”DETECTING THE UNKNOWNS”

MNO’S CYBER RESILIENCE IN RESPONDING TO ZERO-DAY EXPLOITS

Imran Saleem

18 November 2022

mobileum
Action driven by intelligence

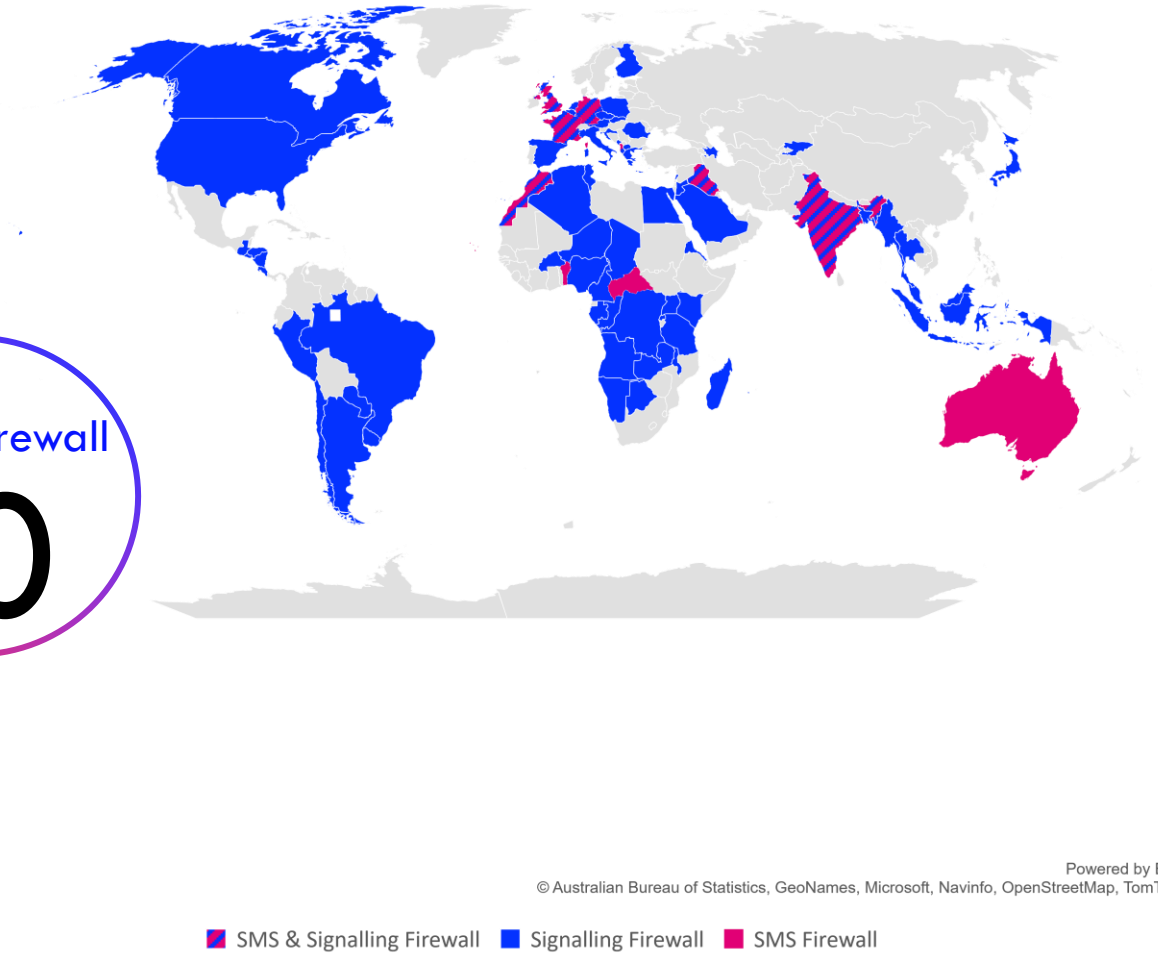
security intelligence
Mobileum platform

LARGEST MARKET SHARE FOR FIREWALL…EXPANDING

3G/4G Signalling Firewall
90+

GTP Firewall
15

SMS Firewall
10



Key contributor to GSMA FS.11 FS.19 and FS.20

AGENDA

1 Who sends illegal Messages?

2 Attackers Analogy and Groups

3 Problem statement

4 Intro to a Zero-Day Exploit

5 Actionable Intelligence

6 Evidence Pack

7 The Imminent Threat

8 Recommendations

WHO SENDS ILLEGAL MESSAGES?

1. We focus on signalling in telecoms.
2. Signalling security helps identify what attackers are trying to do.
3. We go “upstream” from the attacker’s perspective.

ATTACKER'S ANALOGY

Adversaries are:

- Sophisticated and armed with new techniques
- Well informed and intelligent
- Well paid and funded
- Well connected and grouped

How much do we know about them?

- Keep trying approach
- Access to community documents and groups
- Expert in protocols standards
- Aware that most operators use a more tick box security approach and are not enabled with intelligence
- Mobile Operator's don't investigate into unknowns

Groups of Attackers

1. Script Kiddies

- Small number of badly-formed messages
- **Confused with broken equipment**
- Send multiple messages to the same test SIMs
- Often send after work hours

2. Grey Operators

- A2P grey route / SRI-SM location and IMSI checking
- **Mass messages** / bulk business
- Static ranges – some movement of specific GTs
- Focus on **Home Routing bypass** techniques

3. Surveillance Companies

- **Well-funded**
- Centrally co-ordinated across 10-20 GTs
- Use the same software
- Lease A2P GTs
- Creative encoding methods
- **Move their service provider groups around the world**

Groups of Attackers

4. State Actors

- Static, **country-based** GTs
- More standard messages

5. Criminal Service Organizations

- Specific fraud attacks for **online banking**
- Account takeover (2FA) hijack attacks
- Public / dark web websites

6. Security Audit Companies

- **Good guys!**
- Static GTs
- Use their own software stacks
- **Highly innovative attacks** – often copied by others

7. DoS Agents

- Aim to **bring down** networks
- Being tested recently
- Successful in bringing down Network element.

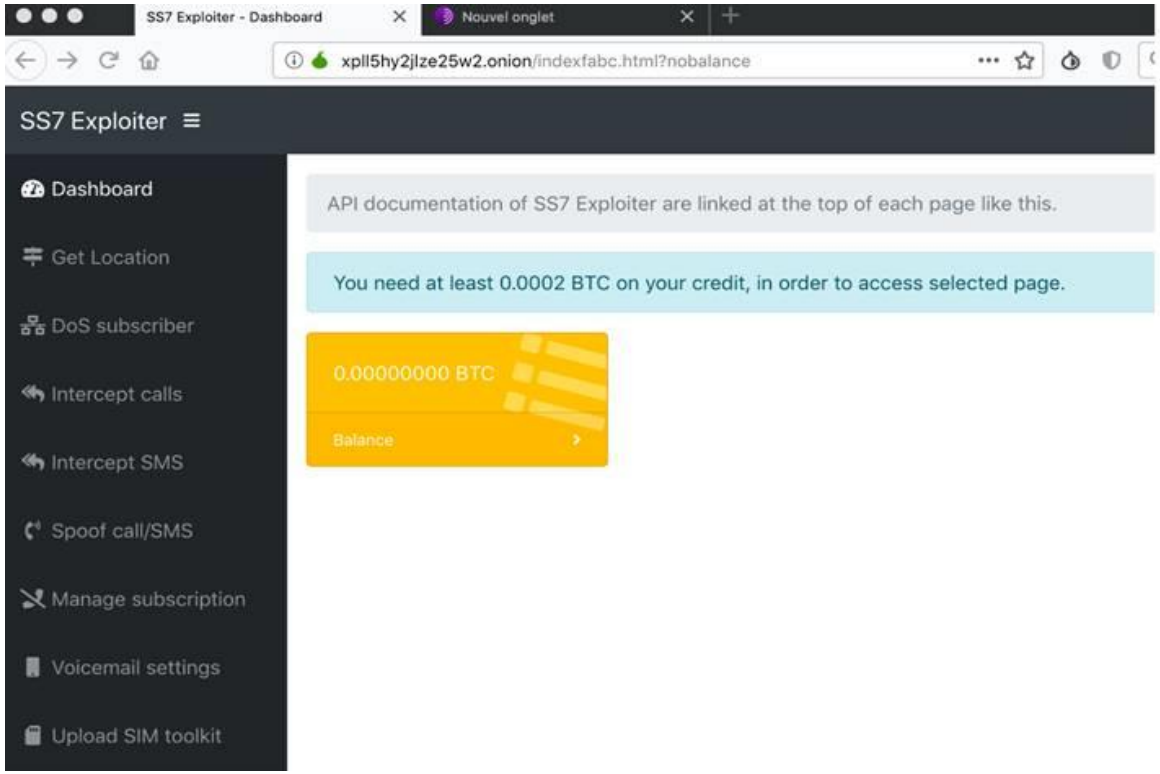
PROBLEM STATEMENT

TRUST IS NOT A CYBERSECURITY STRATEGY

SO… HOW DID WE GET TO THIS SITUATION?

