UKNOF(51)

” WEAPONIZING MOBILE INFRASTRUCTURE”

Are Politically Motivated Cyberattacks
a Threat to Democracy?

mobileum
Action driven by intelligence

security intelligence
Mobileum platform

Lead Security Architect/Researcher

Imran Saleem

AGENDA

1 Role of Cyber attacks in armed conflicts

2 The Missed Intel

3 Political shift can drive cyber-attacks

4 The Financial Impact

5 Work Ethics & Disclosure

6 Recommendations

ROLE OF CYBER ATTACKS IN ARMED CONFLICTS

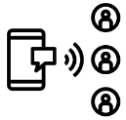
WHY CYBER WARFARE PLAYS A KEY ROLE IN ARMED CONFLICTS?

Espionage : Monitoring other countries to steal state secrets.

Sabotage : Hostile governments or terrorists may steal information or destroy it.

D/DoS : Prevent users from accessing legitimate service.

Electrical Grid or ICS: Attacking the power grid allows attackers to disable critical systems.



Propaganda : Attempts to control the minds and thoughts of people living in or fighting for a target country

Economic Disruptions : Attacking financial institutions or manipulating the stocks.

Historical Outlook to politically motivated Cyberattacks?

Nation state a phenomenon existed in past.

Target	*Attack*	*Attribution*
Estonia 2007	DDoS attacks on online services of banks, media outlets, and government bodies	Russia (state-sponsored groups)
Georgia 2008	Combined cyber and kinetic attack DDoS attacks on Georgian government websites, i.e. the president's website	Russia (state-sponsored groups)
Iran 2010	The Stuxnet worm attacked numerous centrifuges in Iran's Natanz uranium enrichment facility and caused physical destruction on the equipment controlled by the infected computers	The US and Israel (state actors)
WannaCry 2017	Ransomware attacks brought down numerous computer systems worldwide	North Korea (state-sponsored groups)
NotPetya 2017	Ransomware attacks brought down numerous computer systems worldwide	Russia (state-sponsored groups)

Sources: McAfee (2020); McGuinness (2017); Smith (2014); Ransomware Task Force (2021).

“THE MISSED INTEL”

“U.S” withdrawal from “AF”

TIMELINE OF U.S. WITHDRAWAL FROM AFGHANISTAN –REFLECTION

A geopolitical event leads to patterns captured on the global threat landscape which can provides useful insights on these developing situations.

Trump Strikes a Deal

Feb. 29, 2020 — U.S. and Taliban sign an agreement that sets the terms for a U.S. withdrawal from Afghanistan by May 1, 2021,

Biden Follows Through

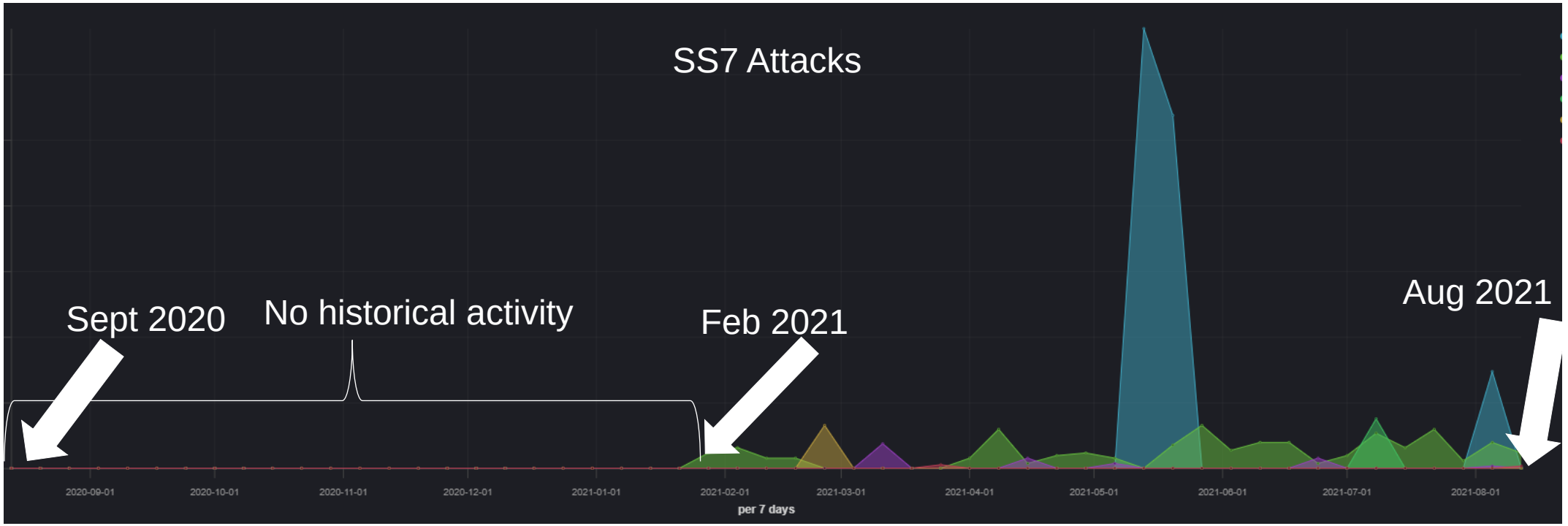
April 14 ,2021— Saying it is "time to end the forever war," Biden announces that all troops will be removed from Afghanistan by Sept. 11.

