AdaptiveMobile Security

Simjacker

Simjacker Technical Paper

10OCT19-v1.01

Legal Notices

Table of Contents

1 Executive Summary

On the 12th of September we revealed high-level details on a mobile vulnerability that we believe was being exploited by an attacker for at least two years. Prior to this, and afterwards, we have been actively sharing specific details with the mobile industry within a responsible disclosure (CVD) process, in order for Mobile Operators globally to determine if they were affected and, if so, to take steps to protect themselves.

At this stage, we can now give an in-depth analysis of the vulnerability and how it is being exploited.

Simjacker is the name we applied to a vulnerability in a technology used on SIM Cards, which we observed has been exploited by a sophisticated threat actor to primarily track the location and get handset information for thousands of Mexican mobile users without their knowledge.

This particular vulnerable SIM Card technology, is called the S@T Browser, the key issue with the S@T Browser technology is that its default security does not require any authentication, and as a result the attacker is able to execute functionality on the SIM card, unbeknownst to the mobile phone user.

In their attacks, we observed the attacking entity target several hundred unique mobile subscribers per week. We believe that prior to discovery they would have successfully tracked the location of many thousands of mobile subscribers over months and probably years.

In our efforts to detect and mitigate these attacks, we have observed the attackers vary their method and application of the attack massively. These variations range from different ways to send the attack, different ways to receive the extracted information, variations in the structure of the request and the extracted information, as well as a host of other modifications to evade detection and blocking. We also observed the attacker experiment over time with new potential forms of attack using the vulnerability. The number, scale and sophistication of modifications of the attack is significantly beyond what we have witnessed from any attacker over mobile networks.

In attempting to attribute responsibility for who is doing these attacks, we took note of several facts. The primary group of targets for this attacker are Mexican mobile users. However, we were able to associate the attacker with a threat actor who execute worldwide attacks on targets from multiple countries over the SS7 network. This SS7 threat actor, who we believe is a surveillance company, has been active from at least 2015, and they are amongst the largest and most sophisticated entities we track as being active in the SS7 attack space. We believe that they developed and used this technique in order to circumvent the layer of SS7 defences which many Mobile Operators have been putting in place over the last few years. While we have additional information, we do not assign any definite attribution in this document other than we believe it is a surveillance company with

extensive signalling and device abilities, who in this case provide intelligence on Mexican mobile subscribers.

The vulnerability has potentially a wider applicability. While we observed primarily Mexican users being targeted, the S@T Browser technology is in use in operators in at least 29 countries worldwide. In theory, subscribers of those operators could be at risk, although the absolute number of vulnerable subscribers depends on the percentage of devices using SIM cards with this technology, and what defences and safeguards the mobile operators put in place. Also, while we observed primarily Location and Handset information being obtained, there is additional functionality which could be exploited via the Simjacker technique. In addition, while we did not directly observe it being exploited, there are other, related SIM Card technologies which are vulnerable in theory and could be exploited.

During the CVD process we shared recommendations, based on practical experience, with the relevant industry bodies in order for them to protect and defend themselves. These recommendations have been communicated to the whole industry. In addition, changes have been made to the standards regulating the S@T Browser technology. If implemented correctly, these recommendations should greatly mitigate the effects of this vulnerability. However, the scale and sophistication of the attacker, compared to previous level of attacks means that Mobile Operators must now prepare to elevate their security to a new standard, with constant operational processes to inspect and look for other types of attacks if they wish their defences to be effective.

2 Background & Timeline

AdaptiveMobile Security produce Mobile Security Solutions which integrate with Mobile Operators, on the core network signalling side. These solutions cover primarily Messaging (SMS, MMS, RCS etc.) and the Signalling side (SS7, Diameter, GTP-C etc.), as well as Intelligence solutions built on top of these. These solutions are run in conjunction with our mobile operator customers by our Threat Intelligence Unit (TIU), which is our managed service team that works to block existing attacks, and detect new ones.

In Q4 2018/ Q1 2019 we saw indications that unusual messaging was occurring in a customer Mobile Operator network. At the same time, we were actively engaged in trying to determine whether we were missing attacks over the SS7 protocol interface in a different mobile operator customer, and were in the process of re-analysing unexpected signalling events that had occurred in the past but had not been solved.

We were eventually able to detect unusual and suspicious SMS events and correlate it with suspicious events we had seen in the past over the SS7 interface. One of these events in particular was a very similar SMS that we had partially captured in Q4 2017 from a highly dangerous and sophisticated SS7 threat actor, that we had seen target mobile devices globally over many years. In 2017, this attack had not been successful, but we needed to know why it had been attempted. The fact we now observed similar suspicious activity meant we had an opportunity to determine their purpose.

The suspicious SMS events we were now observing in 2019 were binary formatted, but their function was unknown. Over a period of time we were able to reverse engineer these SMS and partially determine their malicious function. Over the next few months we spent more time mapping out the full spectrum of attacks that were being executed, as well as the network behind it, in order to block it. We had to change our processes and technology in order to deal with the constant modifications in the attacks, and to ensure they were blocked as much as possible. The changes in attacks were far more sophisticated that the normal attack evasions we observed over the Messaging or Signalling interface, with a high degree of automation and support networks.

In Q2 2019, once we understood exactly how and why these attacks worked in particular Mobile Operators, we submitted the vulnerability we named Simjacker to the GSM Association, through their CVD process. There, it was recognised as a vulnerability, and assigned a CVD number (CVD-2019-0026). From that point on we worked internally with the GSM Association and other industry bodies to ensure that information was shared as quickly as possible within the mobile industry community, and a timeline was established on sharing of information externally. This timeline had to be cognisant of the fact that only Mobile Operators and/or SIM Manufacturers can mitigate any vulnerability, and the vulnerability is relatively easy to replicate by a skilled attacker on unsecured networks, limiting the amount of information that could be shared at the various stages.

This Paper replaces the previous information shared (high-level paper and blog), as it is the main detailed analysis of the attacks and their implications. A separate presentation will also be given at VirusBulletin2019, but in the main this will be an abbreviated slide version of this document.

For reference, the full timeline is as follows

- *First observation of Simjacker related SS7 Threat Actor 2015*
- First Observed related Simjacker Message (retrospective analysis) Q4 2017
- First Detection of Potential Simjacker Activity Q4 2018/Q1 2019
- Customer Defence, Mitigation, Analysis Q1 2019-Ongoing
- GSMA CVD Submitted: Late June 2019
    - Sharing of information within the wider Mobile Community: Q2 2019-Ongoing
- Public Release: September 12th 2019
- Technical Public Release: October 3rd 2019

3 The Attack

In brief, the Simjacker attack involves a specially formatted binary SMS being sent to a Mobile Handset with a vulnerable SIM Card. This binary SMS, contains a number of instructions, which use an unsecured execution environment resident on the SIM Card to execute logic and perform commands both within the SIM Card and from there to the Handset itself.

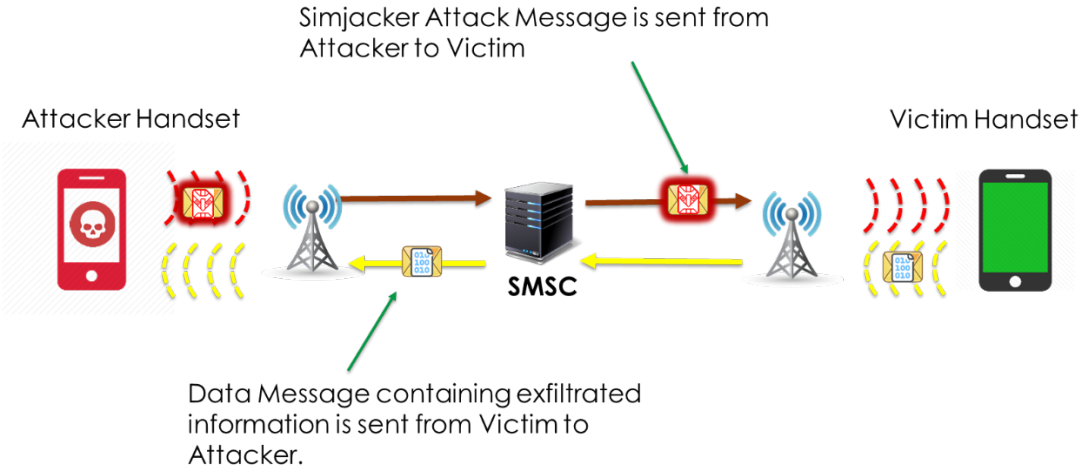
The main attack observed involves two stages:

1) **Attack Stage:** An SMS 'Attack Message' is sent from an attacker to a victim phone number

The Attack Message executable primarily instructs the SIM Card to request Location Information – the current serving Cell-ID of the handset and the IMEI from the Handset, and send the Location and IMEI from the Handset in a 2nd SMS. These instructions are in the form of a series of SIM Toolkit (STK) instructions, which the SIM Card will run to obtain the relevant information.

2) **Exfiltration Stage:** An SMS 'Data Message' is sent from the Victim Handset to a Recipient Phone Number – i.e. the Exfiltration Address.

This activity is not noticeable by the Victim – there is no indication on the handset



Note: This diagram is for illustration. Often the Attackers send the Data Message to a different Recipient Phone Number than that which originated the actual attack. More details of this behaviour are in Section 4

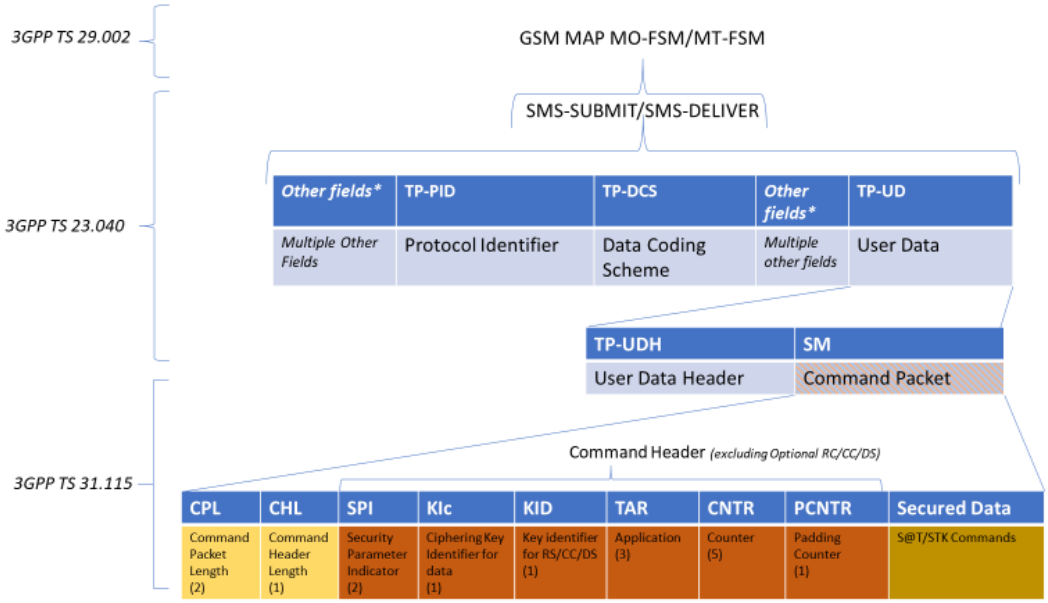
3.1 Conditions for the Attack to be successful

The attack involves two main conditions being met.

3.1.1 SMS Delivery being successful to the targeted Device

The first part is the ability for the targeted device to receive a SMS that contains a set of U(SIM) Application Toolkit Commands[10]. A SMS that contains these commands is commonly referred to as an OTA (Over The Air) SMS. It is one of many types of 'binary SMS', that is, SMS that are not designed for sending ordinary text between people. OTA SMS are normally designed to be sent from an operator to their subscribers to configure the SIM Card and perform other services.

