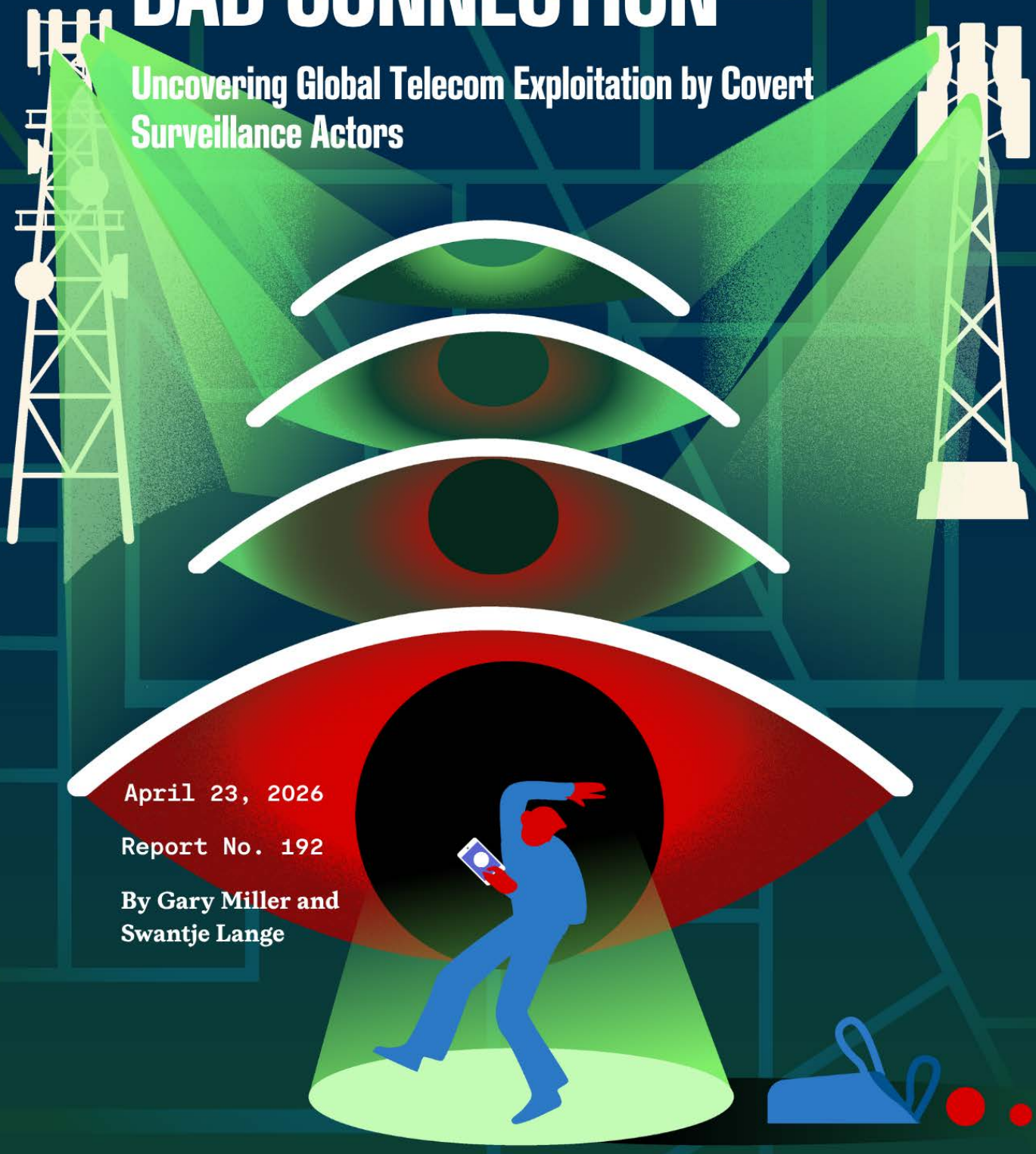
BAD CONNECTION

Uncovering Global Telecom Exploitation by Covert Surveillance Actors



April 23, 2026

Report No. 192

By Gary Miller and Swantje Lange

THECITIZENLAB

munkschool OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

Copyright

Suggested Citation

Gary Miller and Swantje Lange. “Bad Connection: Uncovering Global Telecom Exploitation by Covert Surveillance Actors,” Citizen Lab Report No. 192, University of Toronto, April 23, 2026.

Acknowledgements

The Citizen Lab thanks the research teams of P1 Security and Cellusys, in addition to Telenor Linx and Roaming Audit for sharing metadata related to the surveillance campaigns featured in this report. This investigation would not have been possible without their collaboration and contributions. We also thank Phillipe Langlois and Silke Holtmanns (Blue Hour Consulting Oy) for their expert reviews and technical input.

We are grateful to our Citizen Lab colleagues John Scott-Railton and Kate Robertson for peer reviews and guidance, Siena Anstis for legal support, Adam Senft for editing and organizational support, Alyson Bruce for graphics, media and communications, Claire Posno for editorial support, and Anna Mackay for developing supplemental FAQ material.

Research for this project was supervised by Professor Ronald J. Deibert.

We would also like to thank Nick Jones and Omnitouch for mobile protocol expertise, Stephen Ornadel for his support of this project, and Crofton Black for his continued investigations into operators and organizations exploiting the mobile telecommunications ecosystem.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is a world-renowned research unit led by Professor Ronald J. Deibert at the University of Toronto's Munk School of Global Affairs & Public Policy. We investigate novel threats to democracy, human rights, and global security in the digital ecosystem. Over the past 25 years, the Citizen Lab's evidence-based research has played a critical role in demonstrating how digital technologies are used to undermine human rights. The Citizen Lab has published more than 180 evidence-based, peer-reviewed research reports, available online.

Contents

Excerpt

Our investigation uncovers two sophisticated telecom surveillance campaigns, and for the first time, links real-world attack traffic to mobile operator signalling infrastructure. The findings expose how suspected commercial surveillance vendors (CSVs) exploit the global telecom interconnect ecosystem, leverage private operator networks, and conduct covert location tracking operations that can persist undetected for years.

Key Findings

- **Multi-Vector Surveillance**: We identified actors using multiple techniques to track targets by combining 3G and 4G signalling network protocols with direct device exploitation via SMS.
- **SIM Card Exploitation**: One campaign sent a malicious SMS containing hidden SIM card commands to extract location information, attempting to turn the device into a covert tracking beacon.
- **Sophisticated and Customized Tooling**: Both actors used customized surveillance tooling to spoof operator identities, manipulate signalling protocols, and steer traffic through specific interconnect network paths to evade defenses and mask attribution.
- **Global Network Infrastructure**: The attacks leveraged identifiers and infrastructure associated with operators worldwide, including networks based in the UK, Israel, China, Thailand, Sweden, Italy, Liechtenstein, Cambodia, Mozambique, Uganda, Rwanda, Poland, Switzerland, Morocco, Namibia, Lesotho, and the self-governing Island of Jersey, demonstrating extensive global reach.
- **Persistent Campaign Activity**: Telemetry shared by mobile signalling security provider Cellusys reveals that operator signalling identifiers were reused over multiple years, forming consistent clusters that enabled long-running surveillance operations.
- **Weak Intercarrier Provider OPSEC**: Weak screening of interconnect traffic allowed attackers to route surveillance messages through trusted operator pathways, enabling access to targeted networks.

Introduction

In recent years, several investigations have exposed vulnerabilities in the mobile telecommunications ecosystem and how government security agencies have exploited them to track targets abroad while roaming. These studies include several Citizen Lab reports, along with work from other researchers. Our work builds on those findings, prompting further research into the structural weaknesses that continue to enable and evolve targeted surveillance.

In late 2024, the Citizen Lab launched an investigation into coordinated location-tracking activity following the identification of a series of unusual events in mobile signalling firewall logs and further

intelligence provided by Cellusys. What initially appeared to be an isolated incident targeting a single mobile subscriber led to a broader investigation that uncovered campaigns by two distinct CSVs conducting long-term espionage operations by exploiting the global telecommunications ecosystem.

The first campaign, observed in November 2024, involved a multi-stage effort to track a high-profile mobile subscriber using multiple 3G and 4G networks. Information provided by the targeted user's network operator indicated that the mobile number belonged to a well-known company executive, further described as a "VVIP." This context indicated that the user was a high-value surveillance target.

In early 2025, we identified an additional coordinated-tracking event, with the use of a specially formatted SMS message. While technically distinct, both campaigns demonstrated advanced, highly structured, and repeated methods consistent with purpose-built surveillance platforms.

Our collaboration with mobile industry partners enabled a broad investigation using metadata from signalling logs, packet captures, routing data, and other telecommunications sources to trace the methods and origins of advanced surveillance activity. This analysis identified 4G infrastructure associated with operator networks based in Israel, the United Kingdom, and the Channel Islands. Notably, in prior public reporting these same countries have been linked to CSVs targeting mobile users.

Our findings highlight a systemic issue at the core of global telecommunications: operator infrastructure designed to enable seamless international connectivity is being leveraged to support covert surveillance operations that are difficult to monitor, attribute, and regulate. Despite repeated public reporting, this activity continues unabated and without consequence. The continued use of mobile networks, built on a close inter-operator trust model and relied upon by users worldwide, raises broader questions for national regulators, policymakers, and the telecom industry about accountability, oversight, and global security.

Methods

This report is based on analysis in collaboration with multiple industry firms including the signalling firewall provider Cellusys, international signalling provider Telenor Linx, telecom data intelligence provider Roaming Audit, and telecom network security firm P1 Security.

We validated our research by correlating signalling data with additional independent data sources, enabling analysis of how messages were submitted, routed, and delivered across the global interconnect ecosystem. These sources included:

- Mobile network configurations from mobile operator GSMA (GSM Association) industry filings
- Telecom signalling Domain Name System (DNS) records
- Border Gateway Protocol (BGP) routing data and Autonomous System Number (ASN) registrations

- Publicly available records from national telecommunication regulators

We applied a multi-stage analytical process to attribute observed surveillance activity to distinct threat actors by identifying, clustering, and correlating suspicious signalling indicators across campaigns.

Analytical Approach

1. **Detection of Suspicious Signalling Activity**
   We identified commands in international signalling traffic that match known surveillance techniques across 3G SS7 and 4G Diameter signalling protocols. While some of these commands have legitimate uses, their repeated and patterned use is commonly associated with surveillance activity.

2. **Surveillance Campaign Pattern Identification**
   We analyzed traffic for repeated commands within short time intervals from individual operator signalling addresses, then identified coordinated activity across multiple operators matching that behaviour within the same timeframe. These temporal and behavioural patterns were used to identify distinct surveillance campaigns.

3. **Target Validation**
   Cellusys validated that each campaign targeted specific subscriber phone identifiers (IMSIs), confirming consistent targeting patterns across multiple operator signalling identifiers and correlating the timing and sequence of location tracking attempts.

4. **Actor Fingerprinting and Clustering**
   We identified distinct surveillance actors through technical fingerprinting of signalling characteristics. We looked for sequential or patterned transaction identifiers, non-standard message formats, parameter configurations, reuse of signalling identifiers, and consistent routing behaviour.

5. **Infrastructure Mapping and Routing Analysis**
   We correlated signalling identifiers with external data sources, including operator IR.21 filings, ASN and IP address allocations, BGP routing data, and DNS records to map how attack traffic entered and traversed the signalling interconnect ecosystem.

6. **Historical Correlation**
   Our final step was to correlate observed attack indicators with historical telemetry to measure the duration of campaign activity and repeated use of the same operator signalling infrastructure over multiple years.

Limitations and Attribution

It is important to note that the operator signalling addresses observed in the attacks do not necessarily imply direct operator involvement. In some cases, access to the signalling ecosystem can be obtained through third-party providers, commercial leasing arrangements, or other intermediary services that allow actors to send messages using signalling identifiers from legitimate networks.

This analysis examines how signalling infrastructure was leveraged in the attack campaigns, rather than the intent of the identified operators or network providers. While we do not directly attribute the attacks in this report to a specific government or organization, several indicators point towards the likely involvement of a commercial surveillance platform supporting state-sponsored intelligence activities.

Background: Continued Broken Trust in Mobile Communications

To understand how the attacks detailed in this report were possible, it is necessary to examine how mobile networks communicate with one another, and the operational landscape that enables them. The system connecting mobile operators around the world for international travel and mobile services uses protocols consisting of a blend of SS7, known for older 3G networks, and Diameter for 4G and most 5G networks. While SS7 has long been considered a legacy protocol, it still maintains a critical role for international roaming, SMS, and emergency services. Together, this blended signalling ecosystem of vulnerable protocols creates additional opportunities for surveillance actors.

These vulnerabilities are not the result of software bugs or network misconfigurations; rather, they are inherent to global telecommunications design and business practices. The mobile ecosystem comprises over a thousand operators interconnected through roaming agreements and signalling protocols that prioritize efficiency, service availability, and revenue opportunity over security. As a result, a shadowy marketplace of state-backed and commercial espionage actors has emerged, developing and deploying software platforms that weaponize telecommunication networks for global surveillance.

Insecure by Design

The root of the security problem lies in the foundational signalling protocols themselves. Designed for a trusted community of mobile operators and legitimate third-party service providers, SS7 protocols lack the basic security mechanisms of IP networks, such as authentication and validation to verify the source of signalling messages, integrity checks to ensure that data has not been altered, and encryption to protect its contents.

The Diameter protocol, currently used in 4G and most 5G international roaming implementations, was designed with stronger security controls than SS7, introducing security components to address inherent signalling vulnerabilities. These include support for Transport Layer Security (TLS) and IPsec encryption

to protect signalling traffic, as well as authentication between operator networks.[1] However, in practice, operators have largely failed to implement these protections and instead continue to rely on the same peer-to-peer trust model that plagues SS7. In addition, key operational security measures, such as verifying that security configurations align with roaming partner network information published in GSMA IR.21 documents, are often seldom enforced. As a result, security research has shown that 4G networks remain vulnerable to many of the same user-targeted surveillance techniques associated with 3G.

What is IR.21?