https://www.factcheck.org/2021/08/timeline-of-u-s-withdrawal-from-afghanistan/

U.S. WITHDRAWAL FROM AFGHANISTAN – A GLIMPSE OF INTELLIGENCE

Key Artifacts:

- Afghanistan was never prime target based on historical investigations.
- Malicious activities started to appear in Feb 2021 due to the political events and administrative changes closely aligns to April 2021
- The threat actor behind these operation are nefariously known and potentially have links to Nation state.
- Supported by a few other unresolved sources with the same origin.
- These sources were clustered.



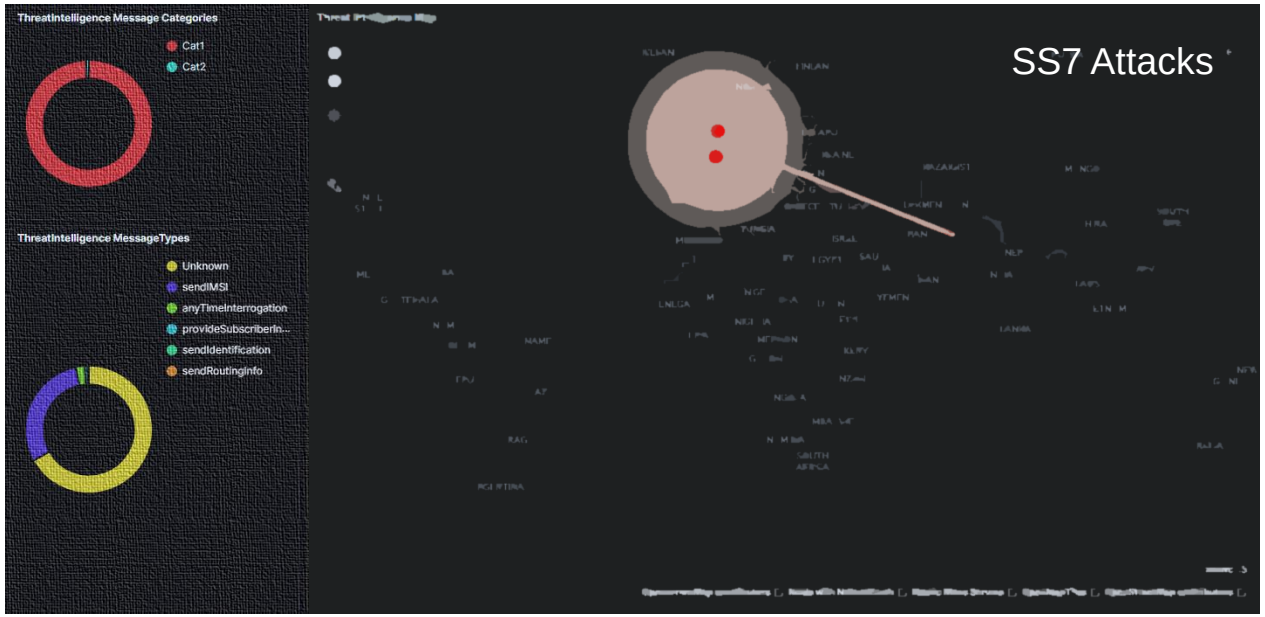
U.S. WITHDRAWAL FROM AFGHANISTAN – MOTIVE & TARGETS

Targets

- Prime targets : AF
- Secondary targets : Roamers in AF (Few from NATO Countries)

Potential victim Organization could be:

- News and Media
- NGO's
- Government Institutions



Motive

- IMSI Gathering and Network discovery
- Users Surveillance and tracking
- Potential communication interception at radio level.

