Security Intelligence

Threat Sharing Report

October 2021

mobileum

Action driven by intelligence

Disclaimer

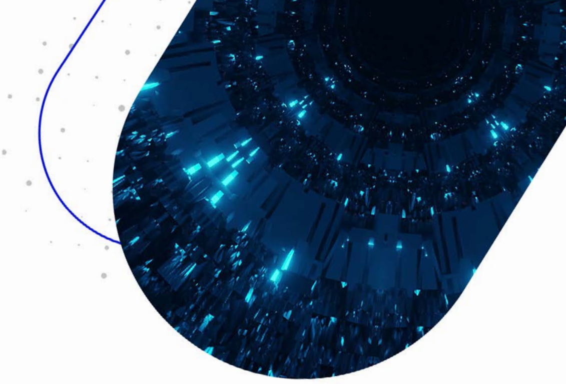
The service is performed in a diligent manner and in accordance with the applicable industry standards. Except for the foregoing warranties specified above or expressly mentioned in your contract with Mobileum, the services and service deliverables are provided 'as is' and we make no other warranty, express, implied, statutory or otherwise, written or oral, including without limitation warranties of merchantability, fitness for a particular purpose and non-infringement. The use of the services and deliverables is at your own risk. Mobileum neither assumes, nor authorizes any other person to assume on its behalf, any liability in connection with the services, data or information, including, without limitation, liability arising out of the provision oruse of the services, service deliverables or any other data or information. We also do not warrant that the deliverables are free from any errors and meet customer's requirements or expectations unless such requirements are expressly agreed as a part of technical specification. Mobileum does not warrant, that the services, service deliverables or any other data or information are transmitted without any errors, interruption or delay.

Please note, that any use of the ThreatDB reports is at your own risk. Before you pass a decision to block any traffic, please monitor the traffic to verify that it is safe to block the GT; please note, that some GTs may produce legal and illegal traffic at the same time; as the GT status may dynamically change, always verify the current state. Please note, that even if these recommendations are fulfilled, the correct active blocking is not guaranteed. Mobileum does not undertake any responsibility for misapplication of the report or for any consequences of incorrect blocking carried out by you.

Readers should note that, throughout this report, we make reference to various Operator Global Titles as the source of attacks. In no way are we stating that the Operator, to whom the Global Title is assigned, is responsible for those attacks. The identity of the party responsible for the attack itself is unknown to Mobileum.

This report was prepared with the proper extent of care, however its fully accuracy and correctness cannot be guaranteed. We assume no responsibility for any errors or omissions, which this report might contain. Neither Molileum Inc., nor the creators of this may be held liable for any possible damages, direct or indirect or consequential losses of any type, connected with the possible errors or related to the performance or use of this report. In case this report contains any products, information or links of the third parties, they are marked respectively. We assume no responsibility for the products of third parties, including their content, accuracy, compliance with copyright, trustworthiness, legality compatibility or any other aspect related to such products. Please note that any product, brand name, logo or company name mentioned in this report are the property of their respective owners and are protected accordingly.

Welcome to our October 2021 Mobileum Threat Sharing Report



There is always a question as to whether stories about privacy and security breaches in the press are good or bad news for security professionals. Bad news, obviously, because we are all dedicated to combatting this pervasive threat. Good news because coverage of the reality of threats and how they translate into real attacks often acts as a wake-up call to those who need to secure their businesses. Personally, I sit on the fence on this question, but I can tell you that I read some of the recent press coverage with enormous interest.

Just this week I read the BBC article "Princess Haya: Dubai ruler had ex-wife's phone hacked – UK court" with great interest. The banal nature of the alleged attack's motivation – apparently in relation to a divorce custody dispute – brought to light just how easily accessible this technology is. The other interesting aspect is that NSO Group, the vendors of the attack software used in this incident, now claim that the UAE is no longer a customer. Does this mean that the ever-increased public scrutiny of these attacks against privacy are limiting the activities of such players? One thing is sure, whilst vendors of such software may face public scrutiny, the same cannot be said of nation states and we see no signs of nation state attacks diminishing in the future.

This month we are sharing two new Threat Reports that our security research labs have published. The first relates to a topic that I have simply never understood. Let me explain. If you received a letter that had "non-existent sender" stamped in red all over the envelope what would you think? If there was also a message on the envelope that stated "likely scam" would you even open it. Let's say you decided to open it and discover that you have received a huge inheritance from an unknown distant relative. The only small issue is that you need to pay a small $1,000 processing fee. What would you do? Would you grab your cheque book and get the process rolling? I don't think so! So why do mobile operators even process signalling messages originating from unassigned number ranges? It is almost the same thing!

TR 20210512 Unallocated Country Code Tripped is not a particularly sophisticated attack but we were shocked at the blatant abuse of numbering plans. The attack details attacks conducted over a three-month period this year originating from country code 979. Country code 979 is assigned to International Premium Rate Services, albeit the NDC used in this particular attack is not assigned. Furthermore, according to Wikipedia, this same country code has been used within an Android malware application!

The second report featured this month is TR 20210325 MNO Vulnerability Scan Detected. This case, which originated from a Swiss Global Title, is of interested since a very large array of opcodes was used in significant volumes. The opcodes used included: anyTimeModification, USSD with code *100#, sendIMSI, ATSI, checkIMEI, SRI-for-GPRS, SRI-for-LCS, SMS-MO, Update GPRS Location, SS manipulation (interrogateSS, registerSS, activateSS, deactivateSS, eraseSS) and Update Location.

Nick Jones
CTO
Security Business Unit, Mobileum

Industry Activities

GSMA contributions:

- Change request in the GSMA documents (FS.34, FS.37, FS.39) is ongoing to support N9 security.

- Participation in GSMA *CVD Panel of Experts (PoE).*
  Mobileum is involved in continuous work in the GSMA PoE.

- Chairing the Global Title Leasing Task Force.
  Our work editing the GTLTF PRD continues with wide industry contributions. On the last call of the Task Forece there was broad agreement to turn this PRD into a publically available code of conduct that all MNOs and carriers will be encouraged to sign up to. This may well prove a powerful tool in addressing the scourge of Global Title abuse.

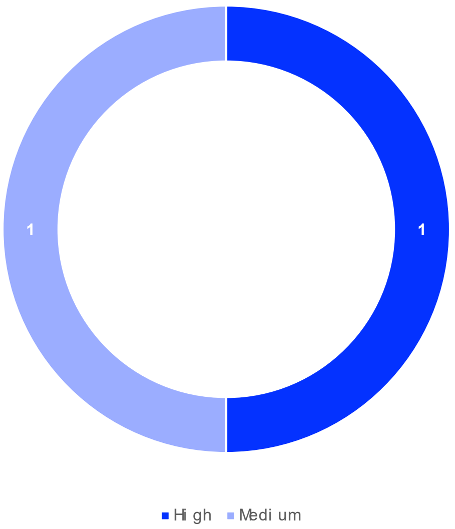
- *5GMMR (5G Mobile Roaming Revisited)* ready to release the "phase 1" technical report providing guidelines on how to deploy 5G roaming. The phase 1 will cover only basic inter-PLMN 5G roaming connections, excluding hubs but including the case where the SEPP is outsourced to a third party. Most of the critical decisions such as use of PRINS, group hubs, roaming hubs, addressing) have been postponed to "phase 2".

Monthly Statistics

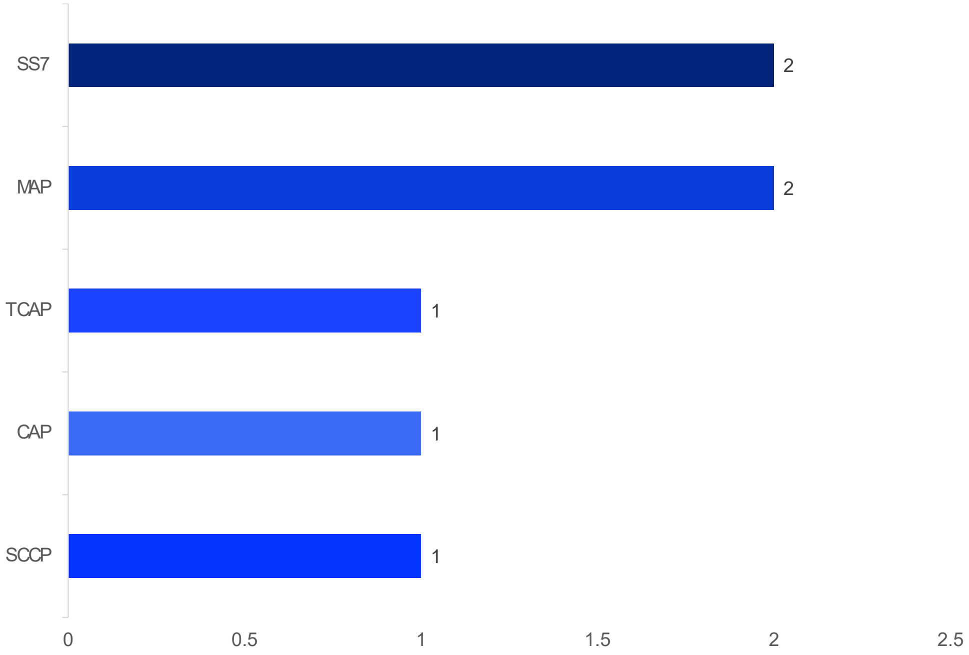
Mobileum ThreatDB

New and updated vulnerabilities by risk

This month we report one new medium-risk and one new high-risk Vulnerability and four new and updated Threat Reports. See page 9 for the detailed description.



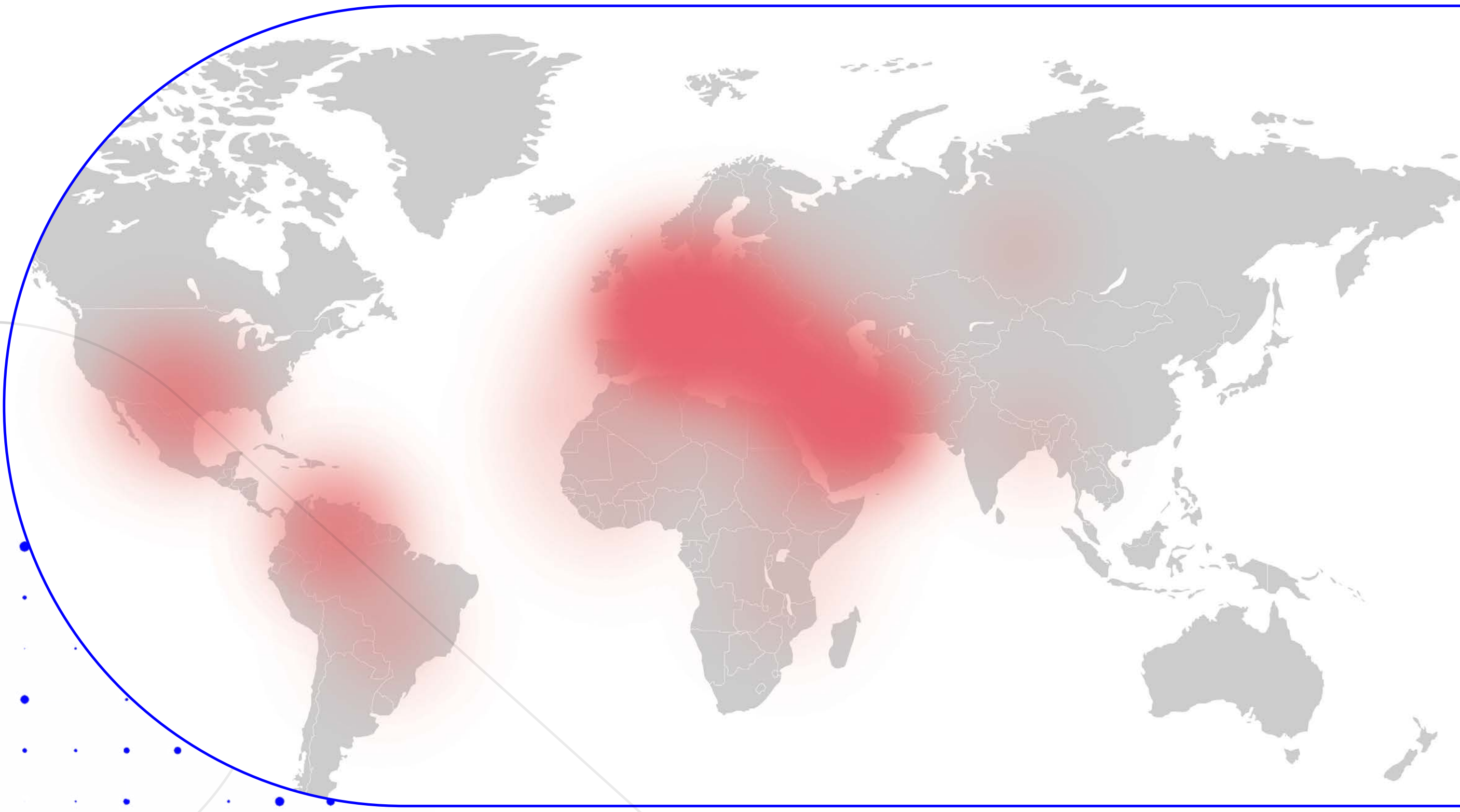
New and updated vulnerabilities by protocol



The vulnerabilities overlap are not additive

Threat Intelligence Heatmap

Showing unique SS7 GTs originating suspicious signalling



The heat map is a visualization of the data that is contained within our Threat Intelligence data repository. The darker the colour the great the level of origination of attacks from Global Titles within the shaded area. It is important to note that this does not represent the actual location of the attacker but rather the location of the Global Title used to conduct the attack.