IR.21 is a document specification shared among mobile operators through the GSMA (GSM Association). It contains technical and operational details about an operator's network, such as network codes, signalling address ranges and network assignments, interconnect details, and other information for managing international roaming services. Attackers with knowledge of IR.21 data can exploit it to identify network elements or create signalling messages that appear legitimate within the global telecommunication ecosystem.

Actors who gain access to the global signalling ecosystem, whether through commercial arrangements with mobile operators, compromised telecom nodes, or control of telecom networks, can send signalling commands to networks around the world. Because these protocols do not authenticate the true source of commands, malicious signalling traffic can be made to appear as if it originates from legitimate operator network nodes, enabling location tracking, denial-of-service attacks, or traffic redirection to attacker-controlled infrastructure.

In practice, access to the signalling backbone is not limited to mobile network operators. A wide range of providers maintain connections to intercarrier networks to deliver services such as HLR lookup, domestic and international messaging, roaming hubs, and mobile virtual network enabler (MVNE) services. These third-party platforms that connect directly to intercarrier providers routinely generate SS7 and Diameter signalling queries on behalf of their commercial customers. Actors that purchase services from these third-party providers and connect to their platform are able to acquire an indirect channel into the private signalling ecosystem.

Additional security risks arise from the interoperability between modern 4G/5G networks and older 3G systems. Operators that have deployed both networks support a procedure known as *combined attach*,[2] which allows a roaming device to register with both 3G and 4G networks simultaneously for service continuity and fallback.

[1] GSMA Document FS.19 Diameter Interconnect Security, Annex D Diameter IPX Network End-to-End Security Solution

[2] GSMA EPS Roaming Guidelines IR.88 [4], 3GPP TS 23.272 [7], and 3GPP TS 24.301 [14]

Attackers with access to both 3G and 4G signalling environments can exploit this dual registration feature to seamlessly pivot attacks between Diameter and SS7 protocols. By switching between the two signalling systems, as shown in **Figure 1**, they gain advantages when operators lack firewall protections from these more advanced cross-protocol attacks. In this way, the insecurity of legacy SS7 protocols is compounded for advanced actors capable of employing both attack vectors.

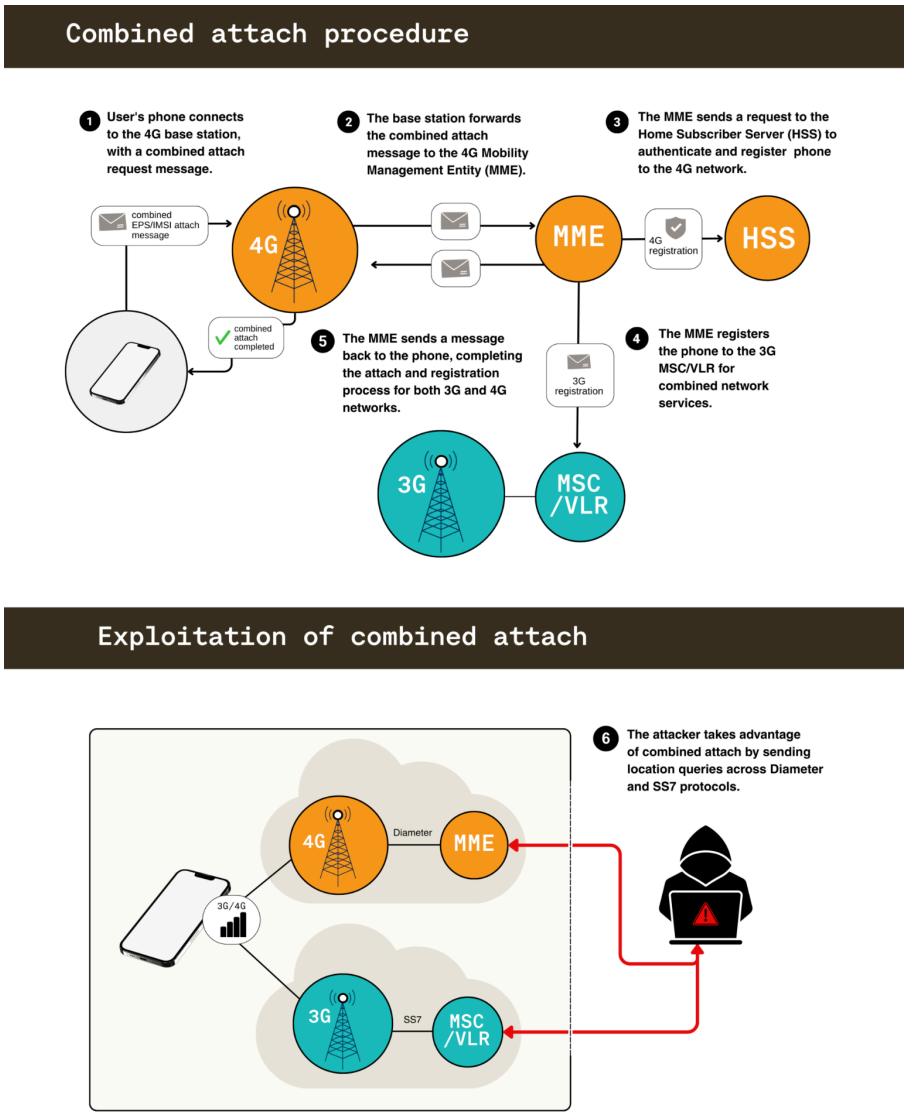


Figure 1: Combined Attach Surveillance Vulnerability

Telecom Surveillance Actors: A Crowded and Shadowy Marketplace

For over a decade, researchers have documented how threat actors exploit network vulnerabilities in SS7 and Diameter signalling. However, conducting attacks at scale requires the complex integration of multiple signalling protocols into a command-and-control (C2) system capable of operating across global telecom networks. This technical and operational complexity requires deep engineering expertise, specialized tooling, and privileged access to private mobile network infrastructure.

These requirements are only within the reach of a relatively small number of well-resourced actors. The telecom surveillance ecosystem is composed of two overlapping groups: state-linked espionage services that conduct signals intelligence operations through telecom networks, and CSVs that develop and sell interception and tracking services to government clients, as shown in **Table 1**. The diversity and persistence of observed telecom attacks suggests that both groups play an active role in exploiting vulnerabilities.

	Affiliation	**Reported Telecom Surveillance Activity**
State-Sponsored Espionage Actor		
Salt Typhoon	China Ministry of State Security (MSS)	Linked to cyber-espionage campaigns targeting telecom infrastructure and government officials across multiple countries.
Liminal Panda (LightBasin)	China-Nexus Espionage Actor	Known for compromising telecom operator networks to collect subscriber information, call metadata, and SMS messages using customized signalling tools.
MuddyWater	Iran Ministry of Intelligence and Security (MOIS)	Conducted cyber operations targeting telecom providers in Africa and the Middle East.
Commercial Surveillance Vendors		
Circles, Cognyte, Rayzone, Defentek	Various	Detailed in a February 2024 letter from US Senator Ron Wyden to then President Joe Biden calling for sanctions linked to multiple telecom surveillance vendors capable of location tracking and interception.

RCS Lab / Tykelab (Cy4gate)	Italy	Providers of hybrid surveillance platforms combining device spyware with telecom signalling surveillance capabilities.
Fink Telecom Services (FTS)	Switzerland	Telecom signalling and SMS routing company reported to have leased SS7 Global Titles with platform capabilities enabling location tracking and interception.
Rayzone Group	Israel	Investigative reporting linked the company to leasing telecom signalling access from operators in Jersey, Guernsey, and other networks worldwide.

Table 1: Examples of state-sponsored and commercial telecom surveillance actors

While most commercial threat groups focus on device implants, there is strong demand by government agencies for "off-the-shelf" telecom surveillance services that use mobile networks to locate and track users, and intercept communications without hacking a target's phone. These services are often brokered through intermediaries with direct or brokered access to mobile operator or provider networks, allowing surveillance traffic to blend into legitimate roaming operations.

The Hidden Layer of Global Surveillance

Unlike conventional cyber campaigns, telecom-level surveillance is almost entirely invisible to the broader security community. Attacks occur within a closed ecosystem of mobile operators, telecom equipment vendors, and mobile interconnect providers that are largely inaccessible to the security research community. This lack of transparency means that attacks rarely surface publicly, and the techniques and infrastructure used for telecom espionage in the wild often remain hidden. This makes the restricted ecosystem ideal for surveillance operations. Signalling messages traverse private international roaming networks and even when signalling firewalls are deployed, enforcement is often inadequate, creating a blind spot that surveillance actors have exploited to operate undetected for years.

This hidden signalling layer also allows attackers to masquerade as trusted operators by using legitimate signalling identifiers and interconnect providers. When operators provide third-party access to their infrastructure through commercial leasing arrangements, surveillance operations assume the identity of the operator, masking attacker attribution.

These practices that provide third-party access to operator infrastructure without oversight or safeguards empower surveillance actors, bringing real-world harm to civil society. Previous research

from the Citizen Lab has reported on the incentives and drivers of location tracking surveillance enabled by the telecommunication ecosystem. This now-mature and unregulated market has become an enabler of espionage where direct attribution to state and non-state actors is difficult.

Network Ghosts: Tracing Sources of Mobile Network Attacks

Historically, operators initially deployed SS7 firewalls designed to block unauthorized signalling messages from foreign networks in response to public reporting of SS7 location tracking attacks and security guidance issued by the GSMA. Over time, operators deployed Diameter firewalls to address 4G network threats. However, industry surveys have reported slow operator deployments, with limited protections against more advanced attacks that combine techniques using 3G and 4G networks simultaneously.

The campaigns we analyzed in this report illustrate how surveillance actors exploit these gaps by using legitimate operator signalling identifiers to send location queries through the global interconnection system. In some cases the identifiers appear to have been obtained through commercial arrangements or intermediary service providers; in others, they appear to have been spoofed to masquerade as legitimate operator infrastructure. Because the mobile roaming ecosystem relies on trusted connections between operators, attacks are designed to appear as originating from legitimate networks. These techniques allow surveillance actors to function as what we refer to as “Ghost Operators.” While remaining invisible through operator identities and access into the private signalling backbone, they appear as legitimate source operators.

As detailed in the following sections, the actors used multiple techniques to maintain access and evade detection. This included shifting between SS7 and Diameter protocols, rotating signalling identifiers associated with different operator networks, and manipulating routing paths to steer messages through specific intercarrier providers. By doing so, they are able to persist by blending their attacks into background roaming traffic.

Operationalizing these techniques requires access to routable signalling identifiers allocated to operators by national telecom regulators and published in IR.21 documents to support global roaming. In practice, such access can be obtained through commercial arrangements and intermediary service providers, as detailed in the following sections.

Because these attacks rely on legitimate operator identities, tracing their origin requires visibility into how signalling identifiers are used and how messages traverse the ecosystem. By analyzing firewall telemetry, routing traces, and interconnection metadata, we mapped how attack messages entered the signalling backbone and reached targeted networks. This analysis shows how surveillance actors operationalize access to mobile network infrastructure, while hiding their point of origin.

Signalling and Routing Indicators: Why the Path Matters

How signalling traffic moves between operators is key to understanding how attackers exploit the mobile signalling ecosystem. Normally, operators send signalling traffic through a global network of providers that exchange messages between operator networks that support roaming services. In SS7 networks, signalling messages are routed using Global Title (GT) addresses assigned to operators by national telecommunications regulators. When a message is sent, it contains the source (Calling Party) GT. That message is forwarded through intermediary routing nodes known as Signalling Transfer Points (STPs) operated by interconnect providers. Each STP is identified by a unique node identifier called a Point Code (PC). As messages are relayed through the signalling backbone, the STP passing the message to the next hop is identified by the Originating Point Code (OPC) field. By observing the OPC of messages at the first transit point into the SS7 backbone, we can determine if the network provider sending surveillance messages differs from what the operator reported in their IR.21 roaming document. This is shown in **Figure 2**.

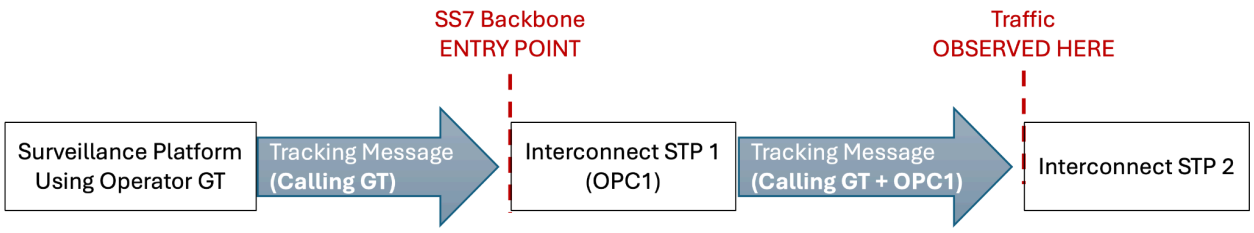


Figure 2: Identifying the SS7 attack point of entry.

In contrast, 4G networks deliver Diameter signalling through IP Exchange (IPX) providers using IP-based hop-by-hop routing with addresses using a hostname + domain format to identify mobile operators. The Diameter `Origin-Host` message attribute identifies the sending node and the target operator network is identified by the `Destination-Realm` attribute. Whereas the OPC identifies SS7 transit points, the *Route-Record* attribute identifies each relay point along the Diameter path so that the submit and response paths remain consistent. An overview of the network identifier formats is shown in **Table 2** below.

Network Identifier	**Format**	**Use in International Mobile Networks**
SS7 Global Title (GT) Address	Country Code (CC)+National Destination Code (NDC)+Subscriber Number (SN)	Routing SS7 signalling messages between operators using the SCCP protocol.

		Note: the Subscriber Number (SN) identifies the network node, not a user's phone number.
Origin-Host	hostname.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org	Identifies the endpoint that sent a Diameter message.
Origin-Realm	epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org	Identifies the sender network of a Diameter message, to route the response back.
Route-Record	hostname.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org	Contains the hostname of the node relaying the message along the routing path.
Destination-Realm	epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org	Identifies the target operator network of the message.