Threat Indicators

- Bypass security controls (If any)

POLITICAL SHIFT IN A REGION CAN DRIVE CYBER-ATTACKS!

IS “UA” – “RU” CONFLICT ANY DIFFERENT THAN “AF”.

Russia hacked Ukrainian satellite communications, officials believe

25 March 2022

Russia-Ukraine war

Russia hacked Ukrainian satellite communications, officials believe - BBC News

Ukraine war: Major internet provider suffers cyber-attack

28 March 2022

Russia-Ukraine war

Ukrtelecom is geographically the biggest fixed internet provider in Ukraine

Ukraine war: Major internet provider suffers cyber-attack - BBC News

- **Organized and coordinated.**
- **Consistent and motivated.**
- **Intel sharing is the key.**

Does Telecom industry have a concrete intel sharing framework?

Russia's war on Ukraine: Timeline of cyber-attacks (europa.eu)

Russia-linked cyberattacks on Ukraine
A timeline

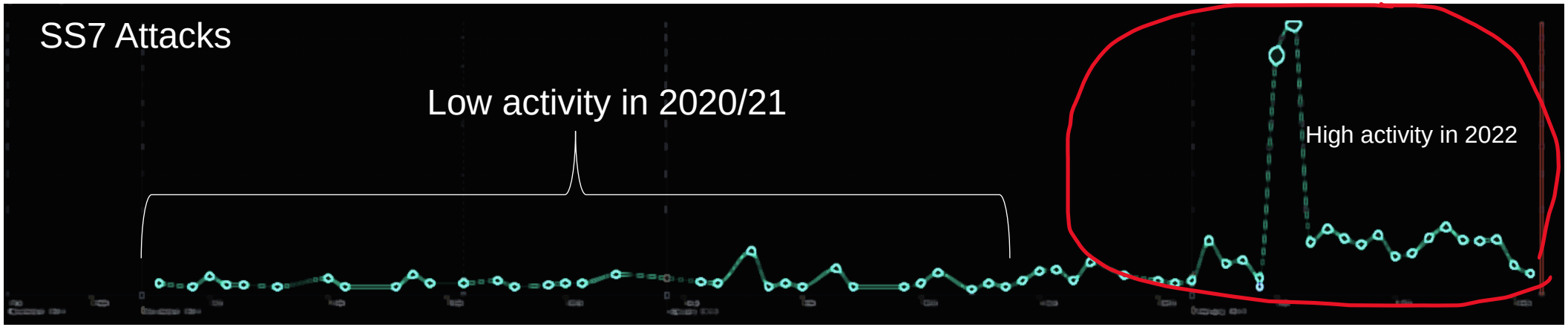
- 9/5 Distributed denial-of-service (DDoS) attack aimed at filtering and re-routing online traffic to Russian-occupied Ukrainian territories.
- 7/5 Cyberattack against Odesa City Council in parallel to missile attack against Odesa's residential areas.
- 22/4 Cyberattack on Ukraine's national postal service.
- 19/4 Ukrainian citizens' payment data accessed via social media page survey.
- 14/4 Public banking data accessed via Trojan malware.
- 8/4 Attempt to interrupt power stations.
- 7/4 Hackers steal media and government entities' user credentials.
- 2/4 Hackers steal Ukrainian government officials' user credentials.
- 30/3 MarsStealer plunders Ukrainian citizens and organisations' user credentials.
- 28/3 Cyberattacks against Ukrtelecom and WordPress websites.
- 20/3 LoadEdge backdoor used to install surveillance software.
- 18/3 Phishing emails target several organisations.
- 17/3 Phishing emails target Ukrainian government and military.
- 16/3 Hacked TV station Ukraine 24 falsely reports that President Zelenskyy has called on the population to surrender.
- 14/3 CaddyWiper malware infiltrates several Ukrainian organisations' computer systems.
- 9/3 Cyberattack on a telecommunications service provider.
- 7/3 Phishing attacks against citizens and government services.
- 4/3 Malware launched against non-governmental, charity and aid organisations.
- 28/2 Attacks on Ukraine's digital infrastructure disable access to financial and energy resources.
- 25/2 IssacWiper attack against government websites and a cyberattack aimed at a border check-point.
- 24/2 Attack against the KA-SAT satellite network facilitates Russian invasion.
- 23/2 Government websites targeted, and the HermeticWiper malware impacts financial, IT and aviation sector organisations.
- 15/2 DDoS attack disables Ukrainian government, banks and radio websites for several hours.
- 14/2 Hackers display 'Wait for the worst' message on 70 government websites.
- 13/2 Microsoft reports the existence of malware targeting the Ukrainian government and several non-profit and information technology organisations.

