AdaptiveMobile Security
an Enea company

STK, A-OK?
Mobile messaging attacks on vulnerable SIMs

Cathal Mc Daid / @mcdaidc

#VB2021 7-8th Oct 2021

Introduction – what did we set out to answer

- In VB2019 we revealed the Simjacker attacks
  - Exploit of SIM Card application by Surveillance companies
  - Extracting info from tens of thousands of mobile phone
  - Vulnerability present on several hundred million SIM cards

More info: www.simjacker.com

- The Simjacker Attack used **binary SMS** as a delivery mechanism. Here we look at:
  1. Binary SMS attacks, are there other similar vulnerable applications?
  2. Reaction of industry and attackers to revelation of Simjacker?

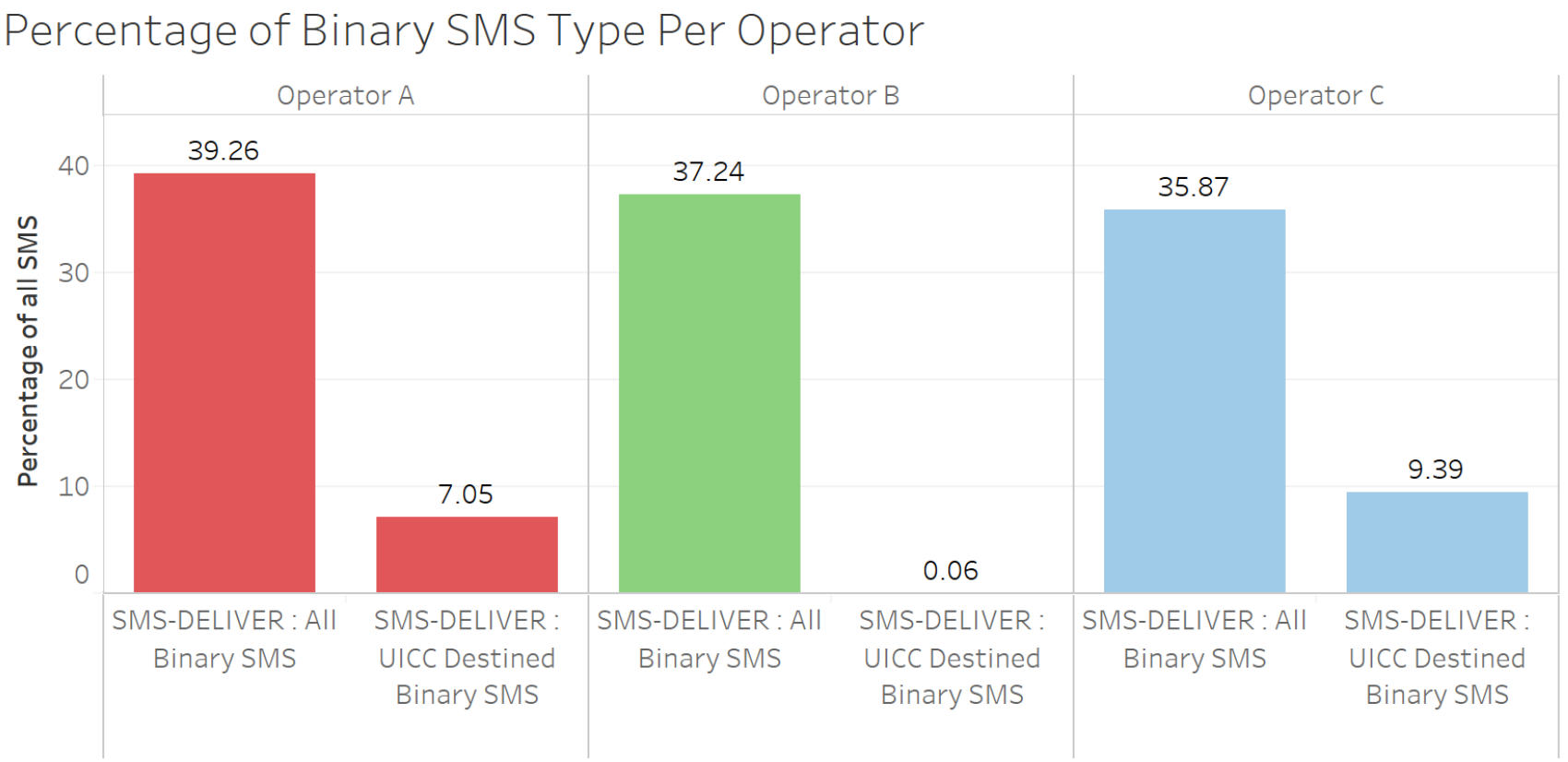
Binary SMS: Scale and Identification

Can occupy a large percentage of Mobile Operators traffic

Uses: Missed call notifications, change roaming settings, change SIM Card settings etc