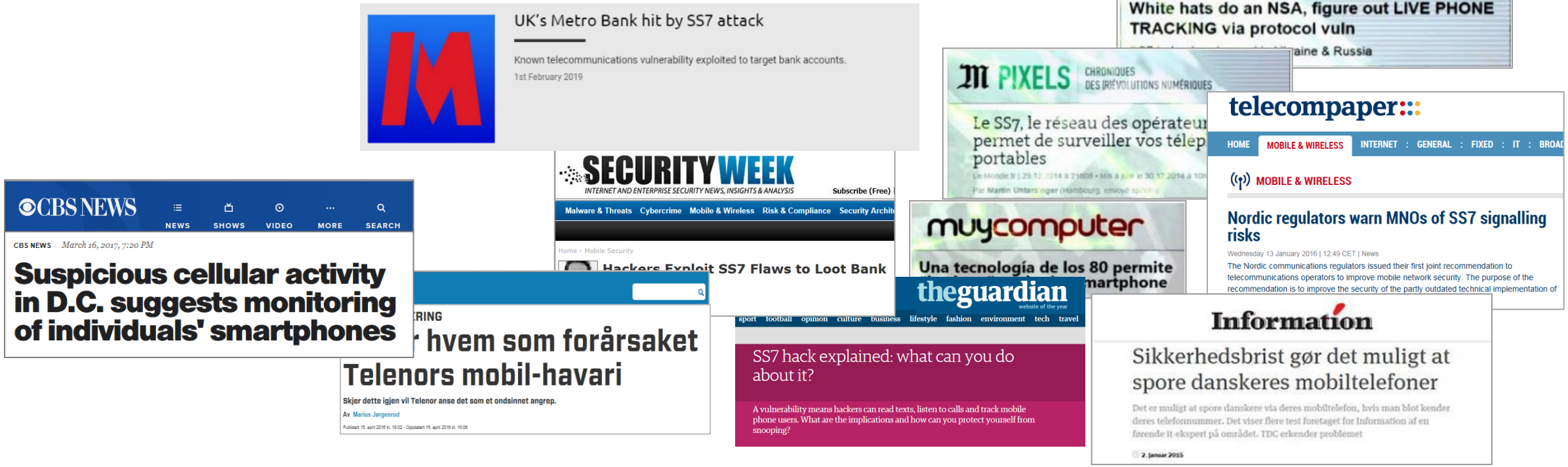
Signalling network is no longer a trusted/ closed environment. (Access can be bought legally as cheap as $1,000)

Hacker's services widely available, no need to be a Signaling tech head. Outsource!

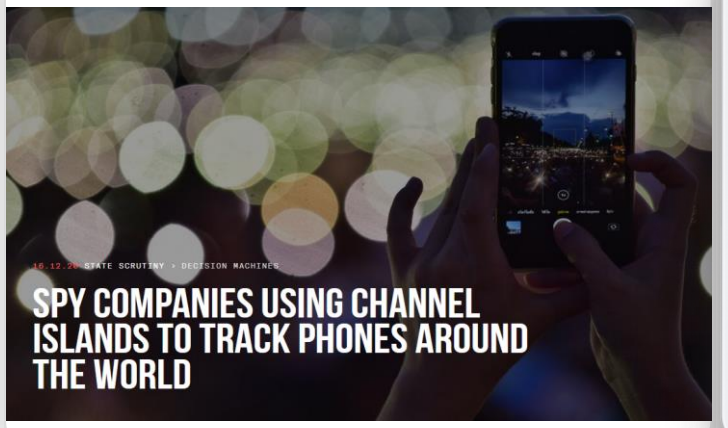


SHATTERING OF TRUST IN THE NETWORK

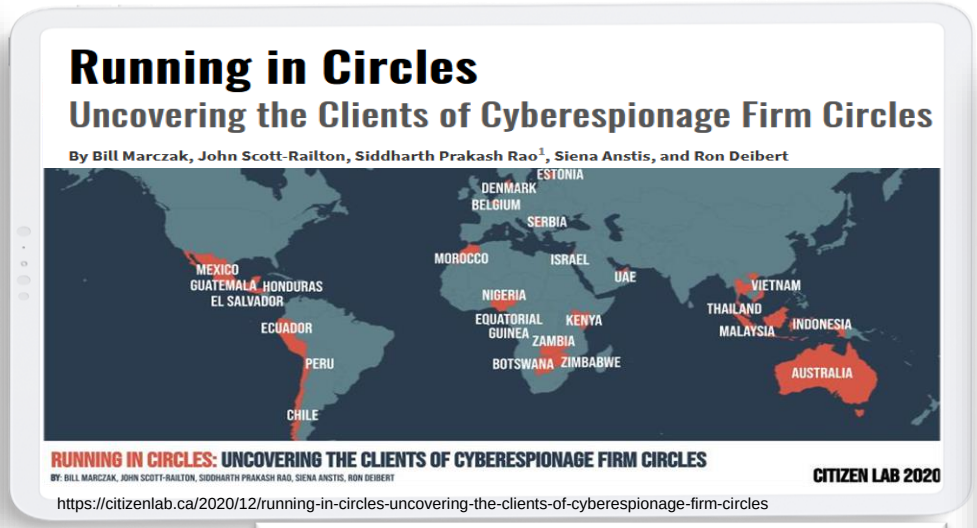
- Telecom networks are now being targeted by the sophisticated threat actors.
- Attacks seen on SS7 are happening now on Diameter and GTP-C.
- Customer privacy and data are at risk.
- Loss of confidence in Telecom infrastructure.



ROLE OF TRUST IN CLOSED ECOSYSTEM



https://www.thebureauinvestigates.com/stories/2020-12-16/spy-companies-using-channel-islands-to-track-phones-around-the-world

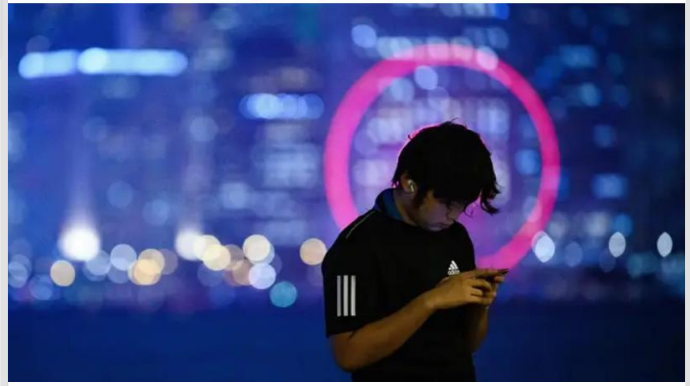


https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles

Israel News | Tech News

Israeli Spy Tech Firm Tracked Mobile Users Around the World, Investigation Suggests

Investigation claims Rayzone used arcane cell network point to 'track the locations of mobile phones across the world'; network vulnerability may have been exploited to track down UAE Princess Sheikha Latifa in attempted 2018 escape ■ Rayzone denies report



Hackers hijack Telegram, email accounts in SS7 mobile attack

by Ionut Ilascu — October 19, 2020 — 12:22 PM

Hackers with access to the Signaling System 7 (SS7) used for connecting mobile networks across the world were able to gain access to Telegram messenger and email data of high-profile individuals in the cryptocurrency business.

HAARETZ

Top News | COVID | Iran cyber | Trump - Biden | UAE visas | Palestinians | Lockdown | Armenia | Zion

Israel News | Tech News

Exclusive: Intricate Hack Against Israeli Crypto Leaders; 'Mossad Investigating'

Dozens of cryptocurrency executives in Israel had their phones hacked and their online identity stolen in a rare and concerning attack

Forget Pegasus, new spyware 'Hermit' now being used by governments

IANS / Updated: Jun 18, 2022, 10:35AM IST

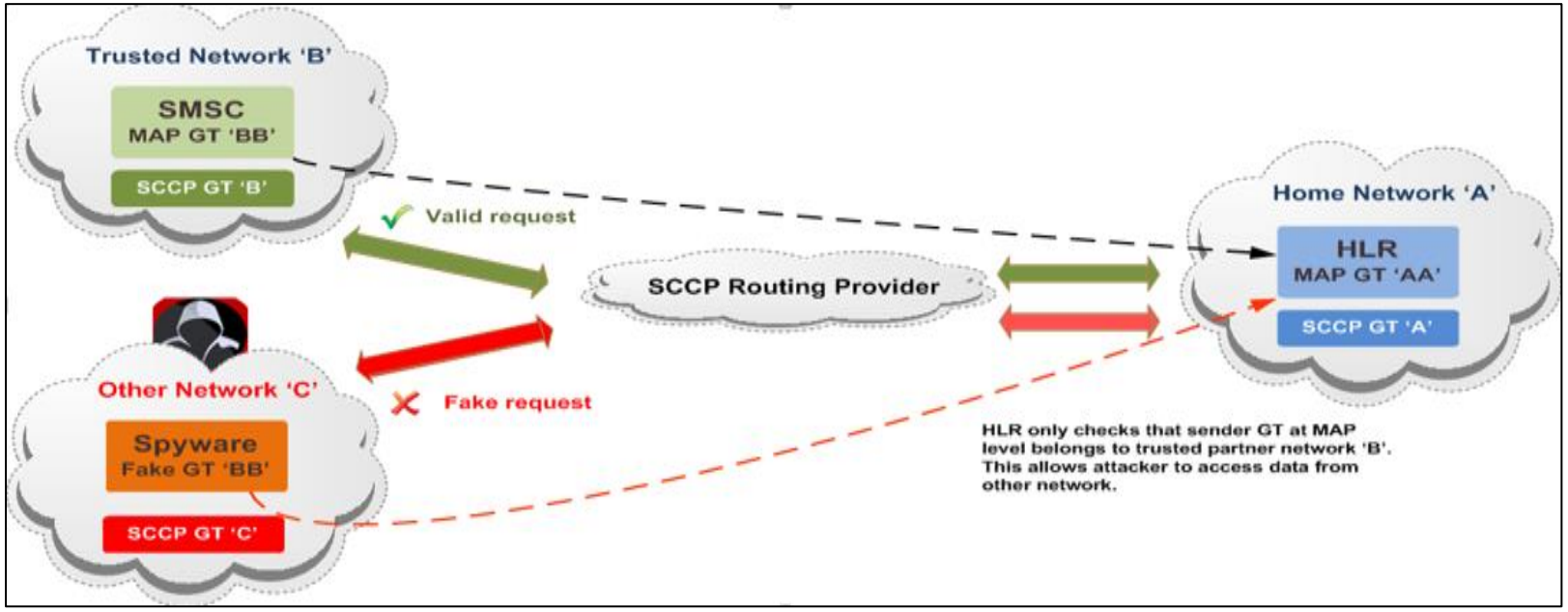
FACEBOOK | TWITTER | LINKEDIN | EMAIL

THE PROBLEM

Exploiting SS7

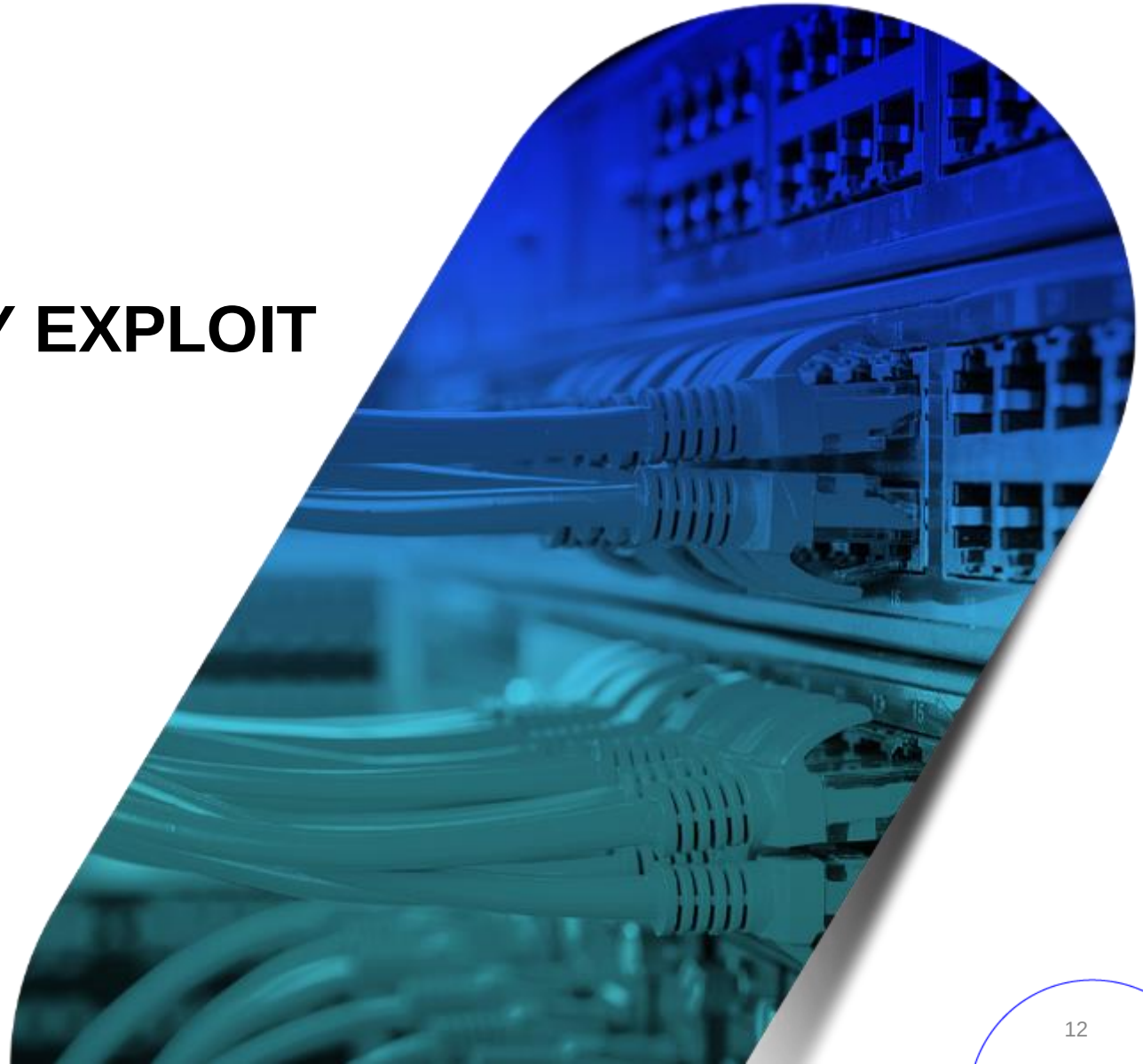
Security vulnerabilities in SS7 can then be exploited

- Lack of end-to-end authentication
- Once access is gained at SCCP level, connectivity to any node addressed by GT is possible
- MAP applications do not validate SCCP originating point of incoming requests



INTRODUCTION TO A ZERO-DAY EXPLOIT

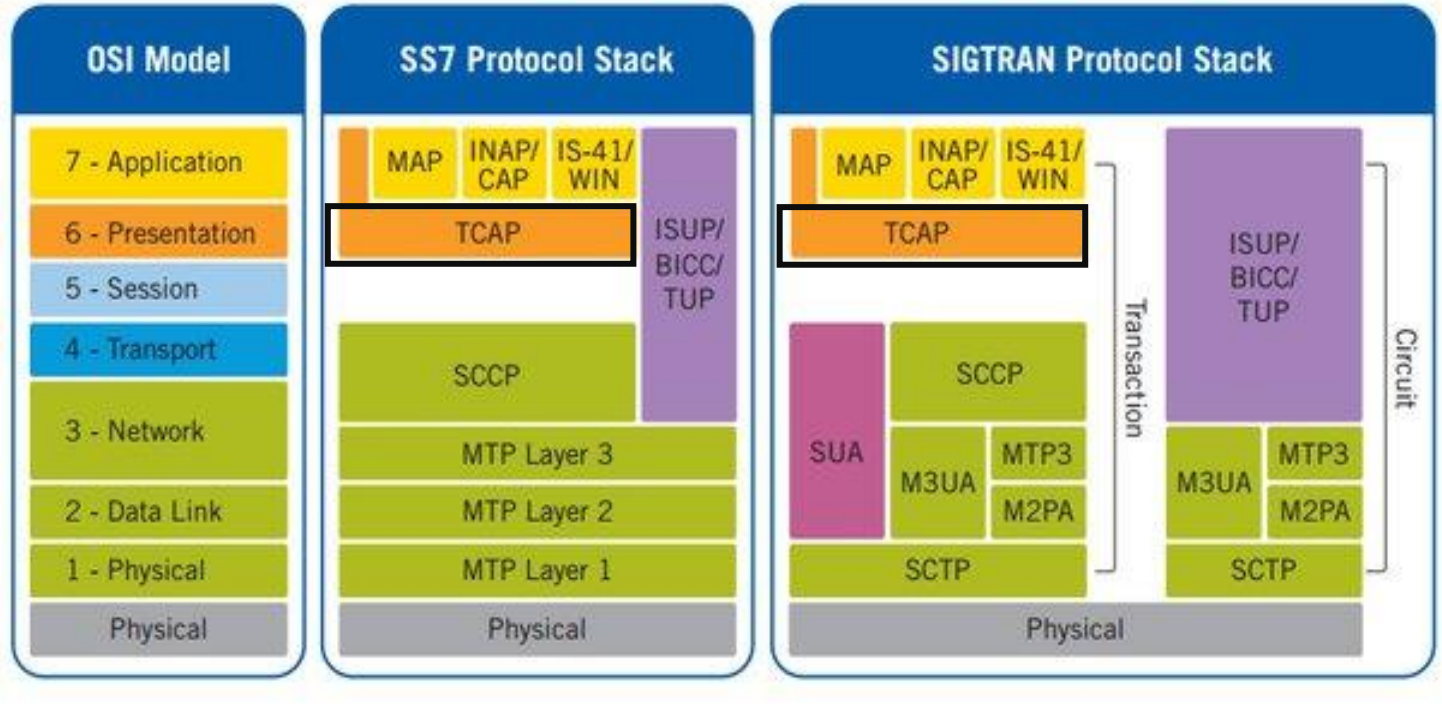
TCAP TAG CLASS ABUSE



WHAT IS TCAP?

How does TCAP work?

- Transaction Capabilities Application Part (TCAP) messages are sent between machines using so-called Transaction IDs.
- TCAP is using an ASN.1 standard encoding/decoding engine for all operation codes.
- Mobile Application Part (MAP) at the application layer is used by mobile network functions such as MSC/VLR, SGSN, HLR.



What is the TCAP TAG CLASS?

The TCAP Tag Class is part of an 8-bit message Tag structure as defined in Q.773:

H	G	F	E	D	C	B	A
Class		Form	Tag code[a)]				

TCAP messages should have Tag Class Universal, which is the most common one:

Class	Coding (HG)
Universal	00
Application-wide	01
Context-specific	10
Private use	11

- Commonly used

- Explicitly supported
- To be agreed upon

HIGHLIGHTS TO TCAP TAG CLASS VULNERABILITY

Silently exploited with coverage seen in around a dozen countries.

