

Saudi Arabia reportedly tracked phones by using industry-wide carrier weakness



reader comments

13 with 11 posters participating

Share this story

The Guardian says it has evidence that Saudi Arabia is exploiting a decades-old weakness in the global telecoms network to track the kingdom's citizens as they travel in the United States.

The publication cited data provided by a whistleblower that

suggests Saudi Arabia is engaged in systematic spying by abusing Signalling System No. 7. Better known as SS7, it's a routing protocol that allows cell phone users to connect seamlessly from carrier to carrier as they travel throughout the world. With little built-in security for carriers to verify one another, SS7 has always posed a potential hole that people with access could exploit to track the real-time location of individual users. SS7 abuse also makes it possible for spies to snoop on calls and text messages. More recently, the threat has grown, in part because the number of companies with access to SS7 has grown from a handful to thousands.

The data provided to The Guardian "suggests that millions of secret tracking requests emanated from Saudi Arabia over a four-month period beginning in November 2019," an article published on Sunday reported. The requests, which appeared to originate from the kingdom's three largest mobile phone carriers, sought the US location of Saudi-registered phones.

The unnamed whistleblower said they knew of no legitimate reason for requests of that volume. "There is no explanation, no other technical reason to do this," The Guardian quoted the source as saying. "Saudi Arabia is weaponizing mobile technologies."

The whistleblower's data appears to show Saudi Arabia sending an unnamed major US mobile operator requests for PSI—short for Provide Subscriber Information. Sunday's report said there were an average of 2.3 million such requests per month for the four months starting in November. The data, The Guardian said, suggests that Saudi Arabian phones were tracked as many as 13 times per hour as their owners carried them about the United States. The Saudi operators also sent separate PSLs. US carriers blocked the requests, indicating that the requests were suspicious.

System-breaking potential

Les Goldsmith, a researcher with Las Vegas security firm ESD, told me the volume reported by The Guardian had the potential to break systems used by the mobile operator being queried.

“Performing so many send subscriber data requests on a carrier could, in fact, result in the carriers’ Visiting Location Register (VLR) or even Home Location Register (HLR) to potentially crash,” he said. “So in essence, excessive tracking by Saudi Arabia could have potentially knocked legitimate users off a US cellular provider as the HLR and VLR reset.”

The Guardian, meanwhile, cited one mobile security expert who reviewed the data and said the requests had the ability to track the owners on a map to within hundreds of meters in a city. Several other experts said the requests indicated systematic spying on the part of Saudi Arabia.

In a statement, AT&T representatives wrote: “We have security controls to block location-tracking messages from roaming partners.” Representatives of T-Mobile and Verizon didn’t respond to a request to comment for this post. It will be updated later if the companies respond.

SS7 largely works on an honor system, although some carriers are in the process of rolling out measures designed to better lock it down. Given the current way mobile networks operate, there is little cell phone owners can do to prevent tracking through the abuse of SS7. Users can turn off phones to temporarily prevent tracking, but even, then adversaries can learn the location just before the device was turned off and obtain the location when it is later turned on.

<https://arstechnica.com/?p=1664380>