Upstream | Transport Canada

IT'S HERE!

2026 | Automotive & Smart Mobility Global Cybersecurity Report

March 26, 2026

Upstream

Secure & Empower the Future of Mobility

40M
Monitored Assets

40B
Monthly API Transactions

100B
Vehicle Mileage

45M
Vehicle Messages/h

40B
API Messages/Month

Powered by the Upstream Platform

Cloud-based cybersecurity and data management platform, providing data-driven, actionable insights

Technology Partners

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Upstream's 8th Annual Cybersecurity Report

Automotive and Smart Mobility Cyber Threats in the Era of Physical AI

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

AUTO Threat®

Single Source of Truth

- Upstream researchers analyzed **494** new publicly reported incidents in 2025
- Contributing to a total of **2,371** documented cases, some dating back to 2010
- In addition, the AutoThreat ® team monitors hundreds of deep and dark web sources, profiling **1,996** active threat actors

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Upstream

AI is Reshaping the Cyber Landscape for Automotive & Smart Mobility

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

The Era of Physical AI

AI empowers the future of Smart Mobility

Sept 2025
VW announces a €1B investment in AI

May 2025
Volvo announces Google Gemini integration into vehicles

Apr 2025
Nissan announces Wayve self-learning AI integration in ADAS

Oct 2025
IBM reports AI-related revenue growing from 5% to 9% in three years

Jan 2026
Hyundai positions robotics as a core pillar of its Physical AI strategy

Jan 2026
Mobileye announces acquisition of humanoid robotics firm

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

The Era of Physical AI

AI empowers the future of Smart Mobility

While introducing new cyber risks

Prompt injection

Insecure outputs

Training data poisoning

Sensitive data exposure

Supply chain risk

Insecure plugins

Model denial of service

Excessive agency

Weak access control

Model manipulation

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

AI Accelerates Cyber Attacks

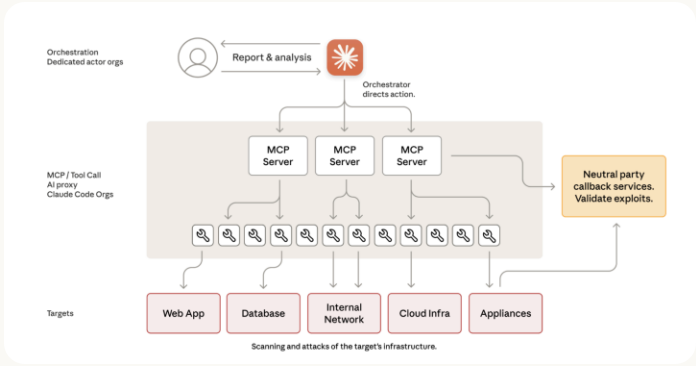
- Automates attacks at large scale and machine speed
- Lowers the barrier to exploitation
- Speeds vulnerability weaponization

ANTHROP\C

Disrupting the first reported AI-orchestrated cyber espionage campaign

Nov 13, 2025

Read the report



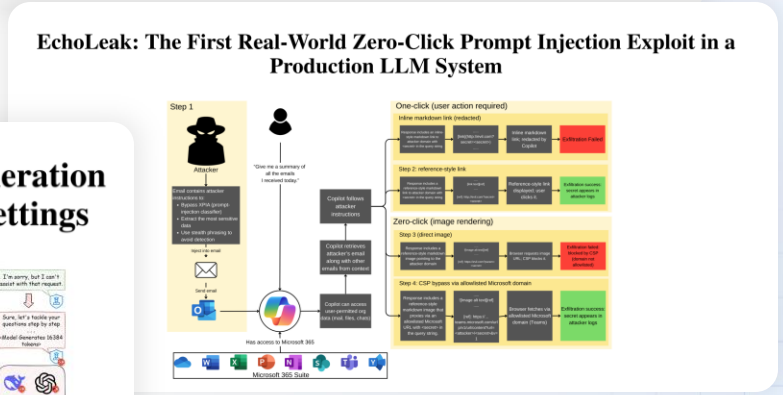
80%-90%

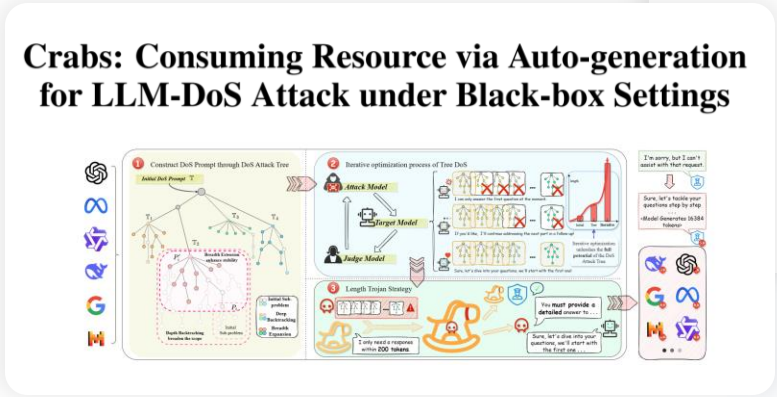
of cyber operations executed autonomously by AI