- March 2014 DDoS attack aims at destabilising Ukrainian computer networks and communications, diverting attention from Russian troop operations in Crimea.
- May 2014 Pro-Russian hacktivist group carries out a series of cyberattacks to manipulate voting in Ukraine presidential elections (malware was removed but the election count was delayed).
- December 2015 DDoS attack affects call centres and the network of three energy distribution companies, causing power outages for over 230 000 consumers.
- January 2016 Disruptions in a Kyiv substation result in a one-hour power blackout.
- June 2017 NotPetya malware hits Chornobyl nuclear power plant and infects multiple government and financial institutions, postal services, newspapers, transport infrastructure and businesses.
- July 2018 Attempted cyberattack on Auly chlorine distillation station, which serves 23 Ukrainian provinces.
- February 2021 Attempted cyberattack targets Ukraine's security service websites.

2022

UNDERSTANDING RUSSIAN SIGNALLING ACTIVITIES

In 2022, Russia sources intensified the activities by up to 150 times comparing to 2020/21 historical records.



- **These activities were supported by malicious threat indicators known to potentially bypass security controls.**
- **Known techniques listed in the FS.11 few others not available in the guidelines.**
- **Key fact “fuzzing executed targeting various networks.”**

UNDERSTANDING THE “RU” BACKED STATE ACTORS

Key behavioural characteristics and threat landscape

- Is Ukraine and NATO countries on the only target = NO
- Attack Intensity = High
- Coverage = Extreme
- Current state = Active
- Targeting inbound roamers in NATO countries
- Clustered group
- Zero-day exploit = Observed (CVD Submission)
- Account takeover
- Identity spoofing
- Fuzzing
- Roughly 60+ countries were targeted.

ARE THESE “APT’S”, GOVERNMENT-BACKED ATTACKERS?

Russian attackers aggressively pursue wartime advantage in cyberspace using global signalling.

Threat Intelligence team has uncovered set of attacks targeted towards Ukrainian and NATO countries with following objectives.

Attacks Involved	Unresolved Russian Origins	Targeted Nations
Network Discovery	Mapping the network topologies through scanning	• Ukraine • NATO Countries • Middle east • Africa
Information gathering	IMSI extractions and profile extractions.	
Location tracking	Performing surveillance on targeted victims.	
Hostile registrations	Hostile location updates made to potentially intercept the comms.	
Account takeover	Social media accounts taken over.	
Fraud	Financial fraud observed several other cases.	

RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – RECON AND TARGETED SCANNING

Massive scale scan to discover and map networks.

Multiple networks and countries were scanned. Sequential network identifiers.

