FAR FROM HOME – Part 2

Active Foreign Surveillance of US Mobile Users

TECHNICAL SUPPLEMENT AND 2020 ANALYSIS

THREAT INTELLIGENCE REPORT

exigent MEDIA

www.exigentmedia.com

Table of Contents

01

INTRODUCTION

INTRODUCTION

2020 has been a year of many dynamics with espionage and mobile networks. The COVID-19 pandemic has stimulated global attention towards using mobile surveillance domestically to facilitate contact tracing. To this end, options proposed using device-centric approaches led by the Apple and Google alliance while network-based solutions from 3rd parties currently in use have both raised privacy concerns from watchdog organizations and the media. Meanwhile, continued geo-political tensions between China and Russia with the US have resulted in attack trends indicating increased coordination between cyber adversaries and mobile operators around the world. Two things remain clear; first, using mobile networks for the purposes of engaging in espionage continues to be a persistent element in the Signals Intelligence portfolio for criminals and nation-states, and the second is that advances in cyber espionage attack vectors remain constant.

As revealed in the **Far from Home – 2018-2019 Threat Intelligence Report**, data has shown source countries and operators who are either threat actors themselves or at the very least threat enablers who host access to threat actors using public mobile networks. And while the report showed insights related to the exploitation of mobile networks with broad impacts, there is more to the story regarding the execution of the attacks, the approaches used, and the technologies employed in the attacks. More details may assist operators in deploying countermeasures, executing penetration testing scenarios to evaluate countermeasures and encourage disclosures for improved mobile operator accountability and compliance.

Fundamental to the principles of threat intelligence, we are providing insights into the following:

1. **Who** – The threat actor and the victim or target
2. **What** – The objectives of the threat actor who is targeting a victim
3. **How** – The threat landscape and how the threat actor achieves their objectives

This report focuses on the current statistics related to 2020 foreign attacks up to the month of July and includes historic threat perspectives as well as recently new players in the surveillance field of view. We will focus on some of the technical aspects related to current exploits, enhanced visibility into trends, tactics of attack strategies relating to 4G and an update on 5G security implications.

Year over year attack distributions reflected some variations in adversary tactics which can be considered bold approaches to take advantage of the lack of security controls in place at networks globally. In 2018, where China and Caribbean countries conducted surveillance at rates seemingly without regard to detection, 2019 attacks from China Unicom fell below the radar relative to other traditional adversaries. As noted, indications of attack by proxy via foreign operators selling access to their networks were also revealed where China, Barbados and the Bahamas were seen targeting the same mobile users.

2019 also showed an emergence of activity by Mexico and Brazil from April and June respectively and persisted throughout 2019, as well as growth in surveillance sourced from Canada.

2020 however is showing some significant shifts in activity, with new trends and participant network operators. Shifts in attack strategy and for some operators a resumption of traditional 3G attacks reveals insights into geo-political dynamics which have yet to be unraveled.

This report focuses on 2 aspects of mobile surveillance; the first is a deep dive into the technical approaches used by threat actors with examples of trace output from individual operators. The second focus is on 2020 activity and some of the major trends influencing future operations.

KEY THEMES IN 2020

1

3G Attacks Reduce While 4G Attacks Increase – Attacks volumes are increasing on 4G networks, overtaking 3G volumes using fake registration methods. There are many possible reasons, but the main driver is higher success rates with lower barriers to entry.

2

The COVID-19 Pandemic had a Moderate Impact on Surveillance Operations – Reductions in travel and lack of focus showed notable reduction in attack volumes from many operators in early 2020, but then picked up significantly in April-July.

3

New Networks are Entering the Sphere of Mobile Surveillance – While familiar threat actors continue attacks, new networks from Slovakia, Bulgaria, Kazakhstan, Belarus, Montenegro, Cayman Islands, Haiti and multiple African nations are just some of the new countries sponsoring attacks targeting US mobile users.

4

2020 Attacks Almost Entirely Use Advanced Methods – Whereas 2018 and 2019 saw a mix of basic location tracking attacks with communications interception, current surveillance almost entirely uses techniques focused on service interruption and communications interception to achieve objectives.

5

US Neighbor Countries are Becoming Threat Actors – While Mexico is known to engage with network selling and surveillance vendors, attacks from Canada are seen with regularity. This raises concerns of neighbor-in-reconnaissance activity as a potential US surveillance proxy.

02

SURVEILLANCE METHODS AND ATTACKER OBJECTIVES

DENIAL OF SERVICE

COMMUNICATION INTERCEPTION

2020 is showing a significant reduction in basic 3G SS7 attacks designed to obtain user location. This can be attributed to mobile operator improvements in security countermeasures to filter and block these attack messages. However, communication interception and denial of service attacks are still very much in play from traditional surveillance threat actor sources.

2020 has also brought with it many new threat acting networks, changes in adversary attack strategies, and new dynamics related to the COVID-19 pandemic.

New threat actors identified in 2020 mostly used advanced attack techniques involving fake user registration to disrupt and intercept communications. The exceptions are 2 operators Vodafone Turkey and Kar-Tel Kazakhstan from where basic interrogation attacks were seen. Volumes from these new networks in 2020 suggest precise user targeting. In addition, a majority of source countries and mobile networks are relatively small, suggesting a likelihood that the operators are selling access to their networks for the purposes of conducting network surveillance by proxy.

2020 New SS7 Threat Actor Sources – Ranking

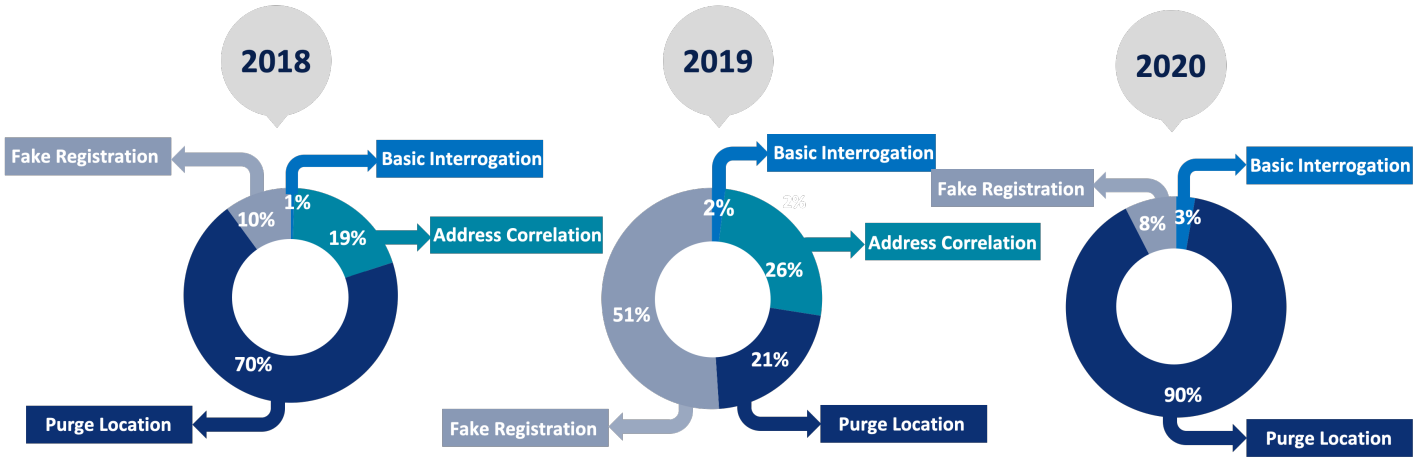
Mobile Operator	Source Country	Attack Volume Distribution
Turk Telecom	Turkey	38.86%
Mobilink PMCL	Pakistan	23.08%
Real Future Co (True Move)	Thailand	7.70%
Pulse Mobile	Guam	5.29%
Telkom Kenya	Kenya	4.83%
Tigo	Rwanda	3.53%
Optus	Australia	3.40%
DTAC	Thailand	1.95%
Mobitel	Sri Lanka	1.18%
Sonatel	Senegal	0.94%
Antel	Uruguay	0.93%
A1 Telekom	Austria	0.87%
Slovak Telecom	Slovakia	0.86%
Vodafone Omnitel	Italy	0.77%
Digi Telecommunications	Malaysia	0.77%
Vitelcom Cellular Innovative Wireless	Virgin Islands	0.59%
Mobile One	Singapore	0.56%
Mtel	Montenegro	0.51%
Cable & Wireless	Cayman Islands	0.50%
NATCOM	Haiti	0.37%
Atheer Telecom (Zain)	Iraq	0.35%
Kar-Tel	Kazakhstan	0.25%
M-Tel (Mobitel EAD)	Bulgaria	0.23%
Life - Belarussian Telecom Network	Belarus	0.20%
Airtel Congo	Congo	0.20%
Hormuud Telecom	Somalia	0.17%
HOT Mobile	Israel	0.15%
Orange	Jordan	0.14%
Turkcell	Turkey	0.13%
SK Telecom	South Korea	0.13%
JMTS (Zain)	Jordan	0.13%
Claro	Puerto Rico	0.12%
Vodafone	Turkey	0.12%
Cyprus Telecommunications (CYTA)	Cyprus	0.11%
Entel	Chile	0.10%

