example of configuration could be the Physical Cell ID (PCI), neighbouring cells, frequencies used, Location Area Codes/Tracking Area Codes (LAC/TAC).(2) The adversary may use methods of capturing control plane or user plane traffic on the radio interface.
Platform:	Mobile network
Procedure Examples:	ID / Name / Description: The adversary passively captures the traffic of interest to prepare it for decryption using the gathered authentication vectors.
References:	(1) Borgaonkar, R. & Shaik, A. (2015). LTE and IMSI Catcher Myths. Black Hat USA 2015 (2) Li, Z. et al. (2017). FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild.

	(3) P1 Security. (2021). All authentication vectors are not made equal.
Analogous technique in other frameworks:	Network Sniffing: Radio interface | MITRE FiGHT™ (FGT1040.501)

4.1.16 Locate Subscriber

Name:	Locate Subscriber
ID:	MOT5012
Source:	Reused FiGHT Technique
Use:	2G/3G/4G
Confidentiality:	Public
Sub-Technique:	MOT5012.504 Core Network Function Signalling
Tactic:	Collection
Description:	*An adversary may obtain the UE location using radio access or core network. Adversary may employ various means to obtain UE location (coarse, fine) using radio access or core network.*
Platform:	Mobile network
Procedure Examples:	
References:	(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor (2) Mc Daid, C. (2019). Simjacker – the next frontier in mobile espionage. VB2019 (3) The Washington Post. (2014). For sale: Systems that can secretly track where cellphone users go around the globe
Analogous technique in other frameworks:	Location Tracking, Technique T1430 - Mobile | MITRE ATT&CK® Locate UE | MITRE FiGHT™ (FGT5012)

4.1.16.1 Core Network Function Signalling

Name:	Core Network Function Signalling
ID:	MOT5012.501
Source:	Reused FiGHT Technique -> Reused FiGHT sub-Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Collection

Description:	*An adversary in the core network exploits signalling protocols to obtain the location of the UE.* *User location tracking is part of normal cellular operation. Adversaries with access to core network or a core network function (NF) can misuse signalling protocols (e.g., SS7, GTP and Diameter or the SBI API calls), or exploit vulnerabilities in the signalling plane, in order to obtain location information for a given UE.*
Platform:	Mobile network
Procedure Examples:	ID / Name / Description The adversary collects location information of the UE via core network signalling interfaces. (1) (2)
References:	(1) Enea. (2022). HiddenArt - A Russian-linked SS7 Threat Actor. (2) Mc Daid, C. (2020) Watching the Watchers - How Surveillance Companies track you using Mobile Networks. #rC3 2020..
Analogous technique in other frameworks:	Locate UE: Core Network Function Signaling | MITRE FiGHT™ (FGT5012.004)

4.1.17 Search Open Websites/Domains

Name:	Search Open Websites/Domains
ID:	MOT1593
Source:	Reused ATT&CK Technique
Use:	Demonstrated
Confidentiality:	Public
Sub-Technique:	MOT1593.001: Social Media
Tactic:	Reconnaissance
Description:	*Adversaries may search freely available websites and/or domains for information about victims that can be used during targeting. Information about victims may be available in various online sites, such as social media, new sites, or those hosting information about business operations such as hiring or requested/rewarded contracts.(1)(2)(3)* Adversaries may gather subscription or residence related information about subscriber(s). Examples are phone number (MSISDN), home address, home mobile network operator. Adversaries may gather information about the mobile network operator to be used in initial access or for preparation of the attack. This can be network architecture, protocols, ports, Global Titles, roaming partners, or suppliers (4).
Platform:	Mobile network

Procedure Examples:	See sub-technique.
References:	(1) Cyware Hacker News. (2019). How Hackers Exploit Social Media To Break Into Your Company. (2) Security Trails. (2019). Exploring Google Hacking Techniques. (3) Offensive Security. (n.d.). Google Hacking Database. Retrieved October 23, 2020. (4) Holtmanns, S. (2018). Secure Interworking Between Networks in 5G Service Based Architecture. ETSI Security Week 2018.
Analogous technique in other frameworks:	Search Open Websites/Domains, Technique T1593 - Enterprise | MITRE ATT&CK® GSMA Non-public materials

4.1.17.1 Social Media

Name:	Social Media
ID:	MOT1593.001
Source:	Reused ATT&CK Technique -> Reused ATT&CK sub-Technique
Use:	Theoretical
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Reconnaissance
Description:	*Adversaries may search social media for information about victims that can be used during targeting. Social media sites may contain various information about a victim organization, such as business announcements as well as information about the roles, locations, and interests of staff.* *Adversaries may search in different social media sites depending on what information they seek to gather. Threat actors may passively harvest data from these sites, as well as use information gathered to create fake profiles/groups to elicit victim's into revealing specific information (i.e. Spearphishing Service)(1). Information from these sources may reveal opportunities for other forms of reconnaissance, establishing operational resources, and/or initial access.* Social media sites may contain information about subscriber phone numbers, address etc, which can be used e.g. when installing false base stations in close vicinity of the victim. (2)
Platform:	Mobile network

Procedure Examples:	ID	Name	Description
			The adversary may use open source intelligence to identify victim's routes and

				current location for establishing a false base station. (1) (2)
References:	(1) Cyware Hacker News. (2019). How Hackers Exploit Social Media To Break Into Your Company. (2) Equifax UK. (2022). The risks of sharing your location on social media.			
Analogous technique in other frameworks:	Search Open Websites/Domains: Social Media, Sub-technique T1593.001 - Enterprise | MITRE ATT&CK®			

4.1.18 Adversary-in-the-Middle

Name:	Adversary-in-the-Middle
ID:	MOT1557
Source:	Reused ATT&CK/FiGHT Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	MOT1557.301 Radio Interface Authentication Relay
Tactic:	Persistence
Description:	*Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing* (1) (2)*.* *Adversaries may leverage the AiTM position to attempt to monitor traffic.*
Platform:	Mobile network
Procedure Examples:	
References:	(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2) P1 Security. (2021). All authentication vectors are not made equal.
Analogous technique in other frameworks:	Adversary-in-the-Middle, Technique T1557 - Enterprise | MITRE ATT&CK® Adversary-in-the-Middle | MITRE FiGHT™ (FGT1557)

4.1.18.1 Radio Interface Authentication Relay

Name:	Radio Interface Authentication Relay
ID:	MOT1557.301
Source:	Reused ATT&CK Technique -> Reused/Modified FiGHT sub-Technique
Use:	2G/3G

	4G: Demonstrated
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Persistence
Description:	An adversary positions itself on the radio interface to capture information to and from the UE. Adversary can deploy a false base station as a back-to-back base station - UE combination to impersonate UE towards the real eNB or core network element (such as MME), and impersonate base station or core network element towards the target UE (1) (2).
Platform:	Mobile network
Procedure Examples:	ID / Name / Description After receiving the spoofed location update request, the network then will authenticate the FBS (impersonating as the UE) by sending a cryptographic challenge, the FBS will relay the challenge to be solved to the legitimate UE and relay the answer back to the network. After this the network accepts the connection between it and the FBS as being authenticated. (1) (2)
References:	(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2) P1 Security. (2021). All authentication vectors are not made equal. https://labs.p1sec.com/2021/09/30/all-authentication-vectors-are-not-made-equal/
Analogous technique in other frameworks:	Adversary-in-the-Middle: Radio interface | MITRE FiGHT™

4.1.19 Supply Chain Compromise

Name:	Supply Chain Compromise
ID:	MOT1195
Source:	Reused ATT&CK Technique
Use:	2G, 3G, 4G
Confidentiality:	Public
Sub-Technique:	MOT1195.002 Compromise Software Supply Chain
Tactic:	Initial Access
Description:	*Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise.*

	Supply chain compromise can take place at any stage of the supply chain including: • *Manipulation of development tools* • *Manipulation of a development environment* • *Manipulation of source code repositories (public or private)* • *Manipulation of source code in open-source dependencies* • *Manipulation of software update/distribution mechanisms* • *Compromised/infected system images (multiple cases of removable media infected at the factory)(1) (2)* • *Replacement of legitimate software with modified versions* • *Sales of modified/counterfeit products to legitimate distributors* • *Shipment interdiction* *While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.*
Platform:	Mobile network
Procedure Examples:	See sub-technique.
References:	(1) The Register. (2023). Millions of mobile phones come pre-infected with Malware (2) Schneider Electric. (2018). Security Notification – USB Removable Media Provided With Conext Combox and Conext Battery Monitor.
Analogous technique in other frameworks:	Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®

4.1.19.1 Compromise Software Supply Chain

Name:	Compromise Software Supply Chain
ID:	MOT1195.002
Source:	Reused ATT&CK Technique -> Reused ATT&CK sub-Technique
Use:	N/A
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Initial Access
Description:	*Adversaries may manipulate application software prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise of software can take place in a number of ways, including manipulation of the application source code, manipulation of the*

	update/distribution mechanism for that software, or replacing compiled releases with a modified version.
Platform:	Mobile network
Procedure Examples:	ID / Name / Description: Weak package onboarding process
References:	(1) The Register (2023). Millions of mobile phones come pre-infected with Malware
Analogous technique in other frameworks:	Supply Chain Compromise: Compromise Software Supply Chain, Sub-technique T1195.002 - Enterprise | MITRE ATT&CK®

4.1.20 Network Function Service Discovery

Name:	Network Function Service Discovery
ID:	MOT5003
Source:	Reused FiGHT Technique
Use:	5G-SA: Demonstrated
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Discovery
Description:	*An adversary may query the Network Repository Function (NRF) to discover restricted Network Function (NF) services to further target that NF.*
Platform:	Mobile network
Procedure Examples:	ID / Name / Description: The adversary sends /nnrf-disc/v1/nf-instances with target-nf-type set to UDM (N27) (2)
References:	(1) R. Pell, S. Moschoyiannis, E. Panaousis, R. Heartfield. (2021). Towards dynamic threat modelling in 5G core networks based on MITRE ATT&CK. (2) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem
Analogous technique in other frameworks:	Network Function Service Discovery | MITRE FiGHT™ (FGT5003)

4.1.21 Exploitation for Credential Access

Name:	Exploitation for Credential Access
ID:	MOT1212
Source:	Reused ATT&CK Technique

Use:	
Confidentiality:	Public
Sub-Technique:	N/A
Tactic:	Credential Access
Description:	*Adversaries may exploit software vulnerabilities in an attempt to collect credentials. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code.*
Platform:	Mobile network
Procedure Examples:	ID / Name / Description: The adversary sends Nnrf_AccessToken_GetRequest with information on the services retrieved in the previous stage to the hNRF via vNRF (N27) (1)
References:	(1) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem
Analogous technique in other frameworks:	Exploitation for Credential Access, Technique T1212 - Enterprise | MITRE ATT&CK® https://fight.mitre.org/techniques/FGT5003/

4.1.22 Data Manipulation

Name:	Data Manipulation
ID:	MOT1565
Source:	Reused ATT&CK Technique
Use:	
Confidentiality:	Public
Sub-Technique:	Stored Data Manipulation
Tactic:	Impact
Description:	*Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data.*
Platform:	Mobile network
Procedure Examples:	
References:	(1) The Register. (2017). After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

	(2) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem
Analogous technique in other frameworks:	Data Manipulation, Technique T1565 - Enterprise | MITRE ATT&CK® Data Manipulation | MITRE FiGHT™ (FGT1565)

4.1.22.1 Stored Data Manipulation

Name:	Stored Data Manipulation
ID:	MOT1565.001
Source:	Reused ATT&CK Technique -> Reused ATT&CK sub-Technique
Use:	
Confidentiality:	Public
Sub-Technique:	Stored Data Manipulation
Tactic:	Impact
Description:	*Adversaries may insert, delete, or manipulate data at rest in order to influence external outcomes or hide activity, thus threatening the integrity of the data*
Platform:	Mobile network
Procedure Examples:	ID: Name: Description: The adversary executes a delete of the subscriber registration on the UDM nudm_uecm/v1/{ueId}/registrations/smsf-3gpp-access in order to delete the 3gpp registration access causing data instability (1)
References:	(1) Mobileum (2023) OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem
Analogous technique in other frameworks:	Data Manipulation: Stored Data Manipulation, Sub-technique T1565.001 - Enterprise | MITRE ATT&CK®

4.2 Mitigations

For further study (FFS).

4.3 Software

4.3.1 Passive False Base Station

Name:	Passive False Base Station
ID:	MOS3001
Description:	Passive False Base Station (FBS), also known as IMSI catcher, is a tool which consists of hardware and software that allow for passive attacks against mobile

	subscribers over radio interface. Where the adversary doesn't need to be positioned between the network and target and is able to monitor or capture the traffic that is being broadcasted to all UEs in a given cell.(1)

Techniques Used:

ID	Name	Description
MOT3001.301	Monitor Radio Interface Traffic: Broadcast Channel	False Base Station uses radio passive sniffing to obtain the broadcasted cell configuration (e.g. radio access technology (RAT), frequency, system information block (SIB) configuration, cell ID).
MOT5019.301	Identify Subscriber: Trigger UE Terminated Activity	The adversary sends silent SMS or makes a call to trigger paging to the UE, and monitors the radio interface with a False Base Station to correlate between the terminating activity and the paged IMSI. (1)
MOT1040.501	Network Sniffing: Radio Interface	The False Base Station passively captures the traffic of interest. (1)

Groups that use this software	
References:	(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks

4.3.2 Active False Base Station

Name:	Active False Base Station
ID:	MOS3002
Description:	Active False Base Station (FBS), also known as Rogue Base Station, is a tool which consists of hardware and software that allow for active attacks against mobile subscribers over radio interface. Active attacks that require the adversary to use the FBS to initially interact with the target or the network, to gain certain access or foothold to initiate further attacks. (1)

Techniques Used:

ID	Name	Description
MOT3006.301	Exploit via Radio Interface: AS Signalling	The False Base Station uses 3GPP access radio to attract the UE to attach to a false base station by broadcasting cell configuration with a higher signal strength than the legitimate cell. (1) (2)
MOT3006.303	Exploit via Radio Interface: Radio	The False Base Station broadcasts a different TAC to

		Broadcast Channel (SIB1)	force the target to initiate a TAU. (2)
	MOT3006.302	Exploit via Radio Interface: NAS Signalling	False Base Station initiates Identification procedure by sending an “Identity-Request” message to UE using NAS signalling, in order to request subscriber’s IMSI. (1)
	MOT1036.301	Masquerading: Originating Entity Spoofing	False Base Station uses duplicated CellID. False Base Station may use spoofed PLMN ID towards the UE. (1) (2)
Groups that use this software			
References:	(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2) Aftenposten. (2015). New report: Clear signs of mobile surveillance in Oslo, despite denial from Police Security Service.		

4.3.3 MiTM False Base Station

Name:	MiTM False Base Station		
ID:	MOS3003		
Description:	MiTM False Base Station (FBS), also known as Rogue Base Station, is a tool which consists of hardware and software that allow for full active attacks against mobile subscribers over radio interface. Where the adversary is positioned between the target and the network having the capability to fully intercept subscriber traffic (control plane or user plane). (1) (2) (3)		
Techniques Used:	ID	Name	Description
	MOT3006.302	Exploit via Radio Interface: NAS Signalling	The adversary attempts to use the captured IMSI to spoof a location update request towards the network, impersonating as the legitimate UE. (1)
	MOT1557.301	Adversary-in-the-Middle: Radio Interface Authentication Relay	After receiving the spoofed location update request, the network then will authenticate the FBS (impersonating as the UE) by sending a cryptographic challenge, the FBS will relay the challenge to be solved to the legitimate UE and relay the answer back to the network. After this the network accepts the

				connection between it and the FBS as being authenticated. (1)
Groups that use this software				
References:	(1) Electronic Frontier Foundation. (2019). Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks (2) ArsTechnica. (2016). Stingrays bought, quietly used by police forces across England. (3) Bloomberg. (2016). Racial Disparities in Police 'Stingray' Surveillance, Mapped.			

Annex A STIX Framework for MoTIF

MoTIF can be represented using the STIX framework, to facilitate exchange of MoTIF threat information. Other technologies to represent MoTIF such as MISP or a custom framework were also considered, however given that these are less mature and that ATT&CK, on which MoTIF is based, also uses STIX, this was felt to be the most suitable.

The below outlines the **indicative** use of STIX for MoTIF for version 1 of MoTIF. This is an example data model which can be enhanced and extended later - future MoTIF versions can modify and expand the use of STIX. The key principle of STIX for MoTIF is to follow as closely as possible STIX for ATT&CK [11], where appropriate. Some fields used in ATT&CK STIX may not be needed, in that case then can simply not be included. Additional fields/objects can also be used, but only if required to fulfil a need.

To illustrate the use of MoTIF STIX, an example modelling of a use case is contained in FS.58 “MoTIF Examples.”

A.1 STIX for MoTIF

As stated, the key principle of STIX for MoTIF is to follow as closely as possible STIX for ATT&CK [11] . The STIX version this uses is STIX (2.1). The mapping of MITRE to MoTIF to STIX objects is below. In general for STIX for MoTIF, we use the same relationships, and for naming we replace mitre with gsma/motif where appropriate:

MoTIF concept	STIX object type	Custom type?
Matrix	`x-motif-matrix`	yes
Tactic	`x-motif-tactic`	yes
Technique	`attack-pattern`	no
Sub-technique	`attack-pattern` where `x_motif_is_subtechnique = true`	no
Procedure	`relationship` where `relationship_type = "uses"` and `target_ref` is an attack-pattern	no
Mitigation	`course-of-action`	no
Group	`intrusion-set`	no
Software	`malware` or `tool` or `infrastructure`	no
Collection	`x-motif-collection`	yes
Data Source	`x-motif-data-source`	yes
Campaign	`campaign`	no

Table 4 – Mapping of MoTIF to STIX objects

The above table is nearly identical to the table in [11] save for the replacement of `mitre` with `motif`, and the inclusion of `infrastructure` as an additional choice for Software.

A.2 Extensions of the STIX spec

Like ATT&CK, there are three general ways that MoTIF extends the STIX 2.1 format:

- Custom object types. Object types prefixed with `x-motif-`, e.g `x-motif-matrix`, are custom STIX types extending the STIX 2.1 spec. They follow the general STIX Domain Object pattern but describe concepts not covered by types defined in STIX 2.1.
- Extensions of existing object types. Fields extending the STIX 2.1 spec are prefixed with `x_motif_`, e.g `x_motif_platforms` in attack-patterns. The following extended fields are common across MoTIF types except where otherwise noted:

Field	Type	Description
`x_motif_version`	string	The version of the object in format major.minor where major and minor are integers. MoTIF increments this version number when the object content is updated. Not found on relationship objects.
`x_motif_contributors*`	string[]	People and organizations who have contributed to the object. Not found on relationship objects. Not used left blank for now
`x_motif_modified_by_ref*`	string	The STIX ID of an identity object. Used to track the identity of the individual or organization which created the current version of the object. Previous versions of the object may have been created by other individuals or organizations.
`x_motif_domains`	string[]	Identifies the domains the object is found in. See domains for more information. Not found on relationship objects.
`x_motif_attack_spec_version`	String	The version of the MoTIF spec used by the object. Consuming software can use this field to determine if the data format is supported. If the field is not present on an object the spec version will be assumed to be 1.0.0. See the MoTIF Spec for the current spec version number.

Table 5 – MoTIF extensions of existing object types

*NOTE: These Fields with asterisks are copied from the MITRE spec and included for completeness, but the current example in section does not include them.

- New relationship types. Unlike custom object types and extended fields, custom relationship types are not prefixed with `x_motif`. The reader can find a full list of relationship types in the Relationships section in [11] , which also mentions whether the type is a default STIX type.

A.2.1 Domains

The original `x_mitre_domain` can represent 3 different domains, however for `x_motif_domain` this value shall be set to "`gsma motif`". Future versions may include the original domains or additional domains as well.

A.2.2 IDs in MoTIF

ID naming shall follow the guidelines in [11], and in section 2.3 Tactic/Technique Numbering.

A.3 STIX MoTIF Types

A.3.1 Matrices

As [11], `x-motif-matrix` replaces `x-mitre-matrix`. Note: the use of this object is not shown in enclosed example.

A.3.2 Tactics

As [11], `x_motif_shortname` replaces `x_mitre_shortname`.

A.3.3 Techniques / Sub-techniques

As [11], `x_motif_is_subtechnique` replaces `x_mitre_is_subtechnique`. For the other `x_mitre_` fields these shall be used as `x_motif_` when required on a case by case basis.

Both technique and sub-technique in MoTIF are represented as attack-patterns. They differ in that sub-techniques have the Boolean field (`x_motif_is_subtechnique`) set to true. Also for a sub-technique this has a relationship of the type `subtechnique-of` where the `source_ref` is the sub-technique and the `target_ref` is the parent technique. See [11] for more details.

A.3.3.1 Additional fields

As of version 1 of MoTIF, 1 additional field is used in MoTIF STIX for techniques/sub-techniques, which is not present in ATT&CK STIX, this is `x-motif-use.` The `x-motif-use field` represents technologies and status in which the technique/sub-technique has been used, see section 2.4 Technique/Sub-technique Labeling for more details. The JSON MTI serialization uses the JSON Object type [RFC8259] when representing `x-motif-use.`

Field	Type	Description
`x_motif_use`	string	Technologies and status in which the Technique/sub-technique has been used, see section 2.4 Technique/Sub-technique Labeling for more details. It is a mix of technology ("2G", "3G", "4G", "5G-SA", "5G-NSA") and optional status in the case if it has not been seen 'in the wild' ("demonstrated", "theoretical").

An example of this is as follows:

```
"x_motif_use": [
   "2G",
   "3G",
   "4G:theoretical"
```

]

A.3.4 Procedures

As [11].

A.3.5 Mitigations

As [11].

A.3.6 Groups

As [11].

A.3.7 Software

As [11], other than the fact that the `Infrastructure` SDO could also be used to represent software. This could be most applicable for Software like Fake Base Stations where the package used to execute the attack is a combination of software and hardware, so ‘Tool’ or malware would not be appropriate choices here.

A.3.8 Data Sources and Data Components

As [11].

A.3.9 Campaigns

As [11].

A.3.10 Relationships

As [11].

Annex B Document Management

B.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	21 Mar 2024	First version of MoTIF principles	ISAG	Cathal McDaid, Enea

B.2 Other Information

Type	Description
Document Owner	Fraud and Security Group (FASG)
Editor / Company	Cathal Mc Daid, Enea
Additional Contributors	Ericsson Huawei Mobileum The MITRE Corporation

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.