Simjacker

Cathal Mc Daid
CTO

3rd October 2019
#VB2019
Introducing **Simjacker**

- Large scale espionage attack on mobile network subscribers from multiple countries: primarily Mexico, also Colombia & Peru

- Tens of thousands of subscribers having location (Cell-ID) and device information obtained over at least 1->2 year(s)

- Exploits vulnerability in SIM Card that allowed mobile devices in targeted operators to be open to allow specific remotely executed commands, many without any user interaction

- Vulnerability believed exploited by professional surveillance company on behalf of a nation-state

- Surveillance company actively testing new variants of the attack and new attacks + very complex efforts to avoid protection in place

- **Simjacker is arguably the most sophisticated attack ever seen over mobile core networks.**
Setting the Scene

• This presentation is final stage of disclosure process within the Mobile Industry

• Brief Timeline:
  – *First Observed related Simjacker Message (retrospective analysis) Q4 2017*
  – First Detection of Potential Simjacker Activity Q4 2018/Q1 2019
  – **GSMA CVD Submitted: Late June 2019**
    • Sharing of information within the wider Mobile Community: Late June-> Ongoing
  – Public Release: September 12th 2019
  – Technical Public Release: October 3rd 2019

• Safety first: Staggered release of information publicly so Mobile Operators have
  – Chance to confirm if vulnerable
  – Put in safeguards if so
High-level view of typical Simjacker Attack

2 Stages:

1. **Attack Stage:** ‘Attack Message’ is sent from Malicious Handset to victim phones
   - ‘Attack Message’ are SIM OTA (SIM Toolkit) Messages

2. **Exfiltration Stage:** The Attack Message executable instructs the SIM Card to request Location (Serving Cell ID) and IMEI from the Handset, and send the Location and IMEI from the Handset in a SMS
   - This is called the ‘Data Message’

• ‘Data Message’ is sent from the Victim Handset to a Exfiltration Number,

• This activity is not noticeable by the Victim – no indication on the handset
Step 1: Attack Stage: How the Attack Happens

‘Attack Message’ is sent to Victim Handset,
Step 2: Exfiltration Stage: How the data is sent back

‘Data Message’ is sent from Victim Handset, to Attacker Handset.
Demo of the attack: Location Tracking – Note, ~5 second delay removed
Location

72f2100bd5b73f000c

272: MCC Ireland
01: Vodafone Ireland
0bd5: LAC (3029)
b73f: CellId (46911)

Note: VF Ireland are the roamed-to operator for the vulnerable SIM, they are not the vulnerable operator.
Location

- **Location**: Map
- **MCC Ireland**: 72f210
- **Vodafone Ireland**: 0bd5
- **LAC (3029)**: b73f
- **CellId (46911)**: 000c

Note: VF Ireland are the roamed-to operator for the vulnerable SIM, they are **not** the vulnerable operator.
How the attack works

1. Attacks exploit ability to send SIM OTA SMS

   **Sound Familiar?**
   
   - 2011 - Bogdan Alecu/m-sec.net, DeepSec2011: SIM Toolkit Attack
   - 2013 - Karsten Nohl/SRLabs, BlackHat2013: Rooting SIM Cards
   - 2013 - NSA-Tailored Access Operations

2. Attacks exploit the presence of S@T Browser on the SIM card for vulnerable subscribers

   **This is the novel part**
What is the S@T Browser?

• Stands for SIMalliance Toolkit Browser
• S@T browser specifications were developed by the SIM Alliance. Aim of these specifications was to allow:
  – thin client on a SIM
  – to run applications in the SIM
  – using commands and content downloaded OTA via SMS or BIP from an external server.
• Utilise STK/OTA mechanisms.
• Last update 2009 (prior to this vulnerability).