New and Updated

Threat Report

Our Threat Intelligence team investigate a range of threats every month. Our Threat Sharing report details all the threats that we have been researching. Each month we will share the most important and interesting cases.

New and Updated Threat Reports	Protocol
Cross PDU’s attributes being tested (part 2)	SS7 MAP
Mapping and locating the A2P Campaigners	SS7 MAP
Unallocated Country Code Tripped	SS7 MAP
MNO Vulnerability Scan Detected	SS7 MAP

New

Vulnerabilities

Our Threat Intelligence team constantly review our database of vulnerabilities, updating older vulnerabilities as and when new information is identified, create a new vulnerability when appropriate. This Threat Sharing report details all new vulnerabilities that have been worked on in the prior month. We will share details of interesting updates with our Threat Sharing report subscribers.

New Vulnerabilities
VULN SS7 MAP manipulating Local opcode Value

Detailed Threats of the Month

October 2021

TR 20210512 Unallocated Country Code Tripped

General Details

Operators	Unknown
Date of Threat	2021/05/08- 2021/08/03
Date of Reporting	2021-08-03 - 2021-10-01
Threat Originating Network	SCCP Calling GT prefixes: 979718118118 979779383383
Protocol	SS7, MAP
Messages	PDU_SS7_MAP_sendRoutingInfoForSM , PDU_SS7_MAP_sendIMSI,
Threat Originating Node(s)	**Unknown:** 979718118118 979718118118 **Unknown:** 979779383383 979779383383
Reason for Analysis	Unknown source reported.

Threat Summary

This isn't typically a nice fancy TR comparing to other previously written TR which are staged and then executed.

This TR is typical due to its nature, the interesting aspect to this TR is not the TTP's or the IoA's that are observed as the TTP and IoA used by the source was already known to the research team, but the origin of the attack source.

Every origin has an identity, but in this case, the attack seen from the source GT is not allocated to any country. There is no country that owns that code allocation according to a common resolution. The GT is seen performing malicious activity and attempting to extract user identifiers.

As per ITU E.164 assigned country codes, this range is assigned to the IPRS (International Premium rate services) shouldn't be seen as a calling party.

