Upstream

2022 H1'2022 AUTOMOTIVE CYBER TREND REPORT

The automotive ecosystem is undergoing a dramatic evolution. The best way to prepare for cyber attacks is to deeply understand what is happening in the wild today. In this short report, we outline three emerging cyber threats automotive stakeholders need to be aware of and prepared for.

CONNECTED VEHICLE CYBER ATTACKS ARE DIVERSIFIED AND ON THE RISE

2022 will prove to be another watershed year for the automotive industry.

The adoption rate of electric vehicles (EV) is growing, demand continues to outpace supply, prices for raw materials are rising due to inflationary pressures, chip shortages persist, supply chains are stressed to the breaking point, and financial markets are heading into recession.

Upstream's research team constantly analyzes automotive and smart mobility-related cybersecurity incidents to provide critical information to our customers and community, while making sure that our technology remains one step ahead of hackers and fraudsters.

Since the beginning of 2022, our automotive cyber threat intelligence analysts have analyzed 100+ publicly reported automotive cyber-related incidents.

In this mid-year report, we'll discuss three emerging risks consumer and commercial automotive stakeholders must mitigate, all brought into sharp focus by increasing connectivity and applying software-driven approaches to modern vehicles:

01

Charging stations' *growing number of reported security vulnerabilities could be EV's Achilles heel.*

02

Cyber attacks on connected vehicles are increasingly relying on ***APIs*** *which interface with mission-critical systems.*

03

Current ***macroeconomic*** *conditions, combined with the proliferation of knowledge and availability of hacking techniques, are drawing adversaries' attention and motivation. Increasing connected vehicle attacks pose a serious threat to global supply chains and geopolitical stability.*

While some cybersecurity trends may take time to develop, the deep and dark web quickly democratizes them and puts anyone who is not prepared at risk.

To mitigate future attacks and minimize risk, it is crucial to understand how hackers and researchers exploit emerging vulnerabilities and what you can do to secure vehicles and mobility applications.