Figure 2: Description of key signalling network identifiers.

To understand how SS7 attack traffic entered the signalling backbone, we compared expected routing paths from the operator IR.21 filings with those seen from the GTs in signalling traffic. Under normal conditions, traffic from an operator is routed through the interconnect providers listed in that operator's IR.21 filings. A key finding from our analysis found repeated mismatches between the expected providers and those observed sending attack traffic, indicating that messages entered the signalling backbone through alternate providers.

By correlating OPC values in traffic with ITU ISPC assignments, we found attack traffic consistently traversing interconnect providers not associated with the originating operator, strongly suggesting actor use of a third-party to send surveillance queries into the signalling network. **Table 3** compares the expected interconnect providers published in operator IR.21 filings with OPCs of providers seen in attack traffic, highlighting routing mismatches that reveal the likely use of a third-party entry point into the SS7 backbone.

Attacking GT	**Mobile Operator**	**Expected Provider (IR.21)**	**Expected OPC**	**Observed Provider in Attack Traffic**	**Observed OPC**	**Routing Mismatch**
855183901014	SEATEL (Cambodia)	Comfone AG	4590/4591	BICS	4201/4215	✕ Mismatch

855180015170	SEATEL (Cambodia)	Comfone AG	4590/4591	Comfone AG	4590/4591	✅ Match
25882200300	Tmcel (Mozambique)	Deutsche Telekom	5091/5092	BICS	4201/4215	✕ Mismatch
85513000755	CADCOMMS (Cambodia)	Comfone	4590/4591	Tata Communications	6233	✕ Mismatch
46764753182	Telenabler AB (Sweden)	Comfone	4590/4591	Tata Communications	6184/6233	✕ Mismatch
393358840745370	TIM (Italy)	Telecom Italia Sparkle	4466	Telecom Italia Sparkle	4466	✅ Match
25671000036	Utel (Uganda)	BICS	4201/4215	BICS	4201/4215	✅ Match
423790105844	FL1 (Liechtenstein)	A1 Telekom Austria	4616	A1 Telekom Austria	4616	✅ Match
250730091970	Airtel (Rwanda)	BICS	4201/4215	BICS	4201/4215	✅ Match
467647531812	Telenabler AB (Sweden)	Comfone AG	4590/4591	Telia Sweden	4745	✕ Mismatch

Table 3: Interconnect provider mismatches seen in attack traffic

To understand how 4G surveillance messages were routed and delivered to their targets, we analyzed the Diameter message headers acquired from the signalling firewall log data. The headers and routing identifiers from those logs enabled us to trace the routing path.

We first looked at the Origin-Host, Origin-Realm, and Route-Record attributes contained in the surveillance message headers. The identifiers in these fields record the hostnames and intermediate routing nodes involved in forwarding the messages. We then used IR.21 documents, BGP routing data, and DNS zone record sources to correlate and attribute the hostnames to specific operator networks and IPX providers.

The evidence from the logs showed both actors spoofing operator hostnames in the Origin-Host fields to evade target operator firewall controls. Additionally, an operator hostname was inserted into the

interconnect routing path shown in the Route-Record attribute, revealing the true operator network source used in the surveillance campaigns. We also noticed an actor using a unique hostname to identify the IPX provider selected to transport a specific attack signalling message. The Origin-Host and corresponding IPX providers routing the attack messages are summarized in **Table 4**.

Origin-Host Operator	**Route-Record 1**	**Proxy Operator**	**Route-Record 2 Hostname**	**IPX Provider Used**
Tango Networks UK	cst001.epc.mnc053.mcc234.3gppnetwork.org	Tango Networks UK	dra01	Tango Networks (hosted by BICS)
019 Mobile Israel	vdrap1.epc.mnc019.mcc425.3gppnetwork.org	019 Mobile	dranl02	Comfone AG
AIS Thailand	vmdra01.epc.mnc019.mcc425.3gppnetwork.org	019 Mobile	ams-01.dra.ipx	Syniverse Technologies
Movitel Mozambique	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org	Jersey Airtel	dranl01	Comfone AG
MTS Namibia	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org	Jersey Airtel	draus01	Comfone AG
Econet Lesotho	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org	Jersey Airtel	draus01	Comfone AG
Inwi Morocco	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org	Jersey Airtel	draus01	Comfone AG
Sunrise Switzerland	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org	Jersey Airtel	draus01	Comfone AG
Polkomtel Poland	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org	Jersey Airtel	draus01	Comfone AG

Table 4: Source 4G/Diameter operator hostnames and route-records.

Fingerprinting Telecom Surveillance Actors

To distinguish the surveillance campaigns identified in this investigation, we analyzed recurring indicators in the signalling traffic and historical attack telemetry. By correlating repeated activity with the headers observed in the attack messages, we were able to identify technical fingerprints associated with each actor's surveillance tooling.

In this report, a "fingerprint" refers to technical details observed across the attacks that indicate a common surveillance platform used and/or operational method. When several of these details appear across multiple events, they reveal a consistent pattern and allow attacks to be clustered with the same actor.

1. **Manipulation of Signalling Identifiers** – Both actors manipulated signalling identifiers embedded in the attack messages to obscure the true origin of the traffic and influence the routing path of message responses. This included modifying hostnames and operator network domains that violate protocol standards and GSMA industry security guidelines.
2. **Ordered SS7 Transaction Identifiers (TIDs)** – Location queries used near-sequential TIDs for surveillance messages across different SS7 networks. Normally, TIDs are generated independently by network elements within each operator network. The presence of sequential identifiers indicates the signalling queries were generated by centralized surveillance C2 platform.
3. **Non-Standard Diameter Session Identifiers** – Session ID values from both actors deviated from 3GPP Diameter standards, using a format of `origin-host;timestamp;local-id`. However, each actor implemented the format differently:
    a. **Actor 1** generated long, randomized, numeric tokens (37–39 digits) resembling 128-bit UUID-style identifiers often seen generated by C2 systems.
    b. **Actor 2** embedded the **target IMSI directly within the Session ID**, allowing the surveillance system to track and correlate message responses associated with specific targeted devices.
4. **Identical Commands Across Networks** – Commands seen in the attack messages used identical parameters across multiple networks. The use of identical SS7 and Diameter parameters shown in **Figures 3** and **4** suggests that the messages were generated by a centralized system sending the same queries.

```
> subscriberIdentity: msisdn (1)
v requestedInfo
    locationInformation
    subscriberState
    currentLocation
    requestedDomain: cs-Domain (0)
    imei
    locationInformationEPS-Supported
```

Figure 3: Identical SS7 message parameters.

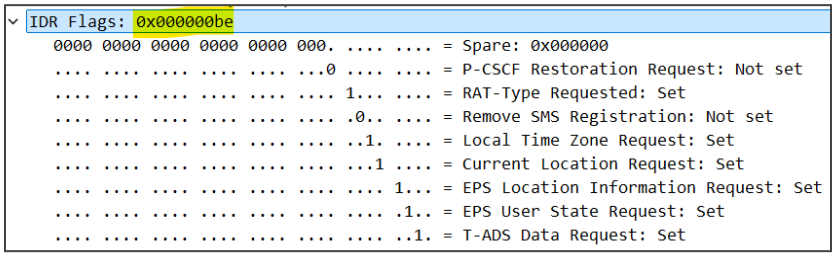


Figure 4: Identical diameter message parameters.

An overview of the commands used by the attacker are summarized in **Table 5** below.

Protocol	Command/Parameter	Explanation
SS7	locationInformation	Requests any available network location data including Cell ID, Location Area Code (LAC), Mobile Country Code (MCC), Mobile Network Code (MNC)
SS7	subscriberState	Requests the device's current network status (e.g., roaming, busy, unreachable, or attached/available)
SS7	currentLocation	Requests the current serving Cell ID associated with the device
SS7	requestedDomain cs-Domain (0)	Indicates that the query targets the circuit-switched service domain used for voice and SMS services
SS7	imei	Requests the International Mobile Equipment Identity (IMEI) of the device

SS7	locationInformationEPS-Supported	Requests whether the network supports providing 4G location information
Diameter	RAT-Type Requested	Requests the radio access technology currently used by the device (e.g., LTE, GSM, or UMTS)
Diameter	Local Time Zone Request	Requests the time zone associated with the device's current location
Diameter	Current Location Request	Requests 4G location data from the network, including Tracking Area Identity (TAI) and E-UTRAN Cell Global Identity (ECGI)
Diameter	T-ADS Data Request	Requests information used to determine whether communications are handled through IMS or circuit-switched networks

Table 5: Summary of identical parameters seen in surveillance messages.

Gateways to Surveillance

The investigations in this report expose three mobile networks that repeatedly appear as the surveillance entry and transit points within the telecommunications ecosystem. These networks function as gateways that allow traffic to move through trusted signalling interconnections while granting access to threat actors that hide behind their infrastructure.

019Mobile (Israel)

019Mobile is a privately owned Israeli-based mobile operator under the brand "Telzar 019." The GSMA website shows they began providing mobile services in 2013, and are the "sole supplier of outbound and inbound roaming services in Israel's International airport."

Our analysis reveals that 019Mobile identifiers repeatedly appear in Diameter surveillance attempts, both as an originating network and as an intermediary node. The Route-Record identifier shows 019Mobile hosts as the first-hop proxy for traffic, positioned as an entry and transit point for 4G location

tracking. We also reveal that 019Mobile is hidden from DNS systems, while BGP routing records confirm reachability through Partner Communications, one of Israel's major telecommunications providers.

Israel has long been a focal point in the global surveillance industry, with multiple companies developing and exporting advanced spyware, cellular communications interception, and monitoring technologies. While we do not attribute observed activity directly to 019Mobile, the network's role configured as a visible signalling intermediary, with Partner Communications as an invisible entry point into the global 4G signalling backbone highlights how operator networks can be leveraged for international surveillance operations.

Airtel Jersey/Sure (Channel Islands)

Airtel Jersey, now part of the Sure Group, operates within the self-governed island territory of Jersey, located within the Channel Islands, a jurisdiction that has repeatedly been the subject of investigative reporting on telecom surveillance and signalling abuse.

The most notable investigation exposing telecom surveillance originating from the Channel Islands was published by The Guardian, in partnership with The Bureau of Investigative Journalism. That story linked telecom infrastructure in the Channel Islands to GT leasing activity and global routing of surveillance traffic, specifically for location tracking operations. The stories specifically identify mobile operators Sure Guernsey and Airtel Jersey as sources of SS7 location tracking queries.

In our investigation, an Airtel Jersey node was seen as the first hop for Diameter signalling surveillance queries, with further surveillance dating back to the 2022 timeframe. Continued use of telecom infrastructure from this jurisdiction suggests a reliable regulatory environment for telecom leasing activity.

Tango Networks UK

Tango Networks UK Ltd is a wholly owned subsidiary of Tango Networks, Inc, a US-based corporation that provides mobile services to enterprise customers. In 2022, Tango Networks UK was assigned Mobile Network Code (MNC) 53 by the UK telecommunications regulator Ofcom, along with the Mobile Country Code (MCC) 234, forming the full MNC 053 MCC 234 following the dissolution of Limitless Mobile UK, which previously operated using those MNC/MCC values.

Our investigation shows a Diameter hostname with the Tango Networks MNC053/MCC 234 signalling identifier used as a second entry point for 4G location tracking queries from the first threat actor detailed in this report. We validated the Tango Networks signalling identifier in the attack as legitimate through IPX DNS records and IR.21-listed network details. We found repeated, multi-year use of Tango Networks Diameter signalling identifiers used in surveillance activity.

Together, these networks illustrate that access is the reality of modern telecom surveillance. Threat actors that strike deals and integrate with legitimate operators to send queries into the global signalling ecosystem can route surveillance traffic at scale.

STA1: A Persistent Location Tracking Campaign

We identify the first threat actor in this investigation as STA1, a persistent and technically sophisticated telecom surveillance group engaged in long-running operations. Our analysis indicates that STA1 possesses a deep understanding of mobile signalling protocols, the international roaming ecosystem, and signalling firewalls. The actor operates across multiple geographic entry points into the private signalling backbone and uses a methodical approach in attempts to bypass network defenses. The observed activity shows the use of a large pool of operator identities and deliberate route manipulation techniques to control and disguise the delivery of surveillance traffic.

The Chronology Of A Multi-Stage Location Tracking Campaign

On November 25, 2024, a sequence of signalling messages sent from multiple foreign operator networks targeted a subscriber of a Middle East mobile operator in an attempt to determine the device location. After being alerted of the attack, the operator confirmed that the targeted IMSI belonged to a “VVIP” subscriber, indicating a high-profile individual and suggesting a targeted surveillance operation. The activity summarized in **Table 6** illustrates tradecraft designed to circumvent signalling firewall controls at the perimeter of the target network.

Phase 1: Reconnaissance (10:39 - 10:41 GMT)

The attack begins with two SS7 `sendRoutingInfoForSM` (SRISM) messages sent from a GT attributed to the SEATEL Cambodia network. These messages attempted to retrieve the device IMSI associated with the targeted user’s phone number. Both attempts were blocked by the signalling firewall.

Phase 2: Initial Location Attempts via SS7 (10:41 - 10:44 GMT)

STA1 immediately shifted to launch multiple SS7 `provideSubscriberInfo` (PSI) messages designed to probe the target network with basic location queries. In just three minutes, PSI requests were sent using geographically distributed GTs from operators in Cambodia (SEATEL, QB Cadcomms), Mozambique (Mcel Mocambique Celular), Sweden (Telenabler AB), Italy (Telecom Italia Mobile), Liechtenstein (FL1 Liechtenstein), and Uganda (Utel Uganda). This rapid cycling through multiple network sources was a clear tactic to find a trusted pathway through the firewall and into the target network, showing STA1’s access to the global SS7 backbone via multiple operator GTs.