(Mostly) 3 GSM-MAP parameters used to Identify Binary SMS

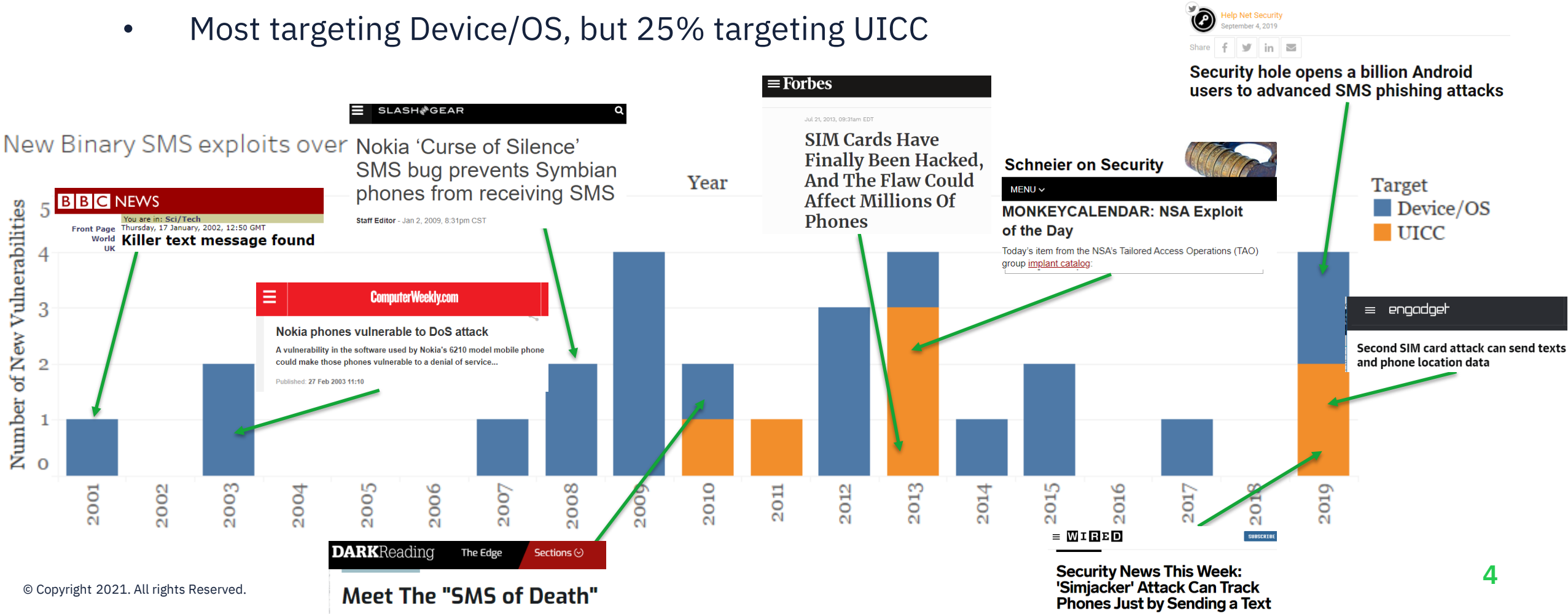
- TP-PID
- TP-DCS
- TP-UDH



Note: See VB2021 Paper for much more details

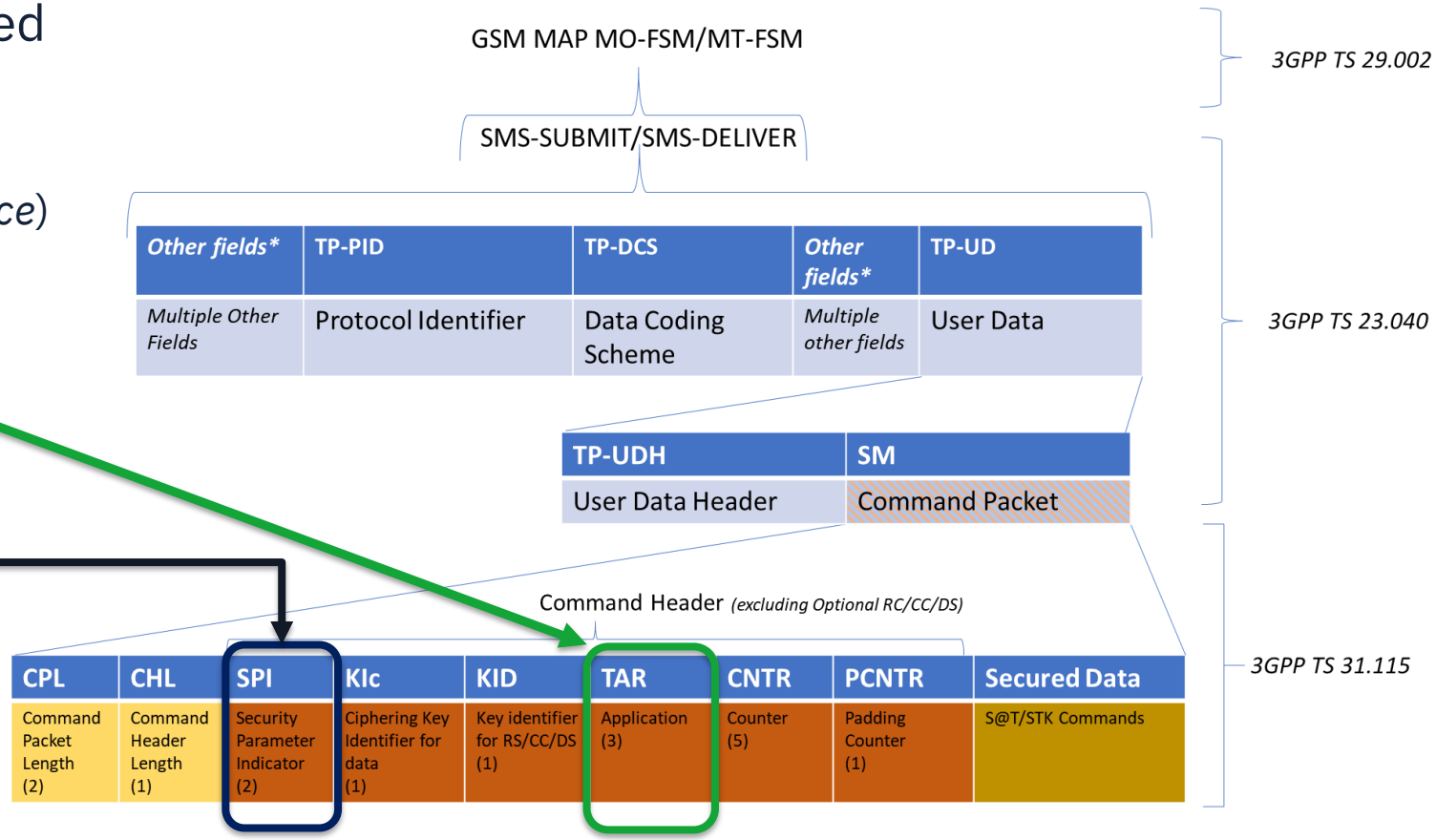
Malicious uses of Binary SMS

- At least 28 (known) separate vulnerabilities in last 20 years:
  - General Complexity increasing over time
    - Initial were simple DoS
  - Most targeting Device/OS, but 25% targeting UICC



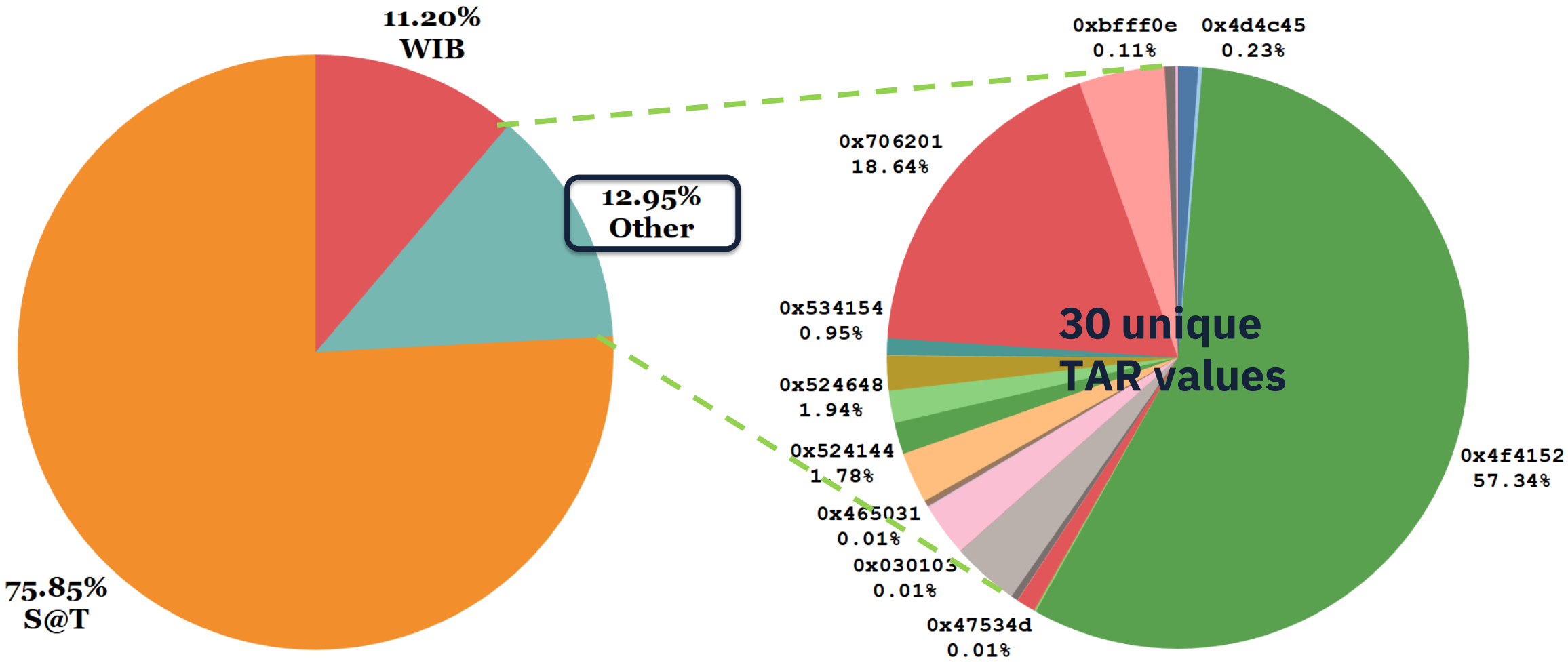
UICC Application destined Binary SMS – When to Worry

- Simjacker (plus others like WIBattack), used binary messages that were directed to the specific vulnerable UICC (SIM Card) application by the **TAR** value
  - Example TARs (*Toolkit Application Reference*) for S@T Browser
    - 0x505348 (PSH)
    - 0x534054 (S@T)
- Allowed to be executed by the UICC application by the SPI value setting
  - **SPI1* Value (Leftmost 5 bits) == 0 / No security**
    - Note: Ambiguous setting of this in S@T specs was cause of Simjacker vulnerability



We looked to see were there **more** of these vulnerable SIM Card Applications

Other Vulnerable SIM Card applications



Source: Analysis of UICC destined Traffic to vulnerable TARs from 1 year of global inbound roamers