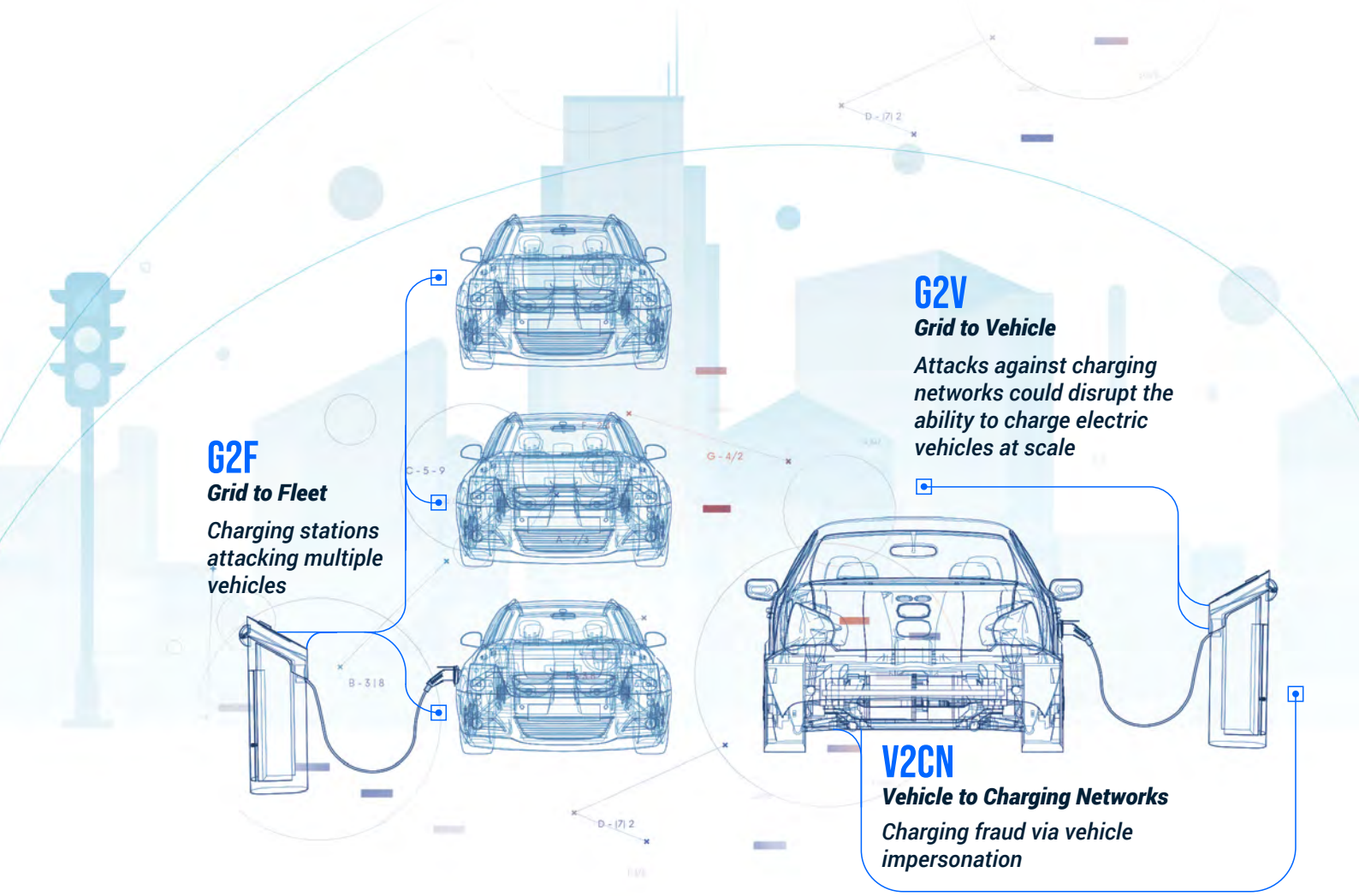
01. CHARGING STATIONS' SECURITY VULNERABILITIES COULD BE EVS ACHILLES HEEL

As the number of EVs continue to rise, so have concerns over the reliability and security of charging points. Available, reliable and safe charging infrastructure is critical to providing a solid customer experience and accelerating EV adoption. As EV charging communication protocols evolve, valuable data is transferred both ways using physical and wireless connections, including Personally Identifying Information (PII) and billing details.

To power their EVs and eliminate adoption barriers, OEMs must rely on complex and multi-layered charging infrastructure to ensure convenient and affordable public chargers are available. But most EV charging stakeholders are only in initial stages of implementing advanced cybersecurity platforms and are not yet required to comply with regulations and standards similar to UNECE WP.29 R155 and ISO/SAE 21434.

The EV gold rush has resulted in severe security flaws in charging infrastructure — exposing EV users to fraud and ransomware attacks, and making chargers vulnerable to physical and remote manipulation that slows them down or stops their functionality altogether.

Furthermore, OEMs and various charging infrastructure stakeholders must mitigate additional risks to EVs across a variety of charging attack vectors:



Here are several EV charging vulnerabilities that have made headlines in the first half of 2022:

January 2022

Seven vulnerabilities found in multiple charging stations which allow remote attackers to impersonate charging station admin users and carry out actions on their behalf.

February 2022

Russian electric vehicle chargers were hacked and disabled by a Ukrainian EV charging parts supplier as part of cyberwar effort.

April 2022

New Combined Charging Stations (CCS) attack technique found with the potential to disrupt the ability to charge electric vehicles at scale.

April 2022

An EV charging station in the Isle of Wight was hacked to show inappropriate content, with some EV owners also experiencing high voltage fault codes, leaving them stranded.

May 2022

Rise in hacks of EV charging stations including ransomware attacks against chargers and EV users.

May 2022

Rise in black-hat cyber criminals targeting EV charging stations to make money illegally, surpassing white-hat hackers working with stakeholders.