The Simjacker 'Attack Message' is a specific type of an OTA SMS, destined directly for the SIM Card. These are often termed SIM OTA SMSs. The set of Application Toolkit Commands themselves are stored in the Secured Data[11] section of the STK Command Packet, which itself is enclosed within the TP-UD[7] parameter within a SMS-SUBMIT or SMS-DELIVER , that make up the SMS.



Specific binary/OTA SMS messages targeting UICC cards have been demonstrated before on how they could be exploited for malicious purposes. An overview of the history of the most relevant is given in Appendix A. Particularly since similar vulnerabilities identified by Karsten Nohl/SRLabs in 2013 [13], operators have implemented blocking on the ability to send and receive binary type messaging like OTA SMS.

However, from our investigation many binary type messaging blocking implementations, while effective for 'standard' attackers, have not been sufficient to prevent these particular attackers from being successful. This is because in many cases the extent of blocking has been sporadic and hard-set, and there has not been sufficient analysis on an on-going basis of any suspicious activity. The attackers in this case have developed multiple ways of seeking to circumvent these blocks. An overview of various ways that the Simjacker-using attackers have used to circumvent defences in is outlined in section 5.1.

3.1.2 A U(SIM)/UICC card that has the S@T Browser technology deployed on it

This is the novel aspect of the vulnerability. Security for incoming messages that seek to use the (U)SIM Application Toolkit follows the protocol as defined in 3GPP TS 23.048 [1] . Each application on the UICC, such as the S@T Browser, has a Minimum Security Level. The Minimum Security Level (MSL) is used to specify the minimum level of security to be applied to Secured Packets sent to the application (S@T Browser). The Receiving Entity (UICC in this case) shall check the Minimum Security Level before processing the security of the Command Packet. This check is done against the first 5 bits of the SPI1[1] within the Command Header in the received message.

5.1.1 Coding of the SPI

The SPI is coded as below.

First Octet:

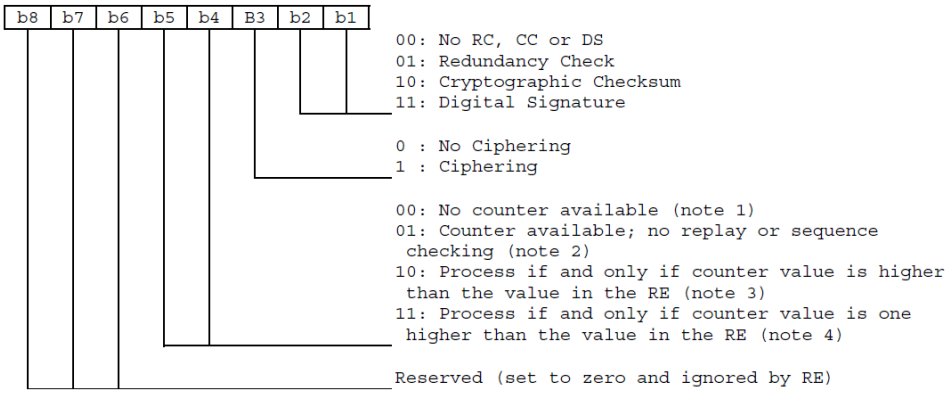


Figure 1: 3GPP 23.048[1] Section 5.1.1 Coding of the SPI

If the check fails, the Receiving Entity shall reject the messages.

The S@T Browser specification, namely section 5.5.2 of the S@T Browser Behaviour Guidelines [2], outlines two particular Security Levels that shall be supported:

[1] [1] – Section A.1.1.4.2.5.2

5.5.2 Security Levels

The following security levels shall be supported by the S@T browser:

SPI	*KIc*	*KID*	*DESCRIPTION*	*NOTES*
0x0000	0x00	0x00	No security applied	Shall be supported for incoming (MT) and outgoing (MO) messages. This security level is not recommended for Administration protocol.
0x1200	0x00	0xX5	Triple DES Cryptographic Checksum (8-byted MAC); counter higher	Shall be supported for incoming (MT) messages. This security level is not recommended for Pull protocol.

Figure 2: S@T 01.50[2] v4.0 Section 5.5.2 Security Levels

Four categories of message are included in the S@T Browser specifications:

- Pull
- Administration
- High Priority Push
- Low Priority Push

High Priority Push and Low Priority Push are the type of messages that are used in the Simjacker attack.

As we can see above [2] recommends that the “no security applied” level is used for Pull messages, and that the Triple-DES cryptographic checksum level is used for Administration messages. The issue is there is no explicit recommendation for what security level should be used for Push messages, but it is clear that the zero-security level is widely used for these in practice. In our analysis of potentially affected operators (see section 7.1), we observed that the overwhelming number of operator implementations of S@T Browser High Priority Push and S@T Low Priority Push used the non-security parameters settings for these messages. This means that any attacker can send a Push message to the target device, with no need to apply any kind of cryptographic authentication, and the S@T Browser will accept the message.

3.1.3 Other Conditions

There is additional condition on the attack being successful, that is related to the capabilities of the SIM Card itself, namely the EF_{SST}.

The values in EF_{SST} are defined in 3GPP TS 51.011[9], but the relevant ones are

- Service no. 26 – Data Download via SMS-PP
- Service no. 29 – Proactive SIM

These two services must be allocated and activated for the message to actually be processed by the SIM Card, but these capabilities are normally common.

3.2 Structure of a typical Simjacker Message

At a logical high level, a typical Simjacker message observed in the wild has the following structure.

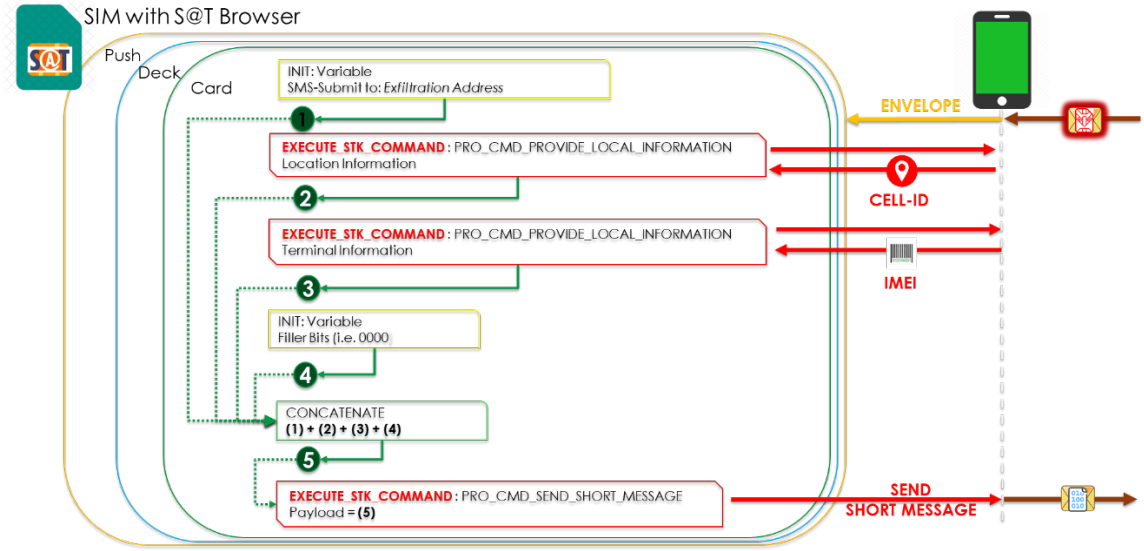


Figure 3: Simjacker Attack Message Structure

The following is the explanation of the commands. Note, in most of the below there are many variations of the attack observed, these are covered in more detail in Section 5.

3.2.1 Simjacker S@T/STK Command Order

We use for shorthand S@T for commands that are defined in [3] , and STK for command that are defined in [10]. If other commands use different specifications they are indicated. Both the S@T and STK commands are defined as TL[A]V variables.

1. S@T Push/ Create Dynamic Deck/ Create Card

A sequence of Push, Create Dynamic Deck and Create Card commands are run. In the attacker's case they normally set a bit that indicates that the Deck shall not be cached by the S@T browser. This is done to ensure there isn't any trace of the message preserved on the SIM. In addition, the attackers often use a ResetVar Attribute value in the Card declaration to ensure that the Variables are reset, after the commands finish see Section 3.2.2

2. S@T Create INIT Variable

The first INIT Variable contains a fully formed SMS-SUBMIT Message Header which was received in the Simjacker message. Its main interest to us is that it contains a TP-DA. This is the Destination address to which the subsequent Data Message should be sent to (i.e. the Exfiltration Address). This information is stored in Variable 1.

3. **EXECUTE STK COMMAND: Provide Local Information – Location Information according to current NAA**

This is a PROVIDE_LOCAL_INFORMATION that has a Command Qualifier of type Location Information. This is sent to the Handset. The response information from the Handset is the current serving Cell of the Handset, and is stored in Variable 2.

4. **EXECUTE STK COMMAND: Provide Local Information – IMEI of the terminal**

This is a PROVIDE_LOCAL_INFORMATION that has a Command Qualifier of type Terminal Identity. This is sent to the Handset. The response information from the Handset is normally the device IMEI, and is stored in Variable 3

5. **S@T Create INIT Variable**

This is normally a set of repeated values, such as 00's or other values. We term this the 'Filler' Byte(s). This is generated as a form of pseudo-randomization in both the structure of the Attack Message and the subsequent Data Message. It can also be used as a form of lengthening of the Data Message. Multiple Filler bytes can be present, in different locations. In this example there is only one Filler. This is stored in Variable 4. Further use of this field is discussed in Section 5.1.

6. **S@T Concatenate**

By using this S@T Browser command, the preceding Output Variables are concatenated into a single string. In this example the concatenation sequence is SMS-SUBMIT Header+Cell-ID+IMEI+Filler. It is important that the SMS-SUBMIT Header specified earlier is the first element concatenated in the sequence, in order for the subsequent text message being sent to be deliverable. The order of the others can and does vary. The output of this is stored in Variable 5.

7. **EXECUTE STK COMMAND: Send Short Message**

This is a SEND SHORT MESSAGE Command, which calls the value saved in Variable 5. This string is then sent to the Handset, which then transmits it to the mobile network to the destination number controlled by the Attacker.

As stated earlier, there is no interaction with the mobile user during any of this. There is also nothing stored in the target's SMS inbox or Outbox, nor in their SIM card message store.

3.2.2 Variable Management in the Simjacker Attack

Variables in the S@T environment are where the respective pieces of information (SMS-SUBMIT Header, Location, IMEI, Filler etc) are stored prior to be sent externally. For the Simjacker attacks the Variables themselves are always stored as temporary variables - see Section 5.3 of [3] -this means they are cleared when:

- the S@T browser goes to the idle state;
- the S@T browser starts a card with ResetVar flag set in the card attribute;
- high priority push is received.

The S@T browser goes to the idle state (S@T browser exits) after the last command of the card has been executed and no branching has been done.

In observation, we see that the attackers are well aware of the need to keep the temporary variables cleared. In situations where they request Location information in quick succession (2 messages to the same target in less than a few seconds) they specify the 2nd request as a High Priority Push, to ensure that there is no retention of the previous temporary values set in the 1st, Low Priority Push Message.

In addition, to further ensure variables are not overwritten, the ResetVar flag is set in the Card value over >44% of the time. The ResetVar is used to reset (i.e. remove) all the temporary variables before executing the first command in the card.

4 Simjacker Attacker Structure and Operating Procedure

The attackers we detected using the Simjacker message vary their methods and use of the Simjacker vulnerability constantly. This is due to changing conditions, objectives and defences being put in place.

