FAR FROM HOME

Active Foreign Surveillance of US Mobile Users 2018-2019

THREAT INTELLIGENCE REPORT

exigent MEDIA
www.exigentmedia.com

mobile intelligence ALLIANCE
www.mobileintelligence.org

Table of Contents

01

INTRODUCTION

In the past few years, mobile phones have been the primary means of shopping, communications, banking, and entertainment. Its use has been further expanded to control services such as home security, health monitoring, vehicle control, and many other functions. With the spectrum of critical mobile services increasing significantly in the coming years, privacy and security must be considered an absolute priority for telecommunications infrastructure. Likewise, mobile operators and their links to foreign roaming networks must be trusted to provide ubuitous services while traveling. Unfortunately, the security and privacy we require and expect is far from reality and the trust model for future services is in jeopardy.

Many security vulnerabilities of the world's mobile networks were first revealed to the industry in 2014, and mass surveillance techniques used by the NSA revealed by Edward Snowden in 2013 have produced increased levels of alarm. More recently, revelations of break-ins into telecommunications networks in the US and other countries have concerned governments worldwide as 5G network deployments become more widespread.

While reports of surveillance programs on its citizens have created an uproar within US borders, should we not also be concerned about our privacy from entities outside of our borders? How real are threats from foreign networks and which foreign countries are involved?

Covert foreign surveillance using mobile networks has been successfully carried out for years using the legacy mobile SS7 signaling system; a patchwork system enabling network operators around the world to communicate with each other for the purpose of providing international roaming services. This system leaves fingerprints on the source networks and countries which are communicating with a user's phone, which in turn enables deployed intrusion detection systems to trace and monitor this communication. Revelations contained in this report may shock many security and policy experts. For others, it may simply be a validation of what has been known for many years as an available tool for organized crime and nation states for signals intelligence.

This report provides insights and evidence of active surveillance and cyber espionage campaigns carried out via international public mobile networks targeting US mobile users. With actual data captured showing this activity, the **Far from Home** reports are the first of their kind showing the countries and networks involved in spying on US phones, with intensity levels and ranking of the activity within the global compass. It also provides situational guidance and evidence of information exchange and collaboration between threat actors and operators around the globe, with an analysis of foreign surveillance trends providing clues regarding potential state-sponsored alliances.

As opposed to "bulk" collection, the term **Active Surveillance** describes the techniques used by foreign networks to conduct espionage. It is different from passive surveillance in the following way:

1. **Active Mode** = Using a foreign mobile network to attack a target mobile phone by altering or manipulating network signaling data to solicit an action from the user's home network.
2. **Passive Mode** = Gaining access to a target mobile device communications and network information by collecting, storing and analyzing data without altering or affecting the system.

The distinction between the two approaches is that in an active mobile cyber espionage operation, the threat actor engages the target phone using a mobile network to attack, in this case a foreign network. Active surveillance is a mechanism used by a foreign network to engage in the mobile signaling with a US network to derive location or communications of a specific user. This consideration is important in the context of targeted espionage where the attacker can actively manipulate calls and text messages.

KEY THEMES

1

Foreign Surveillance Activity of US Mobile Users is Massive in Scale – Mobile networks transport millions of attack messages on a monthly basis. Massive volumes of cyber espionage activity have occurred for years and continues to this day.

2

Allies, Adversaries and Neutral Countries Participate in Mobile Espionage - Surveillance operations against US mobile users are not just limited to our adversaries. US Allies and small neutral countries are also active participants in using mobile networks to monitor a target phone's location and communications.

3

Detecting Surveillance is Much Easier Than Preventing It – Security firewalls are available to provide attack detection and prevention. However, many network operators use conservative prevention approaches to reduce risks of potentially disrupting international roaming service.

4

Attacks Take Place on 3G and 4G Networks while 4G attacks Increase – Mobile devices use 3G and 4G networks simultaneously and threat actors exploit these vulnerabilities to increase success rates of attacks. As 3G security capabilities increase, attackers adapt, favoring 4G attack vectors which poses greater risks to 5G networks.

5

Attacks Are Coordinated Between Foreign Country Networks – In 2018, China, Barbados and Bahamas network were observed attacking the same mobile users with similar techniques. Likewise, attacks from China, Palestine, Bahamas and Panama networks were also observed, indicating network selling for conducting intelligence operations.

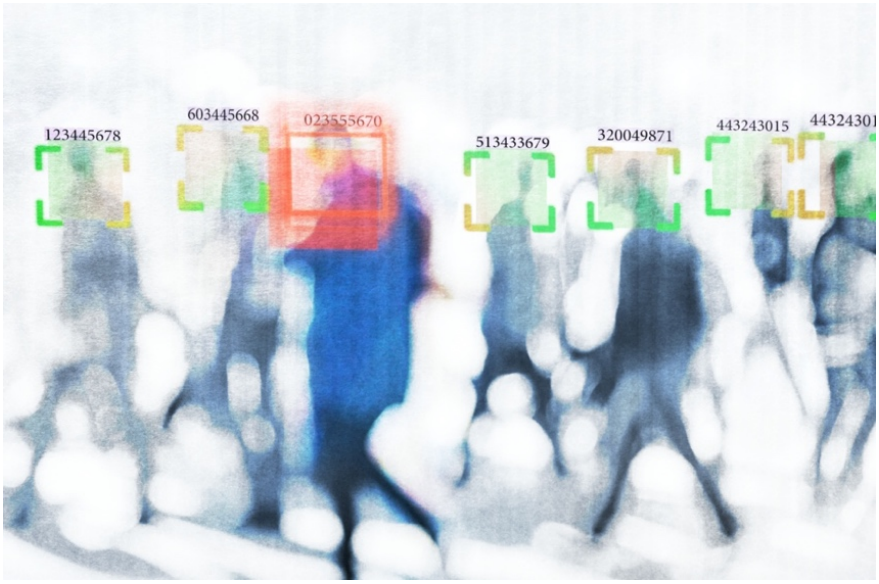
6

Without Mobile Network Security Mandates, Threat Capabilities of Small and Developing Nations have Increased – Current security guidelines are not sufficient to hold networks accountable for attacks. The lack of mandates encourages small nations to become participants in the threat economy, effectively selling their network to adversaries.

OVERVIEW

Telecommunications is a rich and expansive attack surface for organized crime and nation states. As of 2020, only a small percentage of operators globally have implemented signaling security firewalls on both 3G and 4G networks. Due to the growing number of over 5.2 Billion network-enabled subscriptions as reported by GSMA Intelligence, ubiquitous global coverage and easy access, the mobile network is without question a key focal point of adversaries to conduct cyber espionage operations.