Vulnerability aims to bypass Signaling Firewalls and security controls.

Significant impact on the operators globally via Interconnect Signaling.

Potential to perform subsequent attacks i.e., interception, fraud, and account takeover.

Active testing of new variants of this vulnerability in progress.

KEY ATTRIBUTES

Impact Assessment

Impact		
Fraud	High	Perform fraud by the use of ISD,USSD and other messages
Confidentiality	High	Bypass Security firewall (SS7FW) and SMS home routing (SMS HR)
Integrity	High	Bypass Security firewall and be able to perform further attacks
Availability	Medium	Functional Impact on the service nodes

Vulnerability Attributes

Attack Vector	Network
Interface	SS7 International, SS7 National
Protocol	SS7, MAP, CAP, TCAP
Affected equipment	SS7FW, SMS HR, STP, HLR
Affected vendor	Unknown
Affected product and version	Unknown
Discovery date	2021-12-15
Tags	CAT1, CAT2, CAT3

ACTIONABLE INTELLIGENCE

TCAP TAG CLASS ABUSE

ACTIONABLE INTELLIGENCE

Who is this APT?

- The group was first seen in Q1-2021.
- Geographically dispersed with unique sources.
- Testing various zero-day techniques.
- Group still active.

Analysis Approach

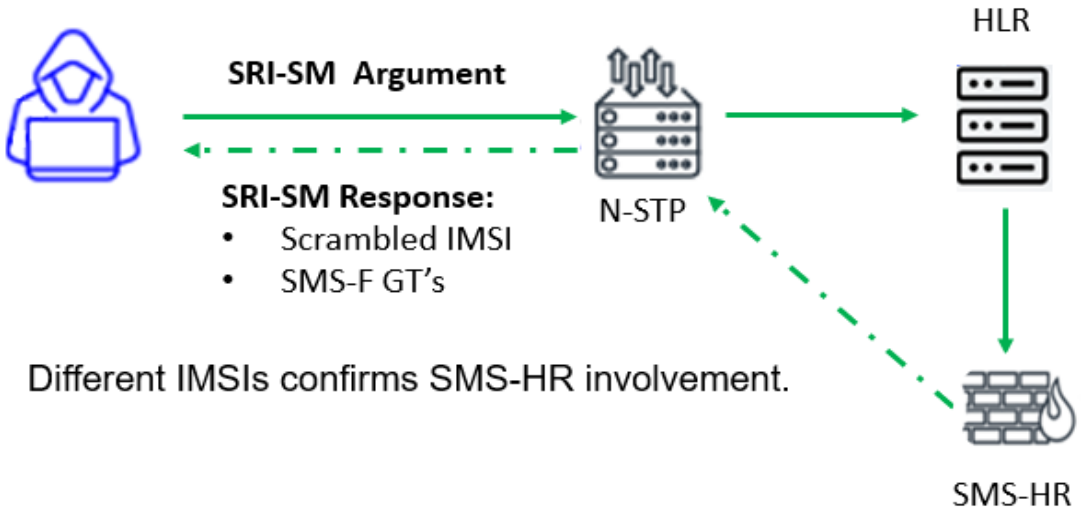
- Moving away from XDR based approach.
- Raw traffic assessment.
- Use of fingerprinting led to larger detection.
- The group remain undetected.

Modus Operandi

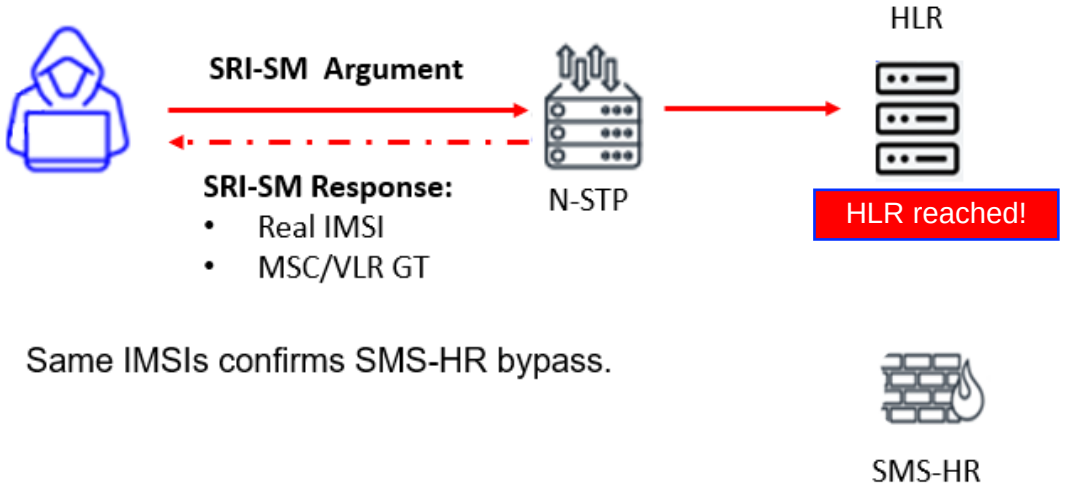
- Service packet are never policed.
- Exfiltrate subscriber PII (IMSI) and Network Info (MSC/VLR/SGSN).
- Exploit targeting layer beneath the application layer.
- Intention to take advantage of TCAP encoding weakness.

STAGING THE TCAP TAG CLASS VULNERABILITY

Initial Access & Recon

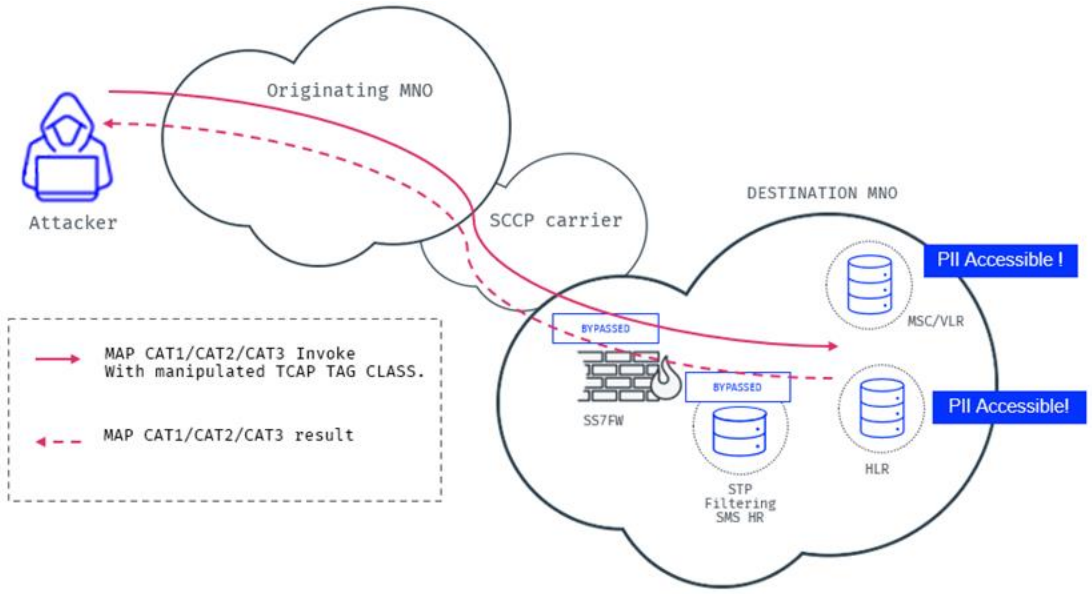


Exfiltration



HOW THE ATTACK WORKS?

Attack Stage



Types of Attacks

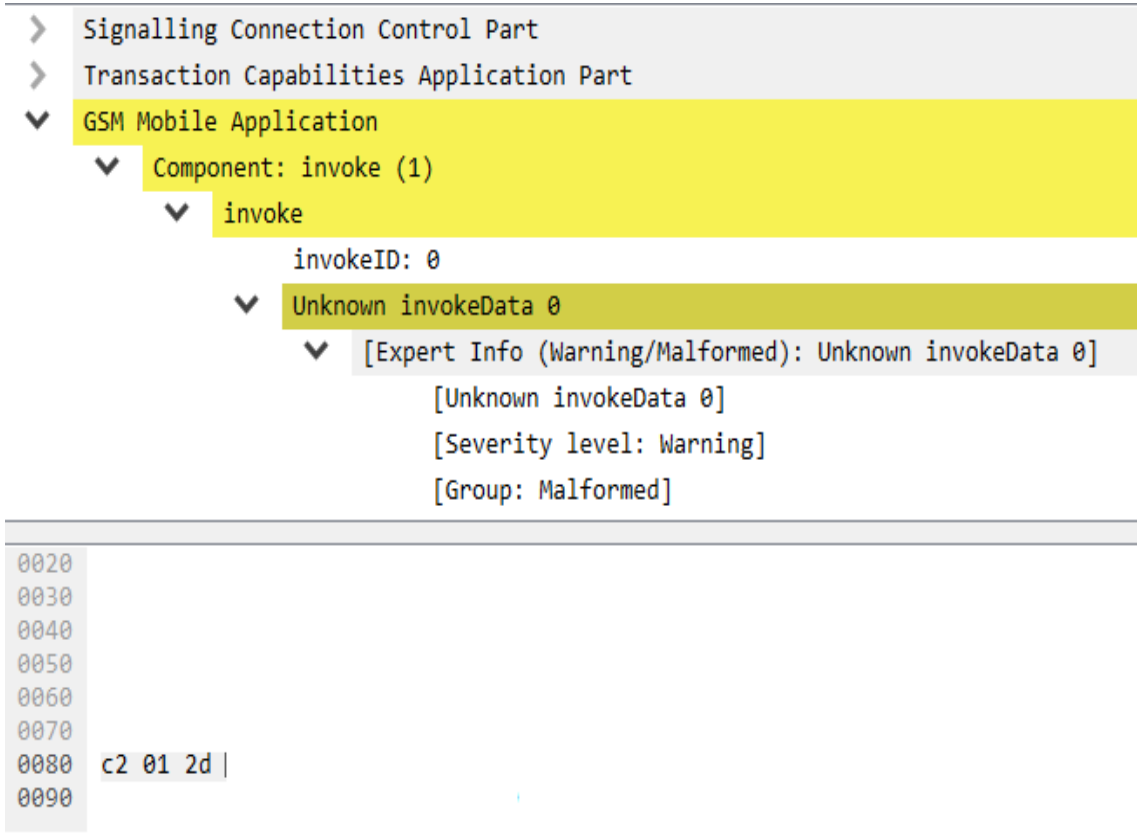
- SMS Spam
- Spoofing
- Location Tracking
- Subscriber Fraud
- Text Message Interception
- Subscriber or Provider DoS
- Routing Attacks
- Call Interception

