SecurityGen

Telecom Security. Transcending Generations.

How to Catch Hackers in Telecom Infrastructure

An IDS Case Study

1 EXECUTIVE SUMMARY

In recent news, we often can see that hackers compromise telecom networks to commit fraud or steal confidential information. One of the latest loud news is a story of the Liminal Panda group [1]. The story shows that an experienced criminal group can bypass the security measures and establish a foothold in the telecom operator network. To detect the hacker activity for the following blocking, Intrusion Detection System (IDS) can be used on the operator's network.

SecurityGen Telecom Security Guard (TSG) intrusion detection system is specifically designed to identify and mitigate malicious or suspicious activities targeting old GSM/UMTS, widely used LTE, and modern 5G networks . Typically, intruders operate from the external side of the mobile operator trying to penetrate inside, but in some cases, they might already have compromised network and execute malicious activity from internal premises to outer. The TSG employs detection mechanisms capable of monitoring both incoming and outgoing traffic, so it is able to recognize the threats originated both externally and internally. These mechanisms are based on our in-house security research and grounded in GSMA security guidelines, including FS.11, FS.19, and FS.20, and utilize predefined signatures that can be manually enabled or disabled to enhance precision.

Let's have a look at an example of a mobile network serving about 65 million subscribers that has the TSG IDS on premises for attack detection. The IDS identified a hacker source attempted to attack the network on the SS7 protocol with both simple attacks and advanced bypass techniques.

First, the intruders tried to use a set of obsolete operations such as SendIMSI, BeginSubscriberActivity, and StatusReport. Some of them (BeginSubscriberActivity and StatusReport) were executed with a bypass technique of the Sub-System Number (SSN) substitution. Apart from that, the intruders attempted one more bypass technique exploiting a handshake procedure on the inconsistent operation.

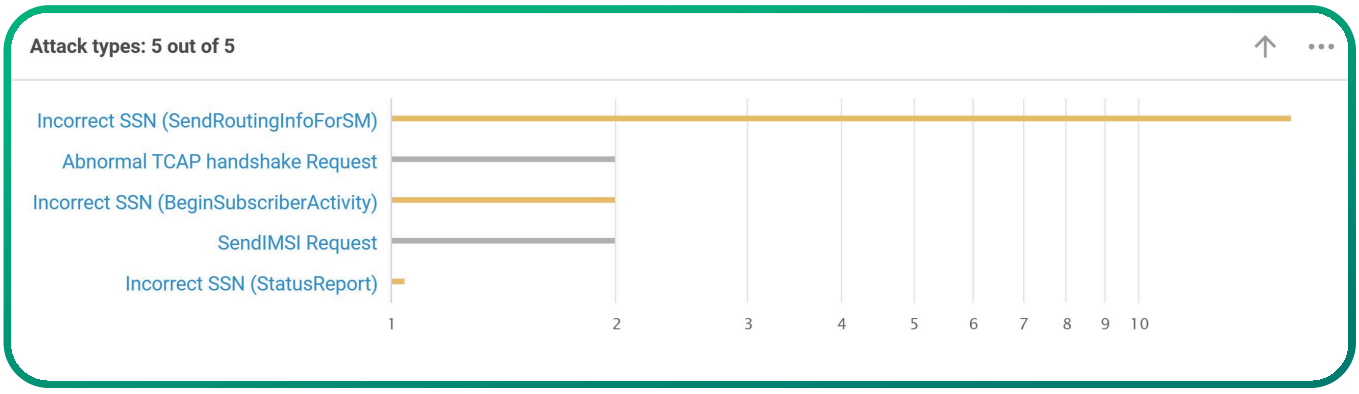

Figure 1 - Detected attack attempts

All attack attempts were unsuccessful. However, the hackers kept the fingerprints that can identify them on another possible intrusions.

2 TECHNICAL DETAILS

2.1. Technique description

The IDS uncovers notable attack attempts. One such instance involved a node connected to the signaling SS7 network employing multiple bypass techniques. In SS7 signaling, the addresses of the source and destination nodes should contain an indication of the roles. This indicator is called sub-system number (SSN). This node intermittently sent signaling messages with altered sub-system numbers, effectively manipulating the roles of the source or destination.

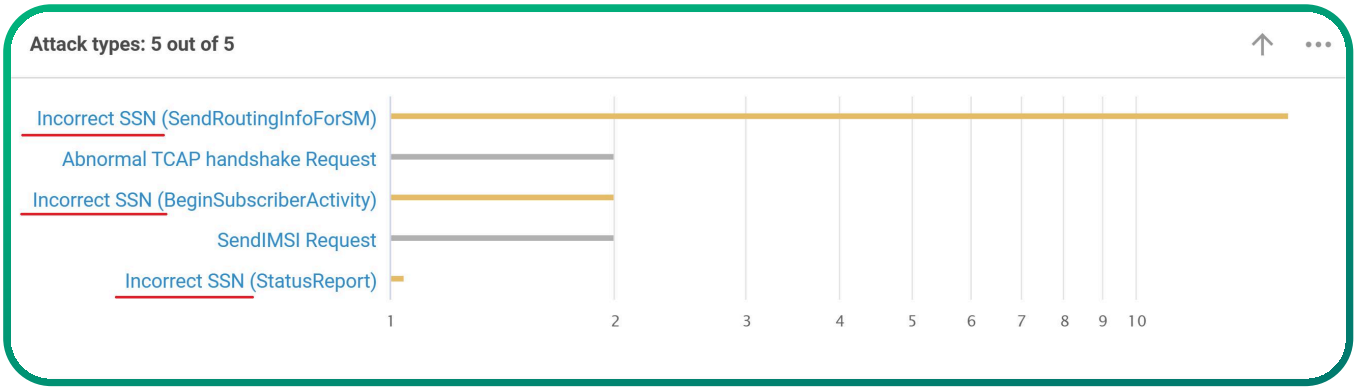

Figure 2 – Detected events with incorrect SSN values

In a mobile network, each node serves a specific function—whether it's the Home Location Register (HLR) managing subscriber data, the Mobile Switching Center (MSC) handling voice calls, or the Short Message Service Center (SMS-C) managing SMS traffic. To distinguish these roles, the SS7 SCCP protocol utilizes SSNs for defining both source and destination nodes. For standard operations, the destination node's SSN is critical, whereas the source node's SSN often goes unchecked. This leniency creates a potential vulnerability in routing logic, where both source and destination SSNs might determine message routing. For example, signaling messages associated with the MAP protocol might require SS7 firewall inspection, whereas CAP protocol messages could bypass it entirely.

Malicious actors exploit this vulnerability by using CAP SSNs as a source, bypassing SS7 firewall inspection and directing messages to their intended targets without scrutiny.

Additionally, the same node attempted to initiate a handshake procedure commonly associated with CAMEL sessions. Originally implemented as a security feature to combat SMS spam, the handshake mechanism involves a two-step process: the initial message includes an Application-Context Name (ACN) related to SMS handling without specific payload details, and the subsequent transaction completes the data exchange. However, some SS7 implementations fail to restrict this mechanism solely to SMS-related signaling, allowing attackers to repurpose it for unauthorized operations. This observed behavior strongly suggested malicious intent, prompting further investigation.

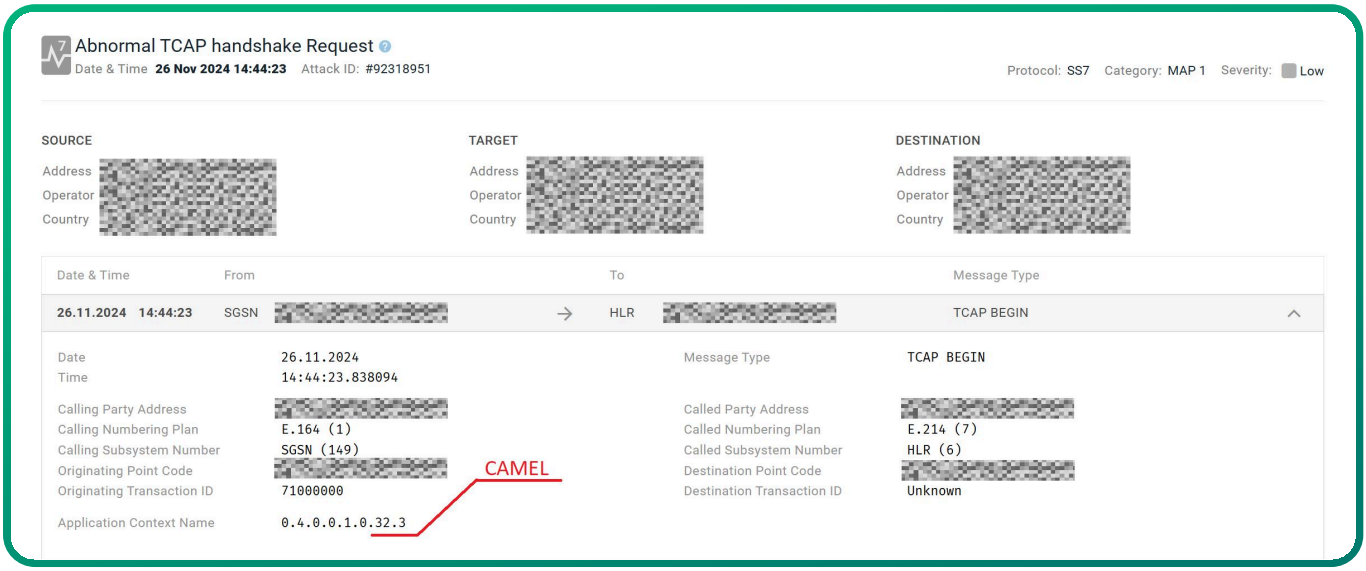

Figure 3 – Abnormal handshake procedure with CAMEL Application Context Name.

Further analysis of the node's activity revealed a repertoire of outdated operations, such as SendIMSI, BeginSubscriberActivity, and StatusReport. These legacy requests are often exploited to probe for weak points in security. What stood out even more were the transaction ID values. Unlike the randomized IDs typically generated by legitimate equipment, this node consistently used IDs starting with "000000," with only the last two digits varying—strong evidence of manually crafted requests from hacker tools.

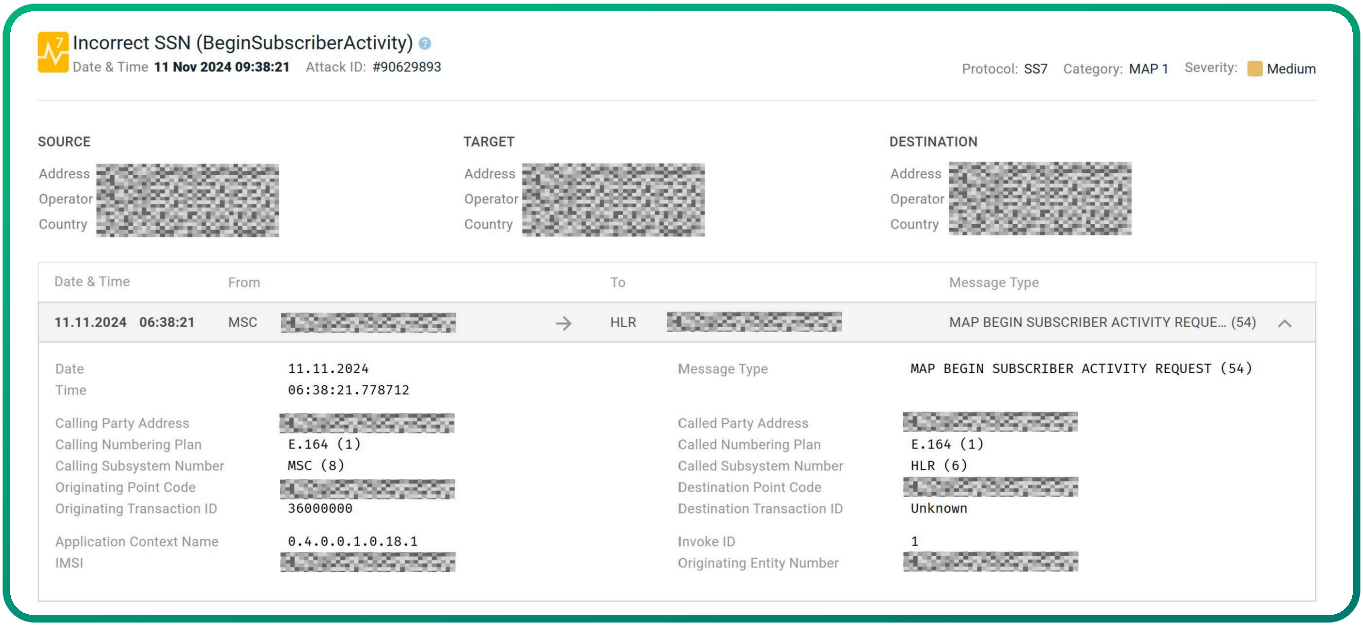

Figure 4 – Example of incorrect SSN detection

Despite these attempts being unsuccessful, we recommended the customer take proactive measures. The source node was blocked, and a formal complaint was lodged with the originating operator, accompanied by detailed logs and evidence of abuse.

This case highlights the indispensable role of an IDS in strengthening network security. Beyond safeguarding against external threats, it serves as a critical tool for detecting and mitigating abuse from internal resources, ensuring comprehensive protection for modern telecommunications infrastructure.

2.2. Tactics, Techniques, and Procedures (TTPs)

The following table maps observed TTPs for the detected intruders to relevant techniques in the MITRE ATT&CK, MITRE FiGHT, and GSMA MoTIF frameworks to provide comprehensive context.

Tactics	Attack Technique	Fight Equivalent	Motif Equivalent
Reconnaissance	T1590.004 - Gather Victim Network Information: Network Topology	FGT1592.501 - Gather Victim Host Information: Internal resource search	MOT1597.301 - Search Closed Sources: Mobile Network Operator Sources
Initial Access	T1199 – Trusted Relationship	FGT1199.501 - MNO Roamer Partners	MOT1199.301 Exploit Interconnection Agreements
Defense Evasion	N/A	FGT5002 – Bypass Home Routing	MOT3005.301 - Disguise Signalling Messages: Unexpected Encoding

3 IMPACT ANALYSIS

Here, we investigate hacker activity—persistent attempts to exploit the network. Fortunately, thanks to IDS adoption and periodic security audits, the network security has already reached a high level, making it nearly impossible for attackers to penetrate using the techniques and procedures observed.

Yet, the sheer volume of exploit attempts before they gave up proves two key points:

- These attackers are well-prepared.
- They are highly motivated, willing to spend time even when facing failure.

This underscores the critical importance of continuous security monitoring—to keep an eye on such malicious activities and stay ahead of threats.

In case of the successful execution, two of the attacks could lead to IMSI identity disclosure. The IMSI – International Mobile Subscriber Identity – is an internal identifier of a SIM card that is normally used by the network equipment to identify a subscriber. When the intruders know this identity, they can then carry out such threats as location tracking, denial-of-service, or intercept voice call or an incoming SMS.

Two more attacks with the operations BeginSubscriberActivity and StatusReport could not have affect on the network apart from node address disclosure. For sure, this data could be also useful for the intruders in the following attacks. However, disclosure of the node element addresses has much lower value for the intruders than IMSI identity. We suppose that these attempts were intended to discover vulnerabilities in the network protection to execute later more interesting attacks.

And the last one attack attempt connected with delivery of a CAMEL payload using the handshake procedure, in case of the successful execution might lead to the fraudulent activity. Using the CAMEL protocol, the intruders would be able to generate fake traffic that would be changed by an external direction pointed out by the intruders.

Since all attack attempts were unsuccessful, quickly detected, and the operator has got a recommendation to block the hostile resource at all, so all assumptions above stayed assumptions.

4 MITIGATION

As we reported repeatedly, all attack attempts described in the title were unsuccessful. However, we cannot exclude that the actions of these hackers will always be ineffective on attacking the network of another operators. To mitigate the threat, the mobile operators should perform some preliminary measures.

4.1. Immediate steps

- Perform signaling security audit to check if the network is vulnerable or may be exposed to signaling attacks from the external interfaces.
- Based on the results of the security audit, evaluate the threats and prioritize risks.
- Make a plan of the network hardening.

4.2. Long-term recommendations

- Check the signaling network security regularly on the external roaming interfaces.
- Introduce continuous signaling security monitoring to detect attack attempts timely.
- Deploy active signaling security means such as signaling firewall to have on-the-go protection against all known signaling attacks.

5 References

[1]. CroudStrike. “Unveiling LIMINAL PANDA”.
https://www.crowdstrike.com/en-us/blog/liminal-panda-telecom-sector-threats/

About SecurityGen

SecurityGen is a global company focused on 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

contact@secgen.com

www.secgen.com

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