Main role of the S@T browser is to act as an execution environment for STK commands.
Why is the S@T Browser vulnerable

- Applications (e.g. S@T Browser) on the SIM Card, have one or more TAR values
- TAR values have a set of Minimum Security Levels (MSL)
- Incoming SIM OTA SMS types, must have security that matches this MSL
  - Security in SIM OTA SMSs defined in the SPI, Klc, KID fields in the SIM OTA Command Header (many complex layers to get here)

There are 4 types of S@T Browser protocols
- Pull
- Administration
- Low Priority Push
- High Priority Push

NO SECURITY LEVEL RECOMMENDED FOR PUSH MESSAGES!!

5.5.2 Security Levels

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

<table>
<thead>
<tr>
<th>SPI</th>
<th>Klc</th>
<th>KID</th>
<th>DESCRIPTION</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0000</td>
<td>0x00</td>
<td>0x00</td>
<td>No security applied</td>
<td>Shall be supported for incoming (MT) and outgoing (MO) messages.</td>
</tr>
<tr>
<td>0x1200</td>
<td>0x00</td>
<td>0x5</td>
<td>Triple DES Cryptographic Checksum (8-byte MAC); counter higher</td>
<td>Shall be supported for incoming (MT) messages.</td>
</tr>
</tbody>
</table>

This security level is not recommended for Administration protocol.
This security level is not recommended for Pull protocol.
What we have detected

• Single, Highly-sophisticated Attacker exploiting S@T Browser Push commands

• Primarily Targeting Subscribers from Mexico
  – Subscribers from Colombia and Peru also targeted

• Primary goal is to obtain Location information (Cell-ID) and IMEI details
  – Small subset of other activity

• Attacks launched from complex network of ‘ordinary’ sending devices, but activity often coordinated with SS7 sources worldwide
Simjacker Internal Execution Structure

1. INIT: Variable SMS-Submit To: Recipient Device
2. EXECUTE_STK_COMMAND: PRO_CMD_PROVIDE_LOCAL_INFORMATION Location Information
3. EXECUTE_STK_COMMAND: PRO_CMD_PROVIDE_LOCAL_INFORMATION Terminal Information
4. INIT: Variable Filler Bits
5. CONCATENATE (1) + (2) + (3) + (4)
6. EXECUTE_STK_COMMAND: PRO_CMD_SEND_SHORT_MESSAGE Payload = (5)

- CELL-ID
- IMEI
- SEND SHORT MESSAGE
- ENVELOPE
Customized Wireshark View

- MTP 3 User Adaptation Layer
- Signalling Connection Control Part
- Transaction Capabilities Application Part
- GSM Mobile Application
- GSM SMS TPDU (GSM 03.40) SMS-DELIVER
- STK Protocol
  - Command Header
  - Secured Data
    - S@T Push
    - S@T Deck
    - S@T Card
      - S@T Variable initialization
      - STK Provide Local Information: Location Information
      - STK Provide Local Information: IMEI Information
      - S@T Variable initialization
      - S@T Concatenate
      - STK Send Short Message:
Flavour of the attacks: 31 day period

- More than 25,000 Simjacker messages attempted to be sent to more than 1,500 Unique Identifiers (subscribers).
- Most targeted subscribers 45% were targeted once, few others were targeted more than 1,000 times.
- 69% of targeted subscribers were targeted on one day, a small number were targeted almost every single day.
- More than 90% of time, Cell-ID+IMEI was requested to be retrieved. Other potential testing activity observed (Denial of service, opening website, call setup etc).
- More than 70% of attacking devices cycle over time, similar number of exfiltration devices.
- Additional 5% of Simjacker originated via external SS7 points, ‘classical’ SS7 attacks also used for specific targets.