Phase 3: Protocol Switching to 4G/Diameter (10:46 - 10:50 GMT)

After the SS7 attempts failed, STA1 pivots to the Diameter protocol, sending six `Insert-Subscriber-Data-Request` (IDR) messages from a Tango Networks (UK) host (`cst001.epc.mnc053.mcc234.3gppnetwork.org`) followed by nineteen more IDRs from 019Mobile (Israel) (`ideabpl1h.epc.mnc019.mcc425.3gppnetwork.org`). This persistent switching of protocol and originating network shows the ability to adapt techniques to circumvent the firewall.

Phase 4: Reversion to SS7 With Escalation (10:56 - 11:20 GMT)

Following 25 failed Diameter attempts, the actor reverts back to the SS7 PSI method, reusing the same GTs used earlier in the attack. After an eight-minute pause they escalated to another SS7 technique, using a command known as `anyTimeInterrogation` (ATI) that is commonly used for mobile location tracking. Twelve ATI messages are sent from the same GT cluster.

Phase 5: Final Act of Diameter Manipulation (13:29 – 14:27 GMT)

After a two hour pause, STA1 returned to Diameter with a new tactic. An IDR message was sent from a new operator hostname associated with AIS Thailand (`ideabpl1h.dea.epc.mnc003.mcc520.3gppnetwork.org`). More suspicious is that the Origin-Realm used a China Unicom network domain (`epc.mnc001.mcc460.3gppnetwork.org`). This spoofing of the host and network domain is intended to transmit the location query through an alternate interconnect provider path.

Summary

Over a four-hour period, STA1 launched a coordinated sequence of location tracking attempts targeting a single user. The actor alternated between SS7 and Diameter protocols, rotating queries through eleven operator identities in nine countries to masquerade as legitimate roaming traffic. The campaign involved manipulation of signalling identifiers and routing paths, including mismatched originating hosts and network domains used to steer traffic through selected interconnect routes.

Time (GMT)	Protocol	Signalling Operation	Source Node	Country	Origin Network/Realm
11/25/24 10:39	SS7	sendRoutingInfoForSM	855183901014	CAMBODIA	SEATEL
11/25/24 10:41	SS7	sendRoutingInfoForSM	855183901014	CAMBODIA	SEATEL
11/25/24 10:41	SS7	provideSubscriberInfo	855180015170	CAMBODIA	SEATEL

11/25/24 10:41	SS7	provideSubscriberInfo	25882200300	MOZAMBIQUE	TMCEL
11/25/24 10:42	SS7	provideSubscriberInfo	85513000755	CAMBODIA	CADCOMMS (QB)
11/25/24 10:42	SS7	provideSubscriberInfo	46764753182	SWEDEN	TELENABLER AB
11/25/24 10:43	SS7	provideSubscriberInfo	393358840745370	ITALY	TIM
11/25/24 10:43	SS7	provideSubscriberInfo	855183901014	CAMBODIA	SEATEL
11/25/24 10:43	SS7	provideSubscriberInfo	423790105844	LIECHTENSTEIN	FL1
11/25/24 10:43	SS7	provideSubscriberInfo	855183901014	CAMBODIA	SEATEL
11/25/24 10:44	SS7	provideSubscriberInfo	25671000036	UGANDA	UTEL
11/25/24 10:46	Diameter	Insert-Subscriber-Data-Request	cst001.epc.mnc053.mcc234.3gppnetwork.org	UNITED KINGDOM	TANGO NETWORKS
11/25/24 10:47	Diameter	Insert-Subscriber-Data-Request	cst001.epc.mnc053.mcc234.3gppnetwork.org	UNITED KINGDOM	TANGO NETWORKS
11/25/24 10:47	Diameter	Insert-Subscriber-Data-Request	cst001.epc.mnc053.mcc234.3gppnetwork.org	UNITED KINGDOM	TANGO NETWORKS
11/25/24 10:47	Diameter	Insert-Subscriber-Data-Request	cst001.epc.mnc053.mcc234.3gppnetwork.org	UNITED KINGDOM	TANGO NETWORKS
11/25/24 10:47	Diameter	Insert-Subscriber-Data-Request	cst001.epc.mnc053.mcc234.3gppnetwork.org	UNITED KINGDOM	TANGO NETWORKS

11/25/24 10:47	Diameter	Insert-Subscriber-Data-Request	cst001.epc.mnc053.mcc234.3gppnetwork.org	UNITED KINGDOM	TANGO NETWORKS
11/25/24 10:48	Diameter	Insert-Subscriber-Data-Request	ideabpl1h.epc.mnc019.mcc425.3gppnetwork.org	ISRAEL	019MOBILE
…	…	…	…	…	…
11/25/24 10:59	SS7	provideSubscriberInfo	25671000036	UGANDA	UTEL
11/25/24 11:17	SS7	anyTimeInterrogation	25882200300	MOZABIQUE	TMCEL
…	…	…	…	…	…
11/25/24 11:20	SS7	anyTimeInterrogation	85513000755	CAMBODIA	CADCOMMS
11/25/24 13:29	Diameter	Insert-Subscriber-Data-Request	ideabpl1h.dea.epc.mnc003.mcc520.3gppnetwork.org	THAILAND/CHINA	AIS/CHINA UNICOM
11/25/24 13:29	Diameter	Insert-Subscriber-Data-Request	ideabpl1h.epc.mnc019.mcc425.3gppnetwork.org	ISRAEL	019MOBILE
11/25/24 13:29	Diameter	Insert-Subscriber-Data-Request	ideabpl1h.epc.mnc019.mcc425.3gppnetwork.org	ISRAEL	019MOBILE
1/25/24 14:27	Diameter	Insert-Subscriber-Data-Request	cst001.epc.mnc053.mcc234.3gppnetwork.org	UNITED KINGDOM	TANGO NETWORKS

Table 6: Attack Sequence for STA1 on November 25, 2024.
Note: This table provides an abridged view of the attack sequence. The full dataset includes 17 additional IDR attempts from 019MOBILE (10:49–10:50 GMT), along with further SS7 PSI and ATI activity from the same Global Title Source Nodes shown above.

Evasion Through Diameter Manipulation

Conducting telecom surveillance at scale requires more than access to the global signalling ecosystem. It also requires stealth to conceal its origin. STA1 achieved this by using multiple SS7 and Diameter entry points while rotating operator signalling identities to make attack traffic appear as legitimate operator signalling.

The concealment was notably visible in the Diameter message headers. The Origin-Host, Origin-Realm, and Route-Record fields identify the sending system and trace the path of a message through the interconnect network. Analysis of these fields revealed three distinct routing patterns, designed to hide the source of queries and improve the likelihood of circumventing the signalling firewall.

1. **Direct Access via Tango Networks UK** - Messages entered through Tango-associated infrastructure and were routed through the BICS IPX network.
2. **Direct Access via 019Mobile Israel** - Surveillance traffic entered through 019Mobile-linked nodes before reaching IPX providers.
3. **Spoofed operator identity path (AIS Thailand/China Unicom)** - Messages combined an AIS Thailand hostname with a China Unicom network realm while routing through 019Mobile to steer traffic through the Syniverse IPX.

Table 7 summarizes the key identifiers shown associated with these routing patterns:

Source Operator ID	Origin-Host	Origin-Realm	First Hop Route-Record	Second Hop/IPX Provider
Tango Networks (UK)	cst001.epc.mnc053.mcc234	epc.mnc053.mcc234.3gppnetwork.org	cst001.epc.mnc053.mcc234	dra01.epc.mnc053.mcc234 (BICS-Hosted)
019Mobile (Israel)	ideabpl1h.epc.mnc019.mcc425	epc.mnc019.mcc425.3gppnetwork.org	vdrap1.epc.mnc019.mcc425	Comfone
AIS (Thailand) + China Unicom	ideabpl1h.dea.epc.mnc003.mcc520	epc.mnc001.mcc460.3gppnetwork.org	mdra01.epc.mnc019.mcc425	Syniverse

Table 7: STA1 Diameter location tracking signalling identifiers and routing paths.

As shown earlier in **Table 3**, the interconnect providers seen relaying SS7 traffic from operator GTs did not always match those reported in IR.21 submissions. By distributing surveillance through different

identities and via indirect 3rd party signalling pathways, the actor was able to deliver surveillance queries with reduced detection exposure while improving the potential of breaching the target network. **Figure 5** shows how STA1 sent surveillance messages into the global signalling ecosystem using multiple operator identities and interconnect routing paths.

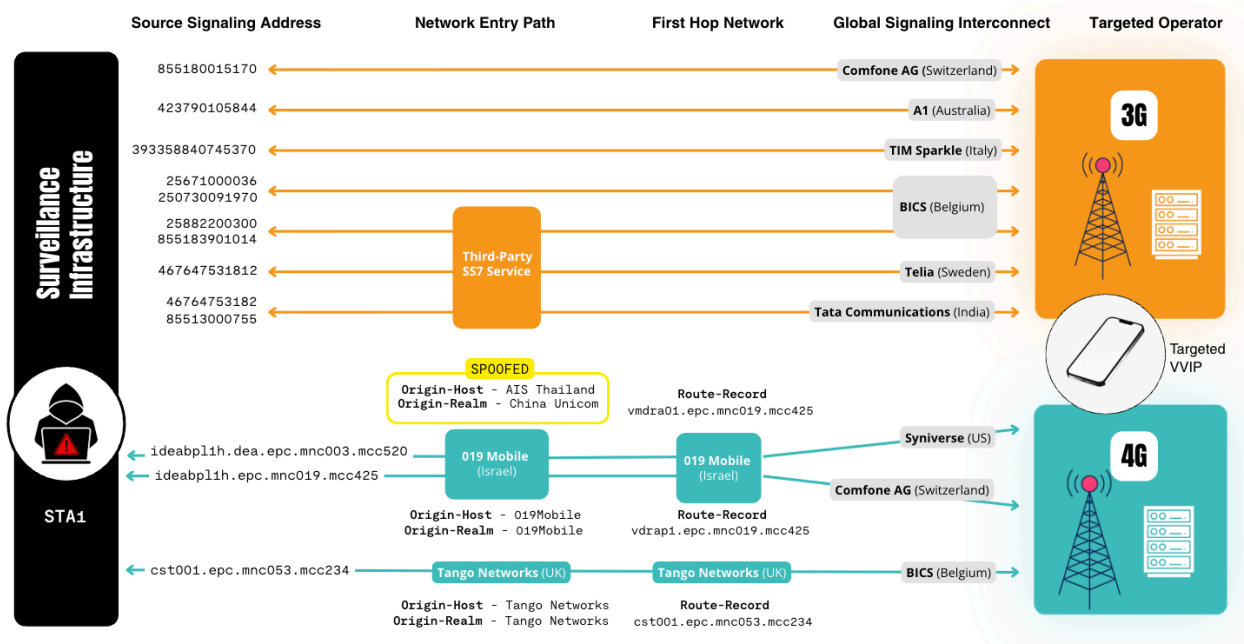


Figure 5: Signalling network paths exploited by STA1.

Figure 5 illustrates the routing paths used in the STA1 campaign across both 3G (SS7) and 4G (Diameter) networks. In the 3G portion (top), multiple operator GTs were used to route surveillance traffic through different network entry points, creating diverse paths through the signalling backbone. In the 4G portion (bottom), the actor leveraged Tango Networks UK to send traffic into the BICS IPX network and 019Mobile hostnames for messages into the Comfone IPX. Finally, AIS Thailand and China Unicom network identities were spoofed to send messages through the Syniverse IPX.

This pattern indicates a centralized surveillance C2 platform with deep integration into the signalling ecosystem, providing multiple routing options to covertly reach target networks around the world.

Tradecraft Used

Route-Record Manipulation (Tango Networks UK)

What is seen: A Tango Networks Origin-Host `cst001.epc.mnc053.mcc234.3gppnetwork.org` is duplicated into Route-Record 1.

Why it is abnormal: Under the IETF Diameter protocol standard RFC 6733, each relay that forwards a request appends its own identity to the Route-Record. The Origin-Host identifies the sending node and would not appear as a relay unless it were forwarding a message through itself.

Impact: This manipulation conceals the first hop in the network path and the routing of message responses, allowing the attacker to hide network paths to and from the targeted network.

AIS Thailand Origin-Host / Origin-Realm Mismatch (China Unicom)

What is seen: A Diameter message using an AIS Thailand Origin-Host `ideabpl1h.dea.epc.mnc003.mcc520.3gppnetwork.org` is paired with a China Unicom network realm `epc.mnc019.mcc425.3gppnetwork.org`, steering traffic through the Syniverse IPX network to route and deliver the message along the interconnection path.

Why it is abnormal: The Diameter protocol Origin-Host attribute identifies the hostname/client sending a signalling message while the Origin-Realm attribute identifies the network belonging to the message. Together, they form the Diameter signalling identity and are crucial for the receiving operator to identify the message owner and must belong to the same network. Cross-operator pairing violates GSMA and 3GPP standards, indicating spoofing and manipulation.

Impact: The mismatch conceals the message point of origin in an attempt to find a trusted path through the firewall and into the target network.

Israeli Network Used to Interconnect Traffic from Thailand/China Networks

What is seen: 019Mobile (Israel) node `vmdra01.epc.mnc019.mcc425.3gppnetwork.org` is a first hop for an attack message originating from AIS Thailand/China Unicom.

Why it is abnormal: According to IR.21 documents, neither AIS nor China Unicom have an IPX agreement with 019Mobile Israel to relay signalling traffic between other foreign operators.

Impact: STA1 is configuring 019Mobile as a routing path to relay 4G surveillance traffic.

Standards Workarounds for Location Queries

What is seen: Because STA1's attempts to obtain the IMSI of the target phone were blocked, they manipulated Diameter and SS7 message parameters as workarounds.

Why it is abnormal: SS7 PSI and Diameter IDR queries are keyed based on a phone IMSI. Using only MSISDN to query the network is non-standard.

Impact: This technique facilitates surveillance by triggering responses from operators with weak firewall controls.