TR 20210325 MNO Vulnerability Scan Detected

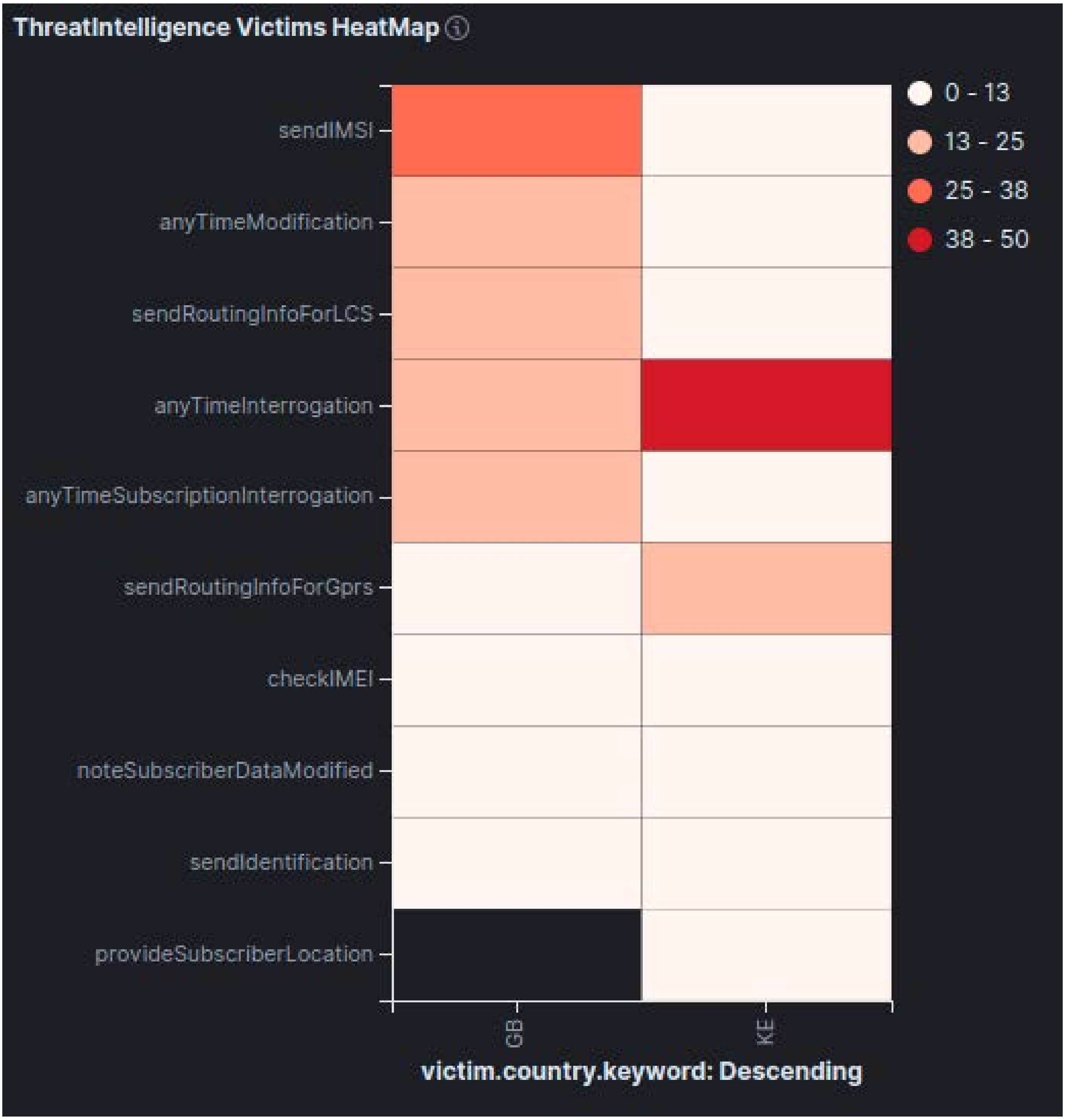
General Details

Operators	Swisscom (Switzerland) Ltd
Date of Threat	2021/01/20 - 2021/03/25
Date of Reporting	2021-03-25 - 2021-10-01
Threat Originating Network	SCCP Calling GT prefixes: Swisscom (Switzerland) Ltd: 41799987845
Threat Originating Node	SCCP Calling GTs: Swisscom (Switzerland) Ltd: 41799987845 41799987845
Protocol	SS7, MAP
Messages	PDU_SS7_MAP_anyTimeModification, PDU_SS7_MAP_sendRoutingInfoForLCS, PDU_SS7_MAP_sendIMSI, PDU_SS7_MAP_anyTimeInterrogation, PDU_SS7_MAP_anyTimeSubscriptionInterrogation, PDU_SS7_MAP_checkIMEI, PDU_SS7_MAP_sendRoutingInfoForGprs, PDU_SS7_MAP_activateSS, PDU_SS7_MAP_deactivateSS, PDU_SS7_MAP_registerSS, PDU_SS7_MAP_eraseSS, PDU_SS7_MAP_interrogateSS
Reason for Analysis	GSMA FS.11 violations.

Threat Summary

Illegal activity has been detected from Switzerland using various SS7 Cat1 messages.

The chart show the activity observed



For the full details on the Threats & Vulnerabilities featured in this newsletter

Subscribe to Mobileum Threat Intelligence Service

Live Threat Center includes:

- **Live Access to global attacks** – the sources and mechanisms
- **Latest in-depth analysis of global threats** and threat actors from security experts
- **Threat database** of latest signalling attack mechanism
- **High risk sources** as analysed by our experts **and risk score for global signaling sources**
- **Collect security events from Signaling (data is privacy protected)**
- **Support** for threat investigations

Request a **Demo** with our **Threat Intelligence Expert**

READ MORE

mobileum

Action driven by intelligence

About Mobileum

Mobileum is a leading provider of Telecom analytics solutions for roaming, core network, security, risk management, domestic and international connectivity testing, and customer intelligence. More than 1,000 customers rely on its Active Intelligence platform, which provides advanced analytics solutions, allowing customers to connect deep network and operational intelligence with real-time actions that increase revenue, improve customer experience and reduce costs. Headquartered in Silicon Valley, Mobileum has global offices in Australia, Dubai, Germany, Greece, India, Portugal, Singapore and UK.

More in www.mobileum.com and follow @MobileumInc on Twitter.

MOBILEUM, INC.
20813 Stevens Creek Boulevard, Ste. 200
Cupertino, CA 95014 USA

Phone: +1-408-844-6600
Fax: +1-408-252-1566

mobileum.com