EVIDENCE PACK

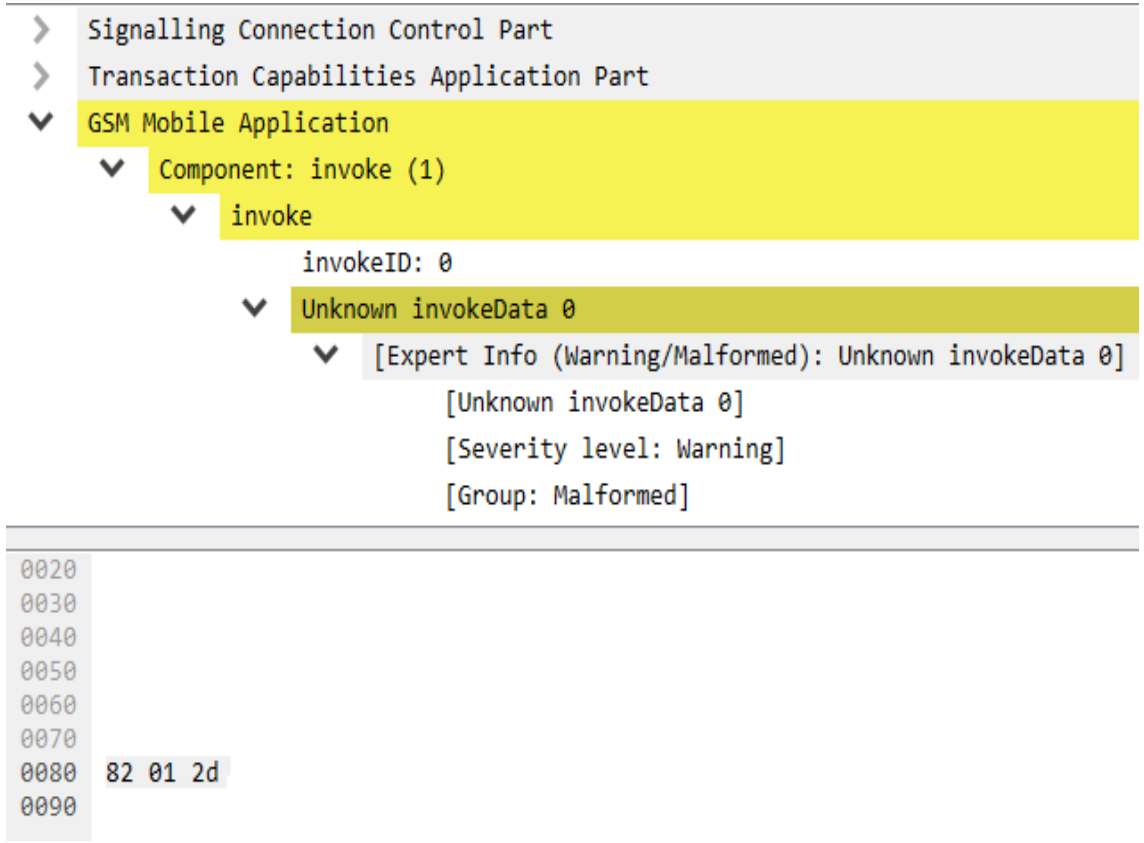
TCAP TAG CLASS ABUSE

THE ATTACK

MAP_SRI_For_SM with Tag Class “Private Use” (11 – represented by ‘c2’)



MAP_SRI_For_SM with Tag Class “Context-Specific” (10 – represented by ‘82’)



NETWORK RESPONSE

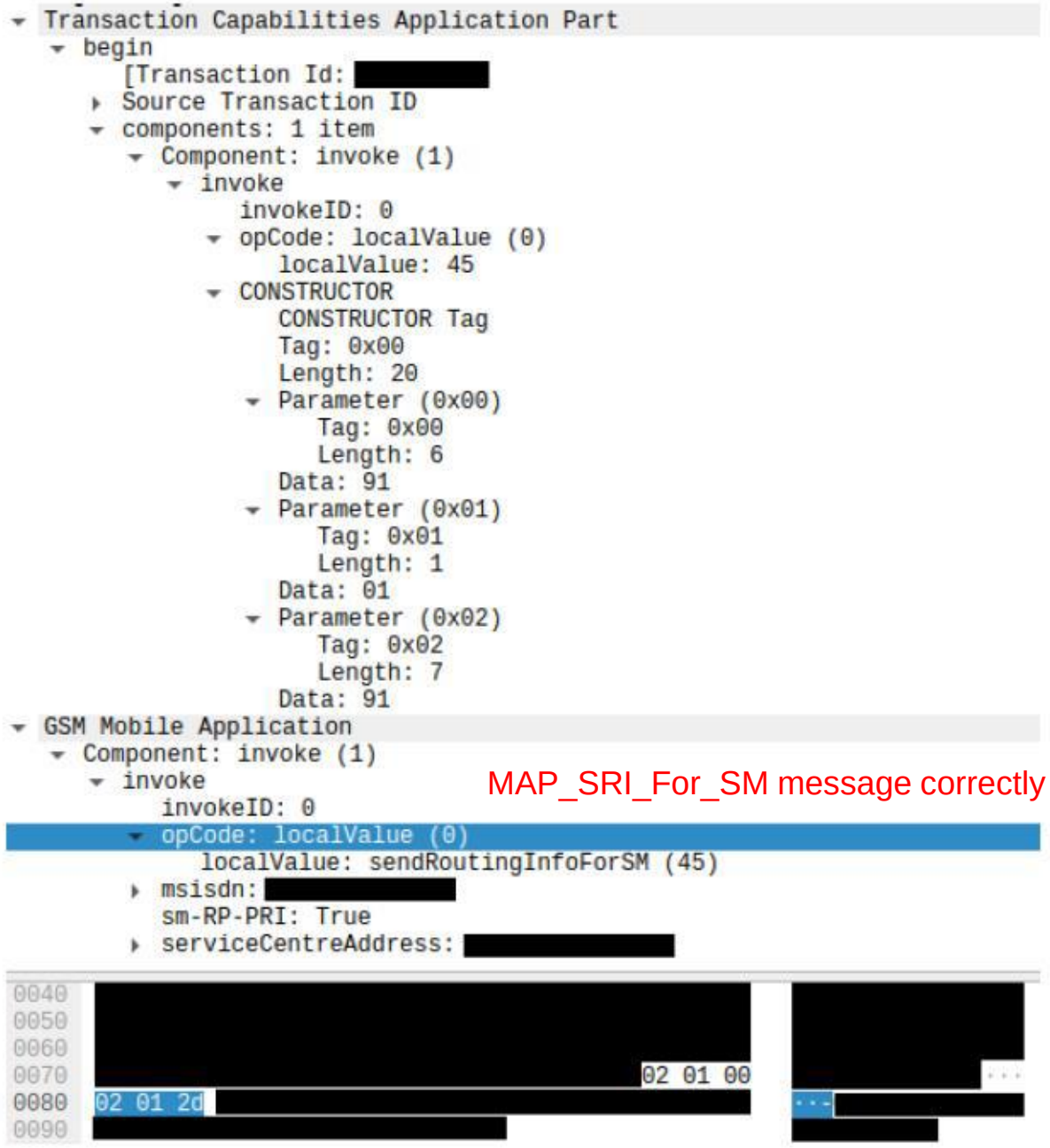
MAP_SRI_For_SM response – PII Leaked

Response captured for one of the MAP_SRI_For_SM requests with manipulated Tag Class.

```
GSM Mobile Application
  Component: returnResultLast (2)
    returnResultLast
        invokeID: 0
      resultretres
        opCode: localValue (0)
            localValue: sendRoutingInfoForSM (45)
          IMSI: [redacted] (real subscriber's information redacted for confidentiality).
        [Association IMSI: [redacted] ]
            Mobile Country Code (MCC): [redacted]
            Mobile Network Code (MNC): [redacted]
        locationInfoWithLMSI
          locationInfo: msc-Number (1)
            msc-Number: 91
                1... .... = Extension: No Extension
                .001 .... = Nature of number: International Number (0x1)
                .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)
              E.164 number (MSISDN): [redacted]
                  Country Code: [redacted]
```

RECONSTRUCTION

MAP_SRI_For_SM with Tag Class Universal (00)



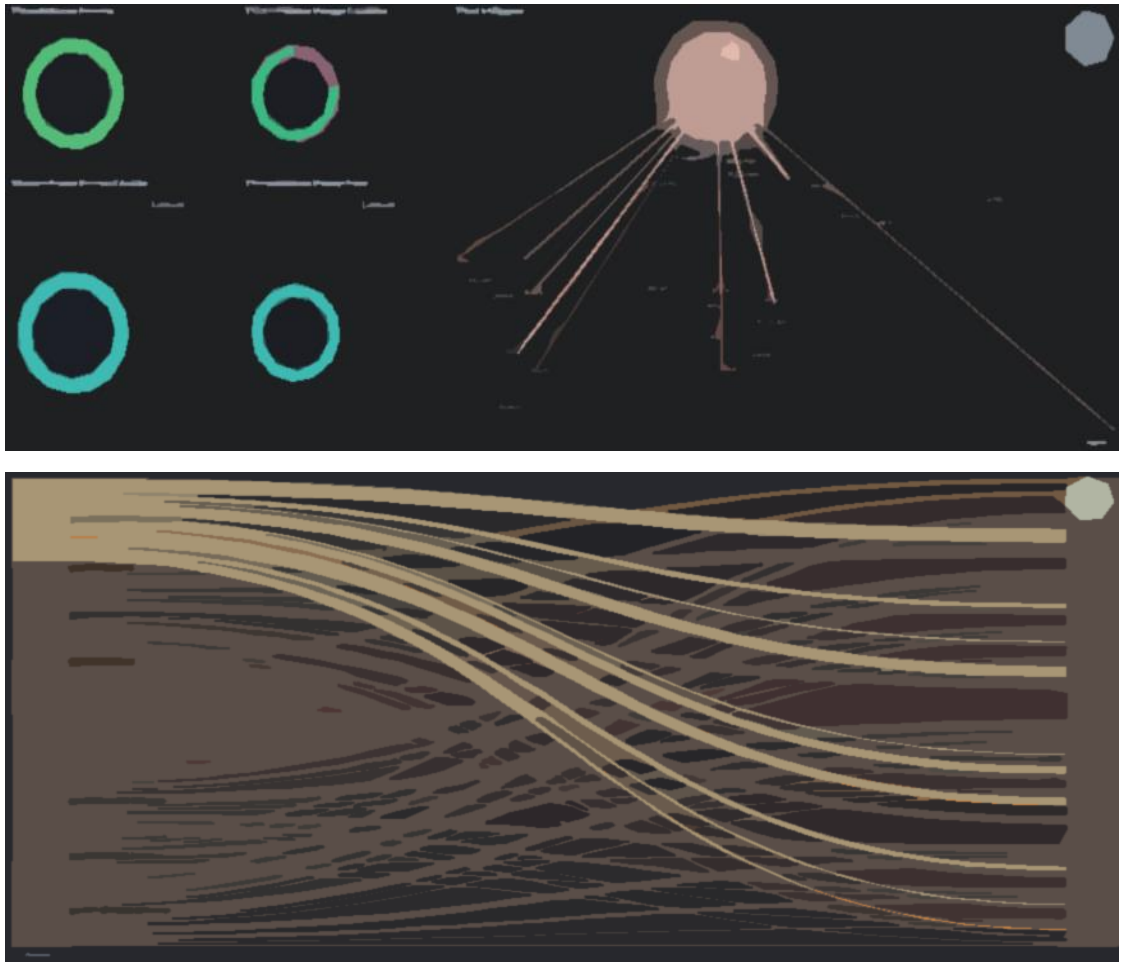
MAP_SRI_For_SM message correctly decoded by the protocol

EXECUTION

Attack Pattern

- Stage 1: Sending SRI-SM with Network responding with varying IMSI.
- Stage 2: Sending SRI-SM with **Global Opcode** network responded real IMSI.
- Stage 3: MSB placed at position “**g**” and “**h**” in the TCAP TAG CLASS set to **Context-specific (10).**
- Stage 4: MSB placed at position “**g**” and “**h**” in the TCAP TAG CLASS set to **Private use (11) .**
- Phase 1 exploitation concluded.

Attack Map

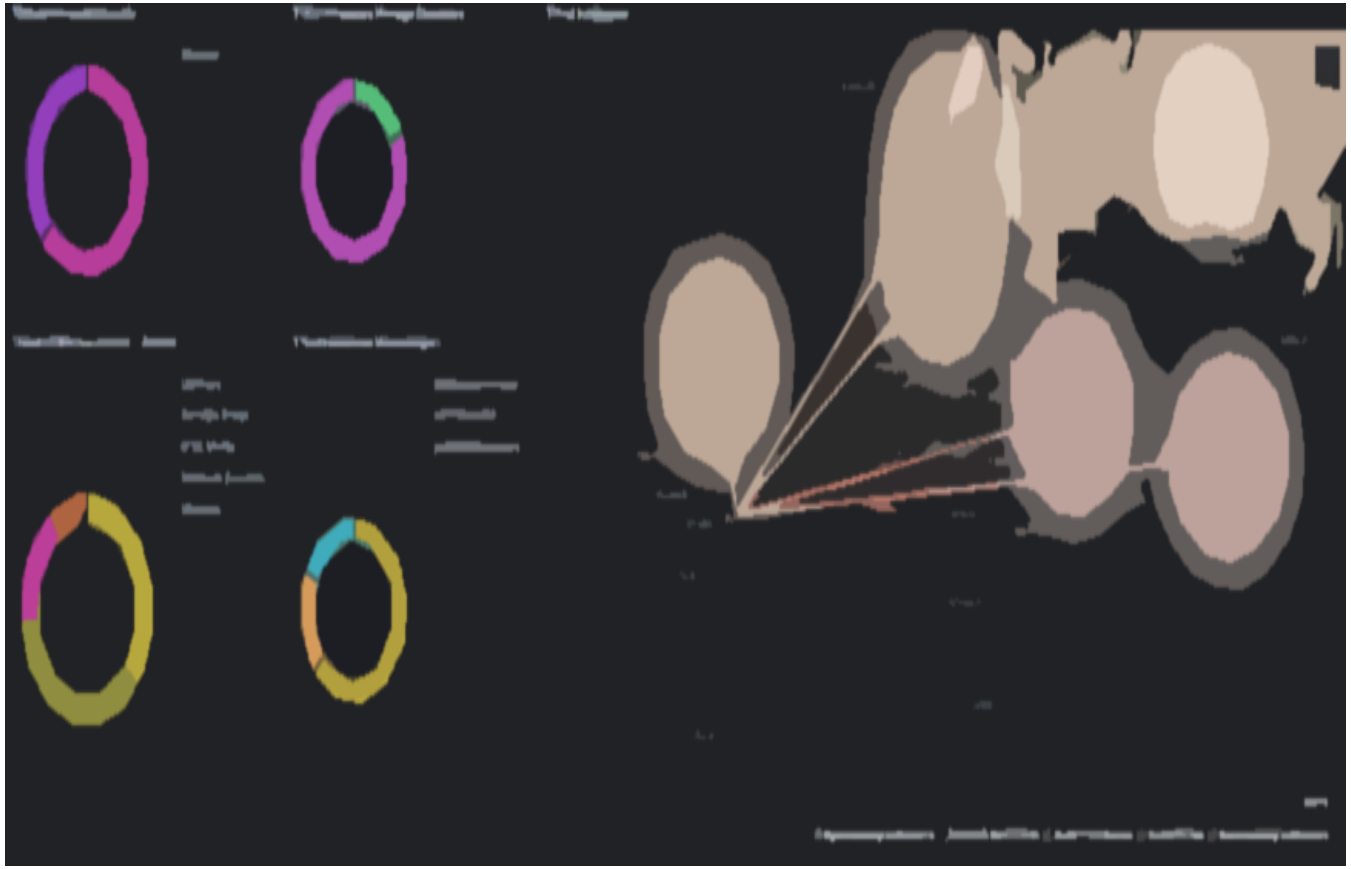


INTELLIGENCE GATHERING

Involved in Cross Protocol Attacks

- Stage 1: **Initial SS7 attack** launched.
- Stage 2: Followed by **Diameter Attack** via S6a on LTE.
- Stage 3: Followed by A “class 0” **silent SMS.**
- Stage 4: Immediately followed by **Binary SMS Attack.**
- Clustered operation : **Cluster-A** executing SS7/SMS attacks and **Cluster-B** Diameter attacks.