As the point of entry, the mobile signalling network is the launch pad for threat actors to actively engage US mobile users. It is represented by the SS7 and Diameter protocols used for 3G and 4G services, respectively. Due to the rich information contained in these signals for communication and mobility management, accessing these networks are critical for the threat actor to exploit and control mobile devices for surveillance operations. Historically, access to these networks have been sold to 3rd parties with little oversight, leaving an open door of attack from any country network.



When mobile operators provide access to the signaling network, it exposes the inherent vulnerabilities of networks across the globe to threat actors due to the patchwork of trusted international roaming agreements, essentially allowing surveillance attack messages to flow freely. In remote island countries and developing nations, it is common for the network operator in those countries to sell the use of its network by leasing a network address called an SS7 Global Title (GT). Through the use of a network connection and a foreign operator's GT address, the threat actor can access **any** network to which that operator has a roaming agreement. Advances in technology have recently enabled insights into the nature of this activity. What were previously seen as speculative vulnerabilities in networks can now be revealed as actual attacks.

The following threat intelligence is the result of years of independent research and analysis of messages exchanged between foreign and US networks. It exposes details on the techniques, tactics and procedures used in surveillance operations with real captures of the attacks. Included is analysis on state sponsored adversarial network attacks, operations from the Middle East and network selling in the Carribbean. Threat trends are revealed, uncovering potential objectives and partnerships between countries with possible covert geopolitical objectives. More details and analysis are available in a second report **Far From Home – Part 2** from Exigent Media which provides the latest trends ocurring in 2020 revealing surveillance with potential US presidential election impacts.

The intention of these reports is to highlight the severity of vulnerabilities to encourage implementation of more effective countermeasures and security policies. The hope is that policymakers, industry standards bodies and intergovernmental agencies can formulate timely and enforceable regulations to minimize future threats to critical 5G services. Through the use of modern security tools, thoughtful configurations and enforceable policies, many of the risks revealed in the report can be mitigated.

02

SURVEILLANCE METHODS

INFORMATION DISCLOSURE

COMMUNICATION INTERCEPTION

ATTACK APPROACHES

Basic and Advanced Techniques

Threat actors use multiple approaches to conduct surveillance operations, and many take on consistent methods which are aligned to the objective. For example, networks from China, Russia, Switzerland, Germany and the Cribbean use multiple methods to achieve success, but for the most part their attack patterns fall into espionage related to communications disruption and interception. Their purpose is to establish a path of access to mobile targets directly via well-known vulnerabilities and interfere in the signaling path used for international roaming. These methods include the following:

1. **Basic Attack - Obtain Network Identity, Location and User Profile Information** – The vast majority of these attacks are designed to identify the location of the mobile device, but they also attempt to disclose user information including the network identity (IMSI) and phone number (MSISDN) of the user so that they can conduct more advanced attacks.
2. **Advanced Attack - Disrupt Communications** – This is frequently achieved by sending messages to cancel or purge the user from the network which can cause communications disruption. In most cases, purging the user from the network enables subsequent fraudulent registration to send or receive communications by the attacker on behalf of the target.
3. **Advanced Attack - Intercept Communications** – This commonly involves orchestrating a fake registration from the attacking network using the IMSI network credentials of the victim to simulate the victim on the network for the purpose to receive or send their communications.

The basic attack has generally been employed by sending messages using scanning/probing techniques to uncover identity and location of the user, known as an interrogation message. The messages used with this method are generally not authorized to originate from a foreign network and thus mostly unsuccessful. They can be successful due to network misconfigurations.

Advanced attacks use authorized messages but utilize techniques to "fake" the home network into believing the mobile user is roaming onto the network where the attacker has obtained access and a GT address. These techniques are advanced because they orchestrate multiple signaling messages using a procedure designed to simulate the mobile device on the network. Organized crime and state sponsors use this method to alter communications. A breakdown of these attacks by year, country and source operator can be found in the **Far From Home - Part 2** report from the Exigent Media website.

Method and Classification

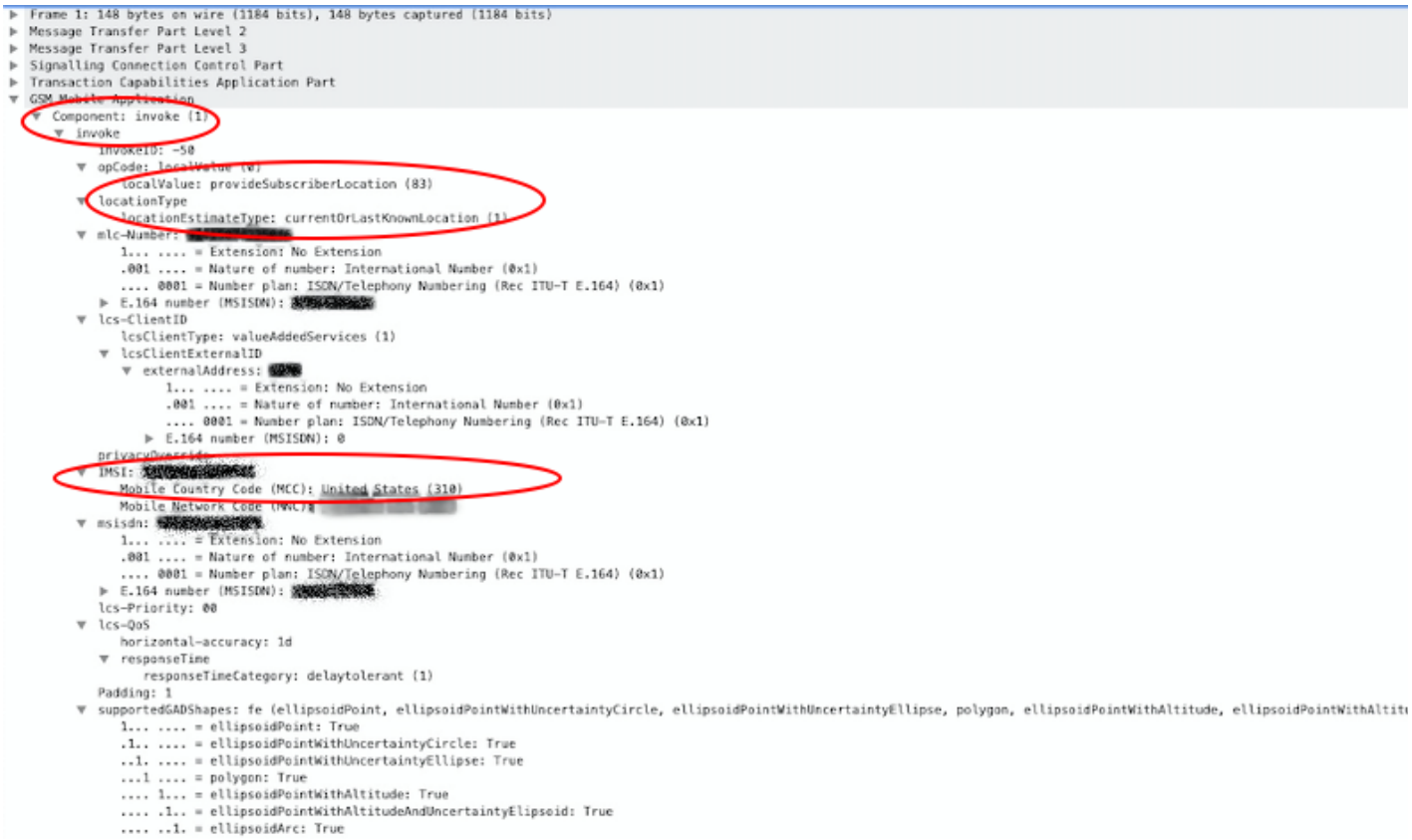
The surface of attack is categorized as using either the 3G SS7 or 4G Diameter protocols. SS7 historically is the dominant vector of attack, but growth in Diameter is seen in 2019 with high success rates due to the lack of security controls in 4G. Evidence is emerging of the use of more sophisticated methods using both SS7 and Diameter together to target a user for increased success, known as cross-protocol attacks. Some networks have used both methods to conduct operations starting in 2019.

