SecurityGen

Telecom Security. Transcending Generations.

2024/25 SecurityGen Guidelines:

Protecting Telecom Infrastructures from Advanced Threats

Table of Contents

01. Introduction

Telecom infrastructures are the critical backbone of modern communication, making them a prime target for a wide range of hacker attacks. These attacks range from opportunistic ransomware campaigns aimed at quick monetization to sophisticated adversaries seeking to infiltrate networks, remain undetected, exfiltrate data, and spread laterally to other peers.

Recent cases have demonstrated that attackers now possess an in-depth understanding of telecom technologies that were once considered obscure or inherently secure. They leverage these methods to gain initial access, bypass defenses, and steal sensitive data, leaving significant impacts on operators and their subscribers.

This guide aims to provide actionable steps for protecting telecom infrastructures from advanced threats. By using real-world examples, such as the recent Liminal Panda case, it outlines best practices, mitigation techniques, and detection frameworks designed to secure telecom networks against evolving attack vectors.

02. Telecom Attack Analysis and Mitigation Guide

Based on Liminal Panda Case

Where do we begin

On 19 November 2024, CrowdStrike shed light on a newly identified advanced persistent threat (APT) group called Liminal Panda, which has compromised at least 13 telecom companies since 2020. The group specializes in **signals intelligence (SIGINT)** operations, a form of intelligence gathering that involves intercepting communications or electronic signals to extract valuable information. Leveraging a deep understanding of telecom networks, Liminal Panda exploits GRX/IPX interconnections between telecom providers, extracts subscriber-related data, and tunnels data through GTP and SS7 protocols to evade detection.

Different hacker groups often have varying goals, distinct toolsets, and their own unique methods of operation. This white paper examines the activities of hacker groups exploiting telecom protocols, using Liminal Panda as a case study. By leveraging the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) framework, we provide insights into how attackers operate and draw conclusions about potential protection measures that organizations can implement to defend against similar types of attacks.

Additionally, we reference frameworks such as MITRE FiGHT and GSMA MoTIF to map the observed Tactics, Techniques, and Procedures (TTPs) of attackers within a telecom-related context.

03. Operations and Tactics

3.1. Initial Access and Execution

Liminal Panda compromised multiple telecom providers by targeting their GRX and IPX DNS servers. These systems are essential for enabling communication and data exchange between mobile network operators, particularly for roaming services. GRX facilitates data transfer for older mobile technologies like 2G and 3G, while IPX handles the same for modern 4G and 5G networks.

The attackers focused on services supported by these servers, including MMS, which allows users to send pictures and videos, and IMS, a framework that enables advanced IP-based services like VoLTE and video calling. Liminal Panda gained access by performing password spraying attacks on weak SSH credentials, exploiting trust relationships between telecom providers, and taking advantage of poor security configurations.

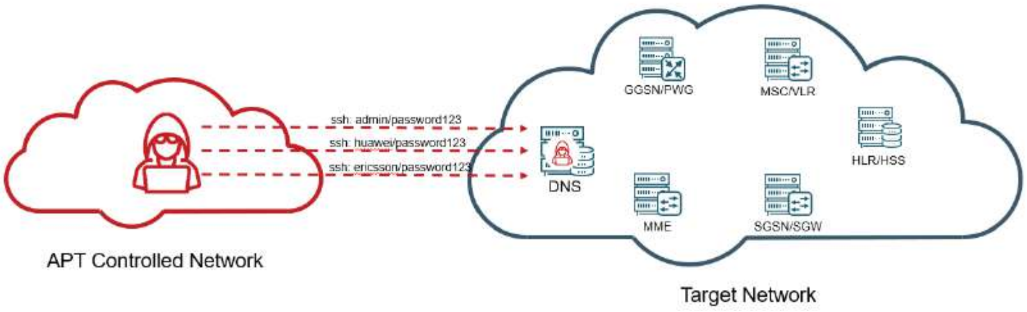


Figure 1 – Example of SSH password spraying

Relevant TTPs:

ATT&CK TECHNIQUE	FIGHT EQUIVALENT	MOTIF EQUIVALENT
T1199 — Trusted Relationship	FGT1199.501 — Trusted Relationship: MNO Roaming Partners	MOT1199.301 — Exploit Interconnection Agreements
T1078.003 — Local Accounts	FGT1078.003 — Local Accounts	NA
T1059.004 — Command and Scripting Interpreter: Unix Shell	NA	NA

3.2. Persistence, Defense Evasion and C2

After gaining initial access, the group deploys a backdoor called PingPong. This backdoor is designed to listen for specially crafted ICMP echo requests, often referred to as "magic" packets, sent from another compromised telecom provider. These requests act as a signal to activate the backdoor, which then establishes a reverse TCP shell. This shell connects back to a remote Command and Control (C2) server using TCP port 53, a port typically associated with DNS traffic. By disguising their activity as legitimate DNS queries, the attackers effectively mask their malicious communication.

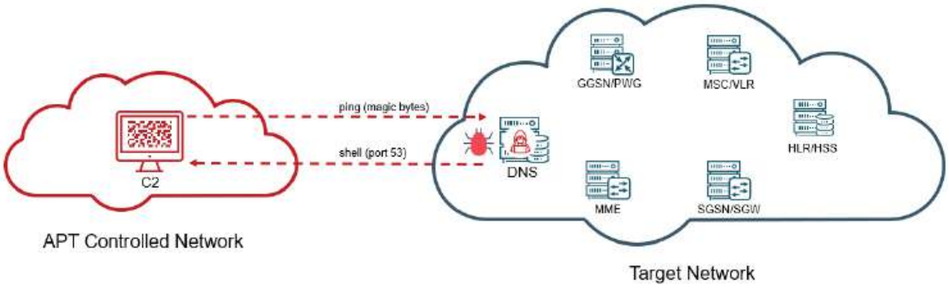


Figure 2 - Installing PingPong backdoor

To maintain persistence on the compromised system, the attackers modify the SSH SysVinit script, ensuring the backdoor automatically launches whenever the SSH service starts. They also implement custom iptables rules on the DNS server, allowing SSH access from five other compromised telecom providers. To evade detection further, the group replaces the standard iptables binary with a custom-built wrapper. This wrapper conceals the malicious rules, making them invisible to regular iptables queries and ensuring their unauthorized access remains hidden from system administrators.

Relevant TTPs:

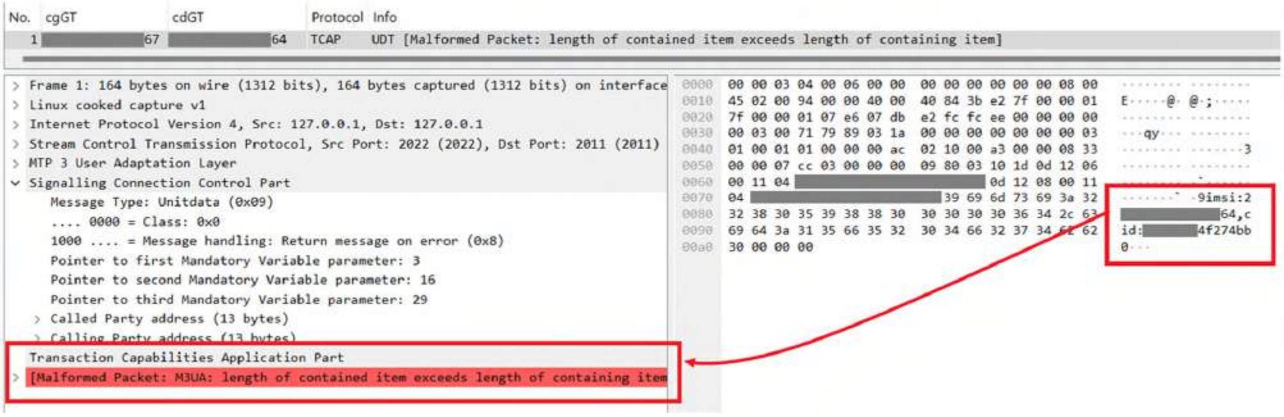
ATT&CK TECHNIQUE	FIGHT EQUIVALENT	MOTIF EQUIVALENT
T1543.002 — Create or Modify System Process: Systemd Service	NA	NA
T1562.004 — Impair Defenses: Disable or Modify System Firewall	NA	NA
T1562.001 — Impair Defenses: Disable or Modify Tools	NA	NA
T1071.004 — Application Layer Protocol: DNS	FGT1437 — Application Layer Protocol	NA
T1105 — Ingress Tool Transfer	NA	NA