Attack Map



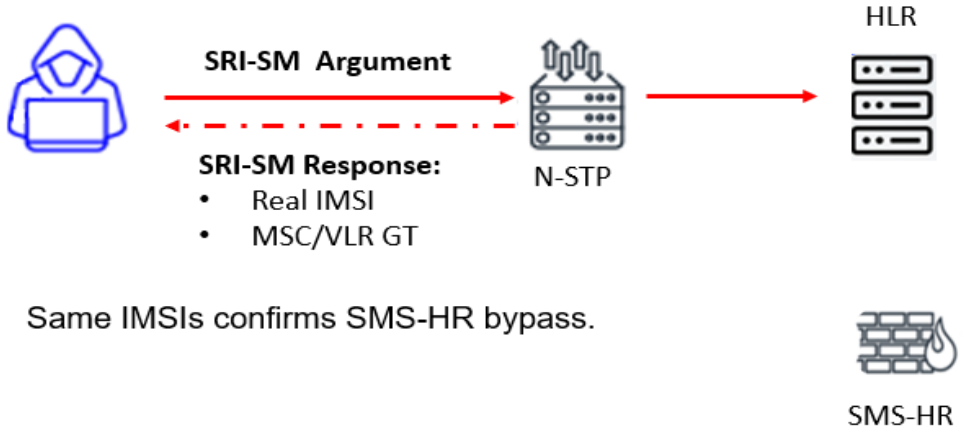
THE IMMINENT THREAT

TCAP TAG CLASS ABUSE

Impact on Mobile Network operators

Confidentiality Impact

- Maps, collects and perform discovery for **network identifiers (MSC/VLR/SGSN) GT's.**



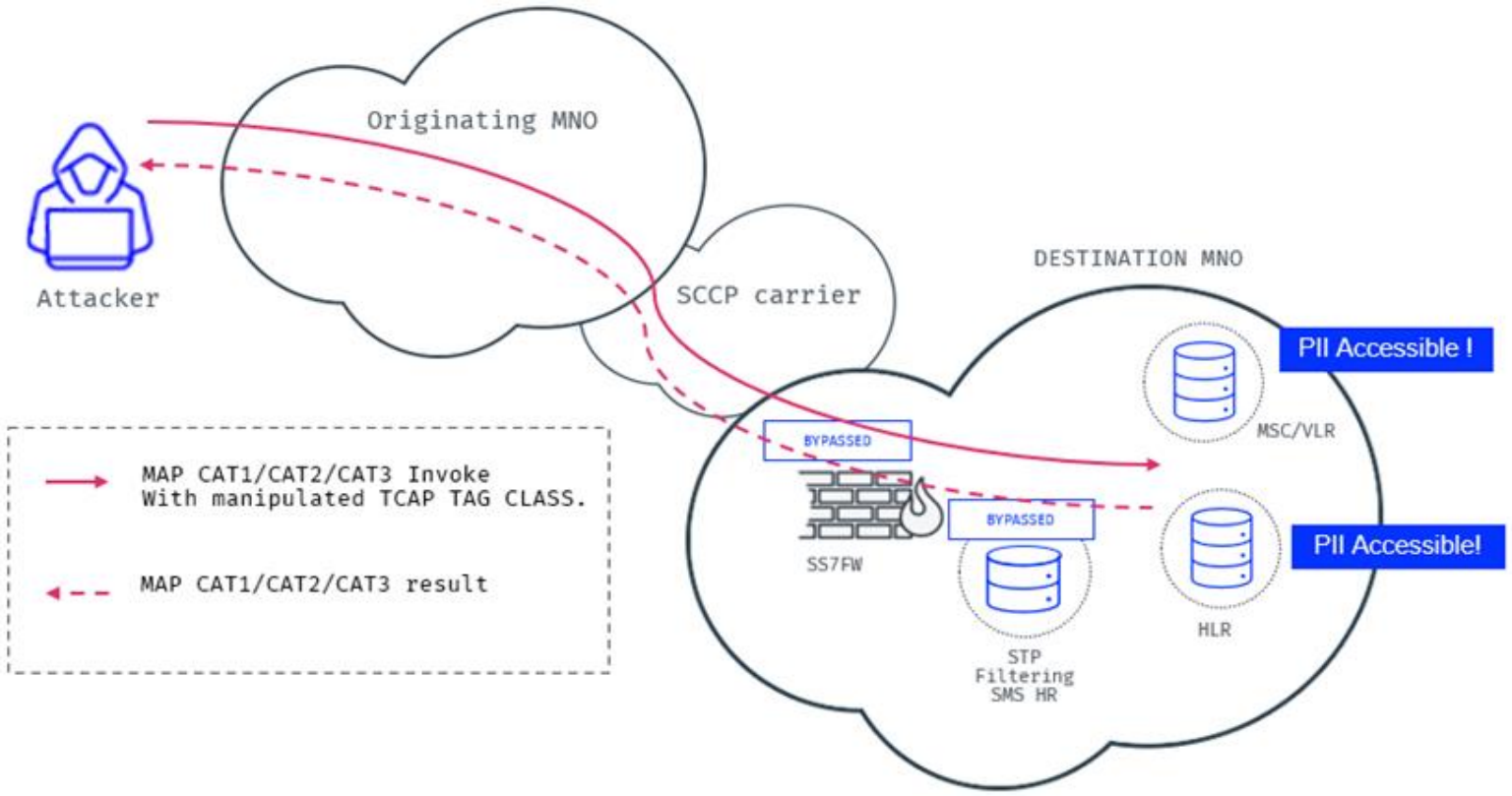
Integrity Impact

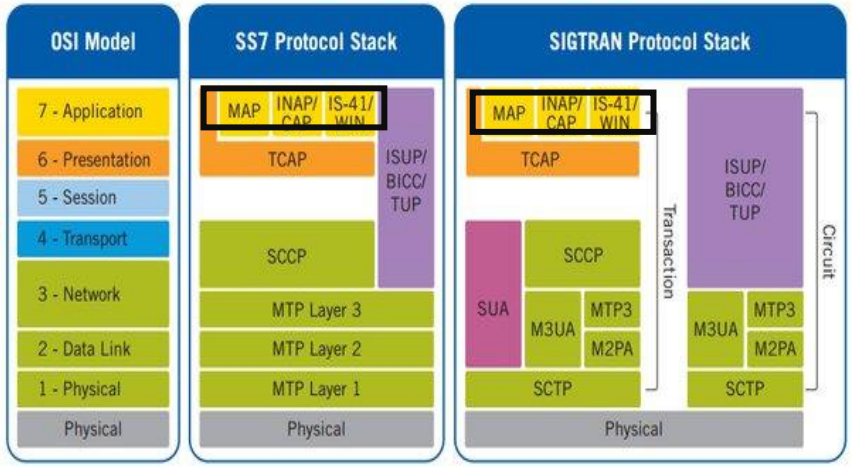
- The subsequent phase can then be used to **corrupt the network node's** (MSC/VLR/SGSN) hosting user profile.

Functional Impact

- The functionality of the HLR/STP has been impacted due to **failure in decoding and bad software stack implementation**.

IMPACT ON SIGNALLING SECURITY VENDORS





- Signaling vendor readiness in handling encoding irregularities.
- Revisit application layer security needs.
- Screen in-consistencies at the encoding layer.
- Building rules and monitor points around anomalous encoding patterns.

Impact on Subscribers

Attack possibilities using TCAP TAG CLASS vulnerability

Confidentiality Impact

- Exfiltration of user data (PII) - (IMSI & MSC/VLR)
- GT of the serving MSC/VLR or SGSN
- Surveillance

Discovered

Integrity Impact

- Call Interception
- Billing fraud
- Account takeover (2FA)

Availability Impact

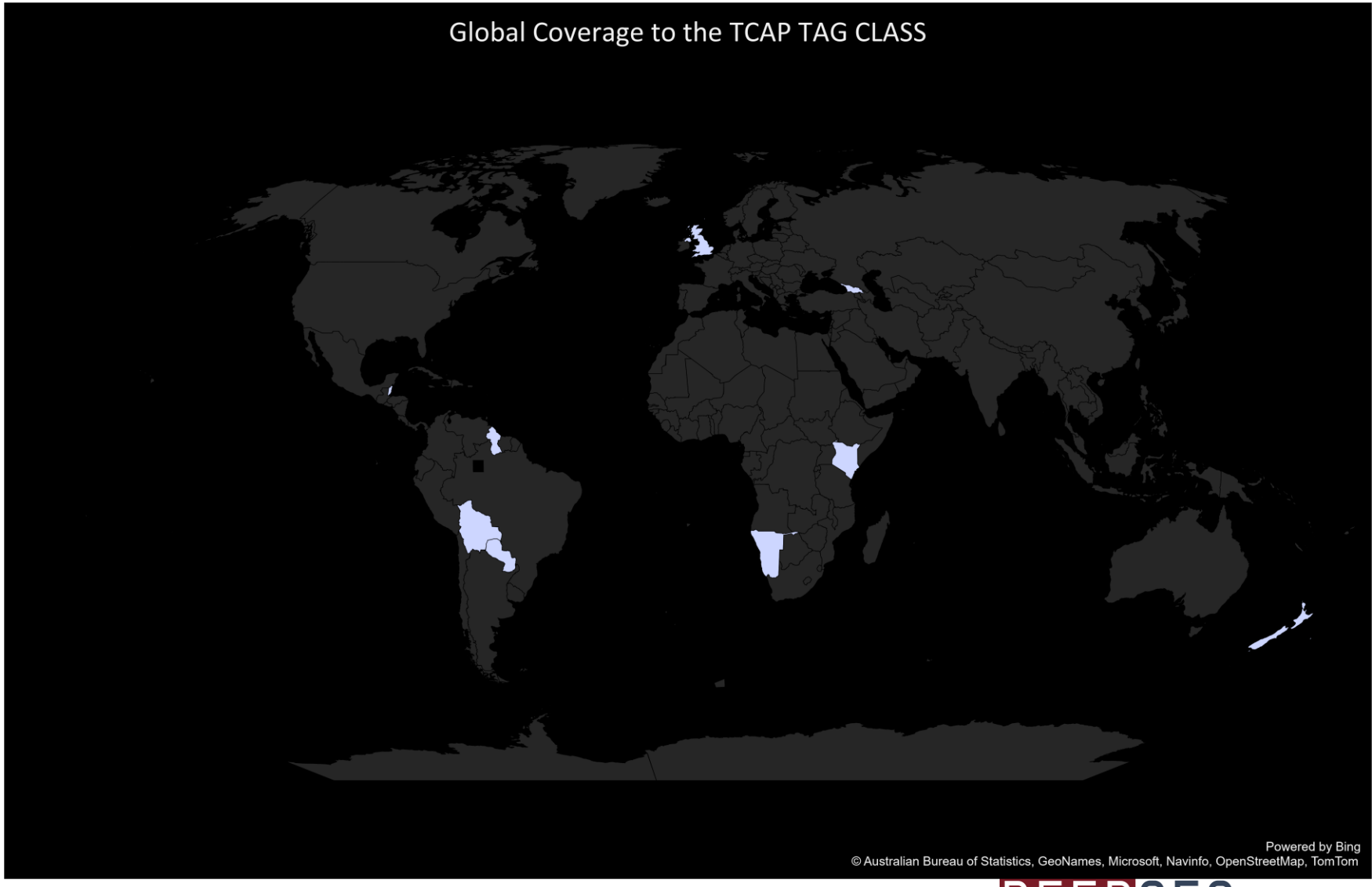
- Subscriber profile manipulation
- Subscriber DoS
- Spam

Potential to be exploited

Quantifying the impact on a global scale

* Multiple operators targeted in a country.