To learn more about H1'2022 incidents and vulnerabilities, checkout Upstream's AutoThreat® intelligence repository

Attacks on charging stations reveal more endemic problems to the EV ecosystem, where being first to market often overrides sound security practices. They have become increasingly nefarious as transportation becomes increasingly electrified. Consumer adoption of EVs, as well as the electrification of vehicle fleets, can be profoundly affected by these risks.

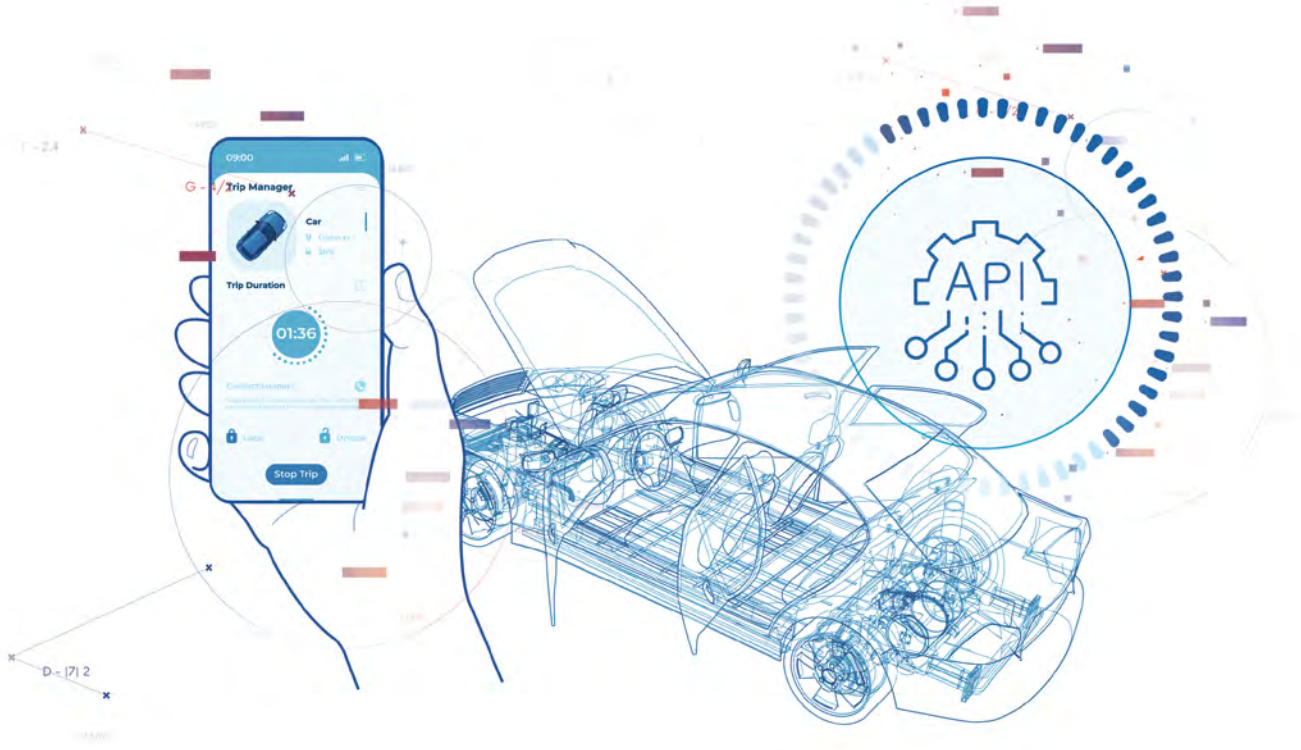
The success of electric vehicles depends on a reliable, consistent network of charging stations. To make sure that consumers can trust the charging infrastructure they use and that EV brands and vehicles are protected at all times, OEMs, charging networks and smart mobility stakeholders need to enforce a new cybersecurity paradigm with minimum standards and interoperability.