3.3. Discovery, Collection and Exfiltration

The group uses a utility called **CordScan** to scan networks and capture packets, enabling them to identify network components and extract sensitive subscriber data, such as traffic patterns and location information. They specifically target network elements like SGSNs (Serving GPRS Support Nodes). These are critical components of mobile networks responsible for managing the flow of data between mobile devices and the core network. SGSNs handle tasks like setting up data sessions, routing mobile data packets, and keeping track of the location of mobile devices within the network.

To evade detection, the attackers route all their Command and Control (C2) communications and stolen data through GTP and SS7 protocols, disguising their activities as legitimate network traffic. They also use an emulator called sgsnemu, which mimics the behavior of an SGSN. This allows them to send fake Packet Data Protocol (PDP) context requests using pairs of international phone identifiers (IMSI/MSISDN numbers), making their communications appear as normal subscriber data traffic.

Additionally, the attackers deploy a tool called SIGTRANslator to send and receive data over the SS7 (SIGTRAN) protocol. This tool encrypts data using a pre-defined XOR key (wuxianpinggu507), further hiding their activities and making the exfiltration of data more difficult to detect.



```
No.  cgGT              cdGT              Protocol  Info
  1  [redacted]67      [redacted]64      TCAP      UDT [Malformed Packet: length of contained item exceeds length of containing item]
```

```
> Frame 1: 164 bytes on wire (1312 bits), 164 bytes captured (1312 bits) on interface
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
> Stream Control Transmission Protocol, Src Port: 2022 (2022), Dst Port: 2011 (2011)
> MTP 3 User Adaptation Layer
v Signalling Connection Control Part
    Message Type: Unitdata (0x09)
    .... 0000 = Class: 0x0
    1000 .... = Message handling: Return message on error (0x8)
    Pointer to first Mandatory Variable parameter: 3
    Pointer to second Mandatory Variable parameter: 16
    Pointer to third Mandatory Variable parameter: 29
  > Called Party address (13 bytes)
  > Calling Party address (13 bytes)
  Transaction Capabilities Application Part
> [Malformed Packet: M3UA: length of contained item exceeds length of containing item
```

```
0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········ ········
0010  45 02 00 94 00 00 40 00  40 84 3b e2 7f 00 00 01   E·····@· @·;·····
0020  7f 00 00 01 07 e6 07 db  e2 fc fc ee 00 00 00 00   ········ ········
0030  00 03 00 71 79 89 03 1a  00 00 00 00 00 00 00 03   ···qy··· ········
0040  01 00 01 01 00 00 00 ac  02 10 00 a3 00 00 08 33   ········ ·······3
0050  00 00 07 cc 03 00 00 00  09 80 03 10 1d 0d 12 06   ········ ········
0060  00 11 04 [redacted] 0d 12 08 00 11
0070  04 [redacted] 39 69 6d 73 69 3a 32                  ·······` ·9imsi:2
0080  32 38 30 35 39 38 38 30  30 30 30 30 36 34 2c 63   [redacted]64,c
0090  69 64 3a 31 35 66 35 32  30 34 66 32 37 34 62 62   id:[redacted]4f274bb
00a0  30 00 00 00                                        0···
```

Figure 3 - Example of data exfiltration using SS7

Relevant TTPs:

ATT&CK TECHNIQUE	FIGHT EQUIVALENT	MOTIF EQUIVALENT
T1046 — Network Service Discovery	FGT1046 — Network Service Discovery	MOT1046 — Network Service Scanning
T1040 — Network Sniffing	FGT1040 — Network Sniffing	MOT1040 — Network Sniffing
T1048.001 — Exfiltration Over Symmetric Encrypted Non-C2 Protocol	FGT1048 — Exfiltration Over Alternative Protocol	NA

04. Mitigation and Detection Guide

The recommendations outlined below highlight actionable steps and best practices to secure telecom networks against evolving attack vectors. Monitoring signaling messages is critical for detecting anomalies, preventing C2 tunneling, and stopping data exfiltration. Combined with robust firewalls configurations, host-based monitoring, and intrusion prevention systems, these measures provide a comprehensive defense for core telecom infrastructure.