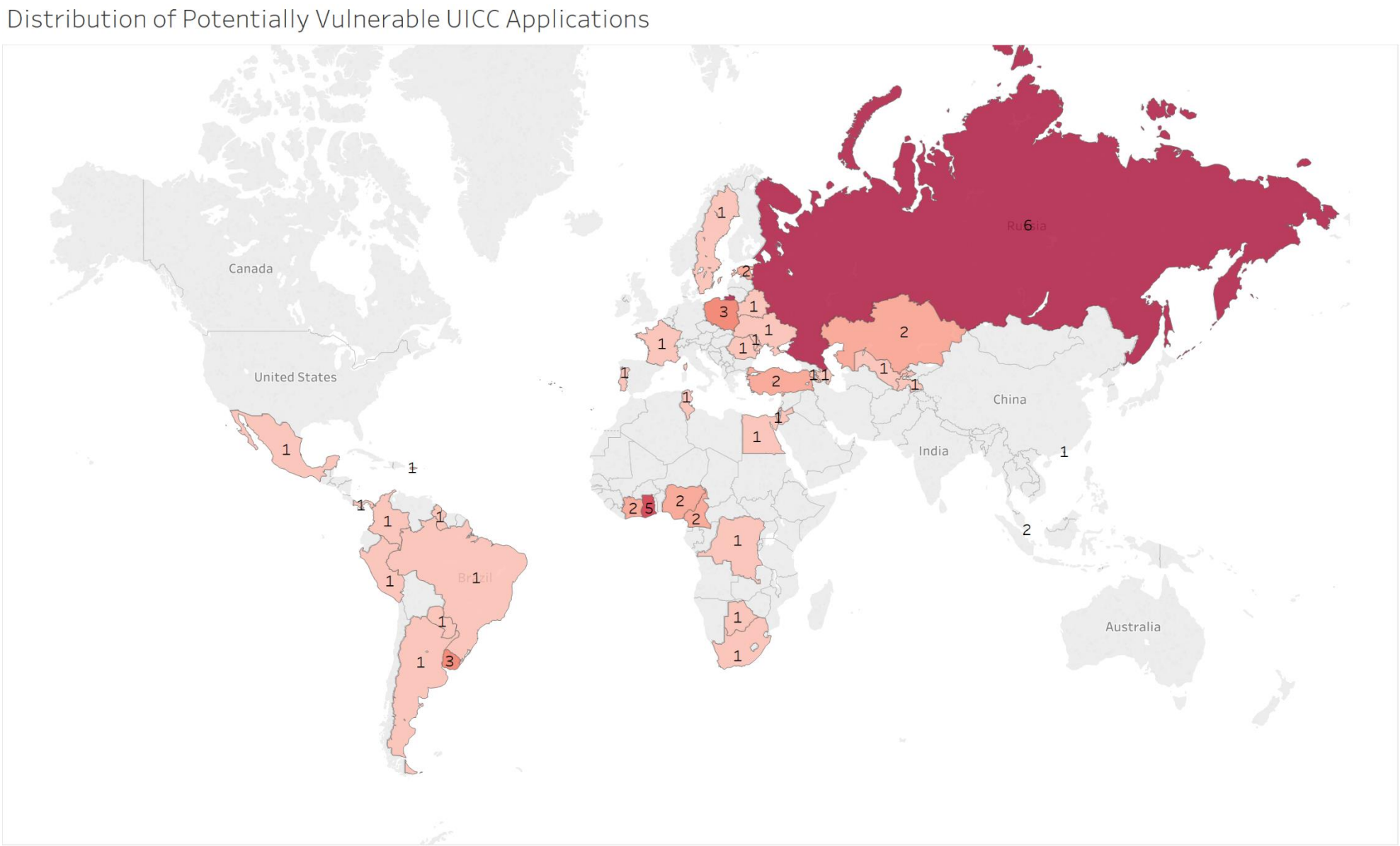
Where are these TARs used

Detected 30 unique TAR values (UICC applications),

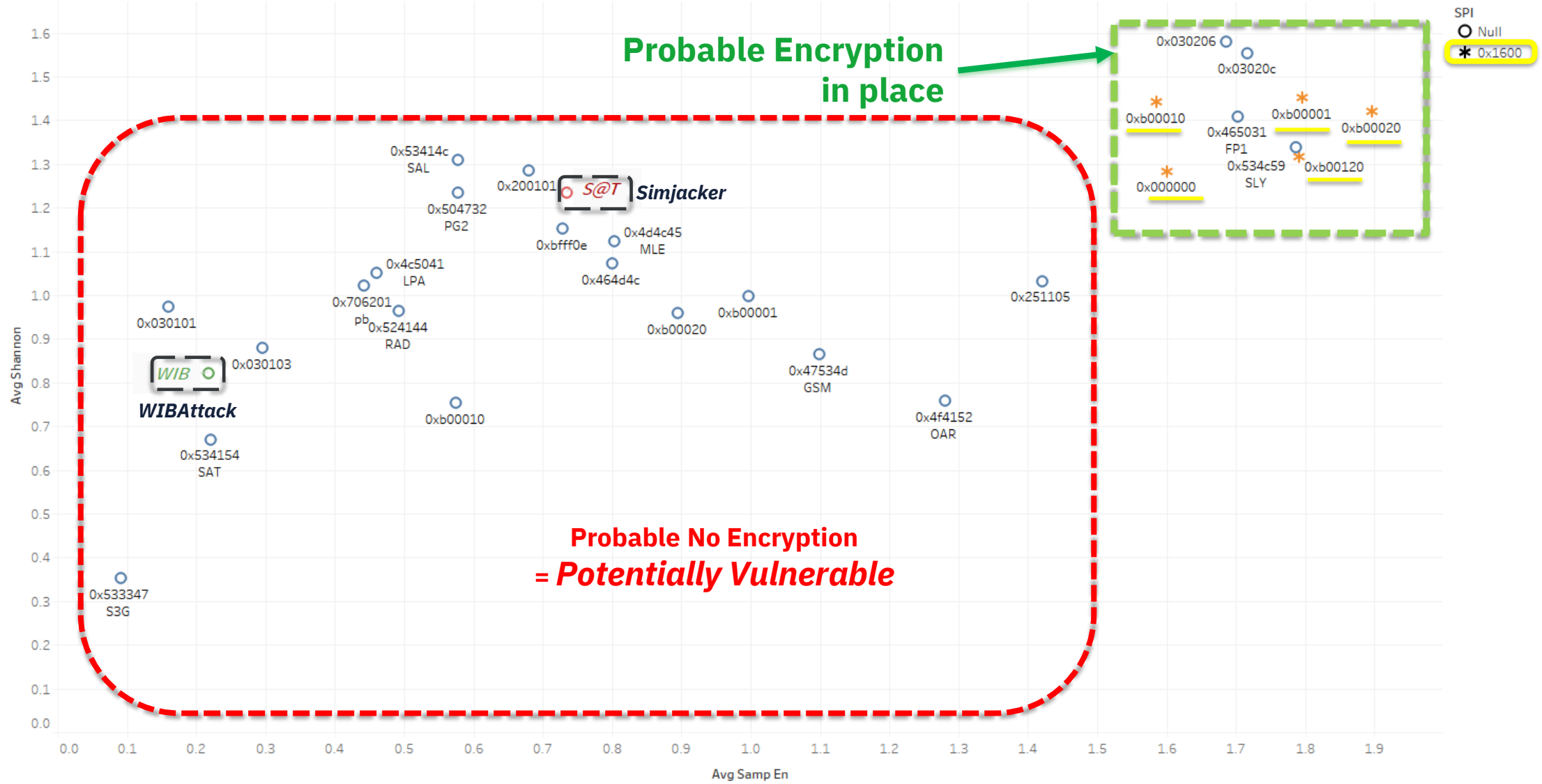
- Active in 50 operators from 39 countries,