Advanced Attack Techniques and Trends

While the shift from basic to advanced attacks during 2020 was expected, mobile operator network security posture generally follows guidelines set forth by the GSMA FASG (Fraud and Security Working Group). By examining these guidelines relative to attack trends, we can view the ongoing efficacy of strategies employed by threat actors and how we expect them to evolve during 2020.

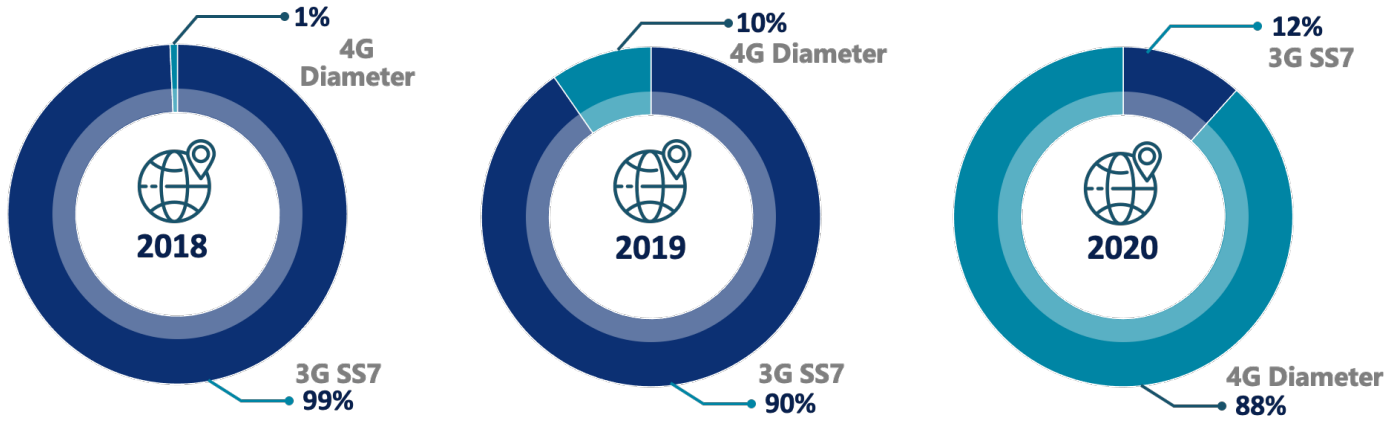
As mentioned previously, basic attacks target vulnerabilities using SS7 messages such as ATI (AnyTimeInterrogation) and others (PSI, PSL, SRIforLCS) from roaming partners and countries where the mobile user is not currently located. Other methods which use advanced techniques attempt to purge the user from the network or falsify the device identity to alter the user's network location.

Following is the distribution by 3G attack methods over the 2018-2020 time period.



The changing distribution of attack patterns between 2018 and 2020 are mainly attributed to the methods used by the aggressive threat actors in 2018 whose activity then dropped in 2019. This includes China and Palestine using the Purge Location technique. Activity then picked up in mid 2020 mainly from China, Canada and Mexico, shifting the distribution back to Purge Location attacks.

The 3G-4G attack distribution is also telling. Whereas 3G attacks in 2018 took the form of mass surveillance attempts and 4G network attacks were rare, 2019 showed a gradual shift toward 4G as the preferred vector of attack. Moving into 2020, we see 4G attacks as dominant against US devices.

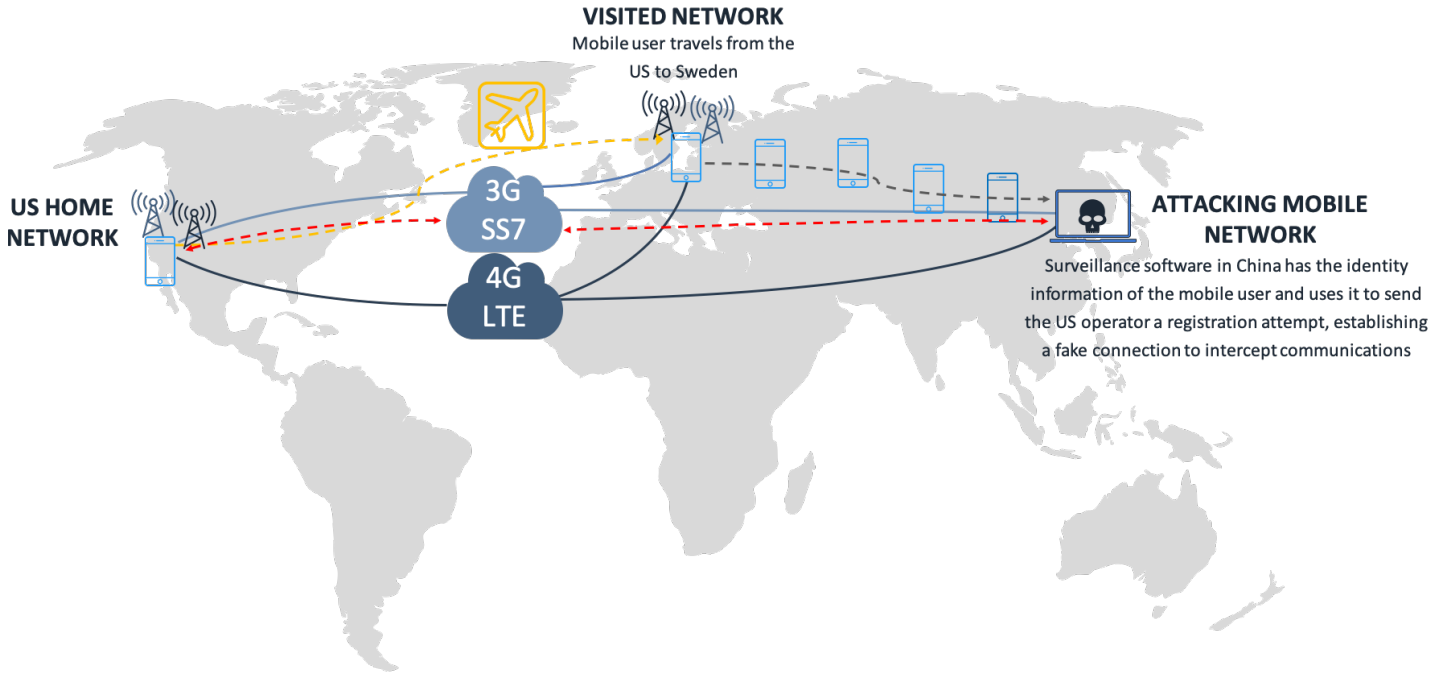


Conclusions

Taking into account that a majority of attacks sought to engage in the communications of the target, both Fake Registration (Intercept) and Purge Location (DoS to Intercept) methods are most popular. Immediate measures should be taken to detect the source of the attacking SS7 Global Title (GT) address and 4G MME and prevent these transactions where user location is mismatched. Operators should identify suspicious foreign network sources to enhance the effectiveness of countermeasures.