This makes profiling what is the 'normal' use of the vulnerability difficult. Nevertheless, we can show what is the typical activity in a time period, as a representative guide. In the below analysis, we have taken a **typical 31-day continuous time period**, from sometime within the last year. This period is a time where we actively engaged in detecting and blocking these attacks with our mobile customers. From retrospective analysis, it is also similar to other time periods when blocking was not occurring, so this 31-day period is representative of the activity throughout the larger timespan.

4.1 Volumes in Period Targeted

In this time period we observed > **25k Simjacker messages** attempted to be sent to >**1500 Unique Identifiers**. These identifiers represent unique Mobile Subscribers being targeted.

The overwhelming majority of targeted mobile subscriber we have observed are from **Mexico**. We have observed at times these particular attackers occasionally target mobile subscribers from **Colombia** and **Peru** but these are far smaller compared to Mexican targeted devices.

In this time period, **45%** of subscribers were targeted only once, while a few individual subscribers were targeted thousands of times in this period.

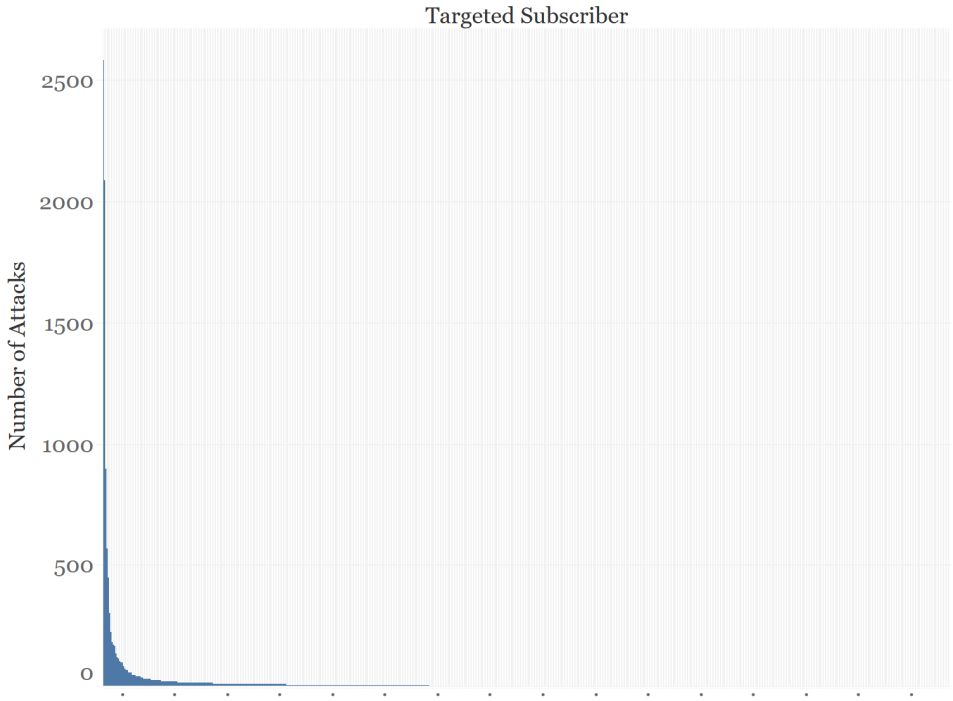


Figure 4: Distribution of number of attacks per each subscriber

Over **69%** of targeted Mobile Subscribers were only targeted on one day, a very small number were targeted almost every single day.

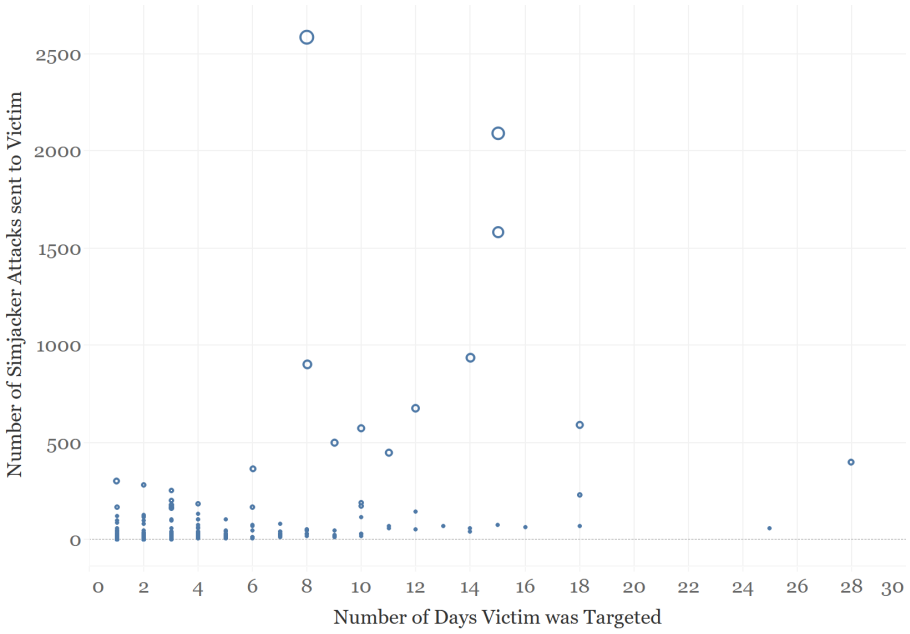


Figure 5: Number of Attacks per Subscriber v Number of Days Subscriber was Targeted

Overall, we can see that a large amount of targeted subscribers are only queried once. On the other hand, a few subscribers are intensely tracked over long duration periods. There is also a long continuum in between these two extremes. Generally, the system seems to be used for multiple different tracking models.

4.2 Information Retrieved

The primary objective **(89.19%)** in these attacks is to obtain both Location Information according to current NAA (Serving Cell ID) and IMEI of the terminal. These are obtained via the Proactive Provide Local Information command. Other Proactive commands are also intermittently **(4.25%)** executed.

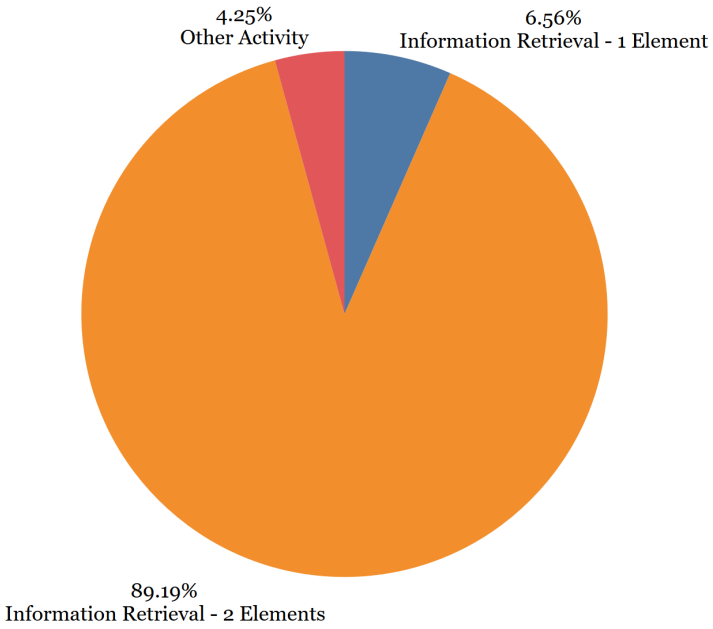


Figure 6: Types of Proactive Command Executed

Other Activity in this case are commands that the attackers execute probably for testing of the functionality and effectiveness of the attacks, i.e.

- Display Text (Test Messages),
- Launch Browser (Test websites),
- Set Up Call (test recipient number) and
- Send USSD (test PIN change)

The breakdown of Information retrieved is of the following type:

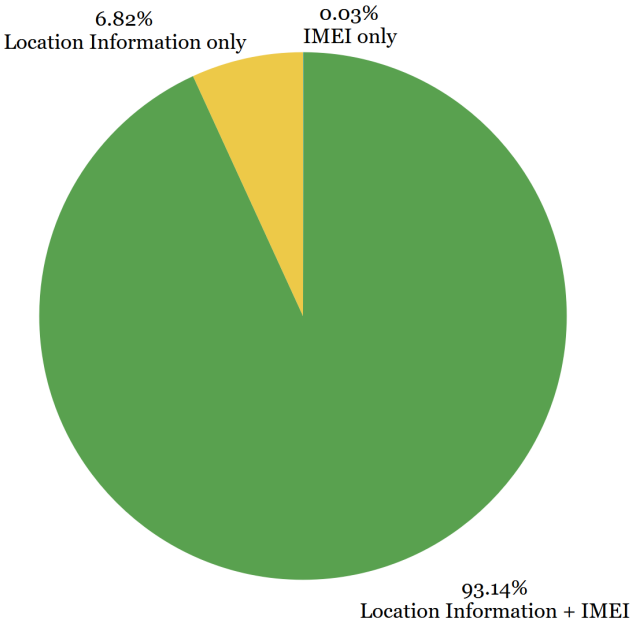


Figure 7: Type of Information being Retrieved

4.3 Simjacker Attack Packet Format

4.3.1 High Priority Push v Low Priority Push

The vast majority **(99.23%)** of Attack messages sent in this period were S@T Browser Low Priority Push messages. High Priority Push messages were only used when targeting the same victim in quick succession after a Low Priority Push message, see Section 3.2.2 for more details on how exactly this works.

4.3.2 SMS Packet Header Encoding

Within this specific time period, we observed over **1000 different types of encoding combinations** attempts of the Simjacker Attack Packet Header i.e. the Protocol ID, message class and the user data header.

We believe that the varying encoding combinations of the header was done to attempt to avoid Mobile Operators network defences (see sections 5.1.3).

4.3.3 Simjacker Attack Message Variants

Within this specific time period, we observed we detected over **> 860 Simjacker Attack sub-variants** in the actual SMS Packet. We identify variants that execute different features, have different values (excluding source/exfiltration addresses) and different Variable IDs.

We believe the variations in the actual Simjacker Attack packet itself was done to also potentially avoid defences, or potentially to tailor the attack per specific Sim card type. Section 5 explains in more detail the techniques used by the attacker.

4.4 Infrastructure Used by Attacker Network

Sending Attack Message: In this period, the Sending Infrastructure comprised of over **70 sending number of devices** sending the attack messages. The main sender sent nearly 22% of attacks, but most sending devices sent less than 5% of attacks in this time.