4.1. Preventing Initial Access and Execution

Ensuring robust GRX/IPX edge firewall configurations and protecting OAM interfaces is crucial for restricting unauthorized access and preventing adversaries from gaining a foothold to execute malicious activities.

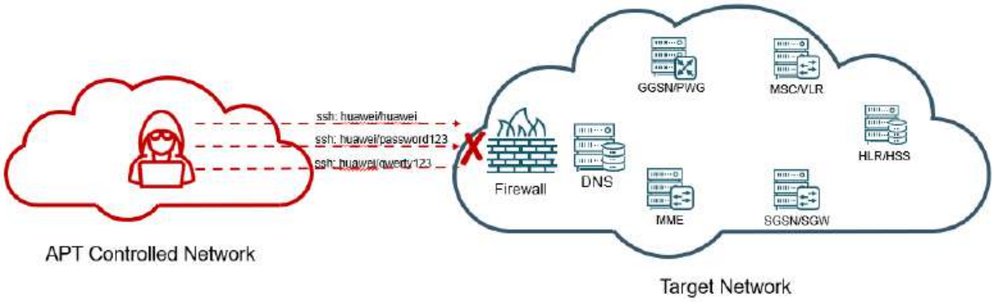


Figure 4 – Restricting OAM interfaces via GRX/IPX edge firewall

Mitigations

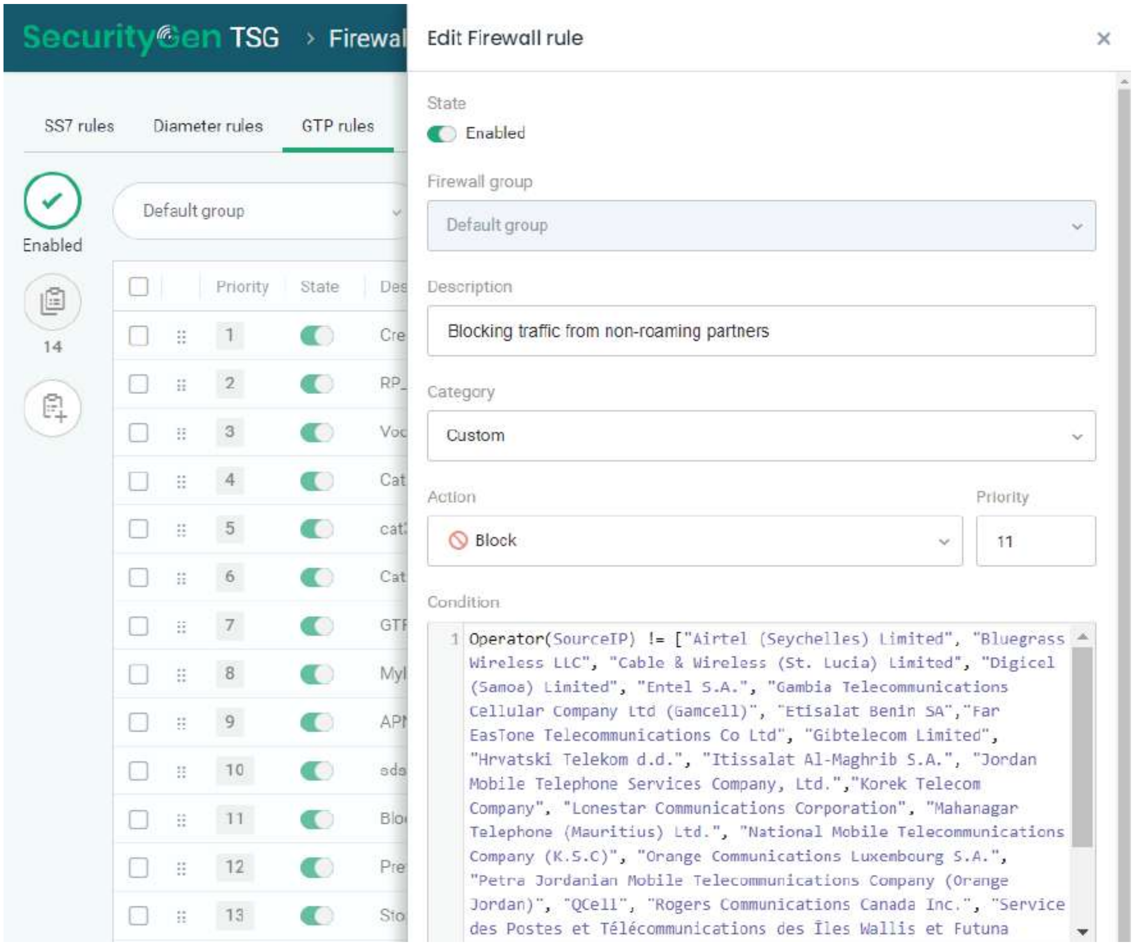
- Configure firewalls at the GRX/IPX network edges to allow GTP interconnect traffic only to and from IP ranges of authorized roaming partners.
- Configure firewalls at the GRX/IPX network edges to allow only GTP-C, GTP-U, and DNS protocols over GTP interconnects. Block access to internal OAM network services, such as SSH.
- Enforce a strong password policy for SSH authentication or switch to secure SSH key-based authentication
- Use out-of-band management channels with dedicated network interfaces for managing core network elements.