Attack Examples – SS7 Communication Interception

In the **Far from Home – 2018-2019 Threat Intelligence Report**, an overview of advanced attacks was discussed as a significant threat in terms of enabling access to potentially highly sensitive mobile communications. The use case in that report discussed a scenario of a fake registration attack where the device identity is used to latch on to a foreign network where the threat actor has software to emulate core network components such as VLR, HLR, SGSN or SMSC. Essentially, any foreign network component involved in communicating with the home network in the US can be emulated through this software. The impersonation removes the target phone from their current network connection and establishes a new connection on the attacker network, thus allowing the attacker to send and receive communications on behalf of the victim. Let's take another look at how this process works and then show some trace examples of this in a live setting.



In the above scenario where a US mobile user is traveling to Stockholm, Sweden the user turns on their phone and registers onto the Telenor Sweden mobile network. The threat actor becomes aware of a target user traveling in Sweden. The threat actor then uses a network GT address from the China Unicom mobile network to conduct the attack with an objective of intercepting communications of the victim. At this point, the attacker software performs the following actions:

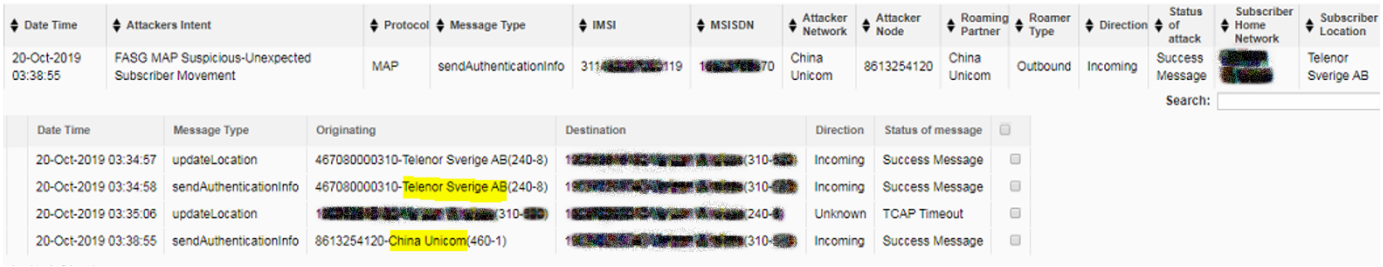
1. Send false **SendAuthenticationInformation (SAI)** message using SS7 from a China Unicom SS7 Global Title using the IMSI of the target device to the US home network HLR to intiate the authentication procedure of the phone.
2. Send an **UpdateLocation (UL)** message to complete the fake registration process. The US home network now believes that the user is located in China, routing all communications associated with the target's phone number to the attacker until the registration of the user from the China network is terminated. At that point the actual mobile user would then register back onto the network in Sweden where normal communications would resume.

Some attackers bypass sending SAI altogether and just send a UL to the home network. There are a few approaches used for fake registration depending on how the home network responds. The threat actor can attempt multiple methods to gain access to the home network depending on which method is most effective. Some of these techniques are discussed below.

A visual example of this attack originating in China can be seen in a detection from October 2019. The screen shot is a trace of the surveillance attempt from the China Unicom mobile network where the threat actor makes a fake registration attempt using the IMSI of the US device currently roaming on the Telenor Sweden network. The US network and mobile user identification information in the screenshot have been obfuscated for privacy reasons.

The attacker sends a false authentication request (SAI) from the China Unicom network within ~3 minutes of the last signaling message of the user located on the Telenor network to make it appear as if the user is now traveling into China. The previous location check between the last message from Sweden and the new request from China is the indicator of this attack, where the travel distance between China and Sweden within 3 minutes is not possible. Once this procedure is complete and successful, an UpdateLocation (UL) message would then be sent on China Unicom to complete the registration process. Communications associated with the target phone are now routed to the attacker until registration from the China network is terminated.

Example 1: Fake Registration Attack – China Unicom



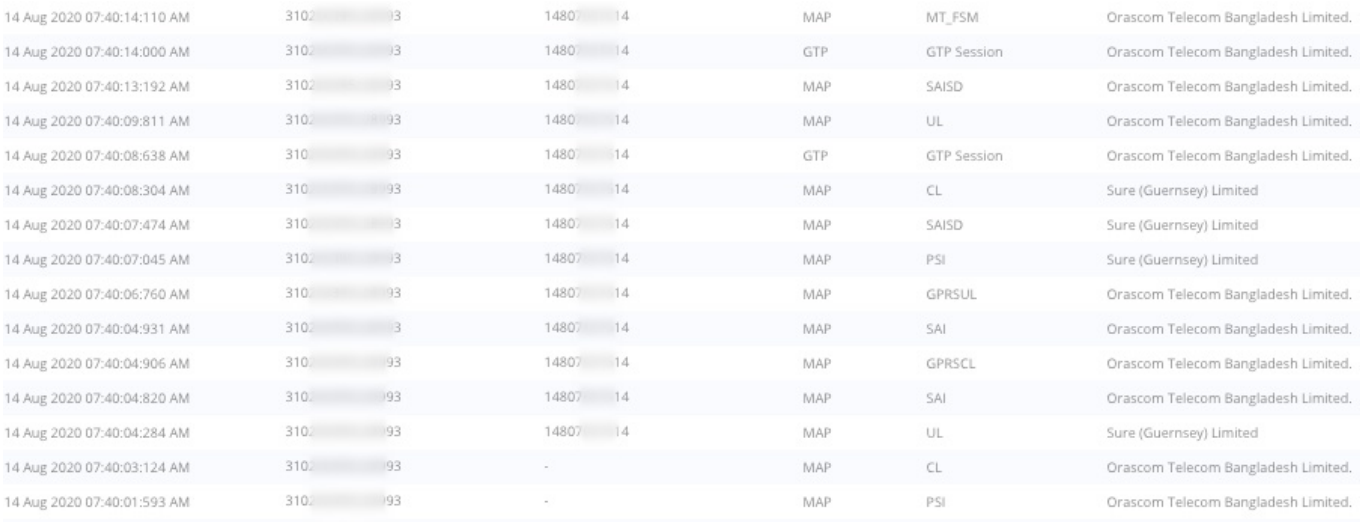
Date Time	Attackers Intent	Protocol	Message Type	IMSI	MSISDN	Attacker Network	Attacker Node	Roaming Partner	Roamer Type	Direction	Status of attack	Subscriber Home Network	Subscriber Location
20-Oct-2019 03:38:55	FASG MAP Suspicious-Unexpected Subscriber Movement	MAP	sendAuthenticationInfo	311[redacted]119	1[redacted]870	China Unicom	8613254120	China Unicom	Outbound	Incoming	Success Message	[redacted]	Telenor Sverige AB

Search:

Date Time	Message Type	Originating	Destination	Direction	Status of message
20-Oct-2019 03:34:57	updateLocation	467080000310-Telenor Sverige AB(240-8)	1[redacted](310-[redacted])	Incoming	Success Message
20-Oct-2019 03:34:58	sendAuthenticationInfo	467080000310-Telenor Sverige AB(240-8)	1[redacted](310-[redacted])	Incoming	Success Message
20-Oct-2019 03:35:06	updateLocation	1[redacted](310-[redacted])	1[redacted](240-[redacted])	Unknown	TCAP Timeout
20-Oct-2019 03:38:55	sendAuthenticationInfo	8613254120-China Unicom(460-1)	1[redacted](310-[redacted])	Incoming	Success Message

The second example is from a US mobile user roaming on the Orascom Bangladesh (Bangalink) Network whose network registration has been attacked by the Sure Guernsey, UK Network. In this example, the threat actor from the Sure network sends a Location Update (UL) message to signal a successful registration while the user is simultaneously connected to the network in Bangladesh. While the messages are received by the US network, the device is able to maintain the registration in Bangladesh. Such rapid geographic network switches are not possible under a normal usage scenario and should be considered as highly suspicious network activity.