02. CONNECTED VEHICLE ATTACKS ARE INCREASINGLY RELYING ON APIS

APIs offer a simple and efficient interface for expanding functionality and improving the connected vehicle experience — fueling the consumerization evolution Automotive stakeholders are experiencing with new and fast growing revenue opportunities for OEMs, suppliers, and technology partners. They provide the critical point of connectivity needed to accelerate time to market of new capabilities and bring together data and services from a broad and diverse range of systems.

APIs present a pathway for agile data access, enhanced digital experiences, and new revenue streams. But more importantly, applications by OEMs and smart mobility service providers use APIs to interface with internal vehicle systems for core utility and functionality. Additionally, APIs facilitate the activation of vehicle features and the provision of subscription-based services, such as remote unlock, remote start, enhanced entertainment, and other features. Protecting APIs from malicious actors seeking access to mission-critical systems and sensitive data is essential.

APIs pose one of the greatest threats to connected vehicles — they can trigger actions in the vehicle, making hacking a vehicle possible without needing physical access to the vehicle itself nor being in proximity to the vehicle.



Here are several Automotive API-based vulnerabilities that have made headlines in the first half of 2022:

January 2022

A white-hat hacker claimed that he had found flaws in encryption protocols of a large EV OEM that allowed him to easily obtain digital car keys to vehicles and unlock doors, open windows, start cars, and disable security systems.

January 2022

Another vulnerability was found in the same EV OEM, allowing attackers to open doors of vehicles, start keyless driving, and interfere with vehicle operation en route using Grafana login access to obtain a token for API calls.

April 2022

A hacker tried to connect to multiple vehicles simultaneously through an OEM-approved smartphone application without the knowledge of the vehicle's owners.

May 2022

Some US EV owners reported that they had been able to connect to their new vehicles before they were ever shipped using the mobile application.

To learn more about H1'2022 incidents and vulnerabilities, checkout Upstream's AutoThreat® intelligence repository

The number of automotive API attacks has increased significantly despite OEMs employing advanced IT cybersecurity protections. IT-based solutions are struggling to handle the scope and magnitude of vehicle attacks, especially as they lack the context and deep understanding of how vehicles behave and operate.

Rethinking API-focused cybersecurity strategies is essential to maximizing API value and avoiding the safety and privacy risks associated with exposing critical backend systems. API security solutions tailored specifically for automotive applications must provide the full range of cybersecurity functionality and contextualize vehicle data to understand how APIs are used and when they are suspicious.

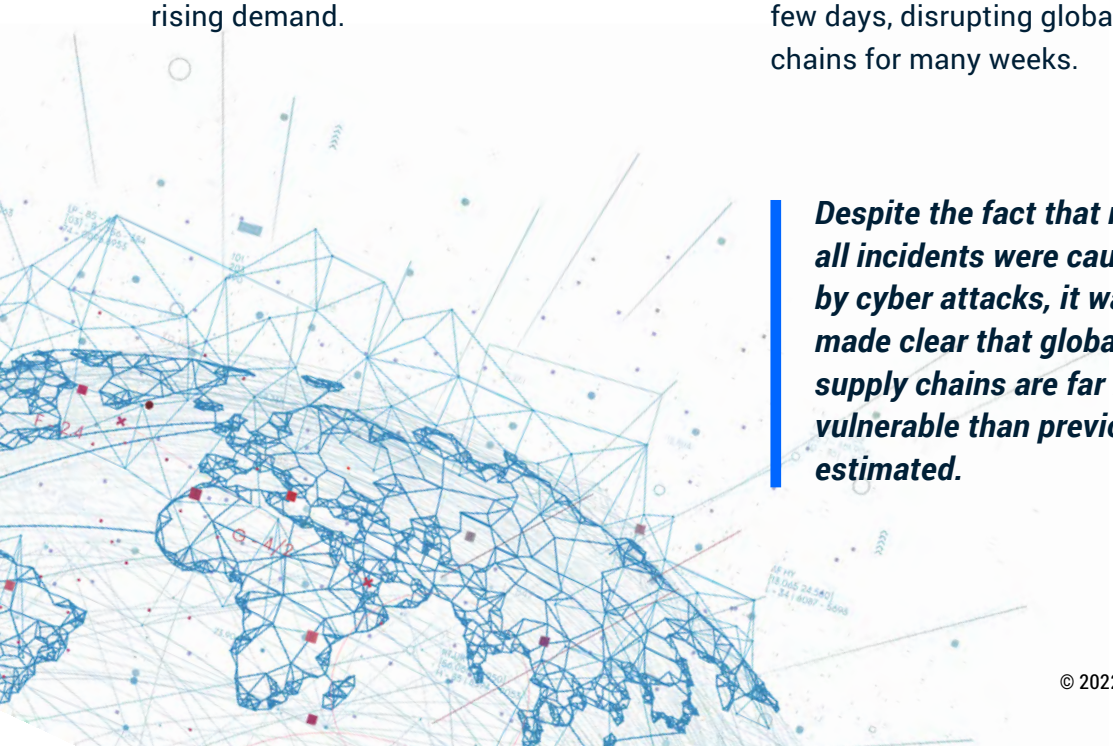
03. MACROECONOMIC CONDITIONS AND GLOBAL SUPPLY CHAIN CHALLENGES ATTRACT ADVERSARIES' ATTENTION