Attack Surface	Attack Method	User Threat
SS7 – 3G	Basic – Prohibited	User Information and Location Disclosure
SS7 – 3G	Advanced – Purge Location	Communications Disruption & Interception
SS7 – 3G	Advanced – Fraudulent Registration	Communications Disruption & Interception
DIAMETER – 4G LTE	Basic – Prohibited	Communications Disruption
DIAMETER – 4G LTE	Advanced – Suspicious	Communications Disruption & Interception

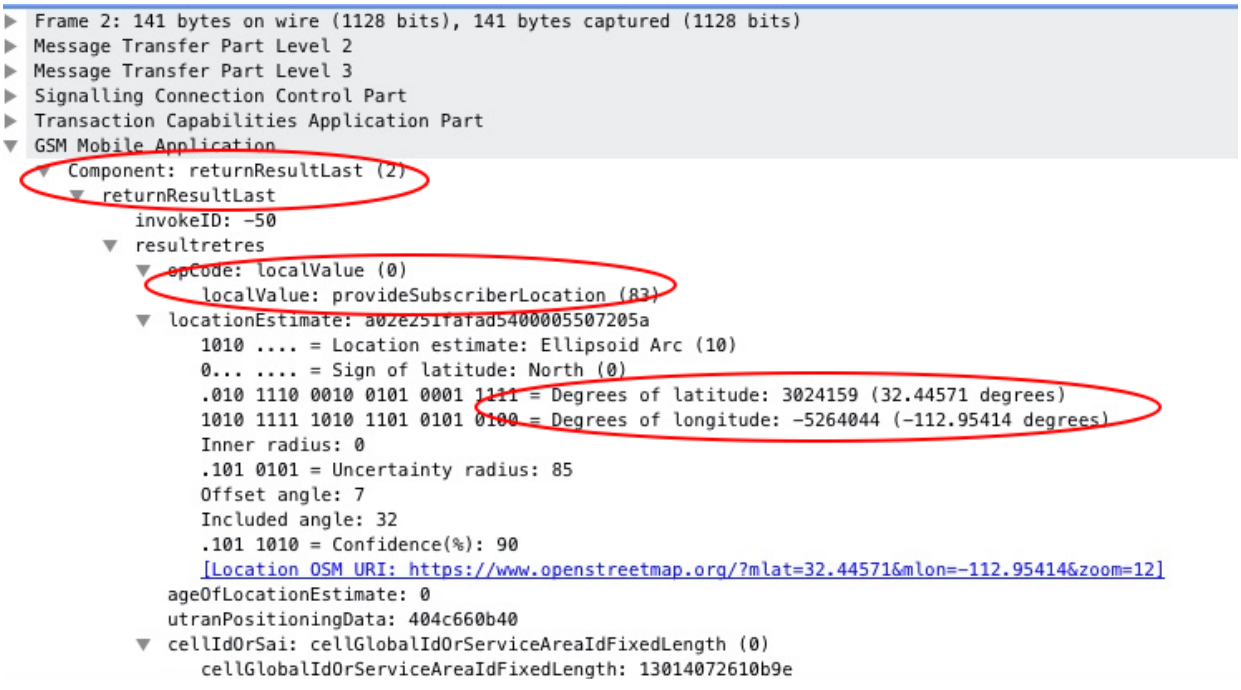
Basic Attack Example – SS7 User Location

An example of an actual location tracking attack is shown below. In this example, a message is sent from the attacking network to the home network of the target mobile user by requesting the current exact location coordinates of the target phone IMSI using the SS7 ProvideSubscriberLocation (PSL) message (seen as **invoke** below). The response message (seen as **returnResultLast**) from the network provides the GPS coordinates of the target phone.

