Abusing API Key

"These are not access token you are looking for"

-B.Dhiyaneshwaran

AGENDA

- Unauthorized Gmap API Key Usage Case
- Where to find these 
- Demo 

- Impact 
- Mitigations 

Unauthorized Gmap API Key Usage Cases?

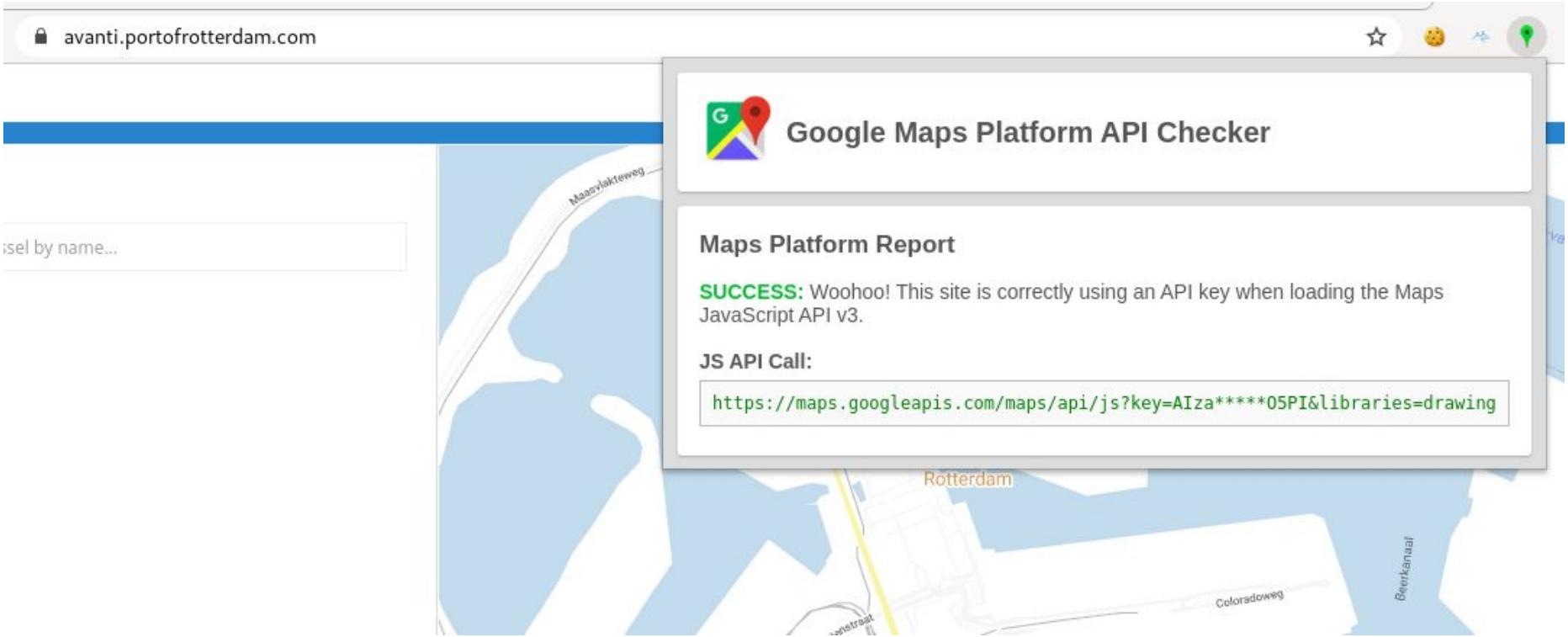
Google Maps API is a paid service which allows applications to embed & search from the Google Maps Database and use it on their own applications. While some of the services was free at the back times of Early 2018, they changed their usage plan after that date.

Where to find these ?

- Applications which used Map feature
- Contact forms & Geo Locations
- Javascript files

Reference :

https://github.com/ozguralp/gmapsapiscanner/



Chrome Extension :
https://chrome.google.com/webstore/detail/google-maps-platform-api/mlikepnkghhlnkgeejmlkfeheihlehne?hl=en


IT'S
DEMO TIME!
memegenerator.es

Impact

- Consuming the company's monthly quota or can over-bill with unauthorized usage of this service and do financial damage to the company.
- Conduct a denial of service attack specific to the service if any limitation of maximum bill control settings exist in the Google account.

Mitigations

For Web Applications

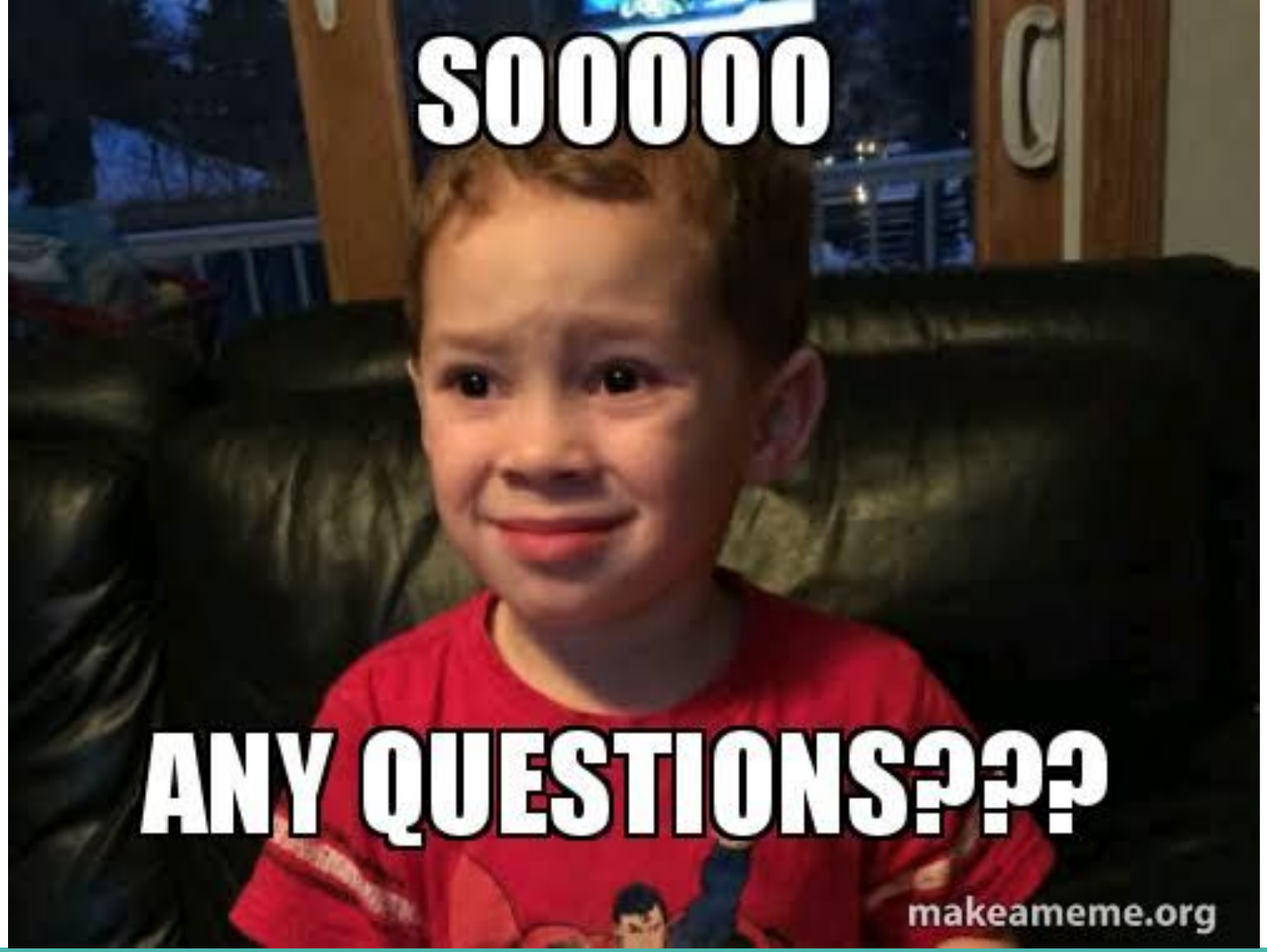
- Do not embed API keys or signing secrets directly in code.
- Do not store API keys or signing secrets in files inside your application's source tree.
- Review your code before publicly releasing it.

For Mobile Applications

- Use a proxy server.
- Obfuscate or encrypt the API key or signing secret.
- Use CA pinning or certificate pinning to verify the server resources are valid.

Reference

- Unauthorized Google Maps API Key Usage Cases, and Why You Need to Care
- Google Maps API (Not the key) Bugs That I Found Over the Years
- #753868 Insecure Storage and Overly Permissive API Keys in Android App
- https://developers.google.com/maps/api-key-best-practices
- https://www.youtube.com/watch?v=2_HZObVbe-g&t=167s


SOOOOO
ANY QUESTIONS???
makeameme.org