Example 2: Fake Registration Attack – Sure Guernsey, UK



14 Aug 2020 07:40:14:110 AM	310[redacted]3	1480[redacted]4	MAP	MT_FSM	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:14:000 AM	310[redacted]3	1480[redacted]4	GTP	GTP Session	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:13:192 AM	310[redacted]3	1480[redacted]4	MAP	SAISD	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:09:811 AM	310[redacted]93	1480[redacted]4	MAP	UL	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:08:638 AM	310[redacted]93	1480[redacted]4	GTP	GTP Session	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:08:304 AM	310[redacted]93	1480[redacted]4	MAP	CL	Sure (Guernsey) Limited
14 Aug 2020 07:40:07:474 AM	310[redacted]3	1480[redacted]4	MAP	SAISD	Sure (Guernsey) Limited
14 Aug 2020 07:40:07:045 AM	310[redacted]3	1480[redacted]4	MAP	PSI	Sure (Guernsey) Limited
14 Aug 2020 07:40:06:760 AM	310[redacted]93	1480[redacted]4	MAP	GPRSUL	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:04:931 AM	310[redacted]3	1480[redacted]4	MAP	SAI	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:04:906 AM	310[redacted]93	1480[redacted]4	MAP	GPRSCL	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:04:820 AM	310[redacted]93	1480[redacted]4	MAP	SAI	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:04:284 AM	310[redacted]93	1480[redacted]4	MAP	UL	Sure (Guernsey) Limited
14 Aug 2020 07:40:03:124 AM	310[redacted]93	-	MAP	CL	Orascom Telecom Bangladesh Limited.
14 Aug 2020 07:40:01:593 AM	310[redacted]93	-	MAP	PSI	Orascom Telecom Bangladesh Limited.

Attacks such as the above occur frequently, routinely amounting to thousands of events per month. Source network attribution is shown in Section 03 of this report.

The primary methods used to manipulate communications include the **Fake Registration** and **Purge Location** attacks. In a Purge Location 3G attack a PurgeMS message is sent to the home network using the target IMSI, causing the network to delete the user registration information. Once removed from the network, the threat actor can then register the target device onto the attacking network to establish and re-route communications to the attacker.

Source Network Operator Advanced Attacks

While absolute attribution of these attacks is difficult, the source network is known by associating the messaging transactions associated with the attack to the source mobile network SS7 GT. The distribution by method from the source network is shown below.

2020 Fake Registration Attacks

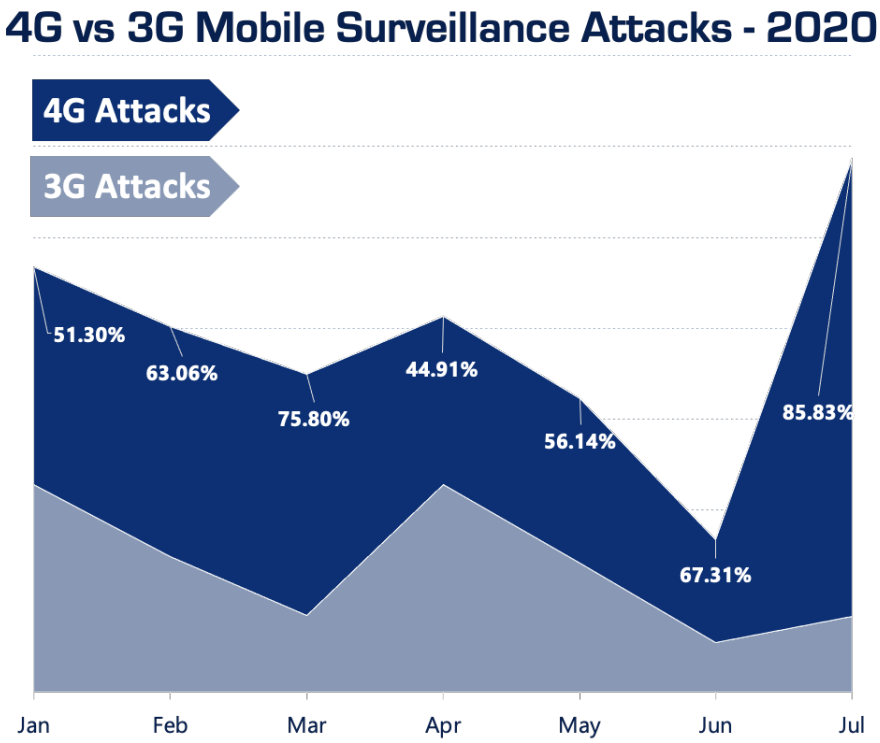
Network Operator	Country	Distribution
Flow Barbados	Barbados	22.12%
Swisscom	Switzerland	15.07%
Real Future Co (True Move)	Thailand	7.69%
Telefonica O2	United Kingdom	7.53%
Bouygues Telecom	France	6.93%
Digicel	Jamaica	4.06%
Smart Communications	Philippines	3.22%
Bell Mobility	Canada	2.63%
Rogers Wireless Fido	Canada	2.28%
DTAC	Thailand	1.95%
Telus	Canada	1.92%
Wataniya	Palestine	1.90%
IAM	Morocco	1.78%
Vivo	Brazil	1.67%
Vodafone	United Kingdom	1.46%
T-Mobile	Germany	1.23%
Mobitel	Sri Lanka	1.18%
China Unicom	China	1.12%
Viettel	Vietnam	1.11%
Sonatel	Senegal	0.93%
Antel	Uruguay	0.93%
A1 Telekom	Austria	0.87%
Slovak Telecom	Slovakia	0.86%
Vodafone Omnitel	Italy	0.77%
Digi Telecommunications	Malaysia	0.77%
Innovative Wireless (Vitelcom)	Virgin Islands	0.59%
Caribbean Cellular	British Virgin Islands	0.58%
PTI Pacifica	Guam	0.57%
Mobile One	Singapore	0.56%
Mtel	Montenegro	0.51%
Cable & Wireless	Cayman Islands	0.50%
Idea Cellular	India	0.45%
Mobilink PMCL	Pakistan	0.45%
NATCOM	Haiti	0.37%
Atheer Telecom (Zain)	Iraq	0.35%
NTT DoCoMo	Japan	0.25%
Vodafone Mumbai	India	0.24%
Vodafone Gujarat	India	0.24%
M-Tel (Mobitel EAD)	Bulgaria	0.23%
Safaricom	Kenya	0.21%
Belarussian Telecommunications (Life)	Belarus	0.20%
Airtel Congo	Congo	0.20%
Hormuud Telecom	Somalia	0.17%
HOT Mobile	Israel	0.15%
Orange	Jordan	0.14%
Turkcell	Turkey	0.13%
SK Telecom	South Korea	0.13%
JMTS (Zain)	Jordan	0.13%
Claro	Puerto Rico	0.12%
Cyprus Telecommunications (CYTA)	Cyprus	0.11%
Entel	Chile	0.10%
Astelit Mobile	Ukraine	0.10%

2020 Purge Location Attacks

Network Operator	Country	Distribution
Telcel	Mexico	22.32%
Bell Mobility	Canada	17.95%
Telus Communications	Canada	16.35%
Telefonica Movistar	Mexico	7.80%
Claro	Puerto Rico	5.62%
Vodafone Mumbai	India	5.40%
Swisscom	Switzerland	4.63%
Turk Telecom	Turkey	3.40%
Airtel	Nigeria	3.18%
PTI Pacifica	Guam	2.40%
Vimpelcom	Russia	2.29%
Mobilink PMCL	Pakistan	1.98%
China Mobile	China	1.39%
Rogers Wireless Fido	Canada	1.14%
China Unicom	China	0.65%
Cable & Wireless	Antigua	0.57%
Pulse Mobile	Guam	0.46%
Telkom Kenya	Kenya	0.42%
BTC	Bahamas	0.31%
Tigo	Rwanda	0.31%
Bouygues Telecom	France	0.30%
Optus	Australia	0.30%
Wataniya Ooredoo	Palestine	0.29%
Vodafone Kerala	India	0.28%
Vodafone Gujarat	India	0.27%

4G Attack Updates

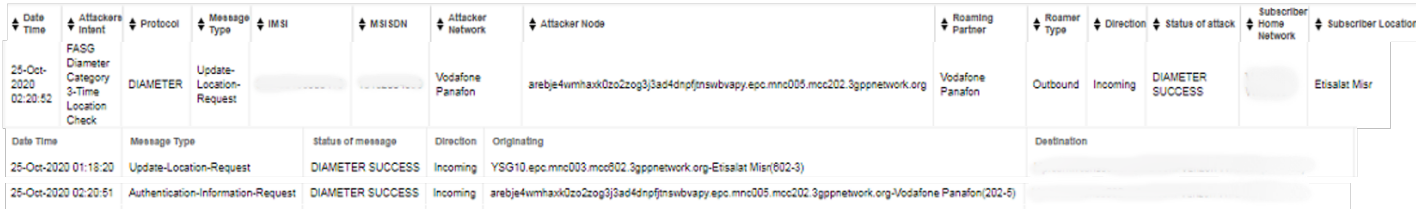
As discussed in the earlier section, the volume of 4G attacks have far outpaced 3G in 2020. The growth in attacks using the 4G Diameter protocol are mostly attributed to attacks from new threat actor source networks located in Bangladesh, Hong Kong, Puerto Rico and the Dominican Republic.