No.	Time	Protocol	Length	Calling Party Digits	Transaction Id	SubSy	Called Party Digits	SubSy	info	opCode	application-context-name
271	202…	TCAP	166		30	MSC…	37	HLR…	Begin otid(	30)	shortMsgGatewayContext-v3
272	202…	TCAP	166		30	MSC…	37	HLR…	Begin otid(	30)	shortMsgGatewayContext-v3
273	202…	TCAP	166		31	MSC…	46	HLR…	Begin otid(	31)	shortMsgGatewayContext-v3
274	202…	TCAP	166		31	MSC…	46	HLR…	Begin otid(	31)	shortMsgGatewayContext-v3
275	202…	TCAP	166		32	MSC…	52	HLR…	Begin otid(	32)	shortMsgGatewayContext-v3
276	202…	TCAP	166		32	MSC…	52	HLR…	Begin otid(	32)	shortMsgGatewayContext-v3
277	202…	TCAP	166		33	MSC…	54	HLR…	Begin otid(	33)	shortMsgGatewayContext-v3
278	202…	TCAP	166		33	MSC…	54	HLR…	Begin otid(	33)	shortMsgGatewayContext-v3
279	202…	TCAP	166		34	MSC…	95	HLR…	Begin otid(	34)	shortMsgGatewayContext-v3
280	202…	TCAP	166		34	MSC…	95	HLR…	Begin otid(	34)	shortMsgGatewayContext-v3
281	202…	TCAP	166		35	MSC…	10	HLR…	Begin otid(	35)	shortMsgGatewayContext-v3
282	202…	TCAP	166		35	MSC…	10	HLR…	Begin otid(	35)	shortMsgGatewayContext-v3
307	202…	TCAP	166		40	MSC…	39	HLR…	Begin otid(	40)	shortMsgGatewayContext-v3
308	202…	TCAP	166		41	MSC…	53	HLR…	Begin otid(	41)	shortMsgGatewayContext-v3
311	202…	TCAP	166		42	MSC…	61	HLR…	Begin otid(	42)	shortMsgGatewayContext-v3
310	202…	TCAP	166		43	MSC…	26	HLR…	Begin otid(	43)	shortMsgGatewayContext-v3
309	202…	TCAP	166		44	MSC…	53	HLR…	Begin otid(	44)	shortMsgGatewayContext-v3
312	202…	TCAP	166		45	MSC…	04	HLR…	Begin otid(	45)	shortMsgGatewayContext-v3
313	202…	TCAP	166		46	MSC…	83	HLR…	Begin otid(	46)	shortMsgGatewayContext-v3
314	202…	TCAP	166		47	MSC…	76	HLR…	Begin otid(	47)	shortMsgGatewayContext-v3
283	202…	TCAP	166		48	MSC…	07	HLR…	Begin otid(	48)	shortMsgGatewayContext-v3
284	202…	TCAP	166		48	MSC…	07	HLR…	Begin otid(	48)	shortMsgGatewayContext-v3
285	202…	TCAP	166		49	MSC…	04	HLR…	Begin otid(	49)	shortMsgGatewayContext-v3
286	202…	TCAP	166		49	MSC…	04	HLR…	Begin otid(	49)	shortMsgGatewayContext-v3

Sequential and incremental session ID

RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – IDENTITY IMPERSONATION

Identity impersonation for social application through account takeover.

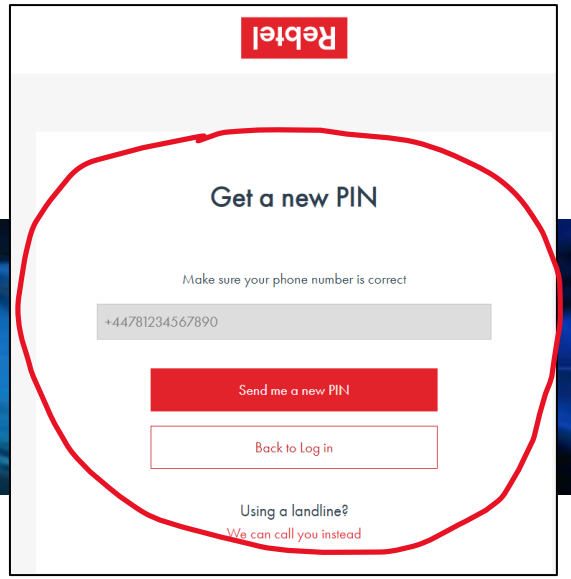
No.	Time	Protocol	Length	Calling Party Digits	Trans	SubSy	Called Party Digits	SubSy	info	opCode	application-context-name	localValue
232	202…	GSM MAP	198	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue	infoRetrievalContext-v3	sendAuthenticationInfo
233	202…	GSM MAP	198	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue	infoRetrievalContext-v3	sendAuthenticationInfo
234	202…	GSM MAP	218	7	19…	VLR…	2	HLR…	invoke updateLocation	localValue	networkLocUpContext-v3	updateLocation
235	202…	GSM MAP	218	7	19…	VLR…	2	HLR…	invoke updateLocation	localValue	networkLocUpContext-v3	updateLocation
238	202…	GSM MAP	350	2	00…	HLR…	7	VLR…	invoke insertSubscriberData	localValue	networkLocUpContext-v3	insertSubscriberData
239	202…	GSM MAP	350	2	00…	HLR…	7	VLR…	invoke insertSubscriberData	localValue	networkLocUpContext-v3	insertSubscriberData
240	202…	GSM MAP	150	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue		sendAuthenticationInfo
241	202…	GSM MAP	150	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue		sendAuthenticationInfo
244	202…	GSM MAP	150	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue		sendAuthenticationInfo
245	202…	GSM MAP	150	7	dd…	VLR…	2	HLR…	invoke sendAuthenticationInfo	localValue		sendAuthenticationInfo
250	202…	GSM MAP	350	2	00…	HLR…	7	VLR…	invoke insertSubscriberData	localValue		insertSubscriberData
251	202…	GSM MAP	350	2	00…	HLR…	7	VLR…	invoke insertSubscriberData	localValue		insertSubscriberData
256	202…	GSM SMS	354	2	16…	MSC…	7	MSC…	invoke forwardSM	localValue	shortMsgMT-RelayContext-v2	mo-forwardSM
257	202…	GSM SMS	354	2	16…	MSC…	7	MSC…	invoke forwardSM	localValue	shortMsgMT-RelayContext-v2	mo-forwardSM