From connected agriculture vehicles to advanced commercial fleets, modern supply chains heavily rely on connected vehicles. Up until recently, there was a general consensus that global supply chains were resilient, and that crises caused by human errors or ransomware attacks would be localized and of little consequence globally.

However, current macroeconomic conditions, coupled with adversaries' growing awareness of the financial gains to be made, are raising concerns about the threat of cyber attacks to agriculture and commercial fleets as well as the wider supply chain.

The world has recently experienced the impact of a paralyzation of commercial fleets:

- In March this year, a German truck manufacturer had to shut down two factories in Europe and reduce production volumes in three other facilities because of a shortage of wiring components from Ukraine.
- As a result of a cyber attack, a Japanese OEM was forced to shut down 14 manufacturing facilities in February 2022.
- Chip shortages are also impacting the entire Automotive ecosystem, slowing new vehicle sales and commercial fleets' ability to meet rising demand.
- Another example goes back to March 2021, when one of the world's largest container ships blocked traffic in the Suez Canal for just a few days, disrupting global supply chains for many weeks.

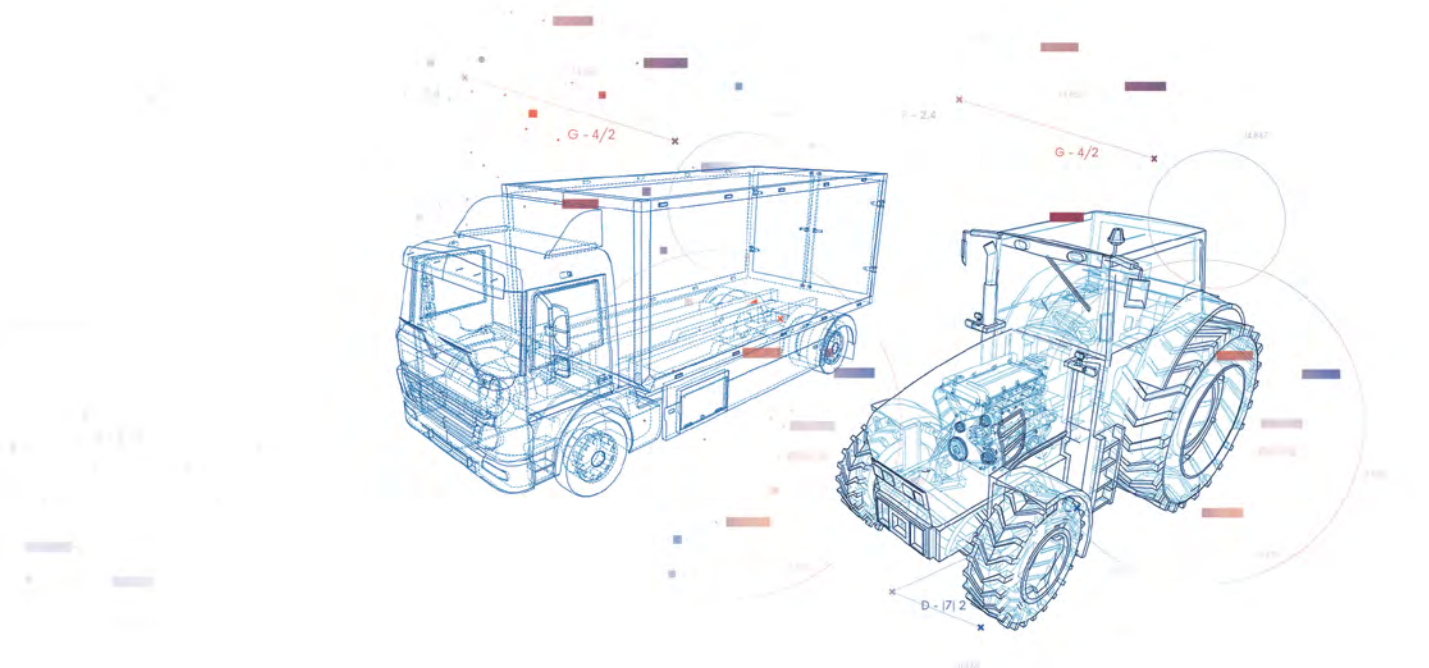


> ***Despite the fact that not all incidents were caused by cyber attacks, it was made clear that global supply chains are far more vulnerable than previously estimated.***

Last year, attempts by farmers to self-repair their agriculture equipment opened the door to additional vulnerabilities in supply chains. Hackers were able to access data of all customers who purchased vehicles from two different manufacturers by convincing them to unknowingly install malware on their vehicles. The data collected by the hackers via malware was later found to have been shared on the dark web.

> **Connected trucks, service vehicles, and agricultural systems occupy critical positions at both ends of the global supply chain.**