Weak Links in the Global Interconnect Chain

019Mobile (Israel) and Tango Networks (UK) as Proxy Nodes

STA1 used both operators as entry and exit points in the routing path for 4G attacks. The use of different 019Mobile hostnames from separate originating networks, shows deliberate traffic steering:

- 019Mobile-originating identity: `vdrap1.epc.mnc019.mcc425.3gppnetwork.org` (019Mobile Proxy 1)
- AIS/China-linked identity: `vmdra01.epc.mnc019.mcc425.3gppnetwork.org` (019Mobile Proxy 2)

This pattern indicates that STA1 used 019Mobile as a proxy to deliver location queries while concealing the origin of the C2 infrastructure.

IPX Traffic Screening Failure

The Syniverse IPX network allowed a signalling message with an AIS host and a China Unicom network domain to transit their IPX network before being delivered to the target operator:

- As global operator interconnect hubs, IPX providers are expected to screen messages from senders and reject those using mismatched network identifiers.
- In this case, Syniverse was non-compliant and a surveillance message passed unchecked, introducing vulnerability risks to the targeted operator.

Strategic Use of IPX Providers

STA1 used specific IPX routing paths, identified by the hostname seen in the message Route-Record field:

- Populating an operator hostname in the Diameter Route-Record influences the routing path, while obscuring the sender of signalling traffic.
- Influencing the transit path of messages provides more opportunities to reach the target network and penetrate the signalling firewall.

Attribution Assessment

Attributing telecommunications surveillance is inherently challenging. The use of legitimate operator identifiers and signalling access through leasing arrangements or third parties provides operational concealment. As a result, we do not attribute this activity to a specific government or organization. Instead, we evaluated available indicators to assess the most likely operational model and actor type. While the technical patterns are consistent with a CSV leveraging a centralized, cloud-based C2 platform offered to multiple clients, we analyzed operator information and routing metadata through collaboration with mobile industry partners.

1. Use of AIS Thailand Hostname Formats and an IR.21-Listed Node

Surveillance activity associated with 019Mobile consistently used the AIS Thailand hostname format ideabpl1h. In its most sophisticated tracking attempt, STA1 configured an AIS Thailand Diameter Edge Agent (DEA) node (see **Figure 6**), typically used for inter-operator routing and topology hiding, while configuring the Origin-Realm as belonging to China Unicom. This combination indicates detailed knowledge of operator infrastructure, interconnection relationships, and access to GSMA IR.21 data. Such capabilities are consistent with a sophisticated commercial telecom surveillance operation.

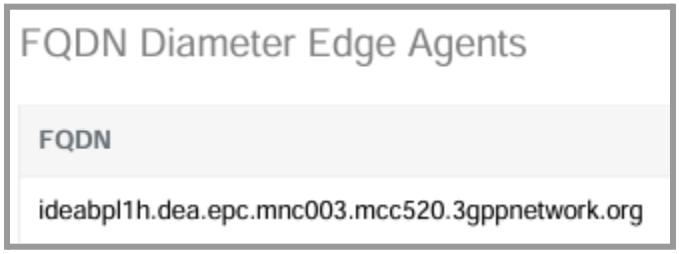


Figure 6: DEA hostname published in the AIS Thailand IR.21 Document.

2. Repeated Campaign Activity

Another surveillance campaign shown in **Figure 7** captured by Cellusys from March 2025 shows multiple location tracking attempts spoofing a China Unicom Origin-Host `dex01.epc.mnc001.mcc460.3gppnetwork.org` with the same 019Mobile Israel Route-Record seen in the November 2024 attack.

Timestamp	Message Types	Source Network	metadata.origin_host	metadata.origin_realm	Diameter-3GPP-S6a-S6d.Insert-Subscriber-Data-Request.Route-Record
2025-03-03 14:48:24	Insert-Subscriber-Data-Request	CHINA UNICOM MOBILE	dex01.epc.mnc001.mcc460.3gppnetwork.org	epc.mnc001.mcc460.3gppnetwork.org	vmdra01.epc.mnc019.mcc425.3gppn [redacted].ipx.syniverse.3gppnetwor [redacted].dra.bics.3gppnetwork.org
2025-03-03 14:48:16	Insert-Subscriber-Data-Request	CHINA UNICOM MOBILE	dex01.epc.mnc001.mcc460.3gppnetwork.org	epc.mnc001.mcc460.3gppnetwork.org	vmdra01.epc.mnc019.mcc425.3gppn [redacted].ipx.syniverse.3gppnetwor [redacted].dra.bics.3gppnetwork.org
2025-03-03 14:48:09	Insert-Subscriber-Data-Request	CHINA UNICOM MOBILE	dex01.epc.mnc001.mcc460.3gpnetwork.org	epc.mnc001.mcc460.3gppnetwork.org	vmdra01.epc.mnc019.mcc425.3gppn [redacted].ipx.syniverse.3gppnetwor [redacted].dra.bics.3gppnetwork.org

Figure 7: Repeated tracking attempts spoofing China Unicom with an 019Mobile network host.

3. Long-Running Campaign Activity

Historical telemetry reveals a long-running activity using the same hostname formats and identifiers from multiple operators dating back to at least November 2022, as shown in **Table 8**. The use of similar hostnames associated with multiple network operators over long durations is consistent with address spoofing designed to hide attack origin. The telemetry reveals these hostnames used in over 500 location tracking attempts.

Date	Origin Host Address	Operator	Origin Host Country	Threat Type	Operation
9-Nov-22	dex01.epc.mnc002.mcc228.3gppnetwork.org	SUNRISE SWITZERLAND	Switzerland	Location Discovery	Insert-Subscriber-Data-Request
9-Nov-22	dex01.epc.mnc001.mcc712.3gppnetwork.org	KOLBI COSTA RICA	Costa Rica	Location Discovery	Insert-Subscriber-Data-Request
9-Nov-22	dex01.epc.mnc001.mcc260.3gppnetwork.org	PLUS POLAND	Poland	Location Discovery	Insert-Subscriber-Data-Request
1-Mar-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
2-Mar-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
22-Mar-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
30-Mar-23	dex01.epc.mnc019.mcc425.3gppnetwork.org	019MOBILE	Israel	Location Discovery	Insert-Subscriber-Data-Request

30-Mar-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
30-Aug-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
18-Sep-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
20-Sep-23	dex01.epc.mnc019.mcc425.3gppnetwork.org	019MOBILE	Israel	Location Discovery	Insert-Subscriber-Data-Request
20-Sep-23	dex01.epc.mnc001.mcc460.3gppnetwork.org	CHINA UNICOM	China	Location Discovery	Insert-Subscriber-Data-Request
26-Sep-23	dex01.epc.mnc019.mcc425.3gppnetwork.org	019MOBILE	Israel	Location Discovery	Insert-Subscriber-Data-Request
26-Sep-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
26-Sep-23	dex01.epc.mnc019.mcc425.3gppnetwork.org	019MOBILE	Israel	Communications Intercept	Authentication-Information-Request
26-Sep-23	st001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Communications Intercept	Authentication-Information-Request
27-Sep-23	dex01.epc.mnc019.mcc425.3gppnetwork.org	019MOBILE	Israel	Location Discovery	Insert-Subscriber-Data-Request
27-Sep-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
10-Dec-23	st001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
10-Dec-23	dex01.epc.mnc019.mcc425.3gppnetwork.org	019MOBILE	Israel	Location Discovery	Insert-Subscriber-Data-Request
11-Dec-23	dex01.epc.mnc001.mcc460.3gppnetwork.org	CHINA UNICOM MOBILE	China	Location Discovery	Insert-Subscriber-Data-Request

14-Dec-23	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
8-Jan-24	cst001.epc.mnc053.mcc234.3gppnetwork.org	TANGO NETWORKS UK	United Kingdom	Location Discovery	Insert-Subscriber-Data-Request
8-Jan-24	dex01.epc.mnc006.mcc454.3gppnetwork.org	SMARTONE	Hong Kong, SAR	Location Discovery	Insert-Subscriber-Data-Request

Table 8: History of STA1 Attacks
Note: The table shows a limited sample of historical attacks from over 500 threat events recorded as attributed to STA1 since November 2022.

4. Global Targeting Patterns

Beyond the initial targeting of a high-profile user in the Middle East, we identified surveillance activity across a wide geographic range. Targets included individual mobile subscribers associated with operators in Thailand, South Africa, Norway, Bangladesh, Denmark, Sweden, Malaysia, Montenegro, and multiple countries across Sub-Saharan Africa. The single user targeting across multiple operator networks and country jurisdictions persisting for years is characteristic of a commercial surveillance platform deployed across multiple operators and likely used by multiple global clients.

5. DNS Validation of Operator-Controlled Signalling Infrastructure

We analyzed IPX DNS records to determine the authoritative operators associated with domains seen in attack traffic. The Tango Networks hostname `cst001.epc.mnc053.mcc234.3gppnetwork.org` resolved successfully via authoritative IPX DNS, confirming it as a valid operator-controlled hostname consistent with Tango Networks IR.21 records. Its repeated use in surveillance activity suggests that STA1 maintained long-term access to Tango Networks infrastructure, likely through a commercial arrangement.

However, analysis of 019Mobile yielded different results. The domain `epc.mnc019.mcc425.3gppnetwork.org` consistently returned NXDOMAIN responses across multiple IPX DNS servers, indicating the domain did not exist, or was deliberately suppressed from the IPX root DNS environment. This suggests a possible technique to hide the discovery of 019Mobile IP addresses attributed to signalling hosts transporting surveillance traffic. To further investigate whether 019Mobile infrastructure was reachable via Diameter signalling, we looked for additional network data.

In the absence of DNS resolution, we examined whether any 019Mobile IP networks were advertised within the IPX. We found two IP address ranges and the corresponding Autonomous System Number (ASN 51825) listed in IR.21 filings from the Israeli-based operator Partner Communications.

```
GRX/IPX Routing for Data Roaming
Connection to Inter-PMN IPv4 Backbone

IP Address(Range)  IPX VLAN          Network Owner

185.24.204.0/29    Data-Roaming      MNO
185.24.204.8/29    Data-Roaming      MNO

Autonomous System Numbers (ASN)

ASN          Network Owner
51825        MNO
```

ASN 51825 is the unique network identifier registered to “Telzar 019 International Telecommunications Services LTD,” the parent company of 019Mobile as shown in **Figure 8**.

Figure 8: 019Mobile IP network and ASN attribution.

This IR.21 association indicates that Partner Communications acts as an upstream signalling interconnect provider for 019Mobile, but raises a critical question: If the 019Mobile network domain does not exist in the IPX, is the underlying infrastructure still reachable within the signalling ecosystem?

To validate this, we analyzed BGP routing information obtained from within the IPX backbone. The results confirmed that the 019Mobile IP prefixes are actively advertised and reachable via Partner Communications, showing a verifiable routing path into and out of the Diameter signalling ecosystem. The BGP routing path was:

```
AS Path: → 12400 → 51825
```

This shows that signalling traffic destined for 019Mobile (AS51825) is routed through an intermediary network belonging to Partner Communications (AS12400) before reaching its point of origin. The presence of the Partner network in the routing path confirms that 019Mobile infrastructure is reachable through an established interconnect relationship. Additional routing attributes show that the path is valid, externally learned, and selected as the best route in the routing table:

```
Origin: IGP | localpref: 100 | valid, external, best
```

This confirms that, despite the absence of the 019Mobile domain from authoritative IPX DNS records, surveillance traffic entering and exiting through this network can be routed and delivered while remaining hidden from DNS discovery. While we don't believe that 019Mobile conducted the attacks, the evidence indicates that its network and Partner Communications were likely used as a transit path for surveillance traffic.

Our findings described above provide insight into the methods used by STA1 to operate within the global signalling ecosystem while limiting attribution. Across both SS7 and Diameter, routing manipulation, path obfuscation, and signalling identifiers associated with multiple operators were used to deliver surveillance traffic. These approaches used over several years indicate a high degree of persistence, sophistication and coordination. The global distribution of targets and infrastructure suggests a system designed for multiple tenants, consistent with a commercially developed telecom surveillance platform supporting government intelligence activities. While at this time we do not attribute this campaign to a specific actor, the evidence shows a deliberate and well-funded operation with deep integration into the mobile signalling ecosystem.

STA2: The SIM as the Spy

Our second investigation, attributed to what we refer to as Surveillance Threat Actor 2 (STA2), used different mobile surveillance techniques. Instead of manipulating SS7 and Diameter signalling protocols for location tracking, STA2 combined device-level exploitation with network-level attacks.

Through detailed analysis of logs and a packet trace showing the header contents of the SMS message, we identified that STA2 sent a specially formatted binary SMS with embedded commands. This was seen during the attack sequence described in this section.

The message was designed to trigger a silent SIM-based exploit without requiring any user interaction, with commands to turn the phone into a location tracking device. We linked the binary payload to a long running campaign likely affecting thousands of devices, known as SIMjacker. Originally exposed by ENEA in 2019, SIMjacker is a Zero-Click SMS exploit that invokes a hidden SIM card application called the S@T browser. The S@T browser is a SIM toolkit (STK) application that interprets S@T bytecode and provides access to STK commands. STK applications are used by mobile operators for service provisioning, operator phone settings, and other value-added services. In this case, STA2 sent a command instructing the STK to retrieve the device location and send it back in a silent SMS message to the attacker infrastructure.

ENEA stated that SIMjacker "is currently being actively used by a specific private company that works with governments to monitor individuals." While ENEA did not name the company, the Citizen Lab has linked the attack sources to SS7 addresses from mobile operators based in Rwanda, Sweden, and Liechtenstein. This attack is a continuation of the SIMjacker threat, where the user's SIM card becomes the sensor and spy, using SMS messages for C2 communication.

How Can an SMS Control a Phone SIM?

SIM toolkit messages (aka SIM OTA messages) look nothing like normal text messages; your phone never shows them and users have no way to know they were received, as they are used by network operators to configure device network settings. Two fields inside the SMS header make this possible:

TP-PID = 127 - "This message is for the SIM card, not the user."
Attackers use this to instruct the device to do the following:

- Don't display the message
- Don't store it in the inbox
- Deliver it to the SIM card for execution

TP-DCS = 22 (0x16) - "Treat this as binary code and send it straight to the SIM."
This ensures the malicious code embedded in the SMS can be recognized and the instructions run by the SIM.