with zero security set

Note: Varying activity per TAR



Threat level: Are all of these TARs Vulnerable?



Threat level: What could be achieved and Scale

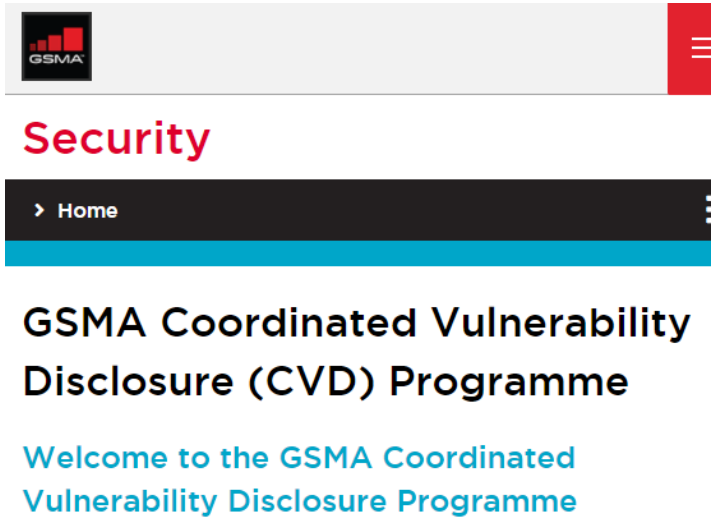
- What do these UICC application do
  - Majority: Notification, Contacts exchange
    - Attacks limited, although these could be exploited
  - However some TARs (e.g 0xb…) have access to sensitive info
    - Could be used for location tracking (EF_{LOCI}), potentially extract info from SIM Card: IMSI, SIM Key (K_C - if phone on), Roaming settings

- Subscribers potentially affected ?
  - Theoretical maximum(unrealistic): ~770 million
    - some TARs were used very infrequently
  - Very conservative : ~37million SIM Card
  - Probable: less than <100m
- **NO** sign of these UICC applications being exploited
- All identified affected operators informed

Simjacker Vulnerability – looking back, and forward

Issues with communicating to industry in 2019:

- Very obscure technology but wide ability, only mobile operators could mitigate
- Being actively exploited by sophisticated surveillance company to track thousands of people
- Widescale use (61+ known mobile operators, 29+ countries, with potentially up to a billion subscribers) **+ unknown more operators**

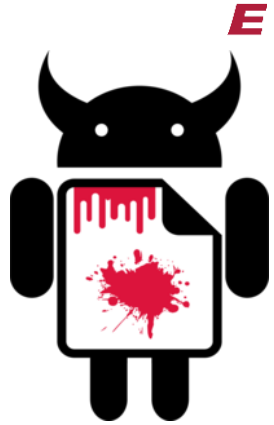


Plan to inform community via **GSM Association CVD program**, but:

- **Gaps** in participation of specific operators in GSMA Working groups
  - Lesser concerns: Effectiveness, leakage (to attacker), others

How to make sure all vulnerable operators know (safely)?

Branded Vulnerability – Everybody loves them?