> **Cyber risks pose a significant threat — one that can halt the global economy and do enormous economic damage, particularly now, when financial systems are burdened by inflation and recession, and supply chains are already stressed from the pandemic and the war in Ukraine.**

Upstream's analysts are on high alert for supply chain manipulation attacks as commercial fleets continue to electrify their vehicles. The security of supply chains depends on cybersecurity operations protecting connected trucks and service vehicles from cyber threats.



ABOUT UPSTREAM

Upstream's mission is to secure and empower the future of connected vehicles.
Upstream helps automotive stakeholders secure their smart mobility assets, comply with regulations, improve vehicle design quality, and identify new business opportunities by unlocking the value in connected vehicle data.

Offering a cloud-based automotive cybersecurity and data analytics platform purpose-built for connected vehicles and smart mobility services, The Upstream Platform is agentless and eliminates the need to install hardware or software in vehicles.

The platform delivers unparalleled automotive cybersecurity detection that enables OEMs to effectively respond and mitigate a wide range of cybersecurity threats and attacks.

The Upstream Platform enables customers to build connected vehicle applications by transforming highly distributed vehicle data into centralized, structured, contextualized data lakes. Coupled with AutoThreat® PRO, the first automotive cybersecurity threat intelligence solution, Upstream provides industry-leading cyber threat protection and actionable insights, seamlessly integrated into the customer's environment and vehicle security operations centers (VSOC).

Upstream is privately funded by Alliance Ventures (Renault, Nissan, Mitsubishi), Volvo Group, BMW, Hyundai, MSI Insurance, Nationwide Insurance, Salesforce Ventures, CRV, Glilot Capital Partners, and Maniv Mobility.

For more information

VISIT US AT:
www.upstream.auto

CONTACT US:
hello@upstream.auto

FOLLOW US: