

shubs

Co-founder of Assetnote, security researcher.

Assetnote Home Github Twitter LinkedIn

unlocking any car from X brand in most of the world

November 7 2026

I've always had a soft spot for this particular car brand. Our family has owned a few of them over the years, and they've served us incredibly well. In 2023, I bought a new four wheel drive/SUV from them, and it was the first time I had access to their connected car platform.

Having looked at platforms like this before (**previous works**), I was sceptical about how secure they really were. I suspected there was something there, but life kept getting in the way of actually looking. This July, I collaborated with Sam Curry to take a look at the security of a major automaker's connected car systems. Throughout this post, I'll refer to them simply as "the automaker".

When you typically think of car hacking, it's often easy to jump into the hardware side of things, but my background sits pretty squarely in compromising internet-facing web applications and infrastructure. Regardless of all the hardware bits and bobs, it all connects back to some service that, by design, has to be reachable from the internet.

The journey started with a simple question: what infrastructure does the app talk to when I remotely unlock my car? To work this out, I downloaded the APK and decompiled it, eventually reconstructing the API requests that were being made.

Going through the code, the primary point of contact seemed to be assets under `*.redacted-telematics.com.au`:

```
dartExecutor.executeDartEntrypoint(createDefault, CollectionsKt.r(gson.toJson(new GlobalCo
nfigParams(false, g11, com.redacted.app.xcapp.a.f69866f, "X", str)), new Gson().toJson(new
ApiConfig("https://api.redacted-telematics.com.au", "https://api.redacted-telematics.com.a
u", "https://api.redacted-telematics.com.au" ...
```

Almost every part of the consumer application called back to `redacted-telematics.com.au`. What else existed under this domain?