- The message contains binary commands
- The instructions should be processed by the device SIM
- The device messaging app shouldn't touch the message contents

A Different Modus Operandi

STA2 signatures are very different from STA1. On February 11, 2025, STA2 attempted a location tracking operation using a sequential approach, combining network and device attack vectors. The attack began with basic SS7 reconnaissance and location tracking attempts, escalated to a SIM exploit, and ended with Diameter location tracking queries. The messages in our analysis, detailed in the following attack sequence, were captured from firewall telemetry, flagged, and blocked by the signalling firewall listed in **Table 9**.

Phase 1 – Testing the SS7 Waters (15:41 GMT)

The attack began with a single SS7 PSI message from GT `467647531812`. This was likely used to probe the target network to see if it would process a basic location tracking request and confirm if the target phone was connected to the network.

Phase 2 – Weaponizing SMS (15:45 GMT)

Minutes later, the same GT sent an SS7 Mobile-Terminated Forward Short Message (`mt-ForwardSM`) carrying a binary payload. This message delivered the SIM exploit.

Phase 3 – Cross-Protocol Camouflage (15:46 – 15:50 GMT)

After the SIM exploit was blocked, the actor pivoted to Diameter and launched a series of `Authentication-Information-Request` (AIR) probing messages, followed by IDR location queries.

- **Network Probing Using Fake Registration**: The actor sent 10 AIR messages populated with the IMSI of the target phone using 5 different operator network identifiers. The messages are configured with an invalid Visited-PLMN Id = 0000. The AIR message is normally used to establish a new phone connection and report the roaming Mobile Country Code (MCC) and Network Code (MNC) values in the Visited-PLMN ID. In this case, the actor was not trying to connect but used a malformed PLMN value to probe the security of the targeted network and influence a successful response for follow-on location tracking attempts.
- **Follow-on Location Tracking**: The actor then sent a series of IDR location queries using network identifiers from 3 different countries, with each Diameter IDR message flag set to retrieve the current network state and cell id location of the target phone.
- **Hostname and Routing Path Manipulation**: The actor used a single, fixed host populated in the Route-Record to direct the path of surveillance traffic to the operator exit path, using two different hostname formats to identify the type of commands used in the attack.
- **Spoofed Networks**: Diameter messages used network identifiers originating from Poland (Plus), Switzerland (Sunrise), Morocco (INWI), Lesotho (Econet), Namibia (MTC), and Mozambique (Movitel), indicating the actor's misuse of international signalling identities from multiple operators.

Timestamp	Protocol	Signalling Operation	Source Node	Source Network	Source Country	Threat Type
2/11/25 15:41:33	SS7	begin, provideSubscriberInfo	467647531812	TELE2	Sweden	Location Tracking
2/11/25 15:45:29	SS7	begin, mt-ForwardSM	467647531812	TELE2	Sweden	Binary SMS
2/11/25 15:55:01	Diameter	Authentication-Information-Request	hss1.epc.mnc001.mcc260.3gppnetwork.org	PLUS	Poland	Malformed Message
2/11/25 15:55:06	Diameter	Authentication-Information-Request	hss1.epc.mnc001.mcc260.3gppnetwork.org	PLUS	Poland	Malformed Message
2/11/25 15:55:28	Diameter	Authentication-Information-Request	hss1.epc.mnc002.mcc228.3gppnetwork.org	SUNRISE	Switzerland	Malformed Message
2/11/25 15:55:33	Diameter	Authentication-Information-Request	hss1.epc.mnc002.mcc228.3gppnetwork.org	SUNRISE	Switzerland	Malformed Message
2/11/25 15:55:50	Diameter	Authentication-Information-Request	hss1.epc.mnc002.mcc604.3gppnetwork.org	INWI	Morocco	Malformed Message
2/11/25 15:55:50	Diameter	Authentication-Information-Request	hss1.epc.mnc002.mcc604.3gppnetwork.org	INWI	Morocco	Malformed Message
2/11/25 16:05:24	Diameter	Authentication-Information-Request	hss1.epc.mnc002.mcc651.3gppnetwork.org	ECONET	Lesotho	Malformed Message

2/11/25 16:05:28	Diameter	Authentication-Information-Request	hss1.epc.mnc002.mcc651.3gppnetwork.org	ECONET	Lesotho	Malformed Message
2/11/25 16:05:36	Diameter	Authentication-Information-Request	hss1.epc.mnc001.mcc649.3gppnetwork.org	MTC	Namibia	Malformed Message
2/11/25 16:05:41	Diameter	Authentication-Information-Request	hss1.epc.mnc001.mcc649.3gppnetwork.org	MTC	Namibia	Malformed Message
2/11/25 16:06:37	Diameter	Insert-Subscriber-Data-Request	hss.epc.mnc002.mcc651.3gppnetwork.org	ECONET	Lesotho	Location Discovery
2/11/25 16:06:43	Diameter	Insert-Subscriber-Data-Request	hss.epc.mnc002.mcc651.3gppnetwork.org	ECONET	Lesotho	Location Discovery
...	...	...	...	...	...	Location Discovery
2/11/25 16:07:31	Diameter	Insert-Subscriber-Data-Request	hss.epc.mnc001.mcc649.3gppnetwork.org	MTC	Namibia	Location Discovery
2/11/25 16:07:36	Diameter	Insert-Subscriber-Data-Request	hss.epc.mnc001.mcc649.3gppnetwork.org	MTC	Namibia	Location Discovery
...	...	...	...	...	...	...
2/11/25 16:12:32	Diameter	Insert-Subscriber-Data-Request	hss.epc.mnc003.mcc643.3gppnetwork.org	MOVITEL	Mozambique	Location Discovery
2/11/25 16:12:37	Diameter	Insert-Subscriber-Data-Request	hss.epc.mnc003.mcc643.3gppnetwork.org	MOVITEL	Mozambique	Location Discovery

Table 9: Attack Sequence for STA2 (February 11, 2025).
Note: *Table is abridged for brevity. Ten additional IDR attempts ECONET, MTC, and MOVITEL, are detailed in the full log data.*

Technical Fingerprints

Several recurring indicators were used by STA2 that helped cluster related activity over time.

1. **IMSI Embedded in the Diameter Message Session-ID field**
   The IMSI of the target device was hardcoded into the *Session-ID* field. This signature links attack messages directly to the target, suggesting customized tooling with poor OPSEC. We observed this signature used in this attack and in future attacks extending from 2025 into the early 2026 timeframe.
2. **Hostname Conventions Used to Label the Diameter Message Command Code Field**
   Hostname formats identified the type of signalling message sent. This naming convention suggests the hostnames were used as internal labels to distinguish surveillance queries.
   - hss1 hostnames were used for AIR probing messages
   - hss hostnames were used for IDR location query messages
3. **Fixed Entry Path Through the Jersey-Airtel network**
   All attacks used the same Route-Record host: `dra1.je211.epc.mnc003.mcc234.3gppnetwork.org`. The repeated use of this same host indicates that STA2 used a single operator network to send surveillance traffic into the IPX backbone.

Deconstructing the Binary SMS: Inside a SIMjacker Over-the-Air Exploit

Historically, malicious actors have used hidden commands within special types of SMS messages. Our deconstruction of the binary SMS sent by STA2 provided unique insights into the surveillance operation. A packet capture and logs from the signalling firewall showed the SMS headers, confirming the message timestamps. A breakdown of how the attack was deployed and the information elements defined within the structure of the SMS is shown in **Figure 9**.

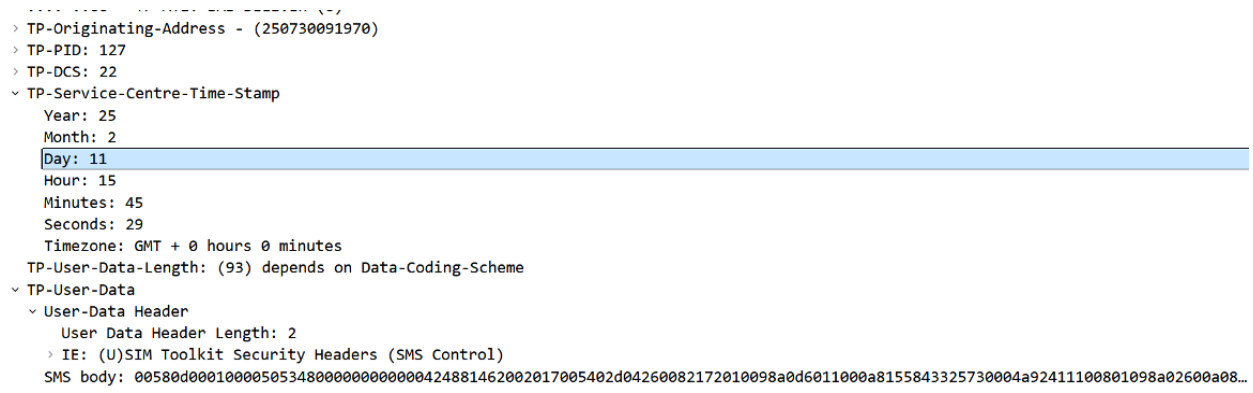


Figure 9: PCAP file of the attack SMS, containing the payload including S@T browser STK commands.

- **TP-Originating Address (TP-OA)**: `250730091970` identifies the SMS sender phone number configured by the attacker as belonging to Airtel Rwanda.
- **TP-Protocol Identifier (TP-PID)**: `127` identifies the message for use by a SIM card application.
- **TP-Data Coding Scheme (TP-DCS)**: `22` identifies the message as binary, so the message is not processed like a regular text SMS.
    - The TP-PID and TP-DCS indicate a SIM toolkit message containing instructions for the SIM card. This type of SMS is invisible to the user and automatically parsed by the SIM, without any user interaction.
- **TP-User-Data**: This field includes the body of the SMS.

SIMjacker attacks exploit a hidden application on the SIM card known as the S@T browser, which is part of the SIM toolkit (STK). This exploit enables the attacker to hijack the SIM card invisibly without user interaction. To perform the attack, STA2 sent an SMS with bytecode containing specialized commands for the S@T browser (see **Figure 10**). The S@T browser interprets and executes the commands immediately, as the communication lacks authentication. Consequently, there is no need for the attacker to send additional messages to authenticate themselves before the S@T browser is ready to receive the commands. We found that the binary SMS blocked by the firewall clearly matches the structure of S@T browser commands. It uses a standardized Tag-Length-[Attribute]-Value (TL[A]V) format to encode the commands and their parameters following the S@T Bytecode specification. The correctly structured bytecode used by the attacker confirms that it was used as a SIM-level exploit rather than ordinary SMS traffic.

What is the TL[A]V format?

Data structures in the Tag-Length-[Attribute]-Value (TL[A]V) format consist of four fields: Tag, Length, Attributes, and Value, whereby the Attributes field is optional.

S@T browser commands use the TL[A]V format, so:

- Every command is identified by a unique one-byte Tag.
- The Tag indicates if the Attribute field is present.
- The Length field specifies how many of the subsequent bytes are part of the command. This includes the Attributes and the Value field.
- The Attributes determine command-specific parameters.
- The Value field contains the data the command is operating on.

For example, the Init Variable command consists of the Tag 0x20 followed by the Length and Value fields. The latter contains the ID and content of the initialized variable.

The payload of the exploit SMS contains a command header with a noticeable byte sequence `0x505348`. This byte sequence represents the Toolkit Application Reference (TAR) indicating a low priority push message, in reference to step (1) in **Figure 10**. The low priority push is designed for messages of low importance without the need for a reply or delivery confirmation. In this way, the messages leave no traces on the SIM card, as they are dropped if the S@T browser is busy when they arrive. The reception and processing of the messages is silent, so nothing is displayed to the user and users are unable to notice them.

Low-priority push messages present an ideal attack surface because they bypass establishment of a session. This allows an attack message to be accepted immediately. No further messages are required beforehand to bring the target application into a reception state.

The Security Parameter Indicator (SPI) in the header is `0x0001` (step (1) in **Figure 10**), indicating that no redundancy check, cryptographic checksum, or digital signature is used in the message, and that a proof of reception is to be sent to the sender.

A Malicious Deck of Cards

A command packet for the S@T browser is organized into structures known as "decks," each containing "cards" that group related commands. Because a packet can include multiple decks, the payload begins with a deck list that defines its structure. The attack SMS contains one dynamic deck with one card (step (2) in **Figure 10**). The S@T browser never saves dynamic decks, so no traces of the attack are left on the SIM. This makes post-incident detection challenging, as it is difficult to determine if an attack was conducted on the device. Only timestamped network traces of the malicious action can provide clues. The card inside the attack SMS encloses five commands. Each bytecode command is identified by a tag. Besides the bytecode commands, the S@T browser is capable of executing STK commands, which are sent as proactive commands from the SIM card to the phone. The phone's response is stored in a variable of the S@T browser. The following commands would have been executed sequentially by the S@T browser if the firewall did not block the SMS:

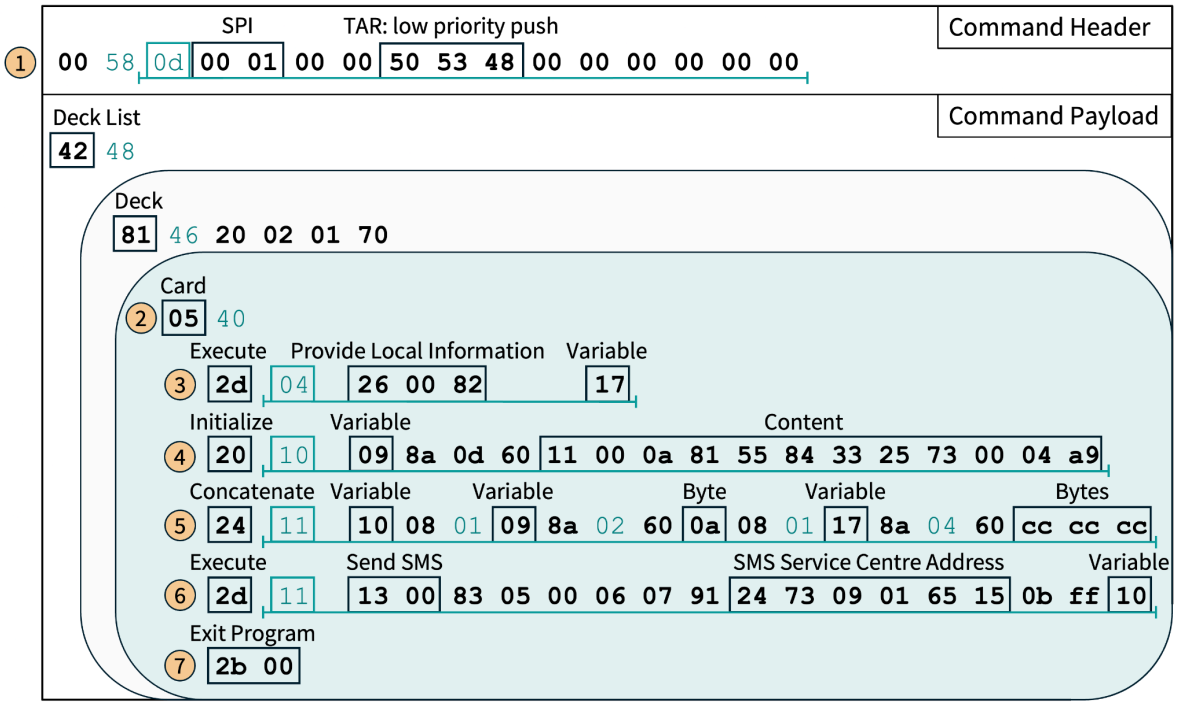


Figure 10: Structure of the binary SMS payload detailing the S@T browser commands.