- Enable multi-factor authentication (MFA) for local accounts to add an extra layer of protection against credential theft and misuse.
- Conduct regular security audits to ensure that non-essential services for international roaming are not exposed on the GRX/IPX network.

Detection

- Analysis of OAM service logs like SSH on the GRX/IPX DNS and core network element may indicate unusual activity.

Below you can see an example of the firewall rule, configured on [TSG GTP FW](), that prevents traffic into the network from unauthorized roaming partners:



Edit Firewall rule

State: Enabled

Firewall group: Default group

Description: Blocking traffic from non-roaming partners

Category: Custom

Action: Block

Priority: 11

Condition

```
Operator(SourceIP) != ["Airtel (Seychelles) Limited", "Bluegrass
Wireless LLC", "Cable & Wireless (St. Lucia) Limited", "Digicel
(Samoa) Limited", "Entel S.A.", "Gambia Telecommunications
Cellular Company Ltd (Gamcell)", "Etisalat Benin SA","Far
EasTone Telecommunications Co Ltd", "Gibtelecom Limited",
"Hrvatski Telekom d.d.", "Itissalat Al-Maghrib S.A.", "Jordan
Mobile Telephone Services Company, Ltd.","Korek Telecom
Company", "Lonestar Communications Corporation", "Mahanagar
Telephone (Mauritius) Ltd.", "National Mobile Telecommunications
Company (K.S.C)", "Orange Communications Luxembourg S.A.",
"Petra Jordanian Mobile Telecommunications Company (Orange
Jordan)", "QCell", "Rogers Communications Canada Inc.", "Service
des Postes et Télécommunications des Îles Wallis et Futuna
```

Figure 5 – Restricting traffic from non-roaming partners

4.2. Persistence, Defense Evasion and C2

Implementing host-based security monitoring on IT nodes supporting the core telecom network, along with deploying network Intrusion Prevention System (IPS) solutions, is critical for detecting malicious activities, disrupting C2 communications, and preventing further progression of the attack chain.