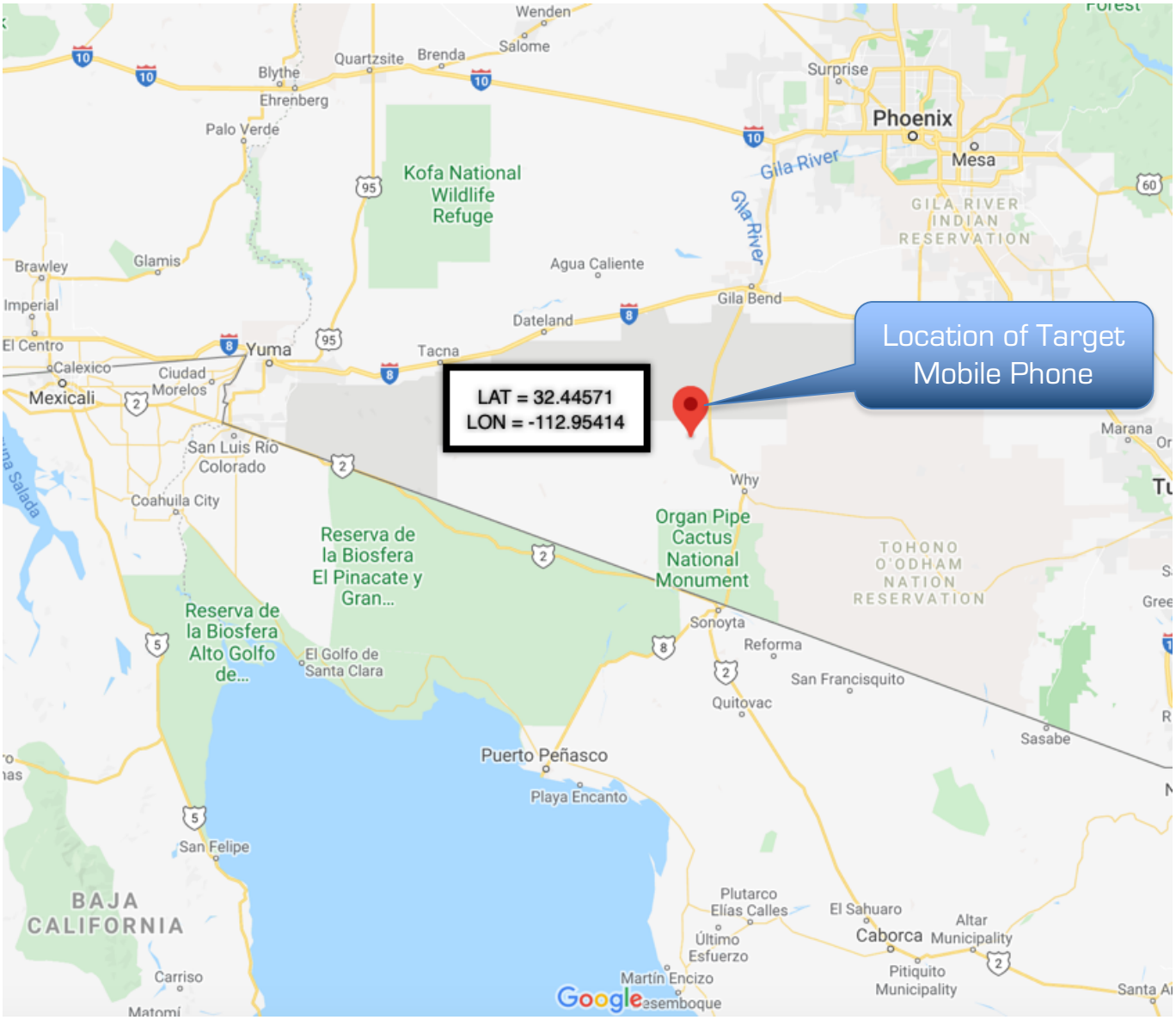
Foreign Network Location Tracking Attack Request



Home Network User Location Response

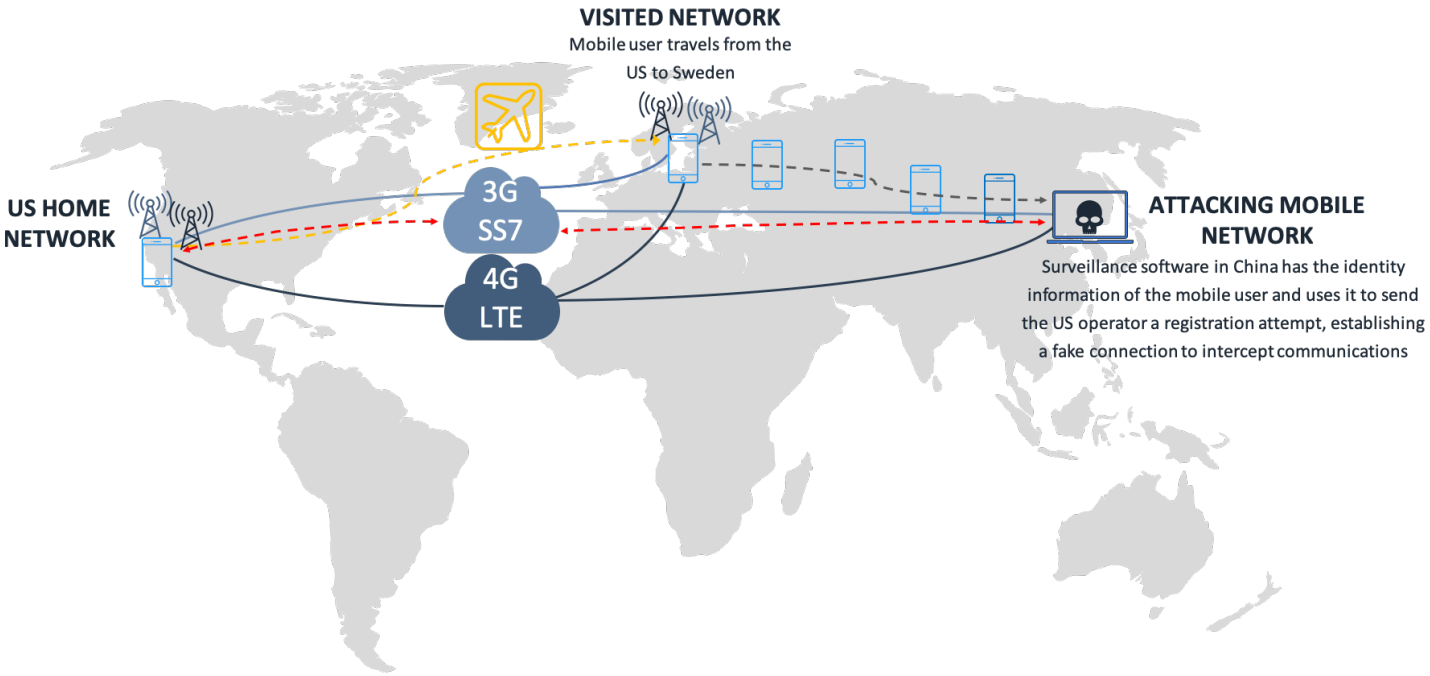


In this particular surveillance event, the response from the home network provides a precise location of the mobile device with the Latitude and Longitude as determined by the network in communication with the device. The location of this user based on GPS coordinates is in a remote area approximately 15-20 miles from the US-Mexico border and within the proximity of the Barry M Goldwater US Air Force Bombing Range. Is this a location tracking attempt for drug trafficking from organized crime? Maybe a state sponsored tracking attempt of an illegal border crossing between the US and Mexico of sensitive materials? Or perhaps it is a key location of illegal Mexico-US human trafficking? These speculations are purely hypothetical, but the main point is that network vulnerabilities can be exploited on a regular basis to target and track mobile users from outside of the US home mobile network.