- **STK command Provide Local Information, step (3):**
  - The first STK command instructs the S@T browser to send a proactive command to the phone, requesting information about the network cell it is currently connected to, i.e., Cell Identifier, Location Area Code (LAC), Mobile Network Code (MNC), and Mobile Country Code (MCC). The location information returned by the phone is stored in variable `0x17`.
  - Based on this data, the position of the phone can be determined with an accuracy ranging from a kilometer in urban areas to a hundred kilometers in rural areas, depending on the cell density.
- **Initialize Variable, step (4):**
  - Then, the variable `0x09` is initialized with 12 bytes of binary data.
  - We analyze the bytes' content in the next section.
- **Concatenate Values, step (5):**
  - Next, variable `0x09` is concatenated with the byte `0x0a`, the variable `0x17`, and the byte sequence `0xcc 0xcc 0xcc`. The concatenation result is stored in variable `0x10`.
  - This command appends the location information stored in variable `0x17` to the binary data in `0x09`, while adding additional bytes to the stream.
- **STK command Send Short Message, step (6):**

    - Finally, the S@T browser issues a proactive command to the phone to send an exfiltration SMS containing the contents of variable `0x10`. It is addressed as `423790105651`, assigned to FL1 Liechtenstein.
    - The SMS parameters are configured so that the user is not notified if the SMS transmission fails, preventing detection of the attack.
      The destination address of the exfiltration SMS reveals the attacker-controlled network, as the attackers need access to it to receive the SMS.
- **Exit Program, step (7):**
    - The last command exits the program.

The Exfiltration SMS

Because the SMS message was blocked, it never reached the targeted phone, and no exfiltration message with location data was actually sent. However, by parsing and decoding the commands embedded in the intercepted SMS payload, we reconstructed how the exfiltration SMS would have been generated and what it would contain if the attack was successful.

We analyzed the command sequence that would have been executed by the SIM card that defines how location data would be collected and transmitted back to the attacker. The exploit would have silently collected and sent its current location via SMS to the SMS Service Centre (SMSC) address configured by the attacker, without any user interaction or visible indication on the device.

1. The SMS Header

The exfiltration SMS is first constructed from the contents of variable `0x10` (see step (5) of **Figure 10**), with the first 12 bytes of this variable including the binary data from variable `0x09` (see step (4) in **Figure 10**). This data forms the SMS-SUBMIT header that controls the type of SMS being sent and how it's handled. In this case, it specifies that the SMS is sent from a device to a remote SMSC, that it should accept duplicates, and does not request a delivery confirmation.

2. The SMS Destination

The subsequent bytes of variable `0x09` are populated with the phone number of the destination user, shown as `5548335237`. This appears as a Brazil number (country code +55), but is incomplete and does not conform to valid country numbering formats. As such, it is unlikely to be used for message routing or delivery. Instead, it may function as a campaign identifier within the STA2 surveillance infrastructure.

However, we were able to confirm that the SMSC address configured for the SMS matches a GT observed in previous location-tracking attacks. Based on this information, we assess with

moderate confidence that the SMSC number was deliberately configured as a C2 endpoint by STA2 to route and collect the SMS payload containing the target device location data (see **Figure 11**). While the destination number is invalid, the attackers can access the message delivered to the SMSC address, enabling them to retrieve the exfiltrated location data without relying on delivery to the end-device.

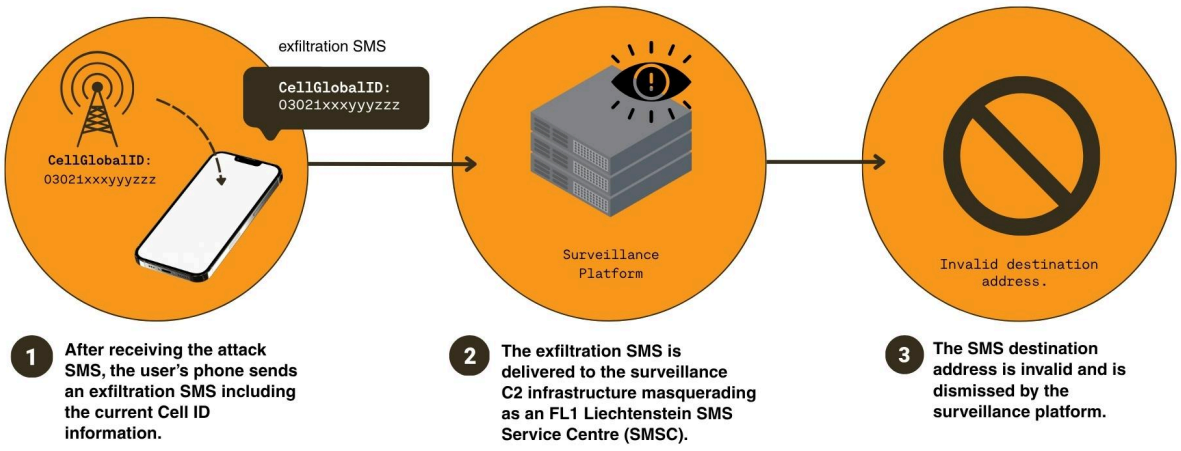


Figure 11: Exfiltration SMS delivery to the STA2 surveillance infrastructure masquerading as an FL1 SMSC

3. The Exfiltrated Data

The location data sent in the SMS is retrieved by the **`Provide Local Information`** command and stored in variable `0x17`. The **`Concatenate Values`** command adds a single length byte of `0x0a` (see step (5) in **Figure 10**), with the last three bytes of the SMS probably used as artificial padding. Through the Initialize Variable and Concatenate Values commands, the attackers craft an exfiltration SMS that contains the location information and destination address likely repurposed as an identifier for the target rather than a true delivery endpoint.

Comparison to SIMjacker

The attack SMS sent by STA2 fits a typical SIMjacker SMS configuration as described in ENEA's 2019 report. Comparing the commands used, we note subtle differences. Nevertheless, ENEA states that the SIMjacker SMSes observed in the wild also show variations. The attack SMS we observed could be a more recent SIMjacker variant, adapting SIM or operator configurations to improve efficacy. The distinctions are listed in **Table 10**.

	Observed Attack SMS	**Common SIMjacker SMSes**
Card element configured to reset all variables in the S@T browser	No reset of variables	Resetting all variables is observed in more than 44% of the SIMjacker SMSes analyzed by ENEA.
Order of commands	Obtains location information first, then crafts the SMS-SUBMIT header	Creates SMS-SUBMIT header first, then retrieves the location and IMEI of the phone.
Data exfiltration	Collects the phone's location but not the IMEI	93% of the traced SIMjacker SMSes collect the location and the IMEI of the target device.
Variable with filler bytes	Does not include a variable with filler bytes but single bytes, which are added during the concatenation step	Often include a variable with filler bytes, placed in different locations of the exfiltration SMS. This is probably done to obfuscate the message.

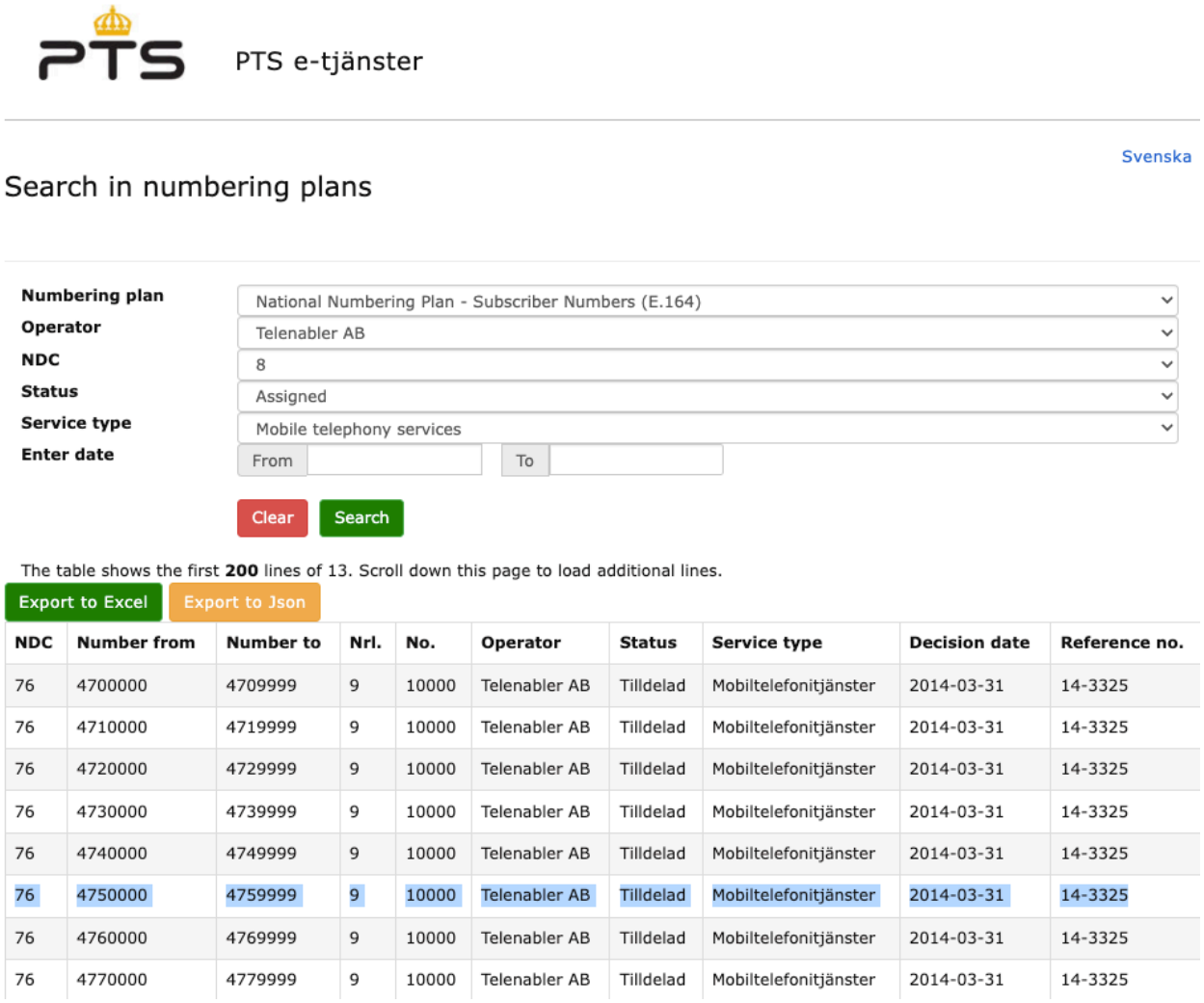
Table 10: Comparison of the observed attack SMS to common SIMjacker SMSes

Sweden Operator Identifier Used as the Entry Point

The first two messages sent by STA2 used the same operator GT 467647531812, affirming its use as a C2 endpoint address. We used a publicly available numbering plan search tool from PTS, Sweden's government telecom authority, shown in **Figure 12**, to confirm that number lies within a range allocated to Telenabler AB. Telenabler is a network provider that offers services to Mobile Virtual Network Operators (MVNOs). Telenabler's website describes itself stating "We are specialists dealing with many different country-specific telecom legislations and we work together with some of the strongest telecommunication partners in the world."

The Citizen Lab previously reported on Telenabler's Global Title leasing business model in the 2023 Finding You report. In that report, we identified this same GT as a frequently detected source address used in location tracking operations. Since that report, the activity from 467647531812 did not stop. Between October 2023 and April 2025, we identified over 1,700 additional SS7 attacks originating from this address, with over 92% of its traffic linked to location tracking. The primary SS7 query types seen

included `provideSubscriberInfo` (1,011) followed by `provideSubscriberLocation` (386) and others. The repeated, high volume use of this GT with different location query types suggests it was assigned specifically for surveillance purposes.



PTS e-tjänster

Svenska

Search in numbering plans

Numbering plan	National Numbering Plan - Subscriber Numbers (E.164)
Operator	Telenabler AB
NDC	8
Status	Assigned
Service type	Mobile telephony services
Enter date	From To

Clear Search

The table shows the first **200** lines of 13. Scroll down this page to load additional lines.