Hostile Registration

Home network shares user profile to malicious source

2FA token access

```
TP-Originating-Address - (INFOSMS)
    Length: 13 address digits
    1... .... = Extension: No extension
    .101 .... = Type of number: Alphanumeric (coded according to 3GPP TS 23.038 GSM 7-bit default alphabet) (5)
    .... 0000 = Numbering plan: Unknown (0)
    TP-OA Digits: INFOSMS
TP-PID: 0
TP-DCS: 0
TP-Service-Centre-Time-Stamp
TP-User-Data-Length: (152) depends on Data-Coding-Scheme
```



- Social Application account takeover
- Input Required : Phone number
- Not linked to email.

RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – IDENTITY SPOOFING

How we back our statement that these are nation backed activities.

No.	Time	Protocol	Length	Calling Party Digits	Trans	Message Type	SubSys	Called Party Digits	SubSys	info	opCode	application-context-name	localValue
1	202…	GSM SMS	283	3	00…	Unitdata	MSC …		MSC …	invoke forwardSM	localValue		mo-forwardSM

SCCP layer Spoofed Identity

Spoofed E.164 numbering plan doesn't belong to any of Operators that owns these low layer identities

```
Message Transfer Part Level 3
  > Service information octet
  v Routing label
    > .... .... .... .... ..01 0110 0101 0011 = DPC:
    v .... 1000 0011 0011 11.. .... .... .... = OPC:
        Signalling Area Network Code (SANC): Afghanistan
        Unique Signalling Point Name:
        Signalling Point Operator Name:
      0000 .... .... .... .... .... .... .... = Signalling Link Selector: 0
```

Low layer Spoofed Identity

```
Message Transfer Part Level 3
  > Service information octet
  v Routing label
    > .... .... .... .... ..10 1111 0000 1011 = DPC:
    v .... 1000 0111 1000 01.. .... .... .... = OPC:
        Signalling Area Network Code (SANC): United Arab Emirates
        Unique Signalling Point Name:
        Signalling Point Operator Name:
      0000 .... .... .... .... .... .... .... = Signalling Link Selector: 0
```

Low layer Spoofed Identity

Link Level analysis revealed traffic initiated via Russian operator

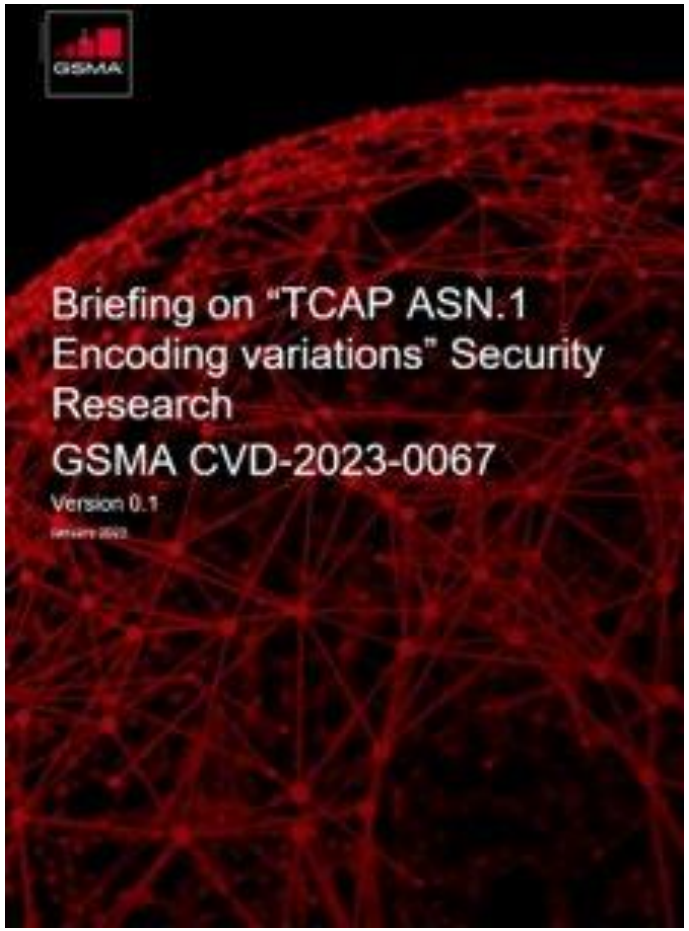
RUSSIAN INFLUENCE IN GLOBAL SIGNALIZATION – ZERO-DAY EXPLOITS

Coordinated Vulnerability Disclosure

- CVD submitted and under final review.
- Plans to releases the briefing paper by Q1 2023.

Actions towards Mobile Operators

- Mobile Operators are requested to reproduce this vulnerability in their labs once the briefing paper is published.



“THE FINANCIAL IMPACT”

Financial loss towards operators for zero-day exploit!

The Mobileum Threat Intelligence team discovered a new vulnerability back in early April 2021

General Details	
Operator(s)	Unknown
Date of Threat	2021/03/31- 2021/04/01
Date of Reporting	2021-04-09
Threat Originating Network	SCCP Calling GT prefixes: Unknown:
Threat Originating Node(s)	SCCP Calling GTs: Unknown:
Protocol	SS7, MAP, SMS
Messages	PDU_SS7_MAP_sendRoutingInfoForSM , PDU_SS7_MAP_mo-forwardSM, PDU_SS7_MAP_mt-forwardSM

A global operator group reported a fraud incident between April and Nov 2021 that exploited that vulnerability

FRAUD INCIDENT: DETAILS	
Dates of fraud incident/s:	*April to November 2021*
Estimated Loss in US$:	*$48K in 12 days*
How fraud committed. Method of fraud – what did they do? Attached diagrams on separate page if required.	*An affiliate was victim of SMS Firewall Bypass where the fraudsters manipulated the SMS signaling while hiding behind a leased GT.* *The SMS signaling manipulation allowed the SRI-for-SM message to be routed directly to the HLR instead of the SMS Firewall and involved manipulating the TCAP TAG parameter of this message, a technique previously reported: see CVD-2021-0052.*
Details of fraudsters: Any information that may assist another operator to identify the fraudsters	*The GT used to commit this fraud was leased from another affiliate on the pretense that it was required by the national police. We don't know if our affiliate received the GT leasing request from fraudsters who impersonated the authorities or from the legitimate authorities.*

Overall financial impact of this zero-day is not fully known.

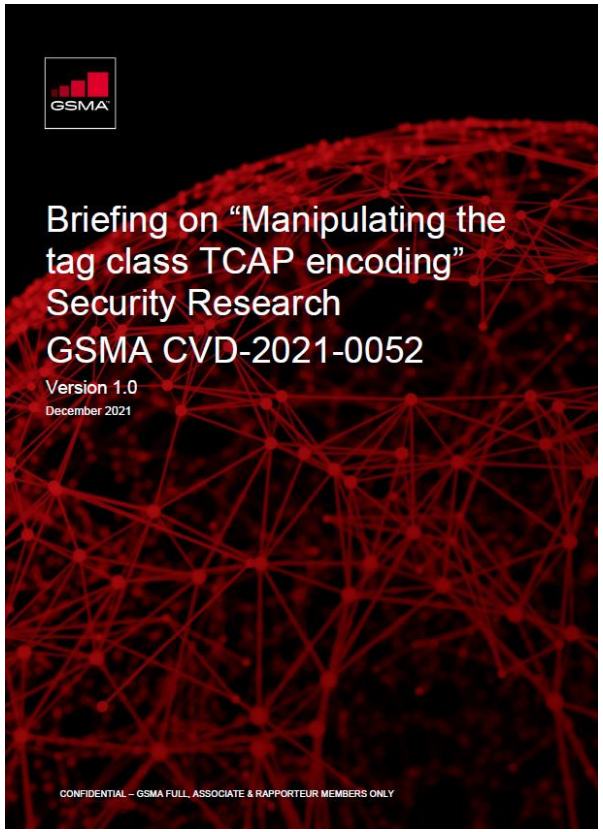
- This can be due to factors like lack of visibility.
- Lack of interest in reporting such incident towards GSMA.

RESPONSIBLE VULNERABILITY DISCLOSURE

Coordinated Vulnerability Disclosure

Actions towards Mobile Operators

- Mobile Operators were requested to reproduce this vulnerability in their labs to assess if controls in places are sufficient.
- Operators should consider adapting to the global threat intelligence services.



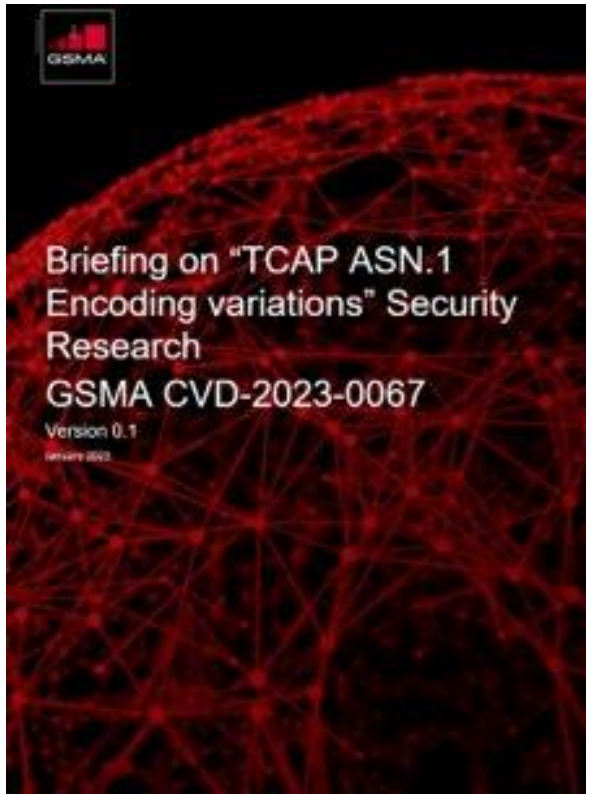
https://www.gsma.com/security/gsma-mobile-security-research-acknowledgements/

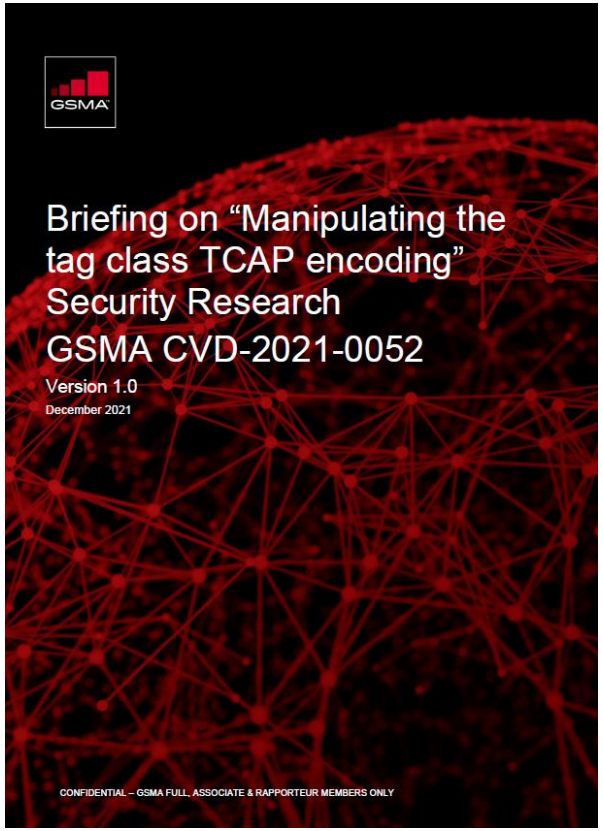
“WORK ETHICS & DISCLOSURE”

WORK ETHICS AND DISCLOSURE

- Share key intelligence gathered through security research back to the Industry.
- Share details on zero day exploits that can avoid security breaches and financial losses.
- Objective driven to secure services offered by operators.

Coordinated Vulnerability Disclosures





What further actions can be taken?

- Industry should learn from enterprise and build a telecom focus intel sharing framework. Like (STIX, TAXI)
- Build and create culture of resilience in an organization.
- Processes are key to the implementation of an effective cyber-safety strategy to handle cyber conflicts.
- Security guidelines are not a measure of absolute security.
- Operators to enable themselves with a mindset of Global Threat Intelligence

THANK YOU

Q & A