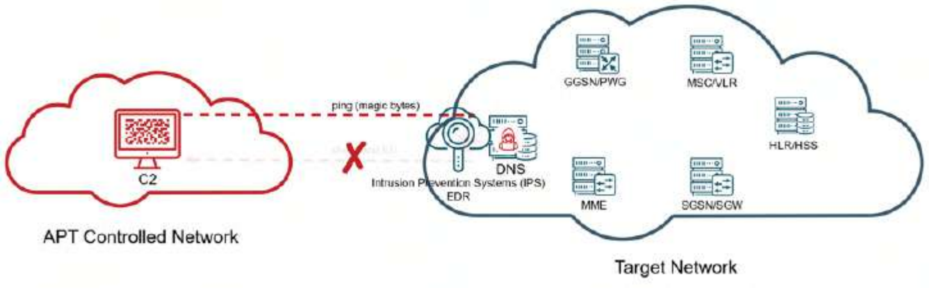


Figure 6 – Network-based IPS for preventing DNS tunneling

Mitigations

- Restrict write access to SysVinit scripts and systemd unit files to only select privileged users who have a legitimate need to manage system services.
- Limit user access to system utilities such as systemctl to only users who have a legitimate need.
- Deploy network intrusion detection and prevention systems that use network signatures to identify C2 traffic for specific adversary malware can be used to mitigate activity at the network level.
- Implement endpoint security monitoring for IT network elements that support the core telecom network, such as GRX/IPX DNS servers.

Detection

- Audit the file creation and modification events of SysVinit scripts and systemd unit files to detect suspicious activities.
- Monitor executed commands and arguments for suspicious activity associated with downloading external content.
- Monitor and analyze traffic patterns and packet inspection for DNS protocol traffic that deviates from expected standards and traffic flows. This includes identifying extraneous packets outside established flows, anomalous traffic patterns, and irregular syntax or structure.

4.3. Discovery, Collection and Exfiltration

Continuous signaling security monitoring is essential for detecting unauthorized core network activities, such as GTP/SS7 traffic from GRX/IPX DNS servers. It also helps identify anomalies or malformed signaling messages, preventing the tunneling of C2 traffic. This approach effectively disrupts the attack chain and prevents data exfiltration.