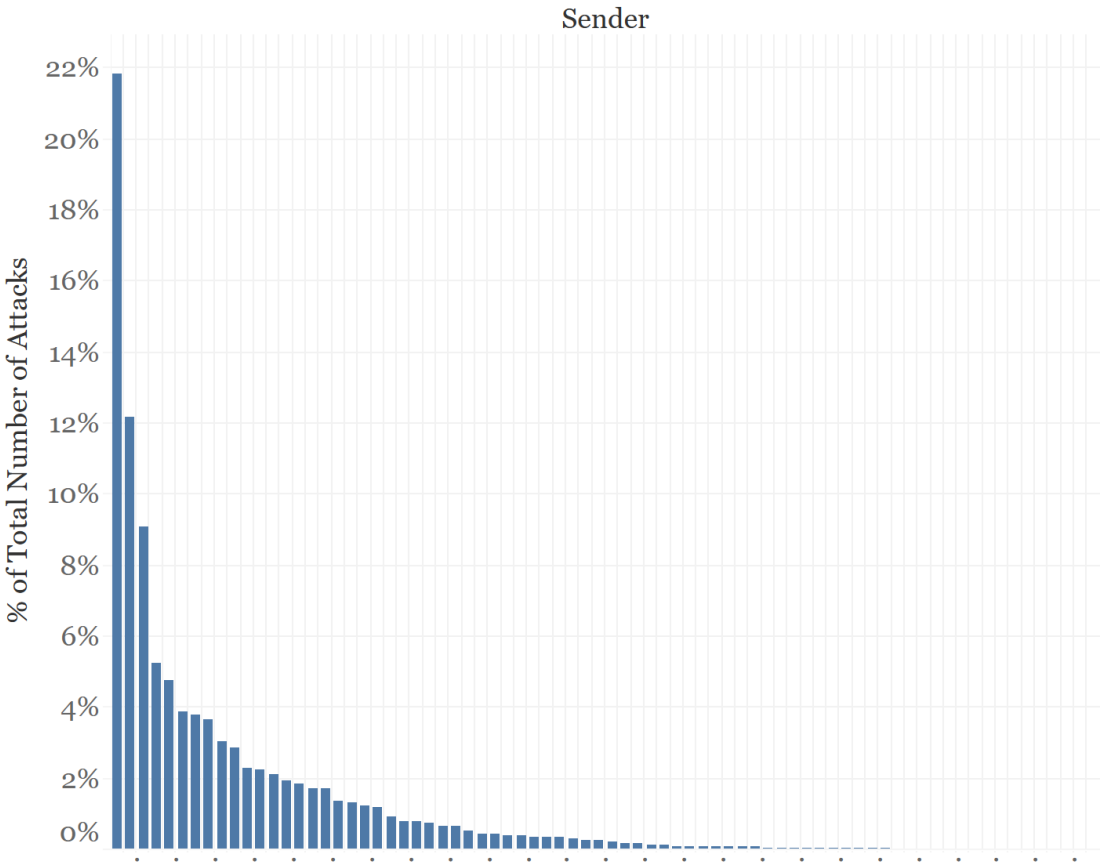


Figure 8: Simjacker Sender % Volumes

Receiving Data Message: Within the Simjacker Attack Messages, we identified over **60 unique Exfiltration address numbers** in the embedded SMS-Submit, these are sent the subsequent Data Message. It seems there were 4 main exfiltration numbers that were designated to receive any subsequent Data Messages in this period, every other number received less than 5%.

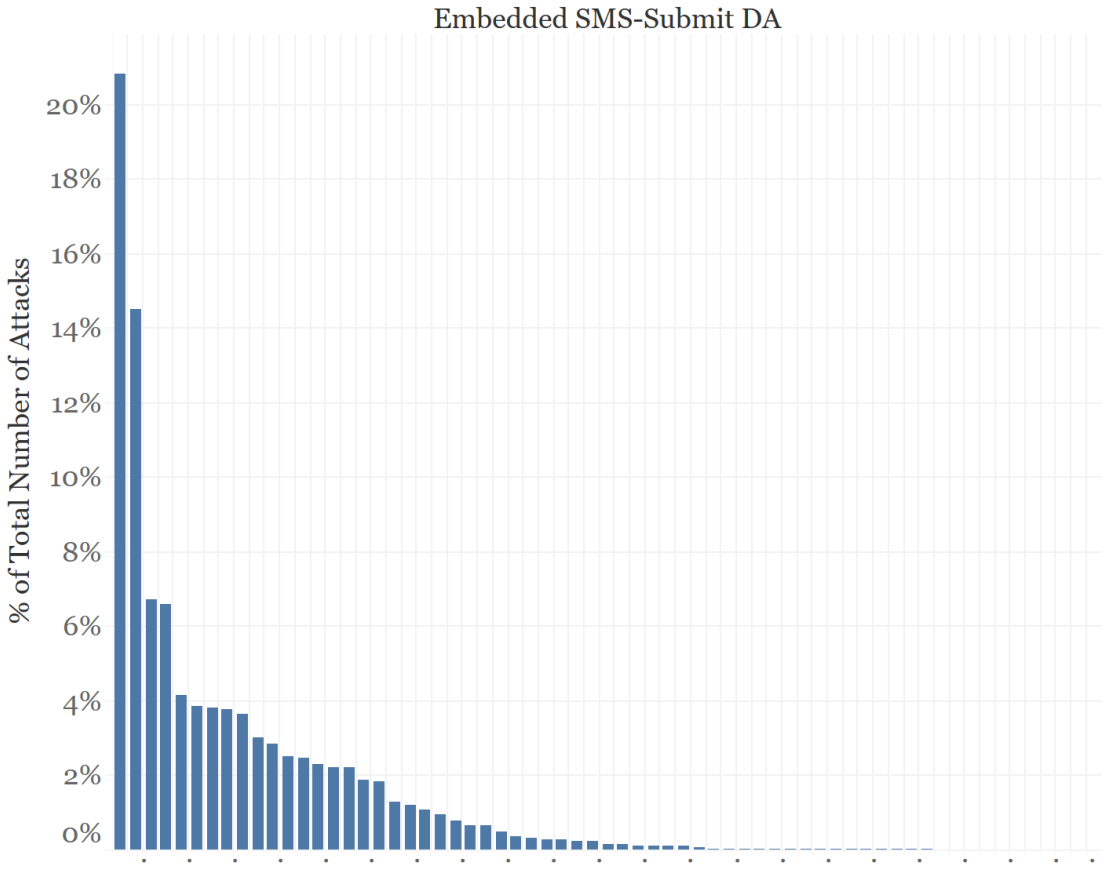


Figure 9: Exfiltration Address % Volumes

We determined that **57%** of the time, the Sender number is also the exfiltration number, but it can vary between particular Senders. In earlier time periods we noticed that the rate of the sender number equalling the exfiltration number was much lower. The high rate here is we attribute due to the Attacker infrastructure coming under pressure due to newer defences in place and becoming simpler.

4.5 External SS7 Network Sources

While the vast majority of sources of the Simjacker Attack Message came from 'real' devices – that is, connected mobile devices that submitted SMS messages via the mobile network, we do observe a certain number of Simjacker messages coming from external, known malicious, SS7 addresses. This means that the attackers also had access to the SS7 Network which is the interconnect network between mobile networks. During this period of time we observed several SS7 addresses - SCCP Global Titles (GTs) - based around the world, attempting to send SMS messages with the Simjacker Attack message to Mexican mobile subscribers.

We did not include these external volumes in the previous measurements. Relatively they account for just under **6%** of total Simjacker attack messages sent in this period.

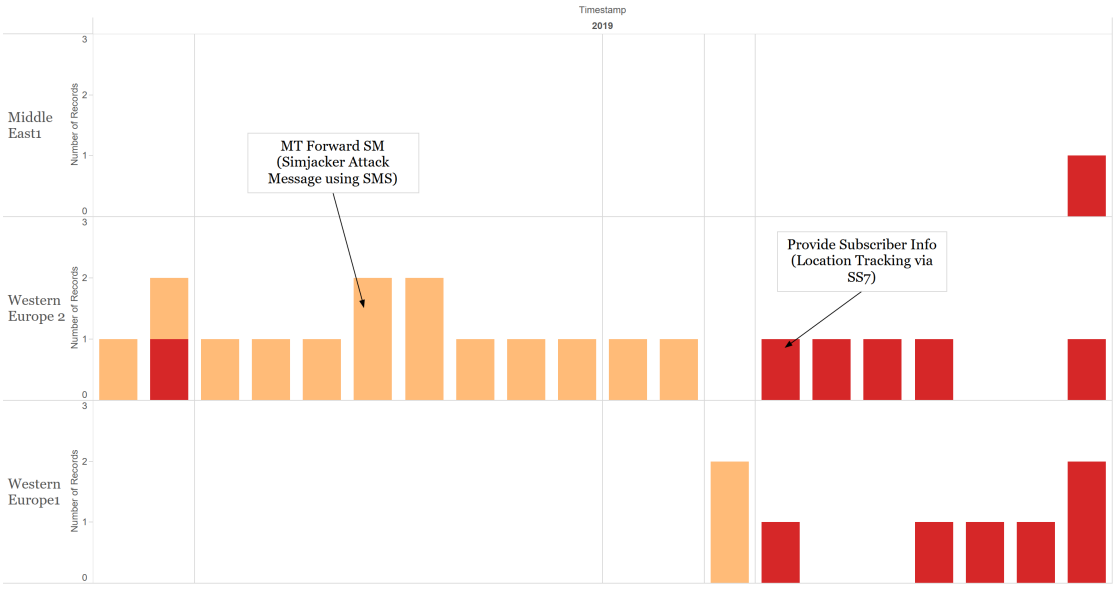


Figure 10: Simjacker and SS7 attacks against single targeted Subscriber

We also observed in this time period, on multiple occasions, the attackers attempting to use dedicated SS7 attacks to obtain the same information, if their initial Simjacker attempts were unsuccessful. The above graph shows the sequence activity of 3 GTs in 3 countries that attempted to obtain location information of a single subscriber over 2 days. Initially the attackers attempted to retrieve this information via SMS messages using the Simjacker vulnerability (Orange), before trying to use GSM-MAP Provide Subscriber Info packets (Red), which also requested Cell-id and IMEI.

A number of other attacks were also attempted over the SS7 interface from these same GTs during the time period under question. As well as location tracking, these attacks also included attacks methods designed for communications interception and information harvesting.

The relative amount of Mobile Device Originated Simjacker Attacks **(94.3%)** v SS7 Simjacker SMS **(5.84%)** v SS7 Location Tracking **(0.13%)** can be shown below. This shows that obtaining location information (Cell-ID) is far more common, for these targets, using the Simjacker method. 'Classical' SS7 attacks are generally preserved for specific, presumably higher priority, targets.

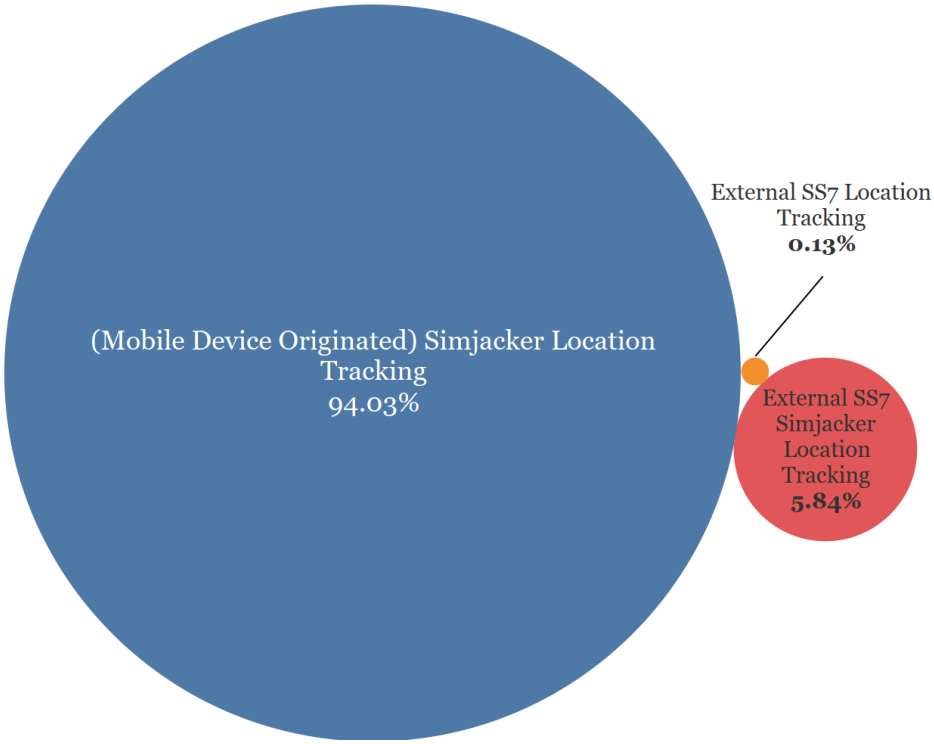


Figure 11: Attacker's Method of Location Tracking via Source

The use of SS7 attacks, in a tight co-ordination with Simjacker activity, strongly indicates that the attacker has access to the SS7 network from global sources. It allows us to use the intelligence that we have built up over many uses in filtering attack over the Mobile Operators' core networks. Namely, we have built up tools like our SIGIL[2] platform that profiles and record the methods, techniques and patterns that various hostile actors exploiting the SS7 network use. By using these tools, we are then able to begin to attribute the Simjacker attacks to specific hostile actor. More details of these attribution are in Section 6.