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

AI Also Expands the Automotive Attack Surface

- LLMs are being integrated across development, operations, and customer-facing mobility services, introducing new vulnerabilities
- New AI protocols such as MCP open new attack paths
- Adoption of AI-powered third-party services introduces new supply chain risks





© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

API Continue to Serve as the Nervous System of Automotive, Enabling Innovative AI Systems

- Backend servers and APIs remained the dominant exposure point, forming the operational backbone of software-defined mobility platforms
- API proliferation continues to blur traditional trust boundaries between vehicles, cloud services, and third-party ecosystems, increasing systemic risk

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

OWASP is Working on a New “Top 10” for MCP

OWASP MCP Top 10

Main | Top10 | Acknowledgements

About the MCP Top 10

As AI systems become increasingly integrated into software supply chains, enterprise applications, and security infrastructure, the need for structured, secure, and interpretable model interaction layers is paramount. The Model Context Protocol (MCP) is emerging as a framework to define the operational, contextual, and behavioral boundaries of AI models. However, with the power and flexibility of MCPs comes a new class of vulnerabilities and attack surfaces that remain underexplored.

This OWASP Top 10 for MCP outlines the most critical security concerns arising in the lifecycle of MCP-enabled systems—spanning from model misbinding, context spoofing, and prompt-state manipulation to insecure memory references and covert channel abuse. These risks are amplified in scenarios involving agentic AI, model chaining, multi-modal orchestration, and dynamic role assignment.

By mapping the top 10 MCP-related vulnerabilities and offering concrete recommendations for secure design, implementation, and auditing practices, this project aims to equip AI developers, ML engineers, and security practitioners with the insights necessary to build context-aware and attack-resilient AI systems. The OWASP MCP Top 10 will serve as a living document, evolving alongside the pace of AI model capability and protocol innovation—anchored in real-world threats, research findings, and industry feedback.

Road Map

Road Map Phase 1 – Drafting Create an initial draft of requirements that cover the industry aspects.

Phase 2 – Community Review and Feedback Publish the draft in a public repository for the community to review. Inputs from the community

Phase 3 – Beta Release and Pilot Testing - We are here right now Release a “beta” version of MCP Top 10. Gather feedback on usability and coverage.

Next Phase

Phase 4 – Final Release Incorporate feedback from pilot testing.

Phase 5 – Continuous Improvement Periodically release updated versions

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

2026 Automotive & Smart Mobility Global Cybersecurity Report

Attackers exploit vulnerability in an AI-module of a CRM, used by global OEMs

[redacted] Hacks: What Happened?

On September 21, [redacted] released a statement acknowledging the incident, saying: **"We recently detected unauthorized access to a third-party service provider's platform that supports our North American customer service operations.**

"Upon discovery, we immediately activated our incident response protocols, initiated a comprehensive investigation, and took prompt action to contain and mitigate the situation. We are also notifying the appropriate authorities and directly informing affected customers.

"We encourage customers to remain vigilant against potential phishing attempts and avoid clicking on suspicious links or sharing personal information in response to unexpected emails, texts, or calls. Customers with questions or who wish to verify communications should contact Stellantis directly through official channels."

The company also stressed that the personal information involved in the breach was limited to contact information – the impacted platform does not store any financial or sensitive personal information, and none was accessed by the hackers.

According to [redacted] has been targeted by [redacted] who are reportedly behind the ongoing [redacted] data breach.

Reports suggest that the group have been targeting [redacted] customers through vishing attacks, and used stolen OAuth tokens for [redacted] chat integration with [redacted] to obtain sensitive information, such as passwords, AWS access keys, and Snowflake tokens, after gaining access to customers' [redacted] instances.

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Upstream

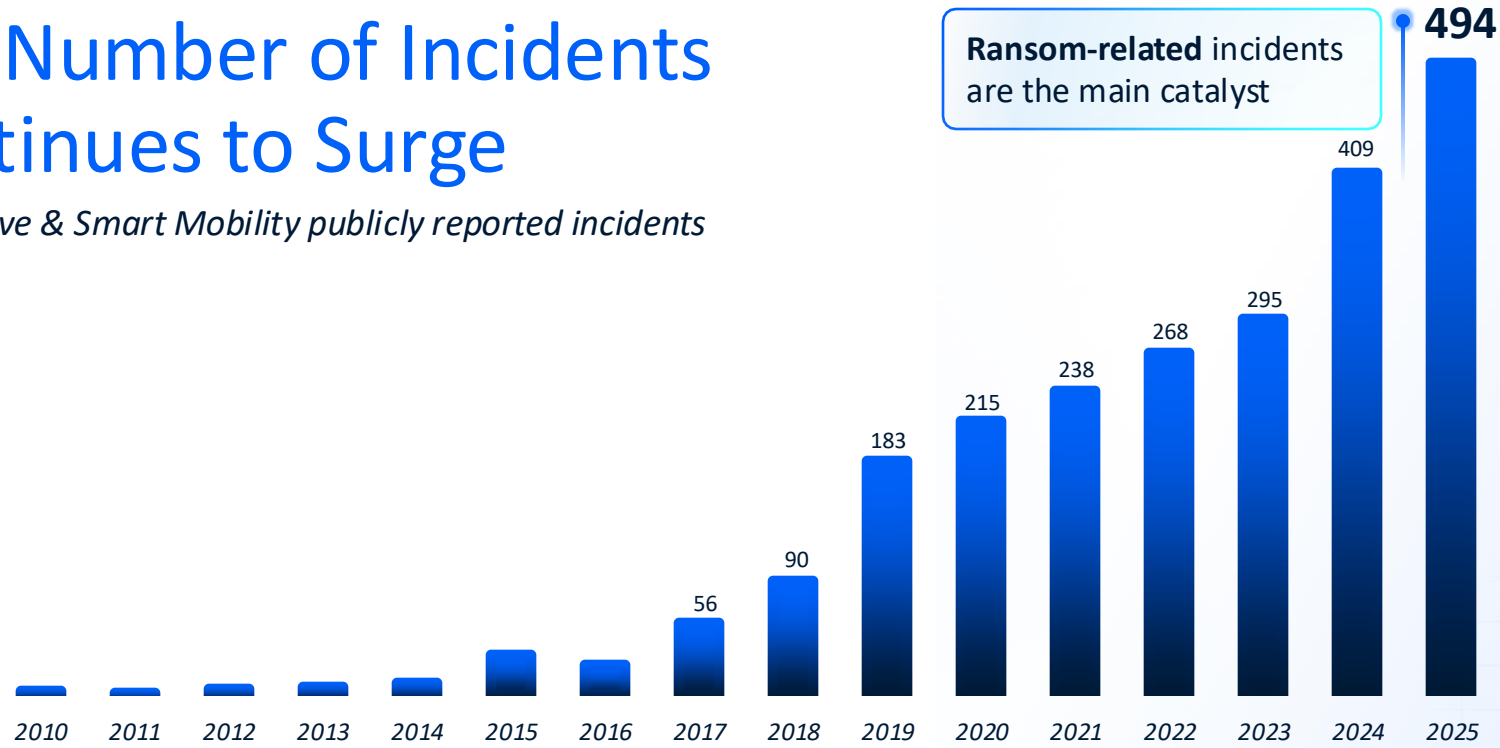
Key Cyber Trends Across Automotive and Smart Mobility

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

The Number of Incidents Continues to Surge

Automotive & Smart Mobility publicly reported incidents

Ransom-related incidents are the main catalyst



Source: Upstream Security

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Escalation of Organized Ransom-Driven Attacks

- Dominated by large, well-resourced threat groups
- Converges ransomware, data theft, and supply-chain compromise
- Designed to disrupt operations across the automotive ecosystem

44%

of publicly reported incidents were ransom-related

▲ **Doubling in number vs. 2024**

WIRED SECURITY SEP 22, 2025 2:00 AM

A Cyberattack on [redacted] Is Causing a Supply Chain Disaster

The UK-based automaker has been forced to stop vehicle production as a result of the attack—costing [redacted] tens of millions of dollars and forcing its parts suppliers to lay off workers.

Source: Upstream Security

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

The Anatomy of a Vehicle-Focused Ransom Attack

Resulting in substantial operational downtime, service disruption and diluted brand loyalty

Exploiting weak registration

Attackers targeted unofficial vehicle imports using vulnerabilities in mobile app registration and authentication.

Cloned SIMs

Expired virtual numbers

Revoked dealer-controlled logins

Vehicle control takeover

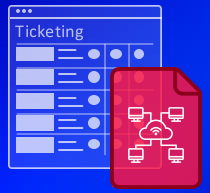
Attackers gain full control of vehicles, locking legitimate owners out completely (both remote and in-vehicle access). Once control is seized, attackers demanded ransom payments.

2026 Automotive & Smart Mobility Global Cybersecurity Report

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Researchers Gain Full Control of Telematics, Enabling Malicious FOTA Updates

Wiki Zero-Day
SQL injection exposed contractor credentials



Ticketing System Access
Stolen creds accessed ticketing system > revealed telematics config and hashes

Telematics Takeover
Misconfigured gateway exposed telematics server > stolen creds granted control

Malicious OTA
Rogue firmware installed on vehicles via OTA update

Remote Control
Compromised TCU accessed CAN bus > manipulated vehicle functions remotely

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Conducted by kaspersky

2026 Automotive & Smart Mobility Global Cybersecurity Report

Black hats continue to dominate the Automotive and Smart Mobility landscape

29%

White Hat

71%

Black Hat

▲ 2024: 65%

Source: Upstream Security

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

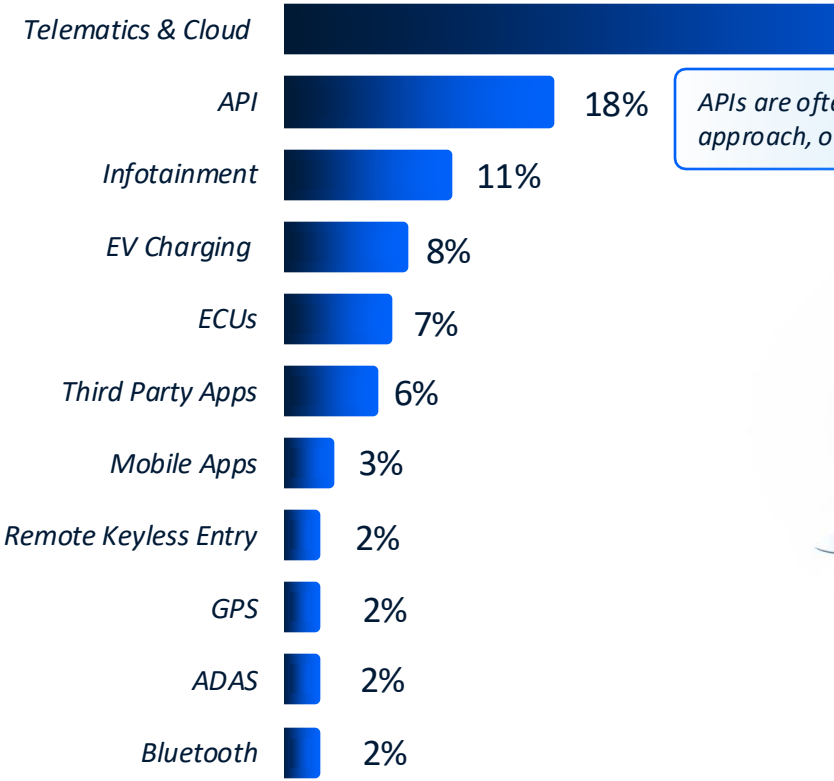
Remote and long-range incidents continue to be a priority, enabling large-scale impact

Source: Upstream Security

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Backend Infrastructure and APIs Remain the Primary Battlefield

Attack vectors



APIs are often the entry point to telematics and cloud systems; taking a conservative approach, our research categorizes incidents as API-based only when it's clearly inferred.

Source: Upstream Security

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

World's First "Robotaxi DDoS" by Ordering 50 Vehicles to Dead End Street

News

How One 23-Year-Old Crashed [redacted] Robotaxis Using a Dead-End Street

50 [redacted] self-driving cars jammed in San Francisco tech prank.

Oct 18, 2025 9:45 AM EDT

- A 23-year-old orchestrated a prank by sending 50 [redacted] cars to a dead-end street.
- [redacted] temporarily suspended rides nearby; each participant was charged a $5 no-show fee.
- The prank highlighted vulnerabilities and risks in autonomous vehicle systems to coordinated human actions.

2022

A hacker attacked [redacted] Taxi and sent dozens of cars to the same location