Images courtesy of https://io.netgarage.org/logo/

Staged Approach to Inform Industry

1. June -> Sept 2019: Inform all community as best as possible through GSM Association via CVD program (and direct contacts)

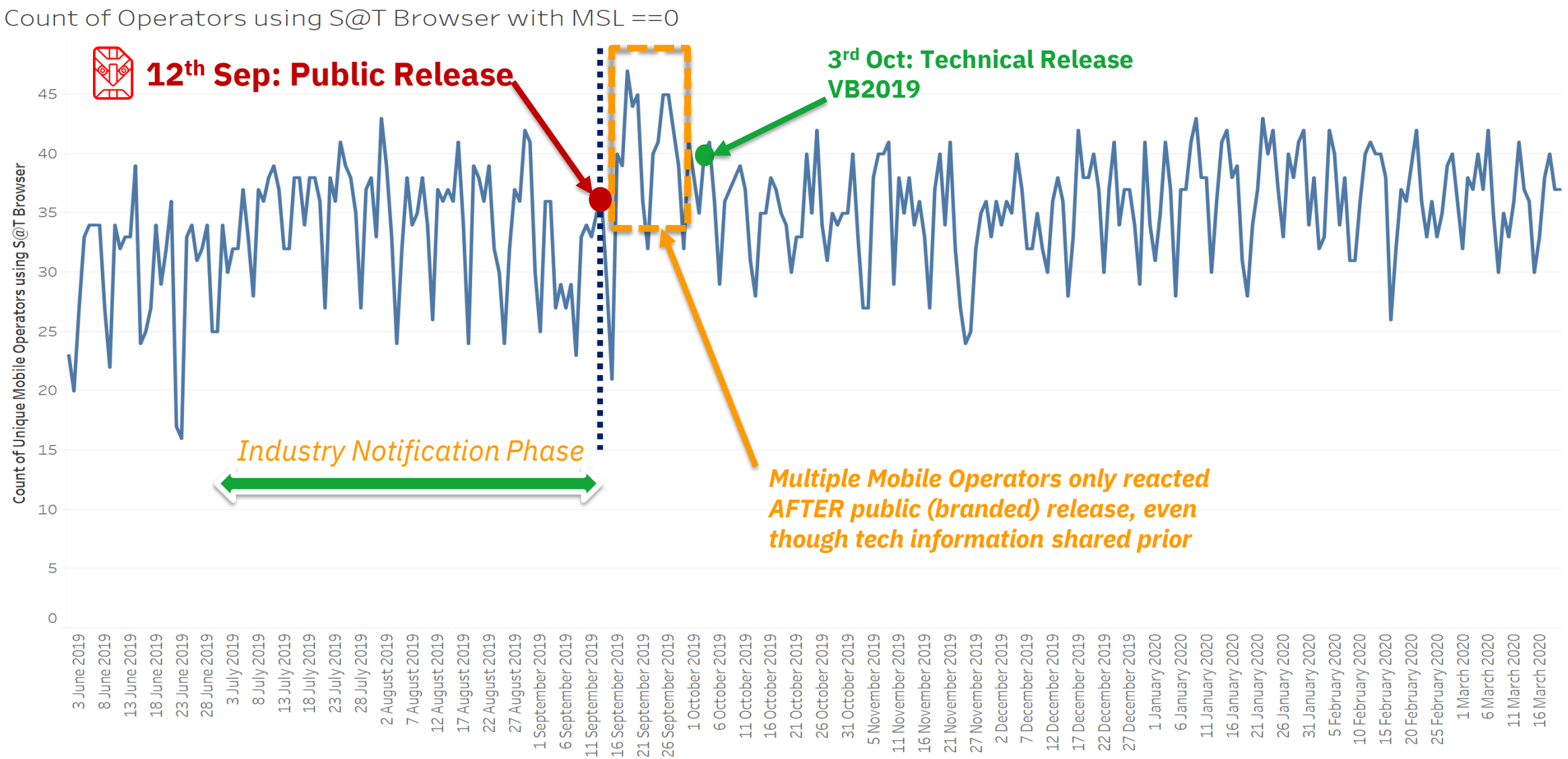
2. Sep 12th 2019: Do initial 'Public notification' with publicity to notify any unaware mobile operators
   - Give concepts but limited technical detail so attacks could not be replicated.
     - However this causes other problems in interim: some observers either confused issue with earlier research OR struggled to believe it
   - Point mobile operators to the GSMA where full technical info available

3. Oct 3rd 2019: Later (+4 weeks) do full public Technical Information release

Was this the right approach?