Export to Excel Export to Json

NDC	Number from	Number to	Nrl.	No.	Operator	Status	Service type	Decision date	Reference no.
76	4700000	4709999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2014-03-31	14-3325
76	4710000	4719999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2014-03-31	14-3325
76	4720000	4729999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2014-03-31	14-3325
76	4730000	4739999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2014-03-31	14-3325
76	4740000	4749999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2014-03-31	14-3325
76	4750000	4759999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2014-03-31	14-3325
76	4760000	4769999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2014-03-31	14-3325
76	4770000	4779999	9	10000	Telenabler AB	Tilldelad	Mobiltelefonitjänster	2014-03-31	14-3325

Figure 12: Number ranges allocated to Tenenabler by Sweden's telecom regulator PTS.

SIMjacker Payload Exposes a Coordinated Attack Cluster

The signalling identifiers used in the SIMjacker exploit formed endpoints for C2 communication. The attack used three numbers from different operators that played unique roles in the attack and in the process, revealed tradecraft showing STA2's detailed knowledge of the operator interconnect routing ecosystem.

- GT address to deliver the payload – `467647531812` – Telenabler Sweden

- SMSC GT address used for exfiltration of location data – `423790105651` – FL1 Liechtenstein
- Spoofed SMS sender address – `250730091970` – Airtel Rwanda

Mobile operators assign GT address ranges to specific core network functions (SMSCs, HLRs, MSCs, etc.) and publish the assignments in IR.21 documents to ensure service availability and correct routing of signalling traffic. Because GTs are routable signalling identifiers, they play a central role for roaming and trust between operators. Many operators rely on address assignments published in IR.21 to enforce security policies, rejecting signalling messages originating with inconsistent network assignments or service functions.

The GT `423790105651` used in the attack falls within a range of addresses assigned by FL1 to SMSCs as published in their IR.21 document (**Figure 13**). However, the configured address used in the attack contains an extra digit beyond the documented range, showing the attacker's knowledge of FL1's IR.21 assignments. Appending an additional digit ensures the routing of the exfiltration SMS to the actor's surveillance C2 infrastructure, while also serving as an internal identifier for the surveillance application labeling it as a SIMJacker operation and to process the target device location information within it.

SMSC	423 79 010500 / 010599

Figure 13: SMSC global title range shown in the FL1 Liechtenstein IR.21.

The `250730091970` SMS sender address used in the SIMJacker attack is mapped to an Airtel Rwanda GT range, but doesn't appear to be designated to any particular network function. However, the attack history behind this GT since 2022 shows over 600 events exclusively used in location tracking operations.

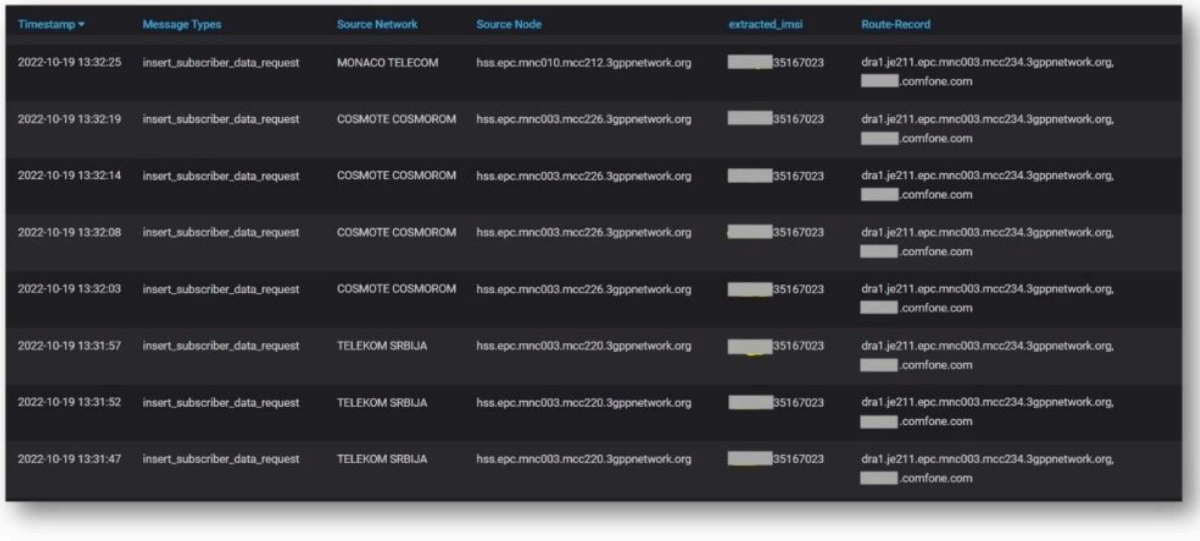
Attribution Assessment

The STA2 campaign shows a unique approach to telecom surveillance, combining SS7 signalling, SIM-based exploitation, and Diameter-based location tracking techniques. While we do not directly attribute this activity to a specific organization, we have aligned the operational model based on historical attack data, technical, and behavioural indicators.

A Long History of Network Surveillance

To assess the scale of STA2 activity, we analyzed historical SS7 and Diameter firewall telemetry associated with the cluster of operator identifiers used in the campaign. We uncovered a prolific operation with more than 15,700 location tracking attempts dating back to October 2022. An example of early activity is shown in the **Figure 14** screenshot, which shows a captured sequence of tracking messages from October 19, 2022, with multiple operator identities all using the same Origin-Host

format (displayed in the “Source Node” column) and the Jersey-Airtel Route-Record. The targeted user IMSI and portions of the IPX provider hostnames are partially redacted for privacy.



Timestamp	Message Types	Source Network	Source Node	extracted_imsi	Route-Record
2022-10-19 13:32:25	insert_subscriber_data_request	MONACO TELECOM	hss.epc.mnc010.mcc212.3gppnetwork.org	[redacted]35167023	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org, [redacted].comfone.com
2022-10-19 13:32:19	insert_subscriber_data_request	COSMOTE COSMOROM	hss.epc.mnc003.mcc226.3gppnetwork.org	[redacted]35167023	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org, [redacted].comfone.com
2022-10-19 13:32:14	insert_subscriber_data_request	COSMOTE COSMOROM	hss.epc.mnc003.mcc226.3gppnetwork.org	[redacted]35167023	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org, [redacted].comfone.com
2022-10-19 13:32:08	insert_subscriber_data_request	COSMOTE COSMOROM	hss.epc.mnc003.mcc226.3gppnetwork.org	[redacted]35167023	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org, [redacted].comfone.com
2022-10-19 13:32:03	insert_subscriber_data_request	COSMOTE COSMOROM	hss.epc.mnc003.mcc226.3gppnetwork.org	[redacted]35167023	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org, [redacted].comfone.com
2022-10-19 13:31:57	insert_subscriber_data_request	TELEKOM SRBIJA	hss.epc.mnc003.mcc220.3gppnetwork.org	[redacted]35167023	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org, [redacted].comfone.com
2022-10-19 13:31:52	insert_subscriber_data_request	TELEKOM SRBIJA	hss.epc.mnc003.mcc220.3gppnetwork.org	[redacted]35167023	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org, [redacted].comfone.com
2022-10-19 13:31:47	insert_subscriber_data_request	TELEKOM SRBIJA	hss.epc.mnc003.mcc220.3gppnetwork.org	[redacted]35167023	dra1.je211.epc.mnc003.mcc234.3gppnetwork.org, [redacted].comfone.com

Figure 14: Early evidence of STA2 surveillance activity (October 19, 2022).

Table 11 summarizes the volume and progression of the STA2 surveillance activity over time.

Protocol	**October 2022**
Diameter	109
SS7	103

Table 11: Progression of multi-year surveillance activity attributed to STA2.

Within that history of attacks, we looked for indicators that might point to a known surveillance actor. The attack history associated with the GTs showed links to Fink Telecom Services (FTS), a Swiss-based telecommunications provider exposed as a commercial telecom surveillance vendor in investigative reporting by Lighthouse Reports and Bloomberg, which found attack clusters using the same signatures as STA2.

The FTS Signalling Overlap

STA2 surveillance activity shows alignment with identifiers and patterns associated with FTS, including same-day location tracking attacks and matching Diameter hostname formats. We analyzed a history of attacks starting in November 2022 linked to both FTS and STA2. Prior to media reports of FTS linked to SS7 surveillance, we identified numerous STA2 surveillance operations indirectly linked to FTS, with

many occurring on the same day and with the same attack objective. A sample of these attacks are listed in **Table 12**.

Date	Source Node	Network	Country	Threat Type	Signalling Operation
4-Dec-22	ss.epc.mnc001.mcc260.3gppnetwork.org	POLKOMTEL	Poland	Location Discovery	Insert-Subscriber-Data-Request
4-Dec-22	46727507103	FINK TELECOM SERVICES	Sweden	Location Discovery	provideSubscriberInfo
15-Dec-22	250730091970	AIRTEL RWANDA	Rwanda	Location Discovery	provideSubscriberInfo
15-Dec-22	25671000034	UGANDA TELECOM	Uganda	Location Discovery	provideSubscriberInfo
15-Dec-22	26482000011	DEMSHI TELECOM	Namibia	Location Discovery	provideSubscriberInfo
18-Dec-22	250730091970	AIRTEL RWANDA	Rwanda	Location Discovery	provideSubscriberLocation
18-Dec-22	25671000034	UGANDA TELECOM	Uganda	Location Discovery	provideSubscriberLocation
19-Dec-22	79588879810	LETAI	Russia	Location Discovery	anyTimeInterrogation
19-Dec-22	26482000011	DEMSHI TELECOM	Namibia	Location Discovery	anyTimeInterrogation
19-Dec-22	250730091970	AIRTEL RWANDA	Rwanda	Location Discovery	anyTimeInterrogation
14-Feb-23	26482000011	DEMSHI TELECOM	Namibia	Location Discovery	provideSubscriberInfo
14-Feb-23	hss.epc.mnc001.mcc260.3gppnetwork.org	POLKOMTEL	Poland	Location Discovery	Insert-Subscriber-Data-Request
14-Feb-23	250730091970	AIRTEL RWANDA	Rwanda	Location Discovery	provideSubscriberInfo

11-Mar-23	hss.epc.mnc063.mcc240.3gppnetwork.org	FINK TELECOM SERVICES	Switzerland	Location Discovery	Insert-Subscriber-Data-Request
11-Mar-23	hss.epc.mnc001.mcc649.3gppnetwork.org	MTS	Namibia	Location Discovery	Insert-Subscriber-Data-Request
5-Apr-23	4672750710	FINK TELECOM SERVICES	Sweden	Location Discovery	provideSubscriberInfo
5-Apr-23	25671000034	UGANDA TELECOM	Uganda	Location Discovery	provideSubscriberInfo
5-Apr-23	hss.epc.mnc001.mcc260.3gppnetwork.org	POLKOMTEL	Poland	Location Discovery	Insert-Subscriber-Data-Request
16-Aug-23	hss.epc.mnc001.mcc260.3gppnetwork.org	POLKOMTEL	Poland	Location Discovery	Insert-Subscriber-Data-Request
16-Aug-23	hss.epc.mnc063.mcc240.3gppnetwork.org	FINK TELECOM SERVICES	Switzerland	Location Discovery	Insert-Subscriber-Data-Request
23-Feb-24	467647531812	TELENABLER AB	Sweden	Location Discovery	provideSubscriberInfo
23-Feb-24	250730091970	AIRTEL RWANDA	Rwanda	Location Discovery	provideSubscriberInfo
23-Feb-24	264820000458	DEMSHI TELECOM	Namibia	Location Discovery	provideSubscriberInfo

Table 12: Firewall telemetry with addresses linked to Fink Telecom Services and STA2.

The attacks summarized in **Table 12** include identifiers seen in the STA2 campaign alongside GTs and Diameter identifiers attributed to FTS highlighted in RED. Notably, the Diameter hostname formats used in the STA2 attacks also use MCC/MNC values associated with FTS. The values listed in published IR.21 documents are shown in **Figure 15**.

EPC Realms For Roaming	*)
mobile.fink-telecom.com	fink-telecom.com
epc.mnc063.mcc228.3gppnetwork.org	epc***XX***.epc.mnc063.mcc228.3gppnetwork.org *)
epc.mnc063.mcc240.3gppnetwork.org	epc***XX***.*epc*.mnc063.mcc240.3gppnetwork.org *)

Figure 15: Signalling domains published in the FTS IR.21 document.

While spoofing cannot be ruled out, the alignment of historical same-day location tracking attacks, Diameter hostname formats used in the STA2 campaign, GT ranges published in FTS IR.21 documents, and journalist publications exposing SS7 attacks attributed to FTS show clear links between STA2 and FTS.

Correspondence

On April 17, 2026, we sent letters with questions about our research to 019Mobile, Airtel Jersey Sure, and Tango Networks. As of the time of writing, only 019Mobile has responded to our questions. Their response[3] can be found here.

Update: After publishing this report, we received a response from Sure. Their response can be found here.

Conclusion

This report is the first to map live SS7 and Diameter attack telemetry to operator identifiers and interconnect routes used in cross-protocol mobile surveillance operations. Rather than implanting device spyware or hacking corporate networks to carry out mobile espionage, the two actors leveraged legitimate operator signalling identities and trusted interconnections to carry out targeted surveillance across country borders. By blending their location queries into normal roaming traffic, and manipulating protocols and network identifiers, they effectively operated as “ghost operators” within the global telecom ecosystem.

The findings in this report expose how advanced actors operationalize telecom infrastructure to carry out campaigns persisting for years without detection. Telecom networks form the backbone of global civil society, and when trust is exploited for surveillance, the consequences extend beyond individual victims to mobile users worldwide. This investigation exposes more than protocol vulnerability issues in telecommunications; it shows governance failures across the entire interconnect ecosystem used for

[3] We received a response from 019Mobile after our deadline but we are including it here. Their assertions do not alter our conclusions, although we will investigate further and remain open to further information from them and other providers.

critical mobile communications. It also demonstrates how those weaknesses enabled the use of telecommunications infrastructure as a covert surveillance platform.

The global telecom ecosystem can no longer rely on legacy trust models. Without authentication, enforceable interconnect controls, transparency in commercial network access, and regulatory accountability, mobile networks will continue to serve as a global platform for covert espionage.