[2] https://www.adaptivemobile.com/products/sigil-signalling-intelligence-layer

5 Attack Format and Evolution

We have observed the Attacker Entity use multiple different methods to avoid detection over the entire period that we have been aware of it. Below is a sample of some of these techniques. The extensive range of these techniques illustrates how complex the attackers are; and their range of abilities.

5.1 Avoidance techniques

5.1.1 Alternative Input Routes

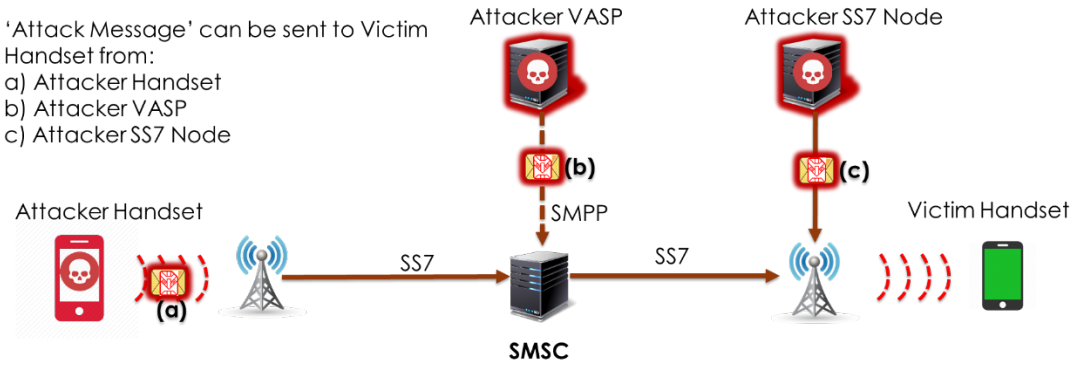
The primary method for injection of the Simjacker Location attacks is via Handset, that is messages were submitted to the mobile network via SMS-SUBMIT/MO-FSM packets. However different methods are possible and were occasionally observed in the wild, as follows:

- **A2P Sources**

  We detected SMS Simjacker Attacks being sent via VASP Shortcodes, which directly submitted these messages to the targeted Operators SMSC. This was done in order to avoid filtering setups which may assume that messages from VASP sources are safe/trusted.

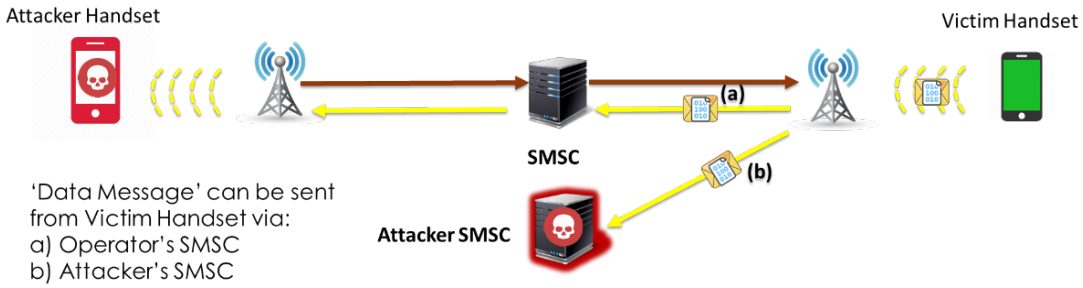
- **SS7 Sources**

  We detected SMS Simjacker Attacks being sent from external SS7 SCCP Global Titles worldwide, being sent to the targeted subscribers currently serving MSC/VLR. This was done in order to exploit any unfiltered ingress points into the operator mobile's network.



5.1.2 Alternative SMS Exfiltration Route

The primary method for exfiltration of the Data Message is to a 'real' device, which is submitted from the target's handset, via his mobile network, to a 'Accomplice Device' controlled by the attackers. However, we observed alternatives to this.



We detected the subsequent Data Message being sent via an alternative SMS Centre, to a dummy number. The use of an 'open SMSC' other than the operators-specified one was accomplished by specifying a different SMS Centre to use in the payload of the original Attack Message. Specifically, this was executed as an additional Address parameter in the SEND SHORT MESSAGE Command.

There are two potential reasons for the use of an alternative SMSC for exfiltration.

1) To avoid a network operator detecting these Data Messages being sent, as this outbound traffic would not travel via their own SMSC
2) To avoid any billing records being generated for the Data Message, if these are generated at the SMSC

5.1.3 Alternative SMS Attack Packet Encoding

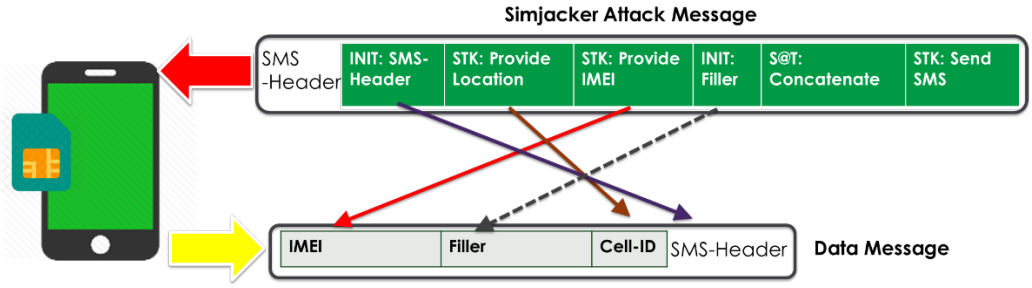
We observed extensive modifications and alternations of the format of the SMS Header in order to avoid blocking. All packet encoding fields at the SMS Transfer Layer (e.g. TP-DCS, TP-PID, TP-UDH, TP-UD) and additional fields in the Command Header have been modified to varying degrees, as the attackers cycle through these values continuously. While not all subsequent combinations are actually useful – i.e. invalid combinations mean that the message is then not understood by the Handset as a SIM OTA message and so not routed to the SIM card – a number of non-standard combinations do turn out to be routed to the SIM card.

In addition, there have been a number of other modifications to the SMS Attack Packet observed. These include:

- Multi-part concatenated SMS messages – the splitting of the Attack Packet over multiple segments
- The use of Reserved Values in the SMS Header
- The use of corrupted/ parameters in the SMS Header
- Omitting specified values in the SMS Header
- Other variations of the SMS Attack packet encoding.

5.1.4 Variations in Data Message Format

We specified in Section 3.2 that the Attacker commonly include in 'Filler' bytes into the Attack Message, which subsequently get sent back in the Data Message. These are inserted we believe for both as a form of obfuscation of the Data Message, and to cause variations in the attack message.



As well as the Filler bytes varying, there can be multiple instances of these, as well as being placed in different locations. We observed the attacker constantly changing the position(s) and value of these Filler bits in the many sub-variants of the Simjacker Attack message.

5.1.5 Other Variations

We have observed other variations, including:

- Sub-Variants of the Attack Message, depending on the target. We are currently tracking over a thousand unique sub-variants, based on structure, functionality requested and makeup.
    - The individual variants might also be tailored to specific SIM Cards/handsets, as well as for avoidance of any exact match based defences
- Corrupted Attack Message Encoding at different levels of the underlying SS7 packet.
- Continuous new Source Addresses of the Attack Message
- Continuous new Exfiltration Addresses to send the Data Message to
- Different S@T Push Type (cycling between Low and High)
- Additional STK Commands (see below)

There are also other variations in use which we currently are not disclosing, in order to preserve effectiveness of our detection and blocking of these messages.

5.2 Additional Functionality Attempted by Attacker

The primary use of the Simjacker exploit by the Attackers is for Location and IMEI information retrieval, though we have observed the following Commands being executed by the Attackers. We believe that these commands were being run as a form of testing of defences and what is possible in various Mobile Operators and devices. We observed:

- Retrieval of Different information, including
  - ICCID, (radio) Access Technology,
- SS & USSD Command Execution, including
  - Get IMEI as stored in the network, Change PIN Code, Check Balance
- Set Up Call
- Send DTMF Tones
- Open Browser
- Run AT Command

As well as that, other functionality was observed which is being investigated. The Run AT Command in particular is interesting. While previous research[3] has shown that AT commands are quite dangerous, it must be cautioned that it is highly unlikely the attackers succeeded using this, for a few reasons. One of these is that AT-Command via STK requires specific settings both on the SIM Card and on the Handset Terminal Profile. An inspection of Terminal Profiles in open source databases[4] reveals very few devices that have this setting. Also, the S@T Browser does not formally support the Proactive Run AT Command.

[3] https://atcommands.org/
[4] https://terminal-profile.osmocom.org/

6 Attribution & Evaluation

6.1 Attribution of Simjacker Attacks

Attribution is always difficult in cyber security, and it is no different in telecom security, however there are a number of pieces of information that help us narrow down who could be using this.

1) While we observe different variants, the overall structure and functionality of the Simjacker attacks are quite similar, so we believe that it is being used by a single attacker entity

2) While we have also observed targeting of Colombian and Peruvian mobile subscribers using the Simjacker attack, what we have observed are this attacker's main targets are Mexican mobile subscribers, so we can conclude it has a specific interest in those.

3) We have seen a close relationship between the Simjacker attacks and a specific Threat actor, who is active over the SS7 interface. Specifically, we have seen some of the same external SS7 sources use both Simjacker and SS7 attack techniques, along with other multiple correlations. This means we can tie the Simjacker attackers with these SS7 sources. These SS7 sources we have previously observed are part of a specific, single Threat Actor that we track being active globally. We mean globally as in this threat actor has been observed attacking over SS7 many of our mobile operator customers worldwide, where they target 'disparate' mobile subscribers.

4) Based on experience that we have built up over the last few years this threat actor pattern does not match a specific nation-state technology origin. Rather this Platform matches the activity of a surveillance company, which sells access to its SS7 attack capabilities to a wide range of nation-state customers. This accounts for its disparate range of targets.

5) We also note that in the past, multiple surveillance companies have been implicated in the targeting of Mexican mobile users. This further strengthens the likelihood that these Simjacker attacks, primarily targeting Mexican mobile users, have been provided by a surveillance company.

6) The complexity of the attacks, and the fact that it has access to multiple sources, means that it is in use by a complex, advanced entity with a wide range of skills, experience and resources. This matches the specific SS7 threat actor, who in our experience operate one of the biggest and most active SS7 attack 'platform' that we have observed in the world. It is a main source of malicious attacks over the SS7

interface, and typically tries the most advanced types of attacks. It is also a threat actor that we have detected being active over SS7 networks for several years, when we first began to deploy Firewalls over the SS7 interface for Mobile Operators. The fact that Simjacker would be used to obtain much of the same information available over SS7, which would not be available due to improvements by Mobile Operators, further strengthens Simjacker attractiveness to a surveillance company who use SS7 techniques.

7) We have more specific information on which surveillance company it could potentially be, but unfortunately, we are not able to reveal this information. To do so would reveal specific methods and information which would damage our ability to detect and block these attacks globally.

Our conclusion is in this case we believe the provider of the Simjacker attacks is a specific large-scale, experienced surveillance company, which has multiple customers worldwide for its SS7 attack functionality, and in this case, we observe it being employed to track the location and obtain handset information of primarily Mexican mobile phone users.

6.2 Overall Evaluation of Simjacker Attacks

We can see that the Simjacker location tracking attack method is being used for a range of uses, it is a continuum that varies between large volumes of once-off attacks for large numbers, to very intensive attacks on specific target subscribers. This means that it is being employed for multiple functions and probably has multiple internal users.

The volumes are also sizable, while we observed over 1500 unique identifiers being targeted in this period, we would expect that **ten to twenty thousand** mobile subscribers would have been targeted within any particular year. The primary objective of these attacks is to obtain both Cell-Id and IMEI of the tracked subscribers, but there is also a certain amount of other activity ongoing. We expect that this activity extended beyond what we directly observed. We can also see that the Simjacker network uses a large infrastructure of sending and receiving devices to extract its information, which we observe changes continuously over time.

Based on the relative volumes of Simjacker SMS attacks from handsets, to Simjacker SMS attacks from external SS7 points, to ‘classic’ SS7 Location tracking attacks, we can say that the Simjacker SMS method is the primary method to obtain location information for these targeted subscribers. This is probably due to several reasons:

- the ease of access (only requiring a SIM and a GSM Modem) that is in contrast to attacks over the SS7 network, which require SS7 access that is difficult to obtain.
- Defences put in place - SS7 network now tend to be much more heavily monitored and defended than they were in the past.

- The volume of targets being attacked. Even over an undefended SS7 network this level of location tracking would not be expected due to suspicions it would raise.

The main limitation of Simjacker versus SS7 methods, is that the S@T Browser is only prevalent in certain countries, unlike SS7/Diameter, which is built into the fabric of the global mobile telephony system. But for attackers who wish to target Mobile Operators, which have the S@T Browser technology in place, then it affords a simple access system for them to use, especially if defences are already in place on the SS7 side.

While the access to send Simjacker messages may be much simpler than equivalent SS7 attacks, the attack format and evolution is considerably more complex. The Simjacker attacks rely on the understanding of multiple protocols (SS7/SMPP/GSM-MAP/SMS/STK/S@T) and technologies (SIM Cards, Mobile Devices, Mobile networks). This is considerably wider that the knowledge needed for attacks just over the SS7 interface, or attacks seen before over the SMS interface.

In addition, the extreme modifications and avoidance techniques the threat actor used are far beyond what has been encountered over Core network signalling interfaces to date. We can safely state that Simjacker represents a leap in complexity from previous SMS or SS7/Diameter attacks, and show us that the range and possibility of attacks on core networks are more complex than we could have imagined in the past.

This means that methods to detect and defend against attacks like these must also become more advanced. Several years ago, the Stuxnet attacks represented an increase in complexity and resources behind the creators of offensive malware, making obvious that there was a new paradigm that the cyber security industry had to respond to. While not at the same scale of complexity or impact, the Simjacker attacks and its associated system also represent the emergence of a new form of offensive mobile attacks, from well-resourced, technically expert and determined attackers, which Mobile Operators will have to respond to as well.

7 Wider Applicability of the Vulnerability

7.1 Countries/Operators Potentially Affected

The main focus on determining the reach of the vulnerability was what number of SIM Cards have the S@T Browser deployed on them. During the GSMA CVD process a list of affected countries or number of affected SIMs was difficult to obtain, other than it was understood that it would be a minority of SIMs globally due to the fact that the S@T Browser technology was not prevalent worldwide.

In the absence of specific numbers, the following is the method we took to understand what countries were potentially impacted / number of affected devices, as well as the limitations in this model. Also, this is not an estimation of the risk of these SIM Cards being successfully exploited, it is just the vulnerability. If Mobile Operators put in place rigorous and comprehensive defences which are monitored continuously over their network to stop these attacks, then even though vulnerable SIM Cards may be present, the risk is greatly reduced. However, as we have shown, the Simjacker Attackers have employed multiple evasive techniques, which would be beyond what the typical Mobile Operator would have planned for. Therefore, it is prudent to profile the scale of the vulnerable SIM Cards on their own.

During our investigation into these attacks, we analysed whether Simjacker type messages were sent to inbound roamers over the SS7 network over the last 3 months. As a side-effect, we could then use this as a proxy of determining what countries use the S@T Browser technology in a vulnerable manner. Specifically, this allowed us to see if:

- S@T Browser Push Types messages.
- with a Command Header indicating that no security was applied
- was sent from a Mobile Operator in a foreign country
- to outbound roamers over the SS7 network

If all 4 conditions were met this gave us a metric that

a) S@T Browser infrastructure, run by an Operator, was being actively used to send messages of this type to subscribers from that country and
b) that the no security level was being applied, so in theory the SIM Cards used by those subscribers were vulnerable.

We also further excluded a number of source countries if they were

- sending Simjacker attacks,
- sending very low volumes of S@T Browser traffic, or
- if they were sending some legitimate S@T Browser messaging for a different mobile operator.

Based on the numbering plans of the source and destination of the remaining analysed activity we were able to detect that at least **29 countries** actively used this technology.

The below map shows those countries distribution.

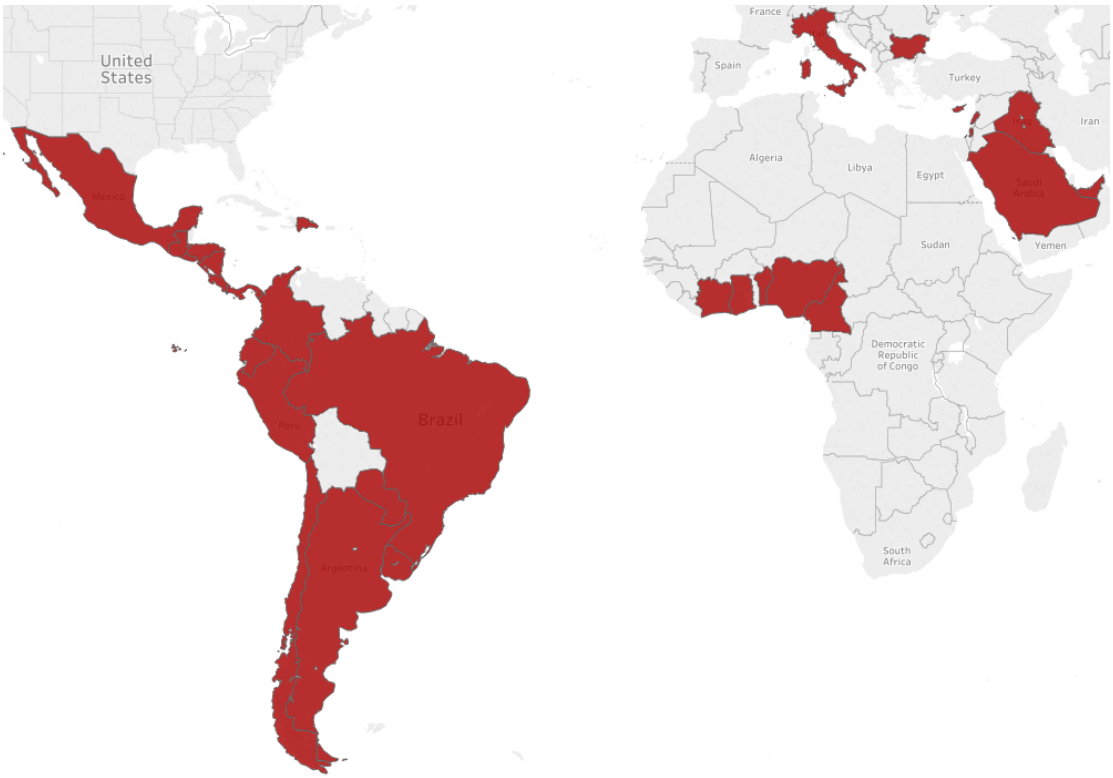


Figure 12: Countries Actively using S@T Browser with no-security level set

The cumulative population of these S@T Browser-using Countries came to 1.02 Billion[5]. This is not a number of affected devices/SIM Cards, but unfortunately it is quite difficult to determine the number of affected SIM cards. There are several variables which would determine whether the actual number of affected devices is lower or higher than this.

Lower:

- Not every operator in the country may use this technology. In follow-up analysis, based on the preceding method, we used numbering plans to identify the individual operators within these countries sending the S@T Browser type messages, and then count reported subscriber numbers of those operators. This varies by country and region. From our analysis we could identify **61 Mobile Operators** (excluding MVNOs) in the 29 countries that use this technology. Based on public reported information the cumulative subscriber numbers of these S@T Browser-using Operators comes to **~861 million mobile connections** (SIM cards).
- Not all SIM cards in the operator may use this technology. In discussions with a few operators in the LATAM region we were informed that the majority of SIM Cards **(>90%)** in their network had it. But in other operators it might not be this high and

[5] Based on UN Population estimates 2019

may be used by legacy devices only, so it would be a much lower percentage. Only the individual Mobile Operators can provide this specific detail, although in some cases they may not have this information readily to hand.

Higher:

- There are countries /operators using the technology which we did not observe directly. This is because our search was based on a side effect of looking for attacks on users, not looking for ordinary activity. Also, more importantly, if there is no roaming between a S@T Browser-using operator and the roamed-to operator where the measurement took place in, then we would not observe any activity from that S@T Browser-using operator. In theory, if we were to assume all Operators in a S@T Browser-using Country also used the technology, and we were to take total connection numbers[6] within the country this comes to **~1124 million mobile connections**. This number is higher that the population of the S@T Browser-using countries due to IoT devices, dual SIM phones etc.

- Some operators may have the S@T Browser on their (older) SIM cards but no longer send/receive S@T Browser activity (messages from these SIM cards). This would be because they have disabled the S@T Browser infrastructure on the network side, but the technology is still resident on their SIM cards, making them still potentially vulnerable. Also, there are public references to RFPs[7] being run in the past by Mobile Operators to acquire SIM card which have the S@T Browser technology on them.

During this process we have been informed by operators in additional countries who state they have this technology. But as we did not directly observe S@T Browser messaging at a no security Level being sent from these countries, we did not include them on the list.

As well, as our own datapoints, there is the recent additional information in the testing that SRLabs[8] did on 800 SIM Card measurements. In this, they reported that *A subset of 5.6% are vulnerable to Simjacker, because their protection level was set to zero*. Given there are 9.320 billion mobile connections active[9] this would give a figure of **~522 million SIM Cards** containing the S@T Browser. However, this value must also be regarded as approximate, as this is based on the origin of the individual SIM card measurements taken over time and does not cover[10] every country in the world.

Taking all this information together, our best estimates of number of SIM cards with this technology must be in a range, with estimates from a few hundred million to over a billion SIM cards. **The most probable, conservative estimate is that mid to high hundreds of**

[6] https://www.gsmaintelligence.com/
[7] https://www.telkom.co.za/about_us/procurement/downloads/StaticContent/RFP_0322_2011.pdf
[8] https://srlabs.de/bites/sim_attacks_demystified/
[9] https://www.gsmaintelligence.com/
[10] https://www.vice.com/en_us/article/qvgzqw/researchers-think-they-know-how-many-phones-are-vulnerable-to-simjacker-attacks

millions of SIM Cards globally are affected. This matches the GSM Association's assessment that a minority of the 9 billion SIM Cards globally are affected.

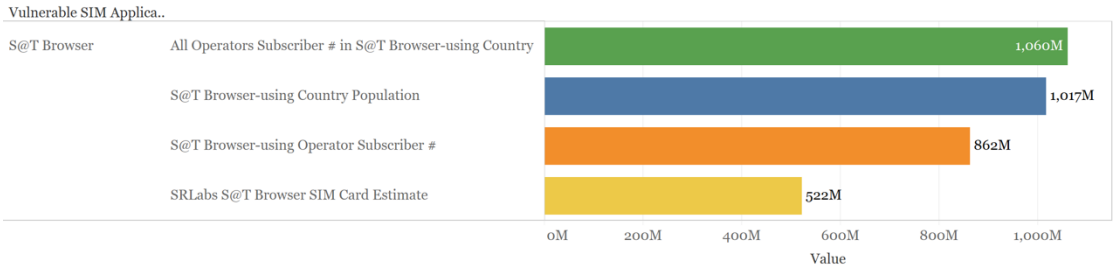


Figure 13: Range of Number of Vulnerable SIM Cards

Again, this measurement of vulnerability excludes the protections that Mobile Operators may put in place over the network side. Effective defences in the mobile network would massively reduce the risk of using this technology, this is further covered in section 8.

7.2 Additional Functionality Potential

As well as the attacks observed, there are a variety of different other attacks possible using the S@T Browser. The complete SIM Toolkit API Command Set accessible from the S@T Browser is as follows:

- REFRESH
- MORE TIME
- POLL INTERVAL
- POLLING OFF
- SETUP EVENT LIST
- SET UP CALL
- SEND SS
- SEND USSD
- SEND SMS
- SEND DTMF
- LAUNCH BROWSER
- PLAY TONE
- DISPLAY TEXT
- GET INKEY
- GET INPUT
- SELECT ITEM
- SET UP MENU
- PROVIDE LOCAL INFO
- TIMER MANAGEMENT
- SETUP IDLE MODE TEXT

Some of these require information to be displayed to the user, whereas others do not. But as per the S@T and USIM standards, and by using these commands, a variety of other attacks seem possible. While not exhaustive, a number of proposed scenarios using these commands are covered briefly below:

- Fraud Applications
- Advanced Location Tracking
- Assistance in Malware Deployment
- Denial of Service
- Information Retrieval
- Misinformation

Note: In our initial blog[11], we showed a larger list of Proactive STK Commands, which we believed were accessible from the S@T Browser. This was due partially to observing the attackers using these additional proactive commands. From subsequent follow-up testing and standards review, we do not believe that these commands are possible in (normal versions) of the S@T Browser, and the blog was subsequently changed.

7.2.1 Fraud Applications

There are several types of fraud which could be executed, here are some example

- **Call Diversion to Premium Rate Numbers**
  This could be done by receiving a Simjacker message with the instruction to initiate Call Diversion (via STK Send USSD commands) to a Premium Rate Number. If this command is successful then if the victim handset is subsequently rung by the Fraudster, the network will redirect this call to the Premium Rate Number. This could cost the victim high amounts of money, as they are liable for paying for the forwarded call. No indication is made at the time that a call is being forwarded, although a call forwarding icon may be displayed on the handset while the feature is enabled.

- **Generating Calls to Premium Rate Numbers**
  This could be done by sending a message with STK Setup Call Commands to ring a Premium Rate Number. This -depending on the S@T implementation - requires human interaction in order to confirm the call, but the text to display at this point can be any text, so spam/social engineering could be used to encourage to recipient to accept. Some devices however will not display any text, and will just dial the number automatically. In addition, devices with no Handset or display may also dial the number automatically.

[11] https://www.adaptivemobile.com/blog/simjacker-next-generation-spying-over-mobile

- **Sending Text messages to Premium Rate Numbers**
  This could be done by sending a Simjacker message with STK Send SMS Command, to request to send to a Premium Rate Number. The user would be unaware this would happen.

7.2.2 Advanced Location Tracking

The Simjacker attack requests Location Information, which for Mobile Devices will be the serving Cell-ID. Generally, we observe that over the SS7/Diameter inter-carrier signalling interface, attackers also request Location information via Cell-ID, even though they have the ability to obtain GPS location information from the device. There are numerous reasons as to why Cell-ID is preferred, including speed of response, no need to rely on capabilities of the handset, and a guaranteed returned value. By using commercial databases of cell-ids, in combination with public domain datasets, the attackers can then use this information to generate consistent location tracking, which can be reasonably precise in an urban setting.

However, if an attacker does wish to get more precise information, they could request a variety of more specific information in the STK Provide Local Information command. Within this command an attacker could request Network Measurement Results and/or on the 3GPP network, Timing Advance. These radio network measurements can be used to generate a more precise form of location tracking which can get down to 80meter resolution in urban areas[12].

7.2.3 Assistance in Malware Deployment

It is possible to either open a new Browser, or change the current Browser to open up a specific website without user interaction by using the STK Launch Browser command. The reasons for doing this is to assist in malware deployment from a compromised website, although a separate client-side vulnerability is still required to download the application automatically, once the link is opened.

This opening of webpages automatically has been used by spyware/surveillance companies in the past, examples of specific Binary SMS that have been used to do this to open up are WAP Push SL messages which have been used to deploy the Pegasus malware[13] as a zero-click vector. These WAP Push SL messages caused "*a phone to automatically open a link in a web browser instance, eliminating the need for a user to click on the link to become infected*". As mentioned: "*Many newer models of phones have started ignoring or restricting WAP Push messages. Mobile network providers may also decide to block these messages.*", so the ability to do this (open a link automatically) is valuable as it means the attackers do not need to rely on social engineering to open a webpage. Currently no standard form of SMS sent by a user should cause a browser to open automatically.

[12] https://pdfs.semanticscholar.org/ebe2/1dd7abda5234efcca4aee0fce9c853d7d819.pdf
[13] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

7.2.4 Denial of Service

By using USSD commands, and attempting to change the PIN code multiple times, the phone could be locked. This could be used to execute a denial of service type attack, as explained in previous research[14], as the victim would not be able to use the SIM until they went to their service providers shop.

However, in our tests, an attacker may not need to go that far, as we were able to cause other forms of Denial of Service. By sending malformed messages within the S@T Browser message, we were able to render the SIM card invalid until we recovered it. This functionality to recover it would not be available to the average user.

7.2.5 Information Retrieval

There are other parameters which could be retrieved from the SIM Card, by using Simjacker commands. As well as the IMEI, the following information could be retrieved via the S@T Get Environment Variables Command:

- ICCID (SIM Card Serial number)
- SIM Card manufacturer
- Terminal Profile

All of these variables are valuable in building up an idea of a target. Other information could then be retrieved via the Provide Local Information command, including connected radio technologies, battery level, connected WLAN IP address etc.

7.2.6 Misinformation

By using the STK Send SMS feature, an attacker could spoof communications from an individual to others, or to applications which authenticate based on the origin of text messages from an individual.

7.3 Other Vulnerable SIM Card Applications

The issue with the S@T Browser is that the SIM card application did not authenticate the source of any commands – the ambiguity in its specification meant that it had effectively no security for Push type messages. This means that a determined attacker could – if they were able to bypass any protection an operator had in place – eventually craft a command that could use the S@T Browser environment to execute logic on the SIM Card.

The S@T Browser is not the only SIM Card application which could be exploited, in theory any SIM Card application could also be targeted with Simjacker-like attacks. One that has received some attention recently is the Wireless Internet Browser.

[14] https://www.troopers.de/wp-content/uploads/2012/12/TROOPERS13-Dirty_use_of_USSD_codes_in_cellular-Ravi_Borgaonkor.pdf

In addition to S@T and WIB, we are also currently profiling a number of additional SIM Applications. This work is on-going, and if any vulnerabilities are found in these, they will be subsequently reported to the GSMA through their CVD program.

7.3.1 WIB (Wireless Internet Browser)

Since we released our initial Simjacker findings, there has been a report from other researchers that other technologies like the WIB[15] could be exploited. This is also a technology that we have been investigating. Wireless Internet Browser (WIB) is specified by SmartTrust for SIM based browsing. Its specification is not generally available, but some documents of other companies' implementation of it can be found on the internet[16]. Unlike the S@T Browser, some WIB documentation does at least state that the no security MSL *should be used for testing only, since it provides no protection whatsoever* (section 3.1.1[17]). While this is not the official specification, it does indicate that at least some manufacturers were aware of the danger of using no security for WIB message

As part of our analysis, we investigated whether Mobile Operator customers were being targeted by other SIM Card technologies such as the Wireless Internet Browser (WIB). While we did not identify any attacks (so far), by doing this we were also able to identify a number of countries and operators who generate no-security SMS OTA messages for the WIB Application, and so build up a global picture of the usage of this technology. Figure 14 shows a breakdown of how many other countries and operators use the WIB application with no-security settings, compared to the S@T Browser.

[15] https://ginnoslab.org/2019/09/21/wibattack-vulnerability-in-wib-sim-browser-can-let-attackers-globally-take-control-of-hundreds-of-millions-of-the-victim-mobile-phones-worldwide-to-make-a-phone-call-send-sms-to-any-phone-numbers/
[16] https://vdocuments.mx/sim-guideline-wib-1-3-equipped-sim-cards.html
[17] https://vdocuments.mx/sim-guideline-wib-1-3-equipped-sim-cards.html

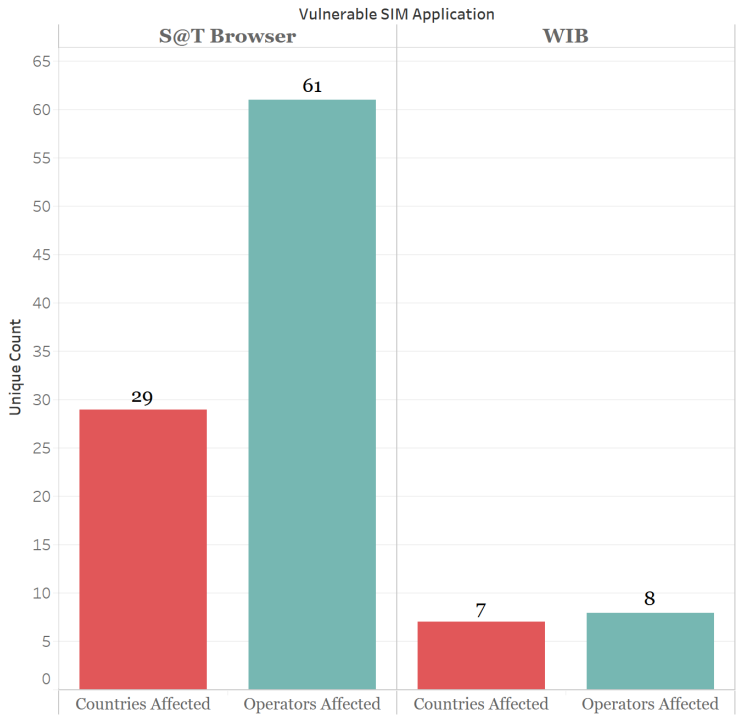
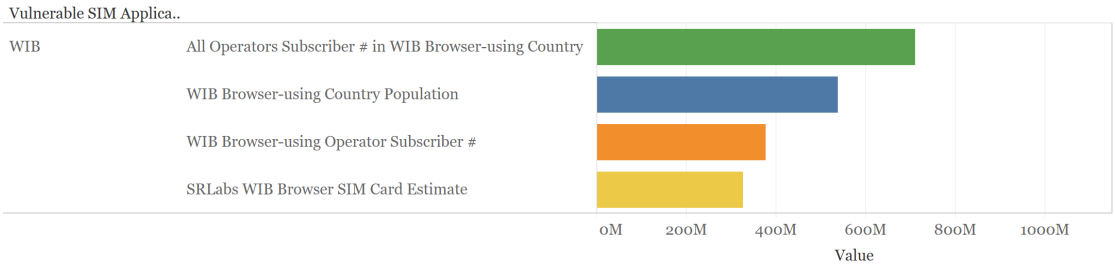


Figure 14: Count of Vulnerable Countries & Operators for S@T and WIB

In general, we found that the WIB application, when used with no security level is used in far less countries: 7 and operators:8, as per Figure 14, albeit the operators that it is currently used in are quite large relatively (based on subscriber numbers). These countries are spread over Eastern Europe, Central America, Asia and West Africa, there are no single regions of heavy use as is evident for usage of the S@T Browser technology. The same issues arise in trying to guess the number of affected SIM cards, a range of reference points is in the diagram below. The most probable, conservative estimate would be that it would be a range in the low hundreds of millions of SIM cards.



The potential mitigations are roughly similar to the S@T Browser. On the network side SMS filtering would be required to block these messages. However, on the SIM side, upgrading the security of the SIM implementation needs to focus on WIB-specific security configuration files. This is because the security for incoming and outgoing message does not depend on the Minimum Security Level (MSL) associated with the application, rather it is determined by specific WIB security configuration files.

8 Recommendations

8.1 Mobile Subscribers

There is no simple way for a mobile subscriber to know whether the S@T Browser is deployed on a SIM or not. One recently developed easy way is to download an application like SIMTester[18] from SRLabs. This also requires a card reader, but a person could use it to determine whether a vulnerable S@T Browser card is present.

However, there is little that a mobile subscriber can do if their SIM card has the technology deployed. The primary protection must come from the Mobile Operators

Apps like SnoopSnitch[19], also from SRLabs can tell if your phone has received one of these SMS OTA messages, but again this is not a defence, and requires a rooted device, which introduces its own security risks. The most effective solution is for the subscriber's Mobile Operator to deal with the issue via network defences and/or upgrading of vulnerable SIM cards.

8.2 Mobile Operators

Multiple recommendations for Mobile Operators have already been distributed within the GSM Association and Mobile Operators are strongly encouraged to consult those, which can be obtained from a GSMA representative. At a high level. Mobile Operators can try to change the security settings of UICCs in the field remotely or even uninstall and stop using the S@T Browser technology completely, but this may be slower and more difficult. As an outcome of this process, the SIMalliance has made new Security guidelines for S@T Push messages[5]. These guidelines cover both the use of higher Minimum Security Levels in communications with the S@T Browser.

Other, more immediate recommendations from both the GSMA and the SIMalliance are to analyse and block suspicious messages that contain S@T Browser commands. This requires that all SMS sent within the mobile network are filtered. Special care must be taken in doing this to ensure that false positives are not introduced, as well as that all the various ingress and egress messaging flows are inspected, including those paths and flows which may previously have been thought as secured or inaccessible. Further information from AdaptiveMobile and the GSMA on network mitigations are available within the GSMA Infocentre[20].

The most important recommendation for Mobile Operators, is that order to be effective, relying on existing hard-set recommendations will not be sufficient to protect themselves, as

[18] https://opensource.srlabs.de/projects/simtester
[19] https://opensource.srlabs.de/projects/snoopsnitch
[20] https://infocentre2.gsma.com/gp/wg/FSG/CVD/CVD%20Repository1/Forms/AllItems.aspx?RootFolder=%2Fgp%2Fwg%2FFSG%2FCVD%2FCVD%20Repository1%2FCVD-2019-0026%20Simjacker%20%28HoF%29

attackers like these will evolve to evade what is put in place. Instead Mobile Operators will need to put in place operational procedures and processes to constantly investigate suspicious and malicious activity to discover ‘hidden’ attacks. Mobile Operators should also expect other vulnerabilities and attacks that evade existing defences to be discovered and abused.

As the attackers have expanded their abilities beyond simply exploiting unsecured SS7 networks, to now cover a very complex mix of protocols, execution environments and technologies to launch attacks with, Operators will also need to increase their own abilities and investment in detecting and blocking these attacks.

9 Conclusion

While similar concepts to Simjacker have been discussed in real-life, actual attacks involving ‘spyware’ over SMS has not been witnessed in real-life before. We have shown how it has been exploited by a surveillance company for at least 2 years, tracking many thousands to tens of thousands of mobile subscribers in that time. In our work to identify and block these attacks, we have also uncovered the large network that it is part of, and the extreme lengths it goes to in order to bypass any defences.

Taken all together; the complexity, scale and reactiveness of the threat actor using Simjacker means that we must regard the wider Simjacker attacks as a huge step forward in ambition and reach for attackers over the mobile network. This has important implications for all Mobile Operators if they wish to deal with attacks from threat actors like this in the future. It means that previous ways of relying on recommendations, with no operational investigation or research won’t be enough to protect the mobile network and its subscribers, and what’s worse, will give a false sense of security.

Simjacker succeeded because the attackers reacted to defences put in place over other layers like the SS7 interface. In reacting, the attackers created a sophisticated, highly complex system capable of recording the location of hundreds of people per day, as well as performing other activity. It would be foolish to think that now having uncovered these attacks and stopping them, that the threat actor(s) will not discover and use other methods to continue their malicious activity.

In exploiting the S@T protocol, the attackers showed that a SIM Card technology, in use by hundreds of millions of SIM Cards, is vulnerable to external attacks. While the Simjacker attackers only focus on specific aims and targets, different attackers in the future may try to exploit this technology - and additional related SIM Applications on other vulnerable SIM Cards - for financial and malicious attacks. These other attackers may not have the same technical expertise and resources to circumvent existing defences in Mobile Operator like the Simjacker attackers did, but the precedent has been set that it could be possible.

All cyber security is normally a race between those who attack and those who defend. With the discovery of Simjacker we can see that the race has been on the attacker’s terms for some time. Now is the time to make sure that the mobile industry catches up and stays ahead of these attackers in the future.

Appendices

A. Previous Related SIM Toolkit Exploits

There is a number of other reported exploits involving SIM Toolkit Messaging over the last few years. This is an overview of the most relevant ones to Simjacker

2011 Bogdan Alecu/m-sec.net, DeepSec2011

This research[21] [22] covered the sending of a SMS formatted to indicate it was a SIM OTA SMS, in order for an error response to be auto-triggered from the SIM Card/device to the sender. This auto-generated SMS response (using the Proof of Receipt flag in the Command Header) could be used to either debit account balance from the victim or be used as a form of DoS. The actual command received in the SMS generated the error as the Command Header values (TAR, KIc, KID etc) were not valid. The SIM Toolkit API environment itself was not accessible during this attack.

2013 Karsten Nohl / SRLabs BlackHat2013

This research[23] covered the use of sending multiple SIM OTA SMS messages to SIM Cards with DES key trying to obtain the DES SIM key. Once this key was obtained (using rainbow tables or brute forcing), the SIM Toolkit API environment was accessible, and an *OTA---deployed SIM virus* could access the set of SIM Toolkit API to perform malicious logic. As a result, this went beyond the work from 2011 as the SIM Toolkit API environment was now accessible. One note is this DES key is unique per SIM card, and so would need to be cracked each time.

An additional part of this work involved investigating whether it was possible to exceed the sandbox of the STK apps, for lateral movement in order to gain access to the most sensitive information within the SIM card – which it was for certain SIM cards.

2013 NSA-Tailored Access Operations

A number of Mobile exploits was revealed when the NSA's Tailored Access Operations (TAO) group implant catalogue was leaked[24] in December 2013. Two of these use SIM OTA SMS, as well as being functionally similar in their aims.

[21] http://blog.m-sec.net/2011/sim-toolkit-attack/
[22] https://www.defcon.org/images/defcon-21/dc-21-presentations/Alecu/DEFCON-21-Bogdan-Alecu-Attacking-SIM-Toolkit-with-SMS-WP.pdf
[23] https://media.blackhat.com/us-13/us-13-Nohl-Rooting-SIM-cards-Slides.pdf
[24] https://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

MONKEYCALENDAR

The first is MONKEYCALENDAR[25]. Dating from 2007/2008, this executed Simjacker Location tracking-like functionality in that it retrieved geolocation information using SIM Toolkit proactive commands and exfiltrate it to a user-defined mobile number via SMS. It differed in that it is resident on the SIM Card, and relies on a trigger to execute. The trigger itself is not specified - it may be a hard-set timer or some functional trigger on the device. It also encrypted the equivalent outbound Data Message. Another key difference is that in order to be loaded onto the SIM card by OTA provisioning - or via a SIM card reader, it may require the SIM key per SIM. This differs from Simjacker which does not require any key.

GOPHERSET

The second related exploit is GOPHERSET[26]. This exploit again uses SIM Toolkit proactive commands, but in this case, it is a more general tool to retrieve Phonebook, SMS and Call log information and exfiltrate it in an equivalent Data Message to a user-defined phone number. This could be most likely achieved by executing RUN AT COMMAND STK commands, with the relevant AT Command to obtain the specific information, although since 2008 it is probable that a lot less devices allow this functionality. Again, encryption is used for the Data Message, and again the limitation is that a SIM key for the SIM Card is required.

[25] https://www.spiegel.de/international/world/a-941262.html
[26] https://www.spiegel.de/international/world/a-941262.html

Telecom Standards References

Ref	Doc Number	Title
[1]	3GPP TS 23.048	Security mechanisms for the (U)SIM application toolkit; Stage 2
[2]	S@T 01.50 V4.0.0	S@T Browser Behavior Guidelines
[3]	S@T 01.00 V4.0.0	S@T Bytecode
[4]	S@T 01.23 V4.0.0	S@T Push Commands
[5]	*S@T August 2019*	Security Guidelines for S@T Push
[6]	3GPP TS 29.002	Mobile Application Part (MAP) specification.
[7]	3GPP TS 23.040	Technical realization of the Short Message Service (SMS)
[8]	3GPP TS 23.038	Alphabets and language-specific information
[9]	3GPP TS 51.011	Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface
[10]	3GPP TS 31.111	Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)
[11]	3GPP TS 31.115	Secured packet structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications

Acknowledgments

This paper was produced by the Data Intelligence team within AdaptiveMobile Security, in conjunction with the Threat Intelligence Unit. We also gratefully acknowledge the assistance of our Mobile Operator customers in helping us identify and research these attacks and thank the GSM Association and the wider Mobile Operator security community for helping to validate and distribute the recommendations.

Revision History

Version	Date	Remarks
1.00	3rd October 2019	
1.01	10th October 2019	Formatting changes, spelling and grammar corrections

About AdaptiveMobile Security

AdaptiveMobile Security is the world leader in cyber-telecoms security protecting over one billion subscribers worldwide and the only mobile security company offering products designed to protect all services on both fixed and mobile networks through in-network and cloud solutions.

With unparalleled global scale and visibility, a unique focus on service providers, and an integrated security solution built in the network, our award-winning Network Protection Platform provides our customers with real-time insight into what is happening across their networks and the actionable intelligence to respond to these threats. Scaling from the largest nation-states, down to the individual user, AdaptiveMobile Security offers the most comprehensive network security products.

The combination of global insight provided by our security specialists teams, our world-leading Threat Intelligence Unit, and our proprietary, telecom-grade Network Protection Platform are trusted by the world's largest service providers to secure their critical communications infrastructure. This unique combination provides constant protection and threat response services against current and future cyber threats to protect networks, nations and individual mobile subscribers.

AdaptiveMobile was founded in 2004 and boasts some of the world's largest mobile operators as customers and the leading security and telecom equipment vendors as partners. The company is headquartered in Dublin with offices in the North America, Europe, South Africa, Middle East and Asia Pacific.

Contacts

AdaptiveMobile™
Ferry House,
48-52 Lower Mount Street
Dublin 2
Tel: +353 (1) 524 9000
Fax: +353 (1) 524 9001

Regional Sales Contact Numbers:
US, Canada, Latin America: +1 972 377 0014
UK Sales: +44 207 049 0421
Middle East Sales: +97144 33 75 83
Africa Sales: +27 87 5502315
Asia Sales: +65 31 58 12 83
European Sales: +353 1 524 9000

Regional Operational Support Contact Numbers:
UK: +44 208 114 9589
Ireland: +353 1 514 3945
France: +33 975 180 171
India: 000-800-100-7129
US, Canada: +1 877 267 0444
Latin America: +52 5584211344