More Details in Technical Briefing Paper on www.simjacker.com (after break!)
Evading/modifying (1) : Injection Method of Simjacker Attack Message
Evading/modifying (2) : Exfiltration Method of Data Message
Evading/modifying (3) : Simjacker SMS Packet Encoding

Constant Changing of SMS Transfer Layer, e.g.
- DCS
- PID
- UDH
- UserData

Also Use:
- Reserved Values,
- Compressed Content,
- Multi-part messages,
- Omitted values
- Corrupted/non-standard parameters
- Others

<table>
<thead>
<tr>
<th>TP-AMI</th>
<th>LocalValue</th>
<th>TP-DCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>33</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>37</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>41</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>43</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>48</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>54</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>55</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>SMS-SUBMIT mo-forwardSM</td>
<td>57</td>
<td></td>
</tr>
</tbody>
</table>
Evading/modifying (4) : Other Variations

• Internal Structure of Simjacker Message
• Corrupted Attack Message Encoding
• Data Message Encoding
• Source Addresses
• Filler/Random Byte Placement

• S@T Push Type
• Source Operator
• Additional STK Commands
• Exfiltration Addresses
• Etc, etc – there are many more
Attacker Testing – Over Time
What else could be possible via S@T Browser

• Fraud Applications
  – Call Forwarding to PRN
  – Setup Call to PRN (new handsets require interaction)
  – SMS to PRN

• Advanced Location Tracking
  – Retrieve CellID+ NMR + Timing Advance (i.e. e-cell ID)

• Information Retrieval
  – ICCID, Terminal Profile, Battery, Language

• Misinformation

• Denial of Service

• Assistance in Malware Deployment
Demo – Browser Hijack – Note, ~5 second delay removed
A bit more meat on the bone,

- **Implant on SIM Card?**
  - MONKEYCALENDAR
  - Set up Event List

- **Inbound Call Interception?**
  - Via SS/USSD – Enable + Disable Call Forwarding
  - Requires 2 Simjacker SMS + VoIP Box
    - man-in-the-middle attack via VoIP
  - Same method as used in SS7 attacks (RegisterSS Inbound Call interception)
Active Users of S@T Browser Technology: 61 Operators, 29 Countries
By-product of protecting all subscribers (including Inbound roamers)
  - list generated from observing S@T Browser traffic with MSL=0
  - Many reasons why could be lower or higher.

Best (conservative) estimates of vulnerable S@T Browser SIM Cards: mid to high hundreds of millions of SIM Cards globally are affected

NB: Assessment of vulnerability, not of Risk – Risk depends on effective mobile network filtering
A word on WIB

Wireless Internet Browser, roughly similar to S@T Browser (although no-security is explicitly not recommended)

Using same method, observed operators with MSL = no security using WIB technology in real life

Many less operators, scattered globally.

Volumes vulnerable probably in low hundreds of millions of SIM Cards
Recommendations (for Simjacker and WIB vulnerability)

For Subscribers:
• Keep in mind, you are (very) highly unlikely to be targeted
• Not much you can do
• SRLabs have released SIMTester + SnoopSnitch

For Mobile Operators
• Contact the GSMA (please!!)
• If you use S@T Browser Technology, investigate whether it can be disabled and removed, or updated to improve MSL
  – Bit different on WIB
• Network Filter on Messaging Level

NB: If Mobile Operators attempt network filtering, must constantly monitor + investigate!
Back to the Attackers – Who are they?

• Focus on Mexican Mobile Subscribers (primarily, but not always)
• Activity strongly correlated with SS7 Threat Actor seen globally
• This SS7 Threat Actor exhibits pattern of surveillance company employed by nation state.
• Multiple surveillance companies have been in the news targeting Mexican Mobile subscribers
• Simjacker attacks are highly complex, determined and well resourced. Matches specific, large-scale and long-lived SS7 Threat Actor
• Have additional info, but cannot reveal as would damage our ability to defend
Conclusion

1. Simjacker is world’s first documented real-life malicious injection of virus/spyware via SMS
2. Attackers have been using Simjacker methods for at least 2 years, to monitor tens of thousands of subscribers.
3. Technologies, infrastructure and methods used indicate huge leap in complexity and abilities of mobile network protocol attackers
4. Emergence of Simjacker attacks means Mobile Operators have to plan to defend against a new type of adversary.