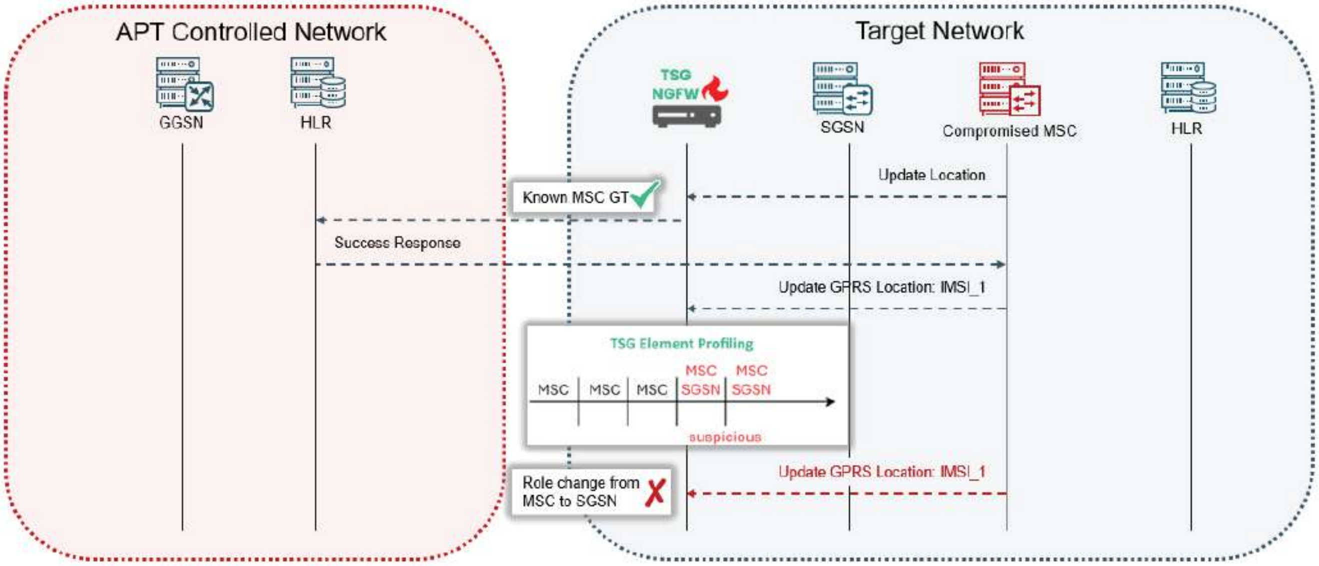


Figure 7 – Example of behavioral analysis of signaling messages

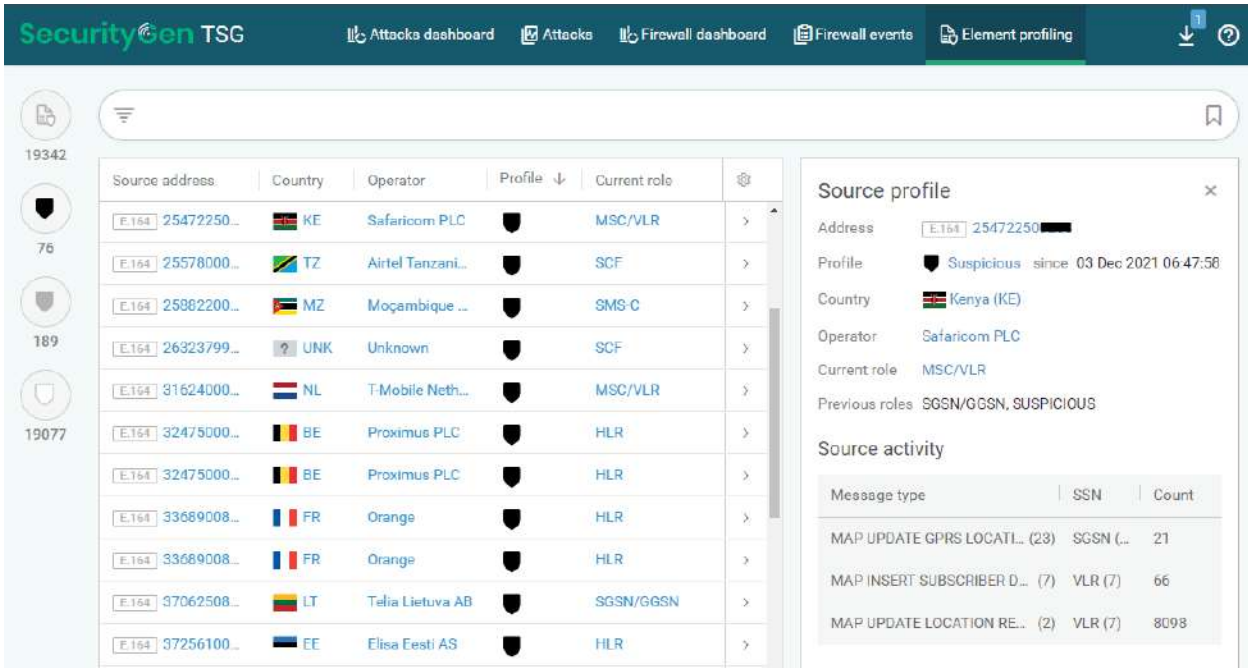
Mitigations

- Configure firewalls at the IPX network edges to allow SIGTRAN interconnect traffic only between the border STP and the authorized IPX provider.
- Deploy a next-generation signaling firewall to perform application-level inspection, analyze protocol anomalies, and block malformed signaling messages used for data tunneling.

Detection

- Deploy a signaling Intrusion Detection System (IDS) to identify deviations in message frequency or rate, as well as anomalous traffic patterns, irregular syntax, or structure, which may indicate tunneling attempts.