Marked countries* are vulnerable to the TCAP Tag Class vulnerability.



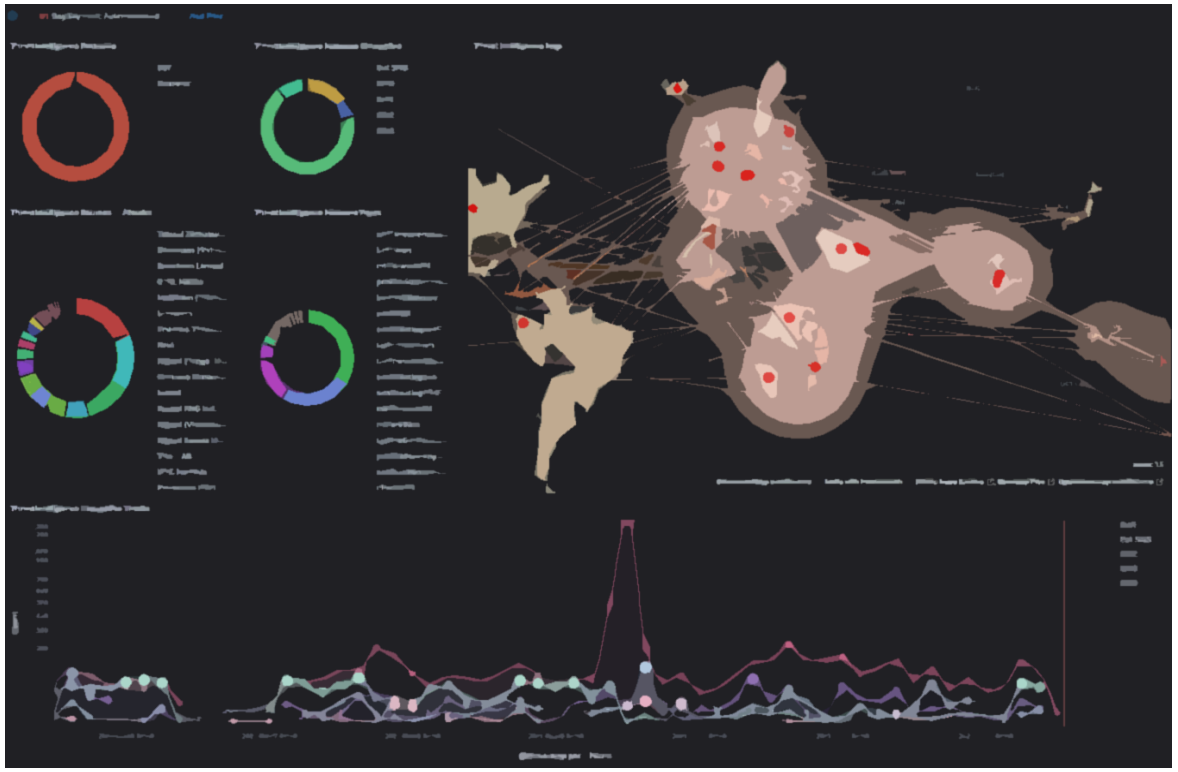
SUMMARY

- **Evidence of source potentially a surveillance group, supported by nation-state.**
- **The use of hosted cloud infrastructure and dispersed globally.**
- **Mobileum's Security Research team has been collecting evidence of new threat indicators.**
- **Large scale attacks in Diameter (4G) with similar sophistication.**
- **An APT identical to NSO, Tykelab has been discovered conducting attacks using Diameter (More on it in next talk).**

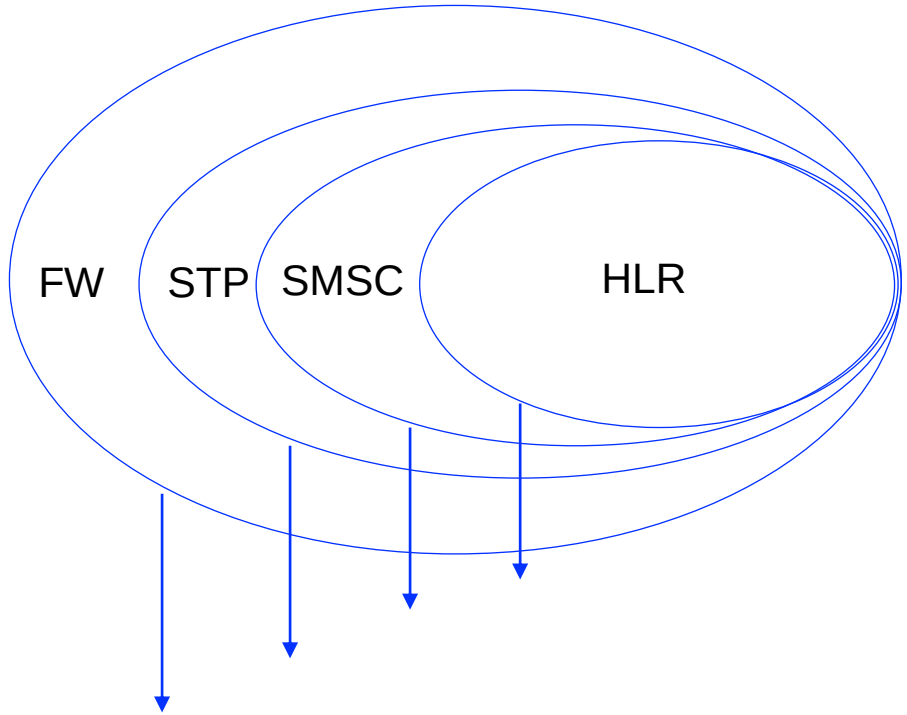
MNO’S CYBER RESILIENCE TO ZERO-DAY EXPLOITS

Global Threat Intelligence an early warning system

- Does local monitoring provide sufficient insights?
- Do firewall EDR’s provide enough data?



Zero trust model for Mobile Operators



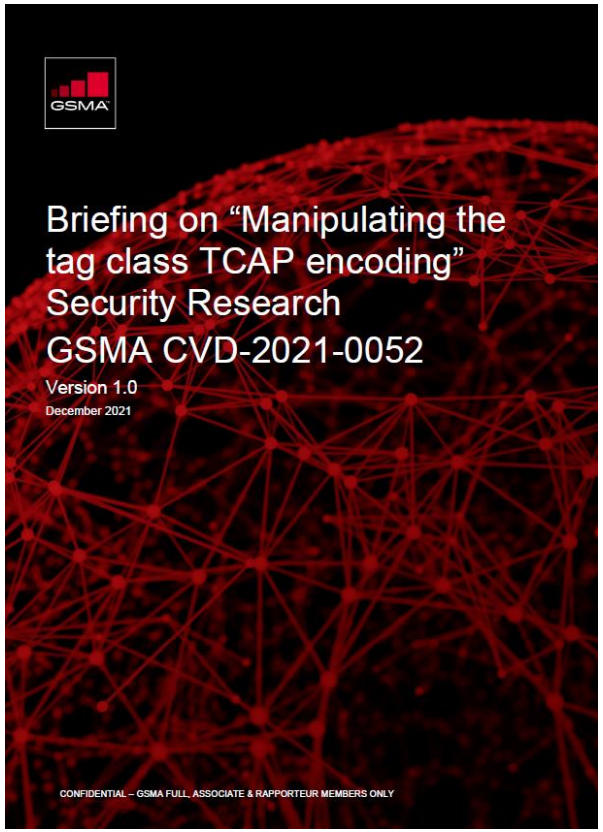
Apply controls at each layer

RECOMMENDATIONS

Actions towards Mobile Operators

- Mobile Operators to reproduce this vulnerability in their labs.
- Edge firewall should look at the full TCAP encoding patterns.
- Operators should consider adapting to the global threat intelligence services.

Coordinated Vulnerability Disclosure



https://www.gsma.com/security/gsma-mobile-security-research-acknowledgements/

What further actions can be taken?

- **Move away from check-box security-based approach.**
- **Security guidelines are not a measure of absolute security.**
- **Introduction to continuous security monitoring.**
- **Operators to enable themselves with a mindset of Global Threat Intelligence.**
- **Regular Penetration testing should be conducted to maintain a robust security posture.**

THANK YOU

Q & A