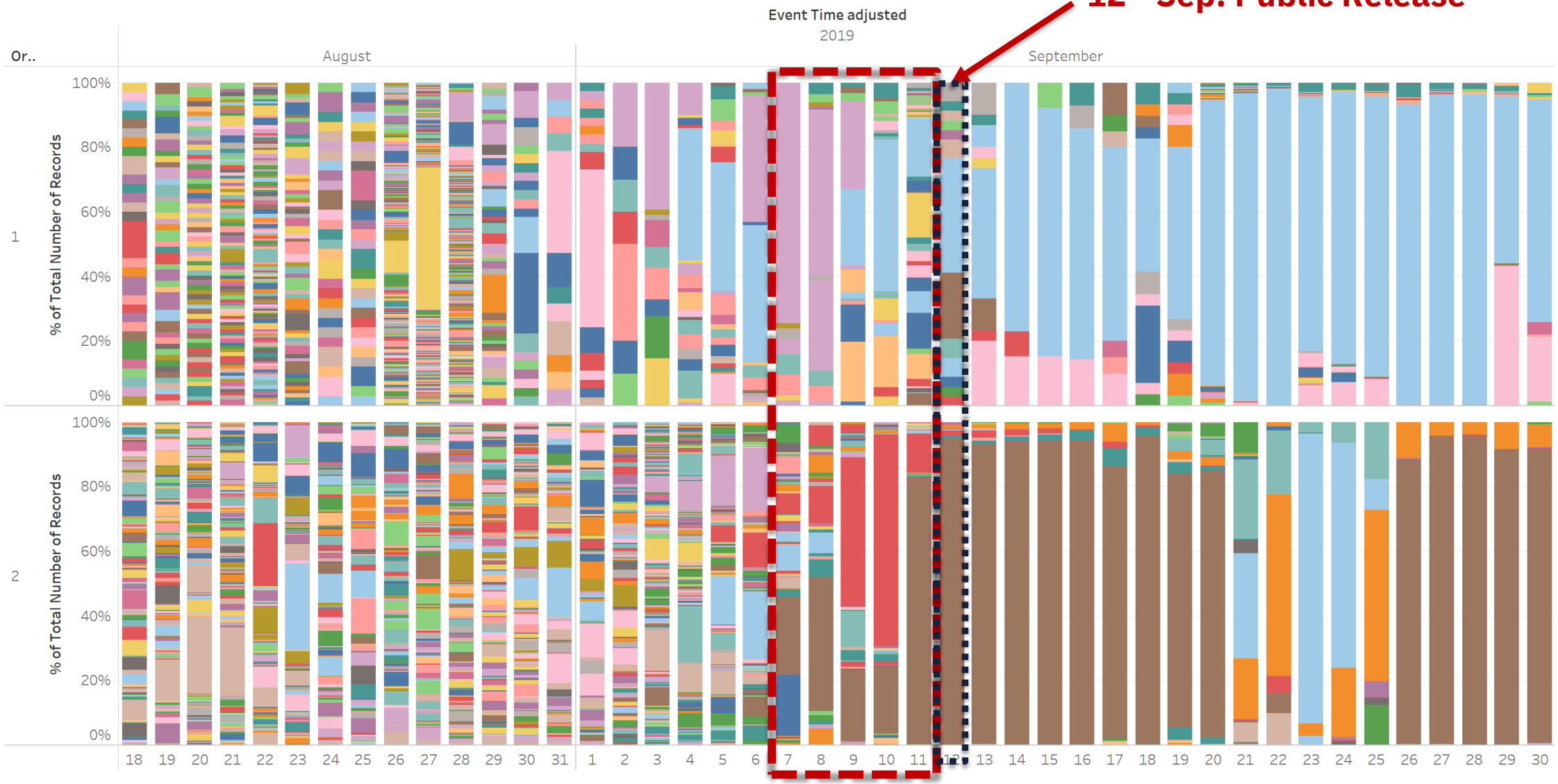

...and I took that personally

Reaction of Mobile Operators

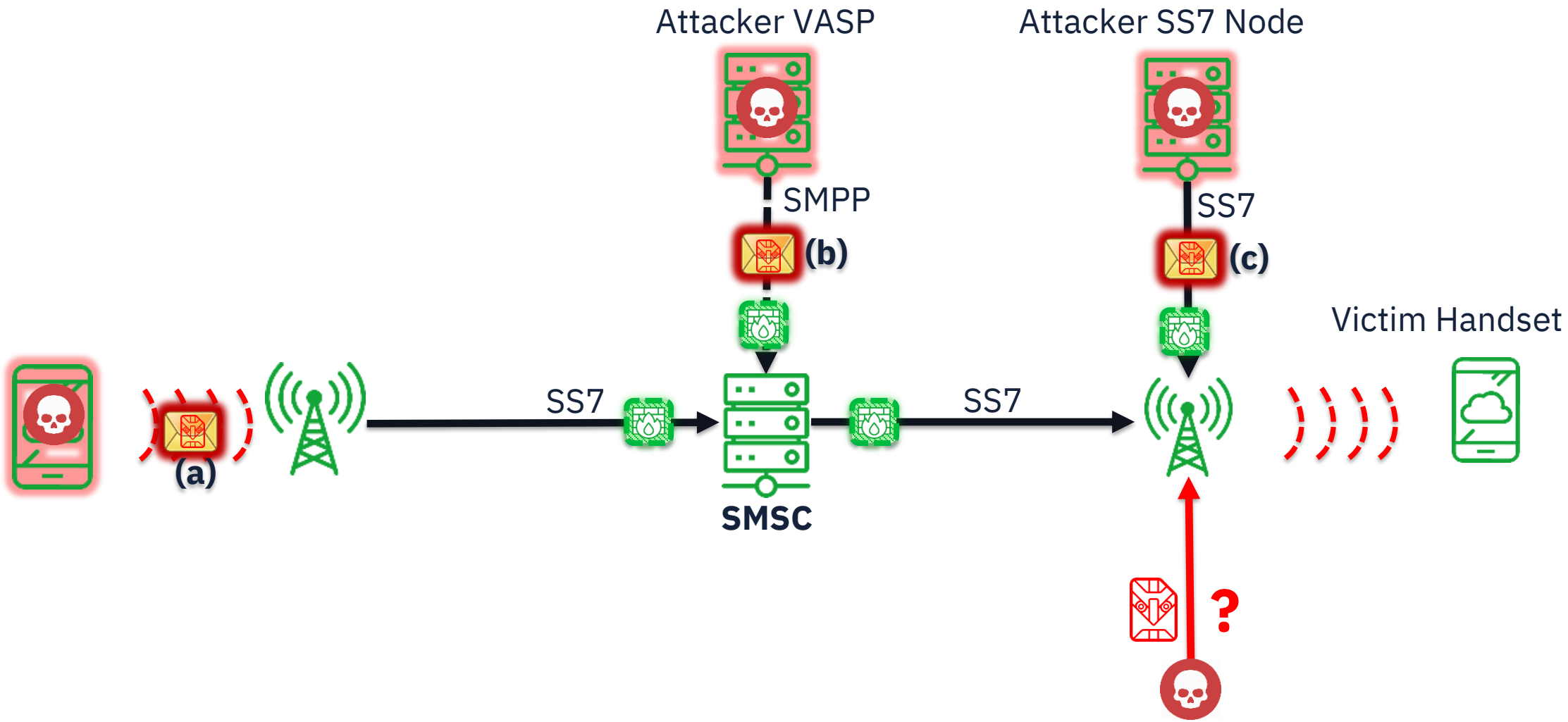


Reaction of Simjacker Attackers

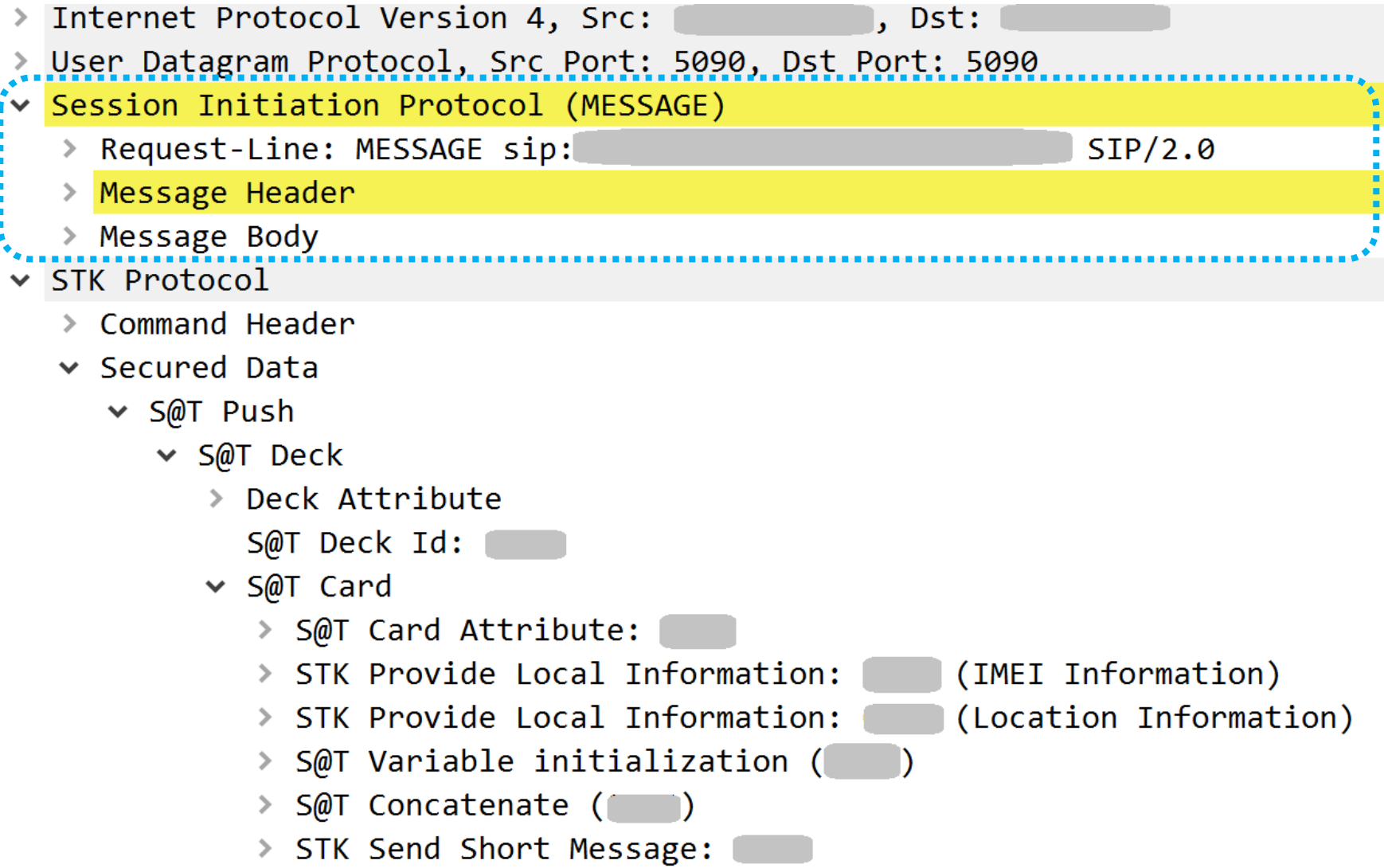
Change Prior to Release - Operator1 & Operator2



Simjacker Evasion techniques



Simjacker Evasion techniques



Attack via
SMS over SIP
MESSAGE

Scale of Attacks

Temporary gaps over time allow us to make estimates on scale & devices tracked

Wide scale of devices tracked:

- Largest Type: 91.7% Smartphone
- Largest Brand: 30.2% Apple
- Largest Model: 4.3% iPhone 12 Pro Max

Representative of Mexican market, not device vulnerability

Extrapolated Simjacker attacks in Mexico pre-detection:

- **~259k** location lookups per year
- **~31k** unique subscribers per year

Attackers not going away – constant exercise to detect and block

Conclusions

- Binary SMS vulnerabilities attacks happen, and will continue to happen
  - *Work ongoing within the industry to define defences*
- We uncovered many potentially vulnerable SIM Card applications
  - *Mobile Operators need to be aware and focus on security*
- Surveillance companies react faster than Mobile Operators
  - *Slow is fast, old is new, but threat intelligence is key*

Thanks to : Ryan Dalton, Martin Gallagher, the Data Intelligence & Threat Intelligence Unit teams within AdaptiveMobile Security as well as our Mobile Operator customers + GSM Association.

AdaptiveMobile Security

an Enea company