4G attacks will continue to dominate in 2020 with increasing levels of sophistication, including cross protocol and GTP attacks focusing on the interception of user mobile data traffic.

The Diameter signaling protocol used in 4G is a source of greater vulnerabilities due to the manipulation of multiple session attributes such as network address, application ID, command code and AVP. In addition, Diameter benefits attackers through weaknesses of network firewalls in detecting fake registration attacks, because of combined attach/registration of both 3G and 4G. Finally, there is an increasing diversity of 4G network-enabled devices in enterprise verticals such as industrial, transport, logistics and smart metering/grids.

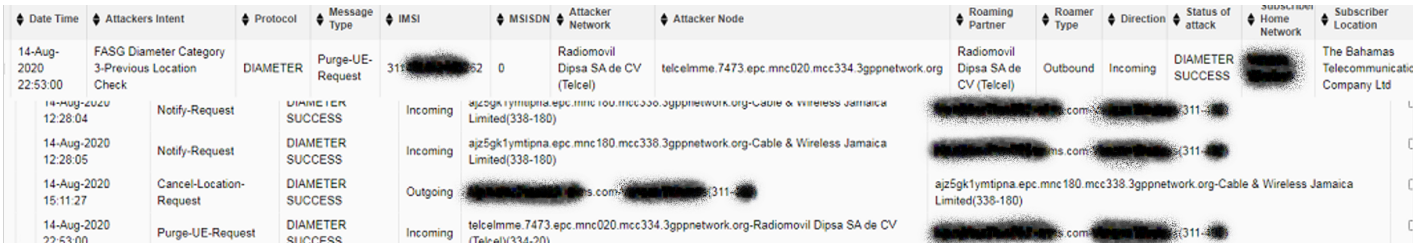
Following is a detection of a fake registration attack attempt of a device in Egypt where the travel time between Egypt and Greece is not consistent with a legitimate device registration sequence.



Date Time	Attackers Intent	Protocol	Message Type	IMSI	MSISDN	Attacker Network	Attacker Node	Roaming Partner	Roamer Type	Direction	Status of attack	Subscriber Home Network	Subscriber Location
25-Oct-2020 02:20:52	FASG Diameter Category 3-Time Location Check	DIAMETER	Update-Location-Request	[redacted]	[redacted]	Vodafone Panafon	arebje4wmhaxk0zo2zog3j3ad4dnpfjtnswbvapy.epc.mnc005.mcc202.3gppnetwork.org	Vodafone Panafon	Outbound	Incoming	DIAMETER SUCCESS	[redacted]	Etisalat Misr

Date Time	Message Type	Status of message	Direction	Originating	Destination
25-Oct-2020 01:18:20	Update-Location-Request	DIAMETER SUCCESS	Incoming	YSG10.epc.mnc003.mcc602.3gppnetwork.org-Etisalat Misr(602-3)	[redacted]
25-Oct-2020 02:20:51	Authentication-Information-Request	DIAMETER SUCCESS	Incoming	arebje4wmhaxk0zo2zog3j3ad4dnpfjtnswbvapy.epc.mnc005.mcc202.3gppnetwork.org-Vodafone Panafon(202-5)	

The same vulnerabilities seen in 3G network attacks also appear in 4G. In this case, the location of a user in the Caribbean is attacked by Telcel Mexico by sending a Diameter PurgeUE message, which is equivalent to the 3G PurgeMS message associated with the Purge Location attack in SS7.



Date Time	Attackers Intent	Protocol	Message Type	IMSI	MSISDN	Attacker Network	Attacker Node	Roaming Partner	Roamer Type	Direction	Status of attack	Subscriber Home Network	Subscriber Location
14-Aug-2020 22:53:00	FASG Diameter Category 3-Previous Location Check	DIAMETER	Purge-UE-Request	[redacted]	0	Radiomovil Dipsa SA de CV (Telcel)	telcelmme.7473.epc.mnc020.mcc334.3gppnetwork.org	Radiomovil Dipsa SA de CV (Telcel)	Outbound	Incoming	DIAMETER SUCCESS	[redacted]	The Bahamas Telecommunicatio Company Ltd

14-Aug-2020 12:28:04	Notify-Request	DIAMETER SUCCESS	Incoming	ajz5gk1ymtipna.epc.mnc180.mcc338.3gppnetwork.org-Cable & Wireless Jamaica Limited(338-180)	[redacted]
14-Aug-2020 12:28:05	Notify-Request	DIAMETER SUCCESS	Incoming	ajz5gk1ymtipna.epc.mnc180.mcc338.3gppnetwork.org-Cable & Wireless Jamaica Limited(338-180)	[redacted]
14-Aug-2020 15:11:27	Cancel-Location-Request	DIAMETER SUCCESS	Outgoing	[redacted]	ajz5gk1ymtipna.epc.mnc180.mcc338.3gppnetwork.org-Cable & Wireless Jamaica Limited(338-180)
14-Aug-2020 22:53:00	Purge-UE-Request	DIAMETER SUCCESS	Incoming	telcelmme.7473.epc.mnc020.mcc334.3gppnetwork.org-Radiomovil Dipsa SA de CV (Telcel)(334-20)	[redacted]

03

FOREIGN ATTACK STATISTICS 2020

+65	+85	+20M
COUNTRIES	NETWORKS	ATTACKS

2020 3G NETWORK ATTACKS – OPERATOR RANKING

Following are attack rankings detected from US mobile operator international signaling links from foreign networks targeting US mobile devices from January-July 2020. The surveillance attack distributions are ranked largest to smallest by source country and network operator from where the attacks originated. Additional operators detected may not be shown in the table below due to low attack volumes.

2020 Ranking by Source Country

Country	Attack Distribution
Canada	33.05%
Mexico	27.62%
India	6.26%
Switzerland	5.45%
Puerto Rico	3.97%
Turkey	3.14%
Nigeria	2.91%
Guam	2.68%
Russia	2.10%
China	1.96%
Pakistan	1.85%
Barbados	1.78%
United Kingdom	0.84%
France	0.84%
Thailand	0.77%
Zimbabwe	0.72%
Panama	0.49%
Palestine	0.42%
Kenya	0.40%
Jamaica	0.33%
Bahamas	0.28%
Rwanda	0.28%
Australia	0.27%
Philippines	0.26%
Morocco	0.14%
Brazil	0.13%
Germany	0.10%
Sri Lanka	0.09%
Vietnam	0.09%
Senegal	0.08%
Uruguay	0.07%
Austria	0.07%
Slovakia	0.07%
Italy	0.06%
Singapore	0.05%
US Virgin Islands	0.05%
British Virgin Islands	0.05%
Cayman Islands	0.04%
Haiti	0.03%
Iraq	0.03%
Jordan	0.02%
Khazakhstan	0.02%

2020 Ranking by Source Operator

Network Operator	Attack Distribution
Telcel Mexico	20.21%
Bell Mobility Canada	16.46%
Telus Canada	14.95%
Telefonica Movistar Mexico	7.06%
Swisscom Switzerland	5.38%
Claro Puerto Rico	5.10%
Vodafone Mumbai	4.90%
Turk Telecom	3.08%
Airtel Nigeria	2.87%
PTI Pacifica Guam	2.22%
Vimplecom Russia	2.07%
Mobilink PMCL Pakistan	1.79%
Flow Barbados	1.75%
China Mobile	1.26%
Rogers Wireless Fido Canada	1.21%
Bouygues Telecom France	0.82%
Oasis India	0.72%
Telecel Zimbabwe	0.71%
China Unicom	0.68%
TrueMove Thailand	0.61%
Telefonica O2 UK	0.60%
Cable & Wireless Antigua	0.52%
Claro Panama	0.49%
Pulse Mobile Guam	0.42%
Ooredoo Wataniya Palestine	0.41%
Telkom Kenya	0.38%
Digicel Jamaica	0.32%
BTC Bahamas	0.28%
Tigo Rwanda	0.28%
Optus Australia	0.27%
Smart Philippines	0.26%
Vodafone Kerala India	0.25%
Vodafone Gujarat India	0.25%
IAM Morocco	0.14%
Vivo Brazil	0.13%
Vodafone UK	0.12%
Mobitel Sri Lanka	0.09%
Viettel Vietnam	0.09%
Sonatel Senegal	0.07%
Antel Uruguay	0.07%

Key Observations

1. In February and March, traditional threat actors reduced activity, or in some cases stopped altogether likely due to acceleration of the Covid-19 Pandemic.
2. Mexico was an exception, as attacks continued from February-April. However, Telcel took over all SS7 attacks from Mexico until May, when Telefonica Movistar resumed its surveillance activity.
3. In May, SS7 activity picked back up in volume. Telefonica Movistar Mexico, Vodafone Mumbai India, Vimplecom/VEON Russia, China Mobile and China Unicom aggressively increased attacks.
4. Attacks from many African nations entered into SS7 surveillance operations aggressively, with interception attacks in volumes seen by more traditional attacking nations. This activity was consistent from April onward including operators from Nigeria, Kenya, Rwanda, Senegal and the Congo.
5. There were a number of previously undetected networks where SS7 surveillance was newly discovered, including networks out of Guam, Turkey, Pakistan and India.
6. From April, SS7 surveillance activity levels increased relative to February and March. Greater activity was seen on 4G Diameter protocols relative to SS7 where Mexico, Canada and Caribbean threat sponsor countries are now dominant with the Diameter attack vector.

2020 4G NETWORK ATTACKS – OPERATOR RANKING

The following rankings are related to surveillance attacks over the 4G Diameter network from foreign mobile networks targeting US mobile devices during the January-July 2020 timeframe. These surveillance attack distributions are ranked largest to smallest by source country and network operator from the origination point of the attack. Additional operators detected may not be shown in the table below due to low attack volumes.

Attack Ranking by Source Country

Country	Attack Distribution
Canada	24.37%
Mexico	24.13%
Hong Kong	15.33%
Barbados	12.45%
Bangladesh	6.06%
Dominican Republic	3.42%
Antigua	3.29%
St Kitts	2.37%
Japan	2.17%
Jamaica	1.90%
France	1.50%
India	1.11%
Puerto Rico	0.87%
Spain	0.47%
United Kingdom	0.46%
Poland	0.08%
Norway	0.01%

Attack Ranking by Source Operator

Network Operator	Attack Distribution
Webbing Hong Kong	14.74%
Telefonica Movistar Mexico	14.56%
Flow Barbados	11.98%
Bell Mobility Canada	10.61%
Telus Canada	10.48%
Telcel Mexico	8.65%
Hong Kong CSL Limited	5.99%
Robi Bangladesh	3.43%
Claro (Codetel) Dominican Republic	3.29%
Cable & Wireless Antigua	3.16%
Rogers Fido Canada	2.36%
Setel NV (UTS) St. Kitts	2.28%
KDDI Corporation Japan	2.09%
Digicel Jamaica	1.83%
Orange France	1.43%
Bharti Airtel India	1.06%
Bharti Airtel UP West India	0.63%
Vodafone UK	0.44%
Bharti Airtel Himachal Pradesh India	0.36%
France Telecom Espana	0.23%
West Central Wireless	0.15%
Claro Puerto Rico	0.14%
T-Mobile Poland	0.08%
France Telecom	0.02%
Mobile Norway	0.01%

Key Observations

1. Unlike 3G attack volumes, which decreased in February and March during the acceleration of COVID-19, 4G network volumes actually increased. Relative volumes increased month over month in both February in March.
2. Caribbean operators maintain a strong surveillance position in both 3G and 4G networks, with increasing month over month traffic volumes using 4G. Most recently, the Dominican Republic is seen as a major participant.
3. New 4G attacking source networks for 2020 include many relatively small operators such as Claro Puerto Rico, T-Mobile Poland and Webbing Hong Kong

04

Advanced Insights

Insights on Traditional Adversaries Reveals New Attack Strategies and Risk Mitigation Recommendations

INVESTIGATIONS AND INSIGHTS

Further investigations into foreign surveillance activity and geo-politics continues to provide indicators of potential threat actor cooperation. These investigations are primarily focused on the cyber activities of traditional US adversaries.

China Adversary Updates – New Sponsor Networks?

The **Far from Home – 2018-2019 Threat Intelligence Report** revealed the engagement of China using both China Unicom and China Mobile networks to conduct state sponsored cyber espionage on US mobile devices.

As evidence emerged of China using Caribbean network operators based out of the Bahamas and Barbados as a source for 3G network attacks, there are indications of yet additional source networks likely used by China for signals intelligence.

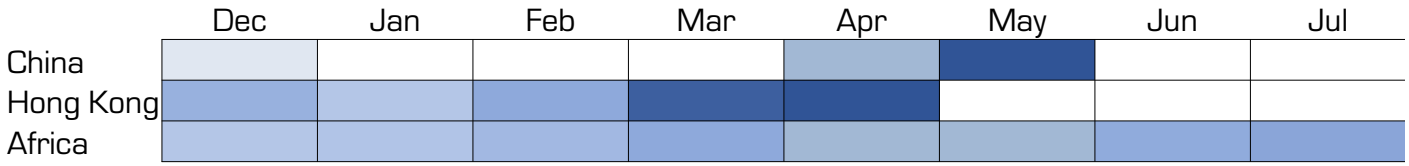
In Q1 of 2020, direct surveillance attacks from China source networks were rarely seen. This could be a result of China's focus on the Covid-19 pandemic, but its more plausible that surveillance attacks were diverted to other network operator partners as seen in the past. Exigent Media has been provided information from sources involved in surveillance detection that organized crime and state sponsors commonly utilize multiple networks to conduct mobile attacks to avoid detection and maintain attack movement. At the time attacks were not directly observed from China, they began to appear prominently in networks from Hong Kong, Africa and even Pakistan.

From December 2019-March 2020, the network Hong Kong CSL Mobile (a subsidiary of HKT) was detected launching significant volumes of unauthorized 4G signaling messages appearing as network spoofing attacks while direct attacks from China reduced. Further, as these suspected 4G attack messages from CSL Mobile stopped in April, 3G attacks from China Mobile were detected in re-started in the April and May timeframe. In addition to CSL, unauthorized signaling was also detected from Webbing Hong Kong, an MVNO network operation in the months of March and April. Webbing is a mobile operator which provides international roaming services for IoT and industrial applications.

The timing of this activity is highly suspicious given the recent Hong Kong security stance taken by China, though this can be perceived as more of a formality. China's relationship with mobile networks in Hong Kong is historically quite close, with China Mobile Hong Kong (CMHK) and China Unicom Hong Kong having operations in Hong Kong as Chinese state-owned enterprises.

In addition, China has significant interest in the telecommunications of Africa, with both ZTE and Huawei having major operations and a significant footprint throughout Africa. While China has invested significantly into African telecommunications, the increasing participants in mobile cyber operations against US devices sourced from Africa should be a strong caution signal to US mobile operators and US cyber agencies. The African nations detected as the source of these attacks include those out of Zimbabwe, Nigeria, Kenya, Morocco, Senegal, Somalia and the Congo.

The volume heat chart below shows the operational surveillance activity by source countries of China, Hong Kong and African nations from December 2019-July 2020.



Russia Adversary Updates – Increased Activity by CIS Allies in 2020

While Russia is known to have vast and advanced capabilities in signals intelligence and data-driven intelligence collection, the direct role of Russian mobile operators in surveillance has been relatively inconsistent. The operator Tele2 (formerly Rostov) was a prominent Russian source of mobile surveillance in 2018 and VEON/Vimplecom was seen in 2019 in small volumes, but it wasn't until 2020 when activity from both Russia and other member countries of the CSTO were seen to amplify surveillance attacks using mobile networks.

It is possible that the 2020 US presidential election may have played a role in supporting the increased detection of mobile network-based campaigns for intelligence collection.

Throughout Q2 of 2020, VEON was seen launching significant Purge Location attacks against US devices. As of June 2020, additional activity of interest was seen originating from the CIS region with potential Russian proxy activity from Ukraine (Astelit Mobile), Belarus (Belarusian Telecommunications Network – branded as "Life") and most recently KAR-Tel (Beeline Kazakhstan). Kazakhstan, for its part in 2020 has recently signed an agreement to boost bilateral military cooperation with Russia.

The chart below shows geographic sourcing of mobile surveillance from these countries in 2020.

	Jan	Feb	Mar	Apr	May	Jun	Jul
Russia							
Belarus							
Ukraine							
Kazakhstan							

While not included in this report, activity from the VEON Russia network was seen to accelerate during the month of September. We will continue to monitor CIS region surveillance activity, as recent trends indicate increasing levels prior to the US election season.

Palestine Adversary Updates

Historically speaking, Palestine has engaged in mobile cyber intelligence collection of US devices throughout 2018 and 2019 with the network operator Wataniya; which is now part of the Ooredoo mobile network group named Ooredoo Palestine. It is observed that the activity is primarily isolated to US travelers entering into Israel. Given that Iran has provided financial and military support to Palestinian militant groups, it should be a concern that any intelligence acquired through mobile espionage from Palestinian networks could be supplied to one of the US most significant adversaries.

Based on signaling traffic analysis, Ooredoo Palestine uses a method to acquire the IMSI of the US traveler by deploying overlapping radio network coverage within adjacent areas of Israel. This can be validated by analyzing the behavior of the device when it attempts to register to the Israel network in 3G mode. In this scenario, the Ooredoo Palestine network sees the device over the cellular radio network and uses a network-based approach to brute force the user's device onto the Ooredoo mobile network using a technique known as Anti Steering of Routing (Anti-SoR). This action bypasses the home operator preferred international roaming operator list and overrides it. Using this approach, the attacking operator can obtain the IMSI as well as perform traffic interception of the user data, voice and SMS through subsequent fake registrations.

A live example of this surveillance attack behavior can be seen below.

Event Time	IMSI	MSISDN	Protocol	Message Type	Partner Network	Result Code
29 Jun 2020 12:11:42:425 PM	310[redacted]181	-	DIAMETER	Cancel-Location-Request	Cellcom Israel Ltd	DIAMETER SUCCESS
29 Jun 2020 05:30:04:362 AM	310[redacted]181	[redacted]	DIAMETER	Cancel-Location-Request	Cellcom Israel Ltd	DIAMETER SUCCESS
29 Jun 2020 05:30:03:940 AM	310[redacted]181	[redacted]	DIAMETER	Update-Location-Request	Cellcom Israel Ltd	DIAMETER SUCCESS
29 Jun 2020 05:30:02:856 AM	310[redacted]181	[redacted]	DIAMETER	Authentication-Information-Request	Cellcom Israel Ltd	DIAMETER SUCCESS
29 Jun 2020 05:23:08:000 AM	310[redacted]181	[redacted]	GTP	GTP Session	Wataniya Palestine Mobile	V1 Request accepted
29 Jun 2020 05:22:39:259 AM	310[redacted]181	[redacted]	GTP	GTP Session	Wataniya Palestine Mobile	V1 Request accepted
29 Jun 2020 05:22:32:000 AM	310[redacted]181	[redacted]	GTP	GTP Session	Wataniya Palestine Mobile	V1 Request accepted
29 Jun 2020 05:20:25:419 AM	310[redacted]181	[redacted]	GTP	GTP Session	Wataniya Palestine Mobile	V1 Request accepted
29 Jun 2020 05:20:01:000 AM	310[redacted]181	[redacted]	GTP	GTP Session	Wataniya Palestine Mobile	V1 Request accepted
29 Jun 2020 05:19:24:141 AM	310[redacted]181	[redacted]	MAP	MT_FSM	-	TCAP Timeout
29 Jun 2020 05:18:39:969 AM	310[redacted]181	[redacted]	GTP	GTP Session	Wataniya Palestine Mobile	V1 Request accepted
29 Jun 2020 05:17:41:511 AM	310[redacted]181	[redacted]	DIAMETER	Insert-Subscriber-Data-Request	Cellcom Israel Ltd	DIAMETER ERROR USER UNK
29 Jun 2020 05:17:04:000 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	V1 Request accepted
29 Jun 2020 05:15:59:026 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	V1 Request accepted
29 Jun 2020 05:08:56:248 AM	310[redacted]181	[redacted]	DIAMETER	Update-Location-Request	Cellcom Israel Ltd	DIAMETER SUCCESS
29 Jun 2020 05:08:55:269 AM	310[redacted]181	[redacted]	DIAMETER	Authentication-Information-Request	Cellcom Israel Ltd	DIAMETER SUCCESS
29 Jun 2020 04:49:17:000 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	Others
29 Jun 2020 04:34:46:000 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	Others
29 Jun 2020 03:32:38:342 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	V2 Request accepted
29 Jun 2020 03:32:37:000 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	V2 Request accepted
29 Jun 2020 02:31:36:966 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	V2 Request accepted
29 Jun 2020 02:31:36:000 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	V2 Request accepted
29 Jun 2020 01:30:35:449 AM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	V2 Request accepted
28 Jun 2020 11:28:32:664 PM	310[redacted]181	[redacted]	GTP	GTP Session	Cellcom Israel Ltd	V2 Request accepted

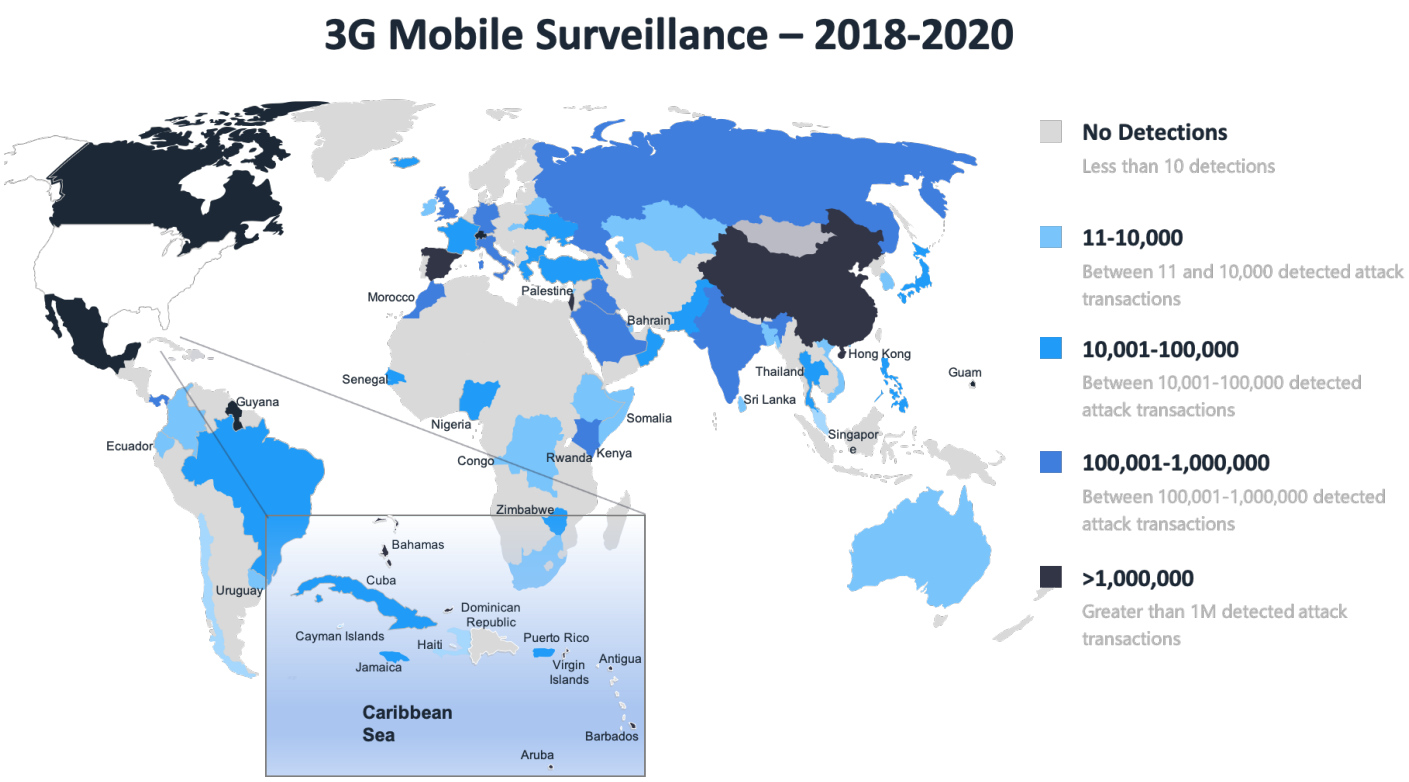
In the trace capture above, it is seen that this mobile user was engaged in a mobile data session (GTP Session) when the session was interrupted by the Wataniya/Ooredoo Palestine network while the user was also registered onto the Cellcom Israel network. The timestamp on the signaling messages and the message sequence shows this event happening without typical registration onto the Ooredoo Palestine network (absent of Authentication Request, Update Location Request messages). This indicates that the device was previously authenticated on the Ooredoo network and that the home network in the US is allowing the signaling to proceed.

These types of attack transactions had occured regularly where mobile users may travel to Tel Aviv, and Ooredoo Palestine forces the device registration onto the Palestine network from Israel. It is possible that this surveillance information is designed for targeted communications interception, as well as for collection of intelligence information by maintaining a historical record of US device and user travel/mobility patterns into and out of Israel.

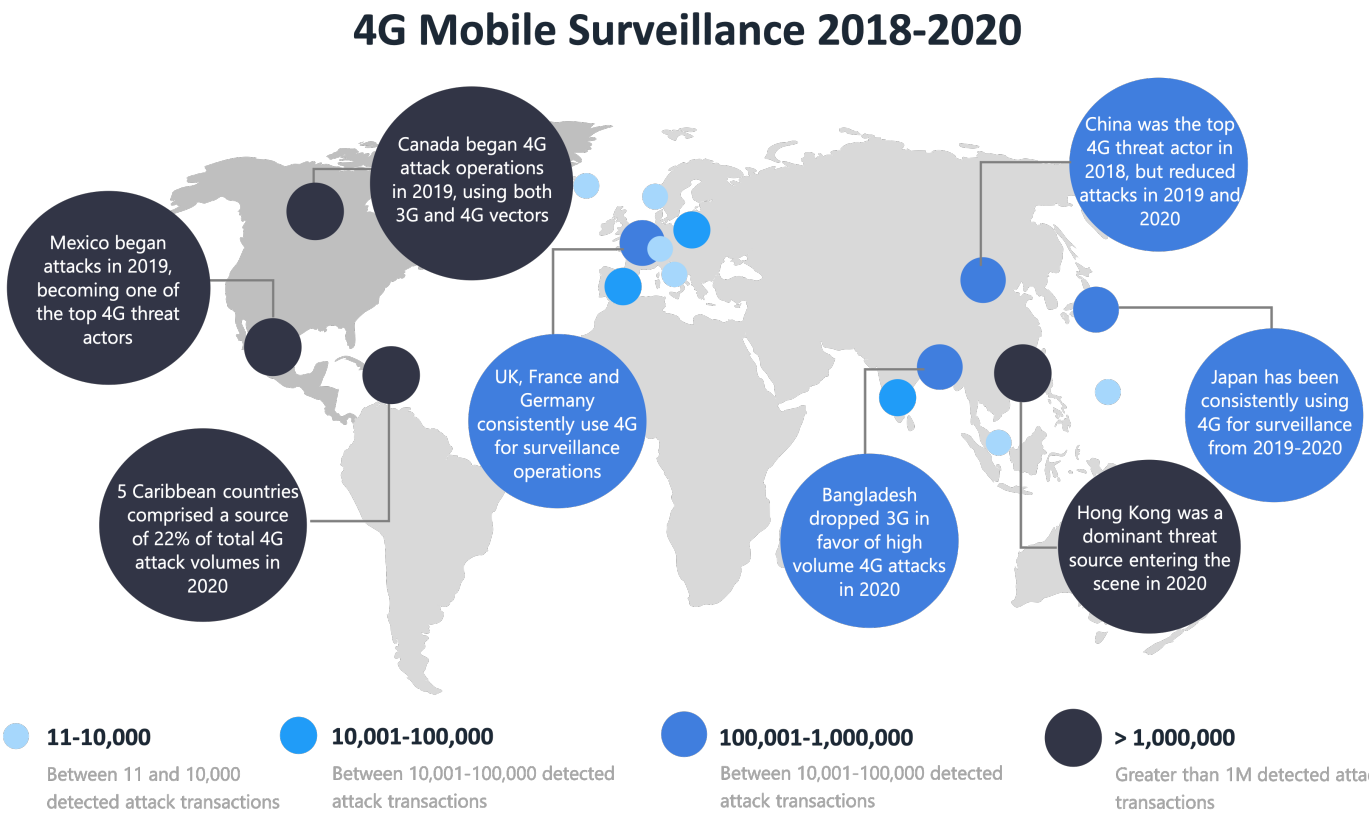
TARGETED SURVEILLANCE STATISTICS

The global heat maps below show the total distribution of surveillance attack volumes from source countries over a 3-year period based on observed 3G and 4G attack vectors.

3G ATTACK GLOBAL HEATMAP



4G ATTACK GLOBAL HEATMAP



Conclusions

Implications for Operators and Policymakers

2020 has seen escalations of new operators participating in surveillance of US mobile devices and their users, with increased levels of activity relative to 2019. While the start of the COVID-19 pandemic may have slowed down this activity somewhat in the February-March timeframe, the activity has continued and accelerated in the 4G network domain. This may have something to do with operators providing more enhanced security controls on 3G foreign signaling interconnect links, thus reducing the effectiveness of 3G attacks. However, the attacks on 4G more than exceed the reduction seen on 3G and should bring a level of increasing concern to user privacy now and in the future.

The expansion of adversary network surveillance footprint, including increasing sponsor networks of 3G attacks using GT selling/leasing and the capabilities of adversaries shows that the lack of consequences and operator controls over this activity have further emboldened threat actors. They are also positioning their capabilities for signals intelligence activity in 5G, should security standards fail to come to fruition in the near future.

The expansion in detections of small source operators in remote countries confirms earlier suspicions of network selling and evidence of "Global Title Burning." This is an activity where threat actors rotate attacks across multiple 3G network Global Title Addresses for detection avoidance and as a backup network in the event an operator blocks or shuts down a primary attacking source network address. This threat enablement activity indicates a vibrant espionage economy and "surveillance as a service" operations.

The implications associated with active mobile network surveillance threats in 2020 should be seen as a troubling sign for US mobile network operators and US policymakers in the future. The diversity of attacks, emboldened threat actors and continued network selling should be expected to increase if there continues to be a lack of policies to address ongoing public network cyber threats.

While vulnerabilities are very well known within the mobile operator industry and among US policymakers, there has been little action to restrict foreign surveillance activity. Discussion without action is the greatest threat to privacy in emerging mobile communications, but with determination is something which can easily be averted.