Advanced Attack Overview

Advanced attacks should be considered more critical, as they represent real time disruption or interception of communications and reflect more sophisticated targeting capabilities of the threat actor. Advanced approaches can utilize a few different techniques, but many involve the tactic of impersonating the victim through registration of the target phone on the attacker's network using a process known as a fraudulent registration. The threat actor uses software with a sponsor mobile network GT signaling address to "fake" registration of the target device. This impersonation removes the actual target phone from their current network connection and establishes a new network connection on the attacker sponsor network, thus allowing the attacker to send and receive communications on behalf of the victim. Below is a visual representation of how this method works.



The above diagram demonstrates a scenario where a US mobile user is traveling to Stockholm, Sweden. Upon arrival in Sweden, the user turns on their phone and registers onto the roaming mobile network in Sweden, as selected by the US home operator. The threat actor becomes aware of the target user located in Sweden and uses their connection to the China Unicom mobile network to conduct the attack with an objective of intercepting the communications of the victim using impersonation via fraudulent registration. Standard text messages are not encrypted, and this allows the attacker to receive, view and respond to messages as well as voice calls. The following attack sequence takes place:

1. A **fraudulent authentication message** is sent using SS7 from China Unicom to the home US network of the device using its IMSI to intiate the authentication process from China.
2. A **fraudulent location update message** is sent from the China Unicom network back to the victim's US home network to inform the home network that the user is located in China for communications, completing the fraudulent registration process.
3. The **user now appears to be registered onto the attacker network**. The US home network now believes that the user is located in China, routing all communications associated with the target's phone to the attacker until the registration of the user from the threat actor is terminated or resumed back on the Sweden network.

Because this can happen very quickly and with complete silence, the actual mobile user often never realizes that they have been attacked, making this surveillance attack highly effective. In the **Far from Home – Part 2** report, a network trace is provided from this attack to show evidence of this event from October 2019, along with evidence of other similar attacks in 2020.

03

FOREIGN ATTACK STATISTICS

+65
COUNTRIES

+100
NETWORKS

+100M
ATTACKS

3G NETWORK ATTACKS – OPERATOR RANKINGS

Following are attack rankings detected from US mobile operator international SS7 signaling links initiated by foreign networks targeting US mobile users/devices. The rankings are based on detections from May 2018 to December 2019. Threat statistics are based on actual network data and not simulated. The attacks are ranked largest to smallest by calendar year, source country and operator. Additional operators detected may not be shown due to low attack volumes.

2018 Attack Ranking by Country 2018 Ranking by Source Network

Country	Attack Distribution	Network Operator	Attack Distribution
China	85.63%	China Unicom	81.15%
Barbados	5.04%	Flow Barbados	5.64%
Antigua	4.18%	Cable & Wireless Antigua	4.68%
Guyana	0.81%	China Mobile	1.93%
Switzerland	0.75%	Orange Caraibe Guyana	0.91%
Palestine	0.66%	Swisscom Switzerland	0.84%
Guam	0.52%	Wataniya Palestine	0.74%
Virgin Islands	0.51%	Caribbean Cellular British Virgin Islands	0.73%
Bahrain	0.42%	Commnet Wireless US Virgin Islands	0.57%
Armenia	0.31%	Viva Bahrain	0.47%
Aruba	0.24%	DoCoMo Pacific Guam	0.41%
Iraq	0.22%	Telcell Armenia	0.34%
United Kingdom	0.14%	Setar Aruba	0.26%
Kenya	0.13%	Ooredoo Asia Cell Iraq	0.25%
Italy	0.10%	PTI Pacifica Guam	0.18%
Morocco	0.05%	Telefonica O2 UK	0.16%
Russia	0.05%	Safaricom Kenya	0.14%
Maritime	0.04%	Telecom Italia Mobile	0.11%
France	0.03%	Bell Mobility Canada	0.08%
Ukraine	0.03%	Wana Maroc	0.06%
Zimbabwe	0.03%	Tele2 Russia	0.05%
Senegal	0.02%	BTC Vivacom Bulgaria	0.05%
Nigeria	0.02%	Emerging Market Communications Maritime	0.04%
Iceland	0.02%	Bouygues Telecom France	0.04%
Greece	0.01%	Kyivstar Ukraine	0.04%
Bangladesh	0.01%	Telecel Zimbabwe	0.03%
Qatar	0.01%	Sonatel Senegal	0.03%
Bahamas	0.01%	MTN Nigeria	0.02%
Pakistan	0.005%	SIMinn Iceland	0.02%
Guernsey	0.003%	Wind Hellas Greece	0.01%

Key Observations for 2018

1. Mass surveillance attacks were led by networks in China and the Caribbean. China comprised 85% of attacks on US mobile users whereas those from the Caribbean were around 10%. China Unicom was dominant in its method of using advanced attacks to disrupt and intercept communications.
2. There are observations of users targeted by both China and Caribbean networks in 2018 which included Barbados, Bahamas and China Unicom suggesting coordinated state-sponsored espionage and network selling.

2019 Attack Ranking by Country

Country	Attack Distribution
Barbados	28.10%
Antigua	18.70%
Mexico	12.92%
Switzerland	6.01%
British Virgin Islands	4.22%
Guyana	3.87%
Palestine	3.58%
Virgin Islands	3.42%
Aruba	3.40%
Guam	2.48%
Maritime	1.72%
Canada	1.26%
Jamaica	1.22%
Germany	1.07%
Saudi Arabia	1.01%
United Kingdom	0.80%
Russia	0.71%
Bahrain	0.70%
Armenia	0.60%
Panama	0.54%
Morocco	0.49%
Kenya	0.36%
Brazil	0.34%
Bahamas	0.34%
Italy	0.32%
China	0.30%
Philippines	0.29%
Cuba	0.29%
Japan	0.27%
France	0.22%
Zimbabwe	0.13%
Senegal	0.10%

2019 Ranking by Source Network

Network Operator	Attack Distribution
Flow Barbados	29.04%
Cable & Wireless Antigua	19.33%
Telcel Mexico	8.56%
Swisscom Switzerland	6.21%
Telefonica Movistar	4.80%
Caribbean Cellular British Virgin Islands	4.36%
Orange Caraibe Guyana	4.00%
Wataniya Palestine	3.70%
Commnet Virgin Islands	3.54%
Setar Aruba	3.51%
Rogers Wireless Fido	1.30%
Digicel Jamaica	1.27%
STC Saudi Telecom	1.05%
Telefonica Germany	0.99%
Tele2 Russia	0.73%
Viva Bahrain	0.72%
Telcell Armenia	0.62%
Claro Panama	0.56%
Telefonica O2 UK	0.53%
PTI Pacifica Guam	0.52%
Safaricom Kenya	0.37%
BTC Bahamas	0.35%
Telecom Italia Mobile Italy	0.33%
Globe Telecom Philippines	0.30%
ETECSA Cuba	0.30%
Vodafone UK	0.30%
Telus Canada	0.29%
NTT DoCoMo Japan	0.28%
IAM Morocco	0.26%
Wana Maroc Morocco	0.25%
Bell Mobility Canada	0.23%
China Unicom	0.19%

Key Observations for 2019

1. Mobile operators based in Bahrain, Senegal and Zimbabwe sent high volumes of basic interrogation attacks from December 2019 to January 2020 seeking user information such as geolocation.
2. Mobile operators based in Palestine, Italy, Kenya, Greece, and Morocco originated advanced surveillance attacks in early 2019 related to communication disruption and/or interception.
3. In April 2019, Mexico came onto the scene aggressively. Both Telcel and Telefonica Movistar conducted significant attacks throughout the year, with speculation of organized crime as the primary threat actor.
4. China reduced its attack volumes, favoring more targeted espionage, likely using proxy networks in the Caribbean and Africa to conduct its attacks, having close ties in both trade and technology investment.
5. Activity from Caribbean operators remained high throughout 2019, with Cuba entering the scene in May.
6. Switzerland began operations in December 2018 with high activity targeting the US, continuing into 2019.
7. Maritime mobile network operators were used for conducting surveillance activity in 2019, including operations from Emerging Market Communications, Inmarsat and Telecom Italia Maritime.

4G ATTACKS – A PATH TO FUTURE 5G RISKS

4G technology is deployed in over 70% of the world's mobile networks. For international roaming, 4G is used for data services, often with 3G for voice services in what is known as combined attach. Combined attach is a mobile signalling procedure which is often used and allows the device to register simultaneously on both 3G and 4G networks, presenting an ability for the threat actor to engage in multiple attack options using both networks concurrently.

Surveillance operations conducted over 4G networks are often highly successful when using advanced attack methods and are highly exploited into 2020 as a dominant method of attack. Non-voice devices such as those used in industrial applications (IoT) are at a greater risk, as 4G is now widely deployed in roaming and is a significant threat for industrial espionage. The reasons include the following:

#1: Lower Penetration of 4G Security Firewalls

While most mobile operators have deployed SS7 Firewalls, Diameter security capabilities used in 4G networks are much less prevalent and understood, resulting in greater opportunities for threat actors to exploit gaps in security using 4G techniques. 4G attacks generally have had high success rates.

#2: 3G and 4G Mobile Phone Network Information is Not Often Correlated for Security

Advanced state-sponsored attacks on the 4G network take advantage of operators who do not have security features to correlate the location of devices concurrently using 3G and 4G networks. This security feature is often only deployed in more advanced and feature-rich network security firewalls.

#3: Absent Cross-Protocol Threat Detection

Threat actors will easily identify and conduct surveillance operations using both 3G and 4G technologies simultaneously, increasing the success rates of espionage-related mobile attacks.

The Diameter signalling in 4G networks is also used in early deployments of international 5G roaming. This means that 4G network attacks can also be replicated on 5G devices. While 4G and 5G networks co-exist, the likelihood that current vulnerabilities, if allowed to persist will also threaten 5G. There are significant risk implications to 5G devices if immediate actions are not taken to mitigate 4G attacks.

And while steps are being taken in the industry standards bodies to mitigate these risks, the rapid progression of data speeds from competitive mobile operators is far outpacing security measures. If actions are not taken proactively, attacks targeting 5G will quickly be the new focus of cyber threats.

An example of a 4G mobile fake registration attack is shown below, where China Unicom is attempting to lure a US mobile phone away from the NTT DoCoMo network in Japan. Time stamps on the message transactions show movement between the countries under travel conditions between China and Japan during a time when there were bans enacted due to COVID travel restrictions.

Date Time	Attackers Intent	Protocol	Message Type	IMSI	MSISDN	Attacker Network	Attacker Node	Roaming Partner	Roamer Type	Direction	Status of attack	Subscriber Home Network	Subscri Locatio
18-Mar-2020 03:57:55	FASG Diameter Category 3-Time Location Check	DIAMETER	Authentication-Information-Request	31[redacted]110	0	China Unicom	mmecce.mmegi8800.mme.epc.mnc001.mcc460.3gppnetwork.org	China Unicom	Outbound	Incoming	DIAMETER SUCCESS	[redacted]	NTT DoCoMo Inc

Search:

Date Time	Message Type	Status of message	Direction	Originating	Destination
18-Mar-2020 01:03:06	Update-Location-Request	DIAMETER SUCCESS	Incoming	mmec13.mmegibc10.mme.epc.mnc010.mcc440.3gppnetwork.org-NTT DoCoMo Inc(440-10)	[redacted]
18-Mar-2020 03:57:55	Authentication-Information-Request	DIAMETER SUCCESS	Incoming	mmecCE.mmegi8800.mme.epc.mnc001.mcc460.3gppnetwork.org-China Unicom(460-1)	[redacted]

The following section shows the distribution of attacks over 4G networks by source country and network operator.

4G NETWORK ATTACKS – OPERATOR RANKINGS

The following rankings are related to surveillance attacks conducted over the 4G Diameter network. Detections in 2018 were acquired from inter-operator IPX signaling and occurred between August-October. More detailed analysis of 4G attack detections was performed starting in May of 2019 onward.

2018 Attack Ranking by Country

Country	Attack Distribution
China	30.72%
France	20.14%
United Kingdom	15.97%
Bermuda	8.52%
Jamaica	7.57%
Germany	4.84%
Japan	4.49%
Barbados	3.39%
Italy	2.38%
Guam	1.77%
Iceland	0.19%

2018 Ranking by Source Network

Network Operator	Attack Distribution
China Unicom	19.34%
China Mobile	11.24%
Orange France	9.57%
Vodafone UK	8.76%
Bouygues Telecom	8.32%
Digicel Jamaica	7.54%
Telefonica UK	7.14%
Digital Bermuda	8.48%
Flow Barbados	3.37%
Telefonica Germany	3.08%
Telecom Italia	2.37%
KDDI Corporation Japan	2.26%
NTT DoCoMo Japan	2.21%
France Telecom	2.16%
PTI Pacifica Guam	1.76%
Vodafone Global Germany	1.73%
Vodafone Iceland	0.19%

2019 Attack Ranking by Country

Country	Attack Distribution
Barbados	28.44%
Canada	21.51%
Mexico	17.67%
Germany	6.32%
United Kingdom	6.30%
France	6.19%
Japan	5.76%
Jamaica	3.07%
St Kitts	2.73%
Antigua	0.85%
China	0.70%
Spain	0.24%
Belgium	0.20%
Malaysia	0.003%

2019 Ranking by Source Network

Network Operator	Attack Distribution
Flow Barbados	25.88%
Telus Canada	10.67%
Bell Mobility Canada	8.90%
Telcel Mexico	8.41%
Telefonica Movistar Mexico	7.67%
Huthison 3 United Kingdom	7.61%
Telefonica Germany	5.75%
KDDI Corporation Japan	5.24%
Vodafone United Kingdom	4.07%
Orange France	3.46%
Digicel Jamaica	2.79%
Bharti Airtel UP West India	2.51%
Setel/UTS NV St. Kitts	2.48%
Bouygues Telecom France	2.18%
Cable & Wireless Antigua	0.77%
China Unicom	0.63%
Everything Everywhere UK	0.34%
Telefonica United Kingdom	0.23%
Wind Telecom Spain	0.22%
KPN BV Belgium	0.19%

4G Attacks – Key Observations

Key Observations 2018

1. In 2018, 4G attacks by volume were dominated by China source networks. This is a strong indicator that China as a state sponsor conducted advanced mass surveillance efforts using both 3G and 4G vectors, collecting intelligence with a level of adversarial sophistication beyond that of other foreign mobile threat actors. The activity decreased in late 2018 with reductions in attack volumes. Attacks from China often achieved a very high rate of success using 4G attack methods.
2. Many networks from US allied countries including France, UK, Germany, and Japan were identified conducting surveillance operations on US mobile users in 2018, throughout 2019 and into 2020. While it is known that the US and their allies participate in intelligence sharing, any operations on US mobile phones during international travel could be related to law enforcement or national security-related intelligence gathering.
3. Consistent with 3G surveillance methods, Caribbean countries including Barbados and Bermuda were also seen as a source of 4G attacks, though to a lesser extent in 2018 as compared with 3G attacks.

Key Observations 2019

4. While late 2018 and into 2019 saw a reduction in attacks from China networks, there was an acceleration of surveillance activity from the Caribbean. As an example, growth in the volume of 4G-related surveillance more than doubled monthly from Barbados.
5. Caribbean network operators Digicel Jamaica, Cable & Wireless Antigua and UTS St. Kitts were seen as attack sources in late 2019. Specifically, St. Kitts began sending significant volumes of 4G attack-related transactions from December and into 2020 at volumes over 100,000 transactions per month.
6. Border operators in Canada and Mexico both engaged in Purge Location Diameter attacks in significant volumes in late 2019.

04

INSIGHTS AND IMPLICATIONS

Alliances Between Adversaries Uncover Escalated Risks

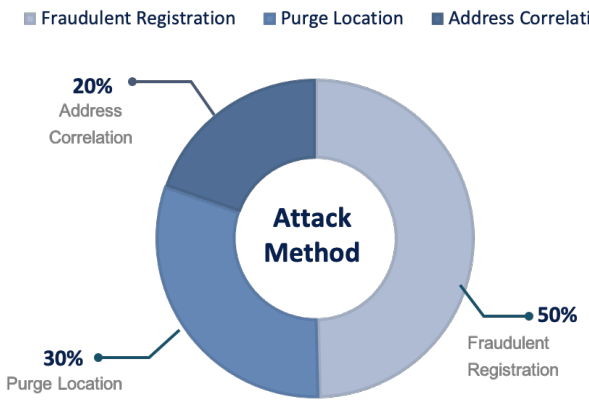
ADVERSARY INVESTIGATIONS

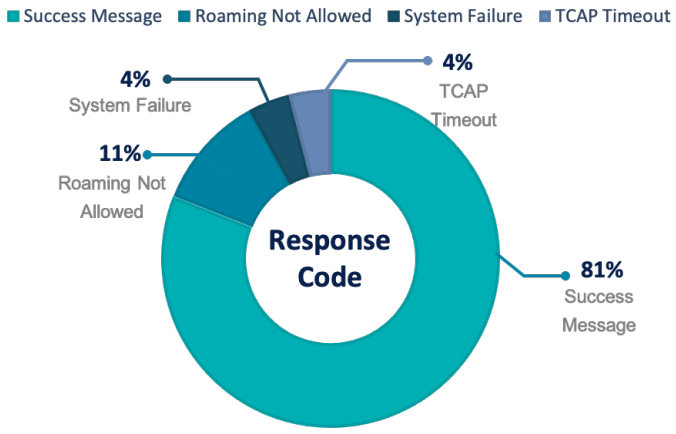
Deeper investigations into mobile espionage shows potential alliances and intelligence coordination between mobile network operators, amplifying the level of future risks from traditional US adversaries. Examination into attack volumes and trends suggests that threat actors are using detection avoidance techniques by using the networks of multiple operators to conduct state sponsored attacks by proxy.

China and the Caribbean – Intelligence Allies or Business Partners?

In 2018, the 2 major mobile networks China Mobile and China Unicom targeted US mobile users in significant volumes. From July through December, 3G attack message volume averaged over 200,000 transactions per day, representing over 3% of all China sourced signalling traffic from that operator: an extremely high distribution.

China Unicom, as the dominant threat acting network achieved a high success rate of the surveillance attacks, as indicated by successful network response codes of 81% for all advanced attacks using a combination of methods shown below.





During this period more than 3000 separate phones were targeted. It was seen that all attacks had been the victims of repeated interception attacks, many with volumes of over 1000 messages. This indicates that the attacks took place over the course of many days where SMS and voice communications may have been intercepted.

Also, during the same time period a cluster of attacks was discovered targeting a group of US phones from networks including China Unicom, Cable & Wireless (Flow) Barbados and Bahamas Telecom (BTC). The attacks against these phones indicated coordination between the operators. This could be achieved by China acquiring network addresses from these two Caribbean operators allowing China to originate attacks, both of which are partially owned by the same parent company Cable & Wireless.

US Mobile User	China Unicom	Cable & Wireless Barbados	Bahamas Telecom (BTC)
IMSI 3850	100	18	3
IMSI 7618	104	17	87
IMSI 6906	18	6	12
IMSI 8346	20	6	14
IMSI 5443	17	6	3

Beyond the multiple attacks against phones among China and the Caribbean networks, the attack trends themselves are notable. As surveillance attacks from China decelerated in late 2018, they accelerated rapidly in more Caribbean countries such as Antigua, Guyana and the Virgin Islands. This activity continued until April 2019, when the attack volumes across all countries decreased on 3G networks and began transitioning to 4G. China has long expanded its investment in the Carbibbean, particularly in the Dominican Republic. Huawei has also had a very close relationship with Cable & Wireless based on investment in 4G upgrades at BTC and network investments with other countries in the region. Could this indicate a strategic signals intelligence alliance between China and the Caribbean? It is also likely that many Caribbean operators have sold or leased SS7 Global Title addresses to other cyber espionage state sponsors and criminal organizations, becoming a threat sponsor either deliberately or unintentionally.

In 2020, Hong Kong operators were also observed attempting large scale attacks with unauthorized signaling messages using the 4G network, which is very suspicious in light of the national security legislation from China passed in June and the subsequent US sanctions. More information and current insights related to China and Hong Kong activity is provided in the **Far From Home 2020 – Part 2** report**.**

Russia and Eastern European Proxies

Mobile operations in Russia have gone through many ownership and branding transitions over the past 10 years. This may influence the type of mobile signals intelligence approaches that Russia has used in recent years. At one point, over 10 mobile operators were active in various regions of Russia. However, many of these networks were consolidated into the ownership of 4 main operators: MTS, VEON (formerly Vimplecom/Beeline), Megafon and Tele2 (formerly Rostov/Rostelecom). Some of these operators have also taken ownership stakes and ventures in other Eastern European countries and in other continents around the globe. As a result, Russia may have influence in providing access to networks outside of Russia due to ownership and affiliation in these networks, increasing the number of attack sources. This could have implications on Russia's ability to conduct surveillance operations sourced from networks outside of Russia.

In 2018, the major Russian operator Tele2 had been detected of originating signaling attacks via its 3G network on a consistent basis. In 2013, network operators Rostov and Tele2 agreed to combine network assets from the completion of an ownership transfer of Rostov, with network consolidation beginning in 2014. Subsequently, in 2016 Dmitry Lebedev, a member of the Tele2 Board of Directors was placed under US Treasury sanctions for providing support to senior Russian officials. Yury Kovalchuk, who is known to be part of the "Inner Circle" of Vladimir Putin was a major shareholder of Tele2 Russia and has also been placed under US Treasury sanctions. This implies an increased risk of business owners with close ties to the Kremlin also with close access to highly vulnerable mobile networks.

Detected surveillance activity from Tele2 declined in late 2018. However, during this time, the Armenian operator Telcell began significant advanced mobile attacks from late 2018 into January 2019. Telcell is a newer mobile operator in Armenia. Armenia has been known to have strategic commercial and military alliance with Russia as part of the EEU and the CSTO.

Vimpelcom, now known as the mobile operator VEON has been detected as a source of relatively small volumes of attacks in 2019 but has since increased surveillance activity against US phones in 2020, which is a troubling sign approaching the US Presidential election.

In 2020, mobile surveillance activity is also seen in the CIS region across multiple potential Russian proxy networks from Ukraine, Belarus and most recently Kazakhstan. Analysis on these 2020 operations is revealed in greater detail in the **Far From Home 2020 – Part 2** report.

Palestine vs Israel – A Mobile Surveillance Tug of War

Palestine has been very active in its surveillance of US mobile devices and was a prominent threat actor in 2018 and 2019 under the network operator Wataniya. Wataniya is now part of the Ooredoo mobile network group and is branded Ooredoo Palestine. Observations are that the attack activity is primarily isolated to US travelers entering into Israel.

Fake registration attacks are the primary method used by Ooredoo, and there is a distinct advantage of Ooredoo Palestine and its proximity to Israel where Ooredoo can use mobile tower signals to briefly acquire a user's mobile IMSI, which is then used to perform periodic surveillance attacks.

These types of attack transactions have occured regularly where travelers to Tel Aviv turn on their mobile phones and Ooredoo forces the device to register onto the Ooredoo Palestine network from within Israel. It is possible that this surveillance approach is designed to target communications interception, as well as to collect footfall pattern information as data collection to maintain a record of US device and user travel pattern history into and out of Israel.

This type of surveillance activity from Palestine has occurred over the last 2 years and is still observed in 2020.

Technical details on how this approach is deployed, with accompanying visual network traces can be found in the **Far From Home 2020 – Part 2** report**.**

Moving Forward

Future Impacts and Security Accountability

Foreign surveillance attacks such as those shown in this report should be of significant concern to the public. If nation states and organized crime entities can actively monitor the location and communications of US mobile phones domestically or in foreign countries, it will represent a security risk to the safety of military or government officials. While US mobile networks have proven to be vulnerable, there are meaningful policies and countermeasures which can be taken to mitigate this activity and ensure a more secure posture with future 5G services.

Over the course of the past 2 years, activity trends in surveillance can be seen from traditional US adversaries, allies, and smaller neutral countries. While generating substance out of these trends is a complex, it is very clear that current vulnerabilities of mobile networks are systematically exploited as a source of intelligence gathering and espionage for foreign adversaries, law enforcement for tracking/monitoring criminal threats and for the execution of organized crime. The threats sourced from small Caribbean countries and multi-vector attacks from small Eastern European and African countries points to widespread and global usage of many foreign networks as state sponsored proxies.

It is also important to note that the attacks seen during international travel also indicate the likelihood of 3rd party sharing of US mobile device profiles, or IMSI's and is possibly sold on the Dark Web. Under normal circumstances, foreign networks would not need to retain the unique details of a foreign phone's IMSI and it's accompanying mobile phone number. However, 3rd party intermediaries who facilitate the exchange of international signalling traffic and provide inter-operator settlement have this information. This is a potential point of vulnerability where surveillance operators could connect and monitor traffic from international signalling hubs between foreign networks and play a role in the ability to execute these attacks. Are mobile industry participants prioritizing revenues over user privacy? It would seem that phone users are completely at the whim of their network provider to ensure communications security.

The shift to 4G attacks over the past year also indicates increased levels of sophistication and an evolutionary trend from increasingly dated 3G attack methods. This shift elevates cyber espionage risks in the era of 5G. 5G deployments are already fully launched in many countries outside of the US including the UK, Scandanavia, Germany, Poland, China, Japan and the Middle East. From some of these same countries we have seen surveillance activity. To what extent can we implicitly trust the security of future roaming partnerships with the networks of these countries?

In summary, it is difficult to imagine public communications networks where there are currently no mandatory requirements to deploy a security appliance on foreign network interconnections. The status quo of implied trust in mobile networks translates into universal risks which drives the foreign surveillance economy. While no posture ensures 100% security and privacy, industry, and regulatory-wide enhancements to protect communications as shown below should be strongly advocated.