Below is an example of malicious node detection based on behavioral analysis. The node suddenly changes its role from VLR to SGSN:



Source address	Country	Operator	Profile ↓	Current role	
E.164 25472250...	KE	Safaricom PLC	⛊	MSC/VLR	›
E.164 25578000...	TZ	Airtel Tanzani...	⛊	SCF	›
E.164 25882200...	MZ	Moçambique ...	⛊	SMS-C	›
E.164 26323799...	? UNK	Unknown	⛊	SCF	›
E.164 31624000...	NL	T-Mobile Neth...	⛊	MSC/VLR	›
E.164 32475000...	BE	Proximus PLC	⛊	HLR	›
E.164 32475000...	BE	Proximus PLC	⛊	HLR	›
E.164 33689008...	FR	Orange	⛊	HLR	›
E.164 33689008...	FR	Orange	⛊	HLR	›
E.164 37062508...	LT	Telia Lietuva AB	⛊	SGSN/GGSN	›
E.164 37256100...	EE	Elisa Eesti AS	⛊	HLR	›

Source profile ×

Address	E.164 25472250[redacted]
Profile	⛊ Suspicious since 03 Dec 2021 06:47:58
Country	Kenya (KE)
Operator	Safaricom PLC
Current role	MSC/VLR
Previous roles	SGSN/GGSN, SUSPICIOUS

Source activity

Message type	SSN	Count
MAP UPDATE GPRS LOCATI... (23)	SGSN (...	21
MAP INSERT SUBSCRIBER D... (7)	VLR (7)	66
MAP UPDATE LOCATION RE... (2)	VLR (7)	8098

Picture 8 – Example of suspicious node detection

05. Table of Terms and Abbreviations

Term/Abbreviation	Definition
APT	Advanced Persistent Threat - A sophisticated, targeted cyberattack that persists over time.
C2	Command and Control - A mechanism used by attackers to remotely control compromised systems.
DNS	Domain Name System - A system that translates domain names into IP addresses.
FiGHT	MITRE Framework for 5G Cybersecurity - A framework addressing cybersecurity in 5G networks.
GRX/IPX	GPRS Roaming Exchange/Internet Protocol Exchange - Networks enabling data exchange between mobile operators.
GSMA MoTIF	GSMA's Mobile Threat Intelligence Framework - A telecom-specific security framework.
GTP	GPRS Tunneling Protocol - A protocol for carrying General Packet Radio Service (GPRS) traffic.
ICMP	Internet Control Message Protocol - A protocol used for error reporting and diagnostic functions in network communications.
IDS	Intrusion Detection System - A tool or software designed to detect unauthorized access or malicious activities in a network or system.
IMS	IP Multimedia Subsystem - A framework for delivering IP-based multimedia services, such as voice and video calls over LTE networks.
IMSI/MSISDN	International Mobile Subscriber Identity/Mobile Station International Subscriber Directory Number - Identifiers used to track and route mobile subscriber traffic.
MMS	Multimedia Messaging Service - A messaging service for sending images, videos, and other multimedia content over mobile networks.
MITRE ATT&CK®	Adversarial Tactics, Techniques, and Common Knowledge - A framework for understanding cyberattacks.
OAM	Operations, Administration, and Maintenance - A set of functions for managing and maintaining telecom networks.
SIGINT	Signals Intelligence - Intercepting communications or signals to gather information.

SGSNs	Serving GPRS Support Nodes - Network components responsible for delivering mobile data to and from devices and maintaining subscriber location data.
SSH	Secure Shell - A protocol for secure remote login and command execution over a network.
SS7	Signaling System No. 7 - A protocol used for setting up and managing telecom calls.
STP	Signaling Transfer Point - A component in telecom networks that routes signaling messages between different network elements.
TTPs	Tactics, Techniques, and Procedures - Methods and strategies used by attackers.
VoLTE	Voice over LTE - A technology that enables high-quality voice and video calls over LTE networks.

06. References

1. CrowdStrike — Unveiling LIMINAL PANDA
https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/

2. MITRE ATT&CK Framework
https://attack.mitre.org/

3. MITRE FiGHT Framework
https://fight.mitre.org/

4. GSMA MoTIF Framework
https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-57-mobile-threat-intelligence-framework-motif-principles/

About SecurityGen

SecurityGen is a global company focused on cybersecurity for telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure safe and robust network operations. Our extensive product and service portfolio provides complete protection against existing and advanced telecom security threats

Connect With Us

Email: contact@secgen.com
Website: www.secgen.com

UK | Italy | Czech Republic | Brazil | Mexico
India | Malaysia | UAE | Egypt | Lebanon