The truth about those claims of Qualcomm chips secretly snooping on you

Thomas Claburn ⋮ 7-9 minutes ⋮ 4/27/2023

Analysis Cellphones using Qualcomm chipsets may transmit data sometimes classified as personal information, specifically IP addresses, back to Qualcomm. But where such transmission is occurring, it's not secret and it has been going on for years.

That doesn't mean, however, there's no privacy risk in Qualcomm-based phones or in devices with rival chip sets for individuals like journalists or human rights advocates with sophisticated adversaries. Such scenarios, however, are unusual and not much of a worry for most mobile phone users.

Recently, hardware security firm Nitrokey published an advisory claiming that "smartphones with Qualcomm chips secretly send personal data to Qualcomm" and do so "without user consent, unencrypted, and even when using a Google-free Android distribution."

Post author "Paul Privacy" found that a Sony Xperia XA2 smartphone with a Qualcomm Snapdragon 630 processor, running /e/OS, a version of Android stripped of Google services, started communicating with Izat Cloud over unprotected HTTP.

The post goes on to claim that Izat is part of Qualcomm's XTRA service. As Qualcomm explains on the izatcloud.net website, "the Qualcomm Location XTRA Service generates and provides accurate satellite positions for extended periods of time to a mobile device."

It's basically a way to make GPS more precise and reliable while reducing use of energy-intensive radio hardware. The Izat servers provide information about satellite positions, which Qualcomm-powered phones download over HTTP. Doing so reveals to the servers the public IP addresses of the phones plus, according to NitroKey, some device metadata. That's really what this all boils down to.

"Qualcomm’s proprietary firmware is not only downloading some files to our phone to help establish the GPS location faster, but also uploads our personal data, such as the devices’ unique ID, our country code (Germany in this case), our cellphone operator code (allowing identification of country and mobile operator), our operating system and version and a list of software on the device," as Nitrokey put it, arguing this supplied metadata amounts to a unique per-person signature that harms privacy and occurs even when GPS is turned off.

A Qualcomm spokesperson disputed the research. "The article is riddled with inaccuracies and appears to be motivated by the author’s desire to sell his product," a company spokesperson told *The Register* in an email. "Qualcomm only collects personal information when permitted by applicable law."

"As disclosed in our publicly available privacy policy, the relevant Qualcomm technologies use non-personal, anonymized, technical data to enable device manufacturers to provide their customers location-based apps and services that end users expect from today’s smartphones."

- Google: Turn off Wi-Fi calling, VoLTE to protect your Android from Samsung hijack bugs
- To cut off all nearby phones with these Chinese chips, this is the bug to exploit
- One malicious MMS is all it takes to pwn a Samsung smartphone: Bug squashed amid Android patch batch
- The App Gap and supply chains: Purism CEO on what's ahead for the Librem 5 USA

Martijn Braam, a core developer for Alpine-Linux-based postmarketOS, has published a similarly scathing dismissal of the research as empty marketing. He noted the Qualcomm-initiated HTTP communication does not contain any private data. "It's just downloading a GPS almanac from Qualcomm for A-GPS [assisted GPS]," he observed.

Qualcomm Location Service, which was formerly known as IZat Location Services or IZat, is an opt-in service. It works by periodically downloading to phones data about the locations of nearby cell towers and Wi-Fi access points. The data may be augmented with device sensor data, such as gyroscope or accelerometer measurements, to help with location calculations and to save battery power.

"Qualcomm Location Service periodically sends us a unique software ID, the location of your device (longitude, latitude and altitude, and its uncertainty) and nearby cellular towers and Wi-Fi hotspots, signal strength, and time (collectively, 'Location Data')," the Snapdragon goliath explained on its website. "As with any Internet communication, we also receive the IP address your device uses."

The Nitrokey post goes on to claim that Qualcomm's XTRA service is not part of /e/OS or Android, but operates from the Qualcomm firmware known as AMSS. "This covert operating system operates on the broadband processor (modem) and manages the real-time communication with the cell towers," the advisory stated.

Piffle

A former mobile industry executive familiar with Qualcomm technology told *The Register* that characterizing AMSS as "a covert operating system" is "total nonsense."

However, our source explained, what goes on in phones at a low level isn't really understood by the general public.

"The way chipsets work, there's an application processor family," our source explained. "Underneath there's a kernel that hosts and virtualizes the operating system. And there are various subsystems – the modem, the Wi-Fi, peripherals like USB, the display driver, and the GPU. The vendors all have large amounts of software like AMSS that runs there. And they have a choice on what to compile from that image."

All the chipset makers, such as Huawei, Samsung, Qualcomm, and Apple, our source said, "any of these guys are going to have all kinds of different fetches that they're going to make [over the network]."

GrapheneOS, a privacy-focused version of Android, discloses these sorts of transmissions in its documentation. The only way to be sure about how one's phone behaves is to test it with a network traffic tool like Wireshark, our source said.

That's necessary, our source said, "because you can't get a straight answer from the vendors. Some of these features may have five or 10 switches to turn it on. There is a lot of old software. There's a lot of new software. It's very complex and there is a huge amount of it. And it has evolved from generation to generation. It's pretty much hideous, like any major operating system. The only thing I wouldn't call it is 'covert,' because it's been there forever."

On the other hand...

Mobile device data transmissions may pose a problem in high-risk environments because network identifiers such as IP addresses can be considered personal data, particularly when paired with hardware identifiers or other sorts of data.

"Say the Iranians are sitting there watching all traffic in and out of their country on the SS7 link, or on the internet, and every time they see one of these requests come by, which is totally easy to filter, they look at the identifier and say, 'is this is this an Iranian domestic? Is this our country code or somebody else's?'" our source said.

"And then they can screen on any identifier that's in the in the message and then they can say, 'Oh, well, we've got these 25 people that are resident in our country', and they may be carrying Iranian SIMs but they may have been able to associate that there was a SIM swap based on a more permanent identifier like a hardware identifier.

"If you want to hide in a country, you can never turn on that phone and have any hardware identifier get used in another network, because they could have trapped it. In some countries, they have the opportunity to know all the hardware coming in."

If your life depends on not being tracked through your phone, don't use a phone. For less pressing privacy scenarios, enjoy your chosen handset with the knowledge that you're probably leaving some kind of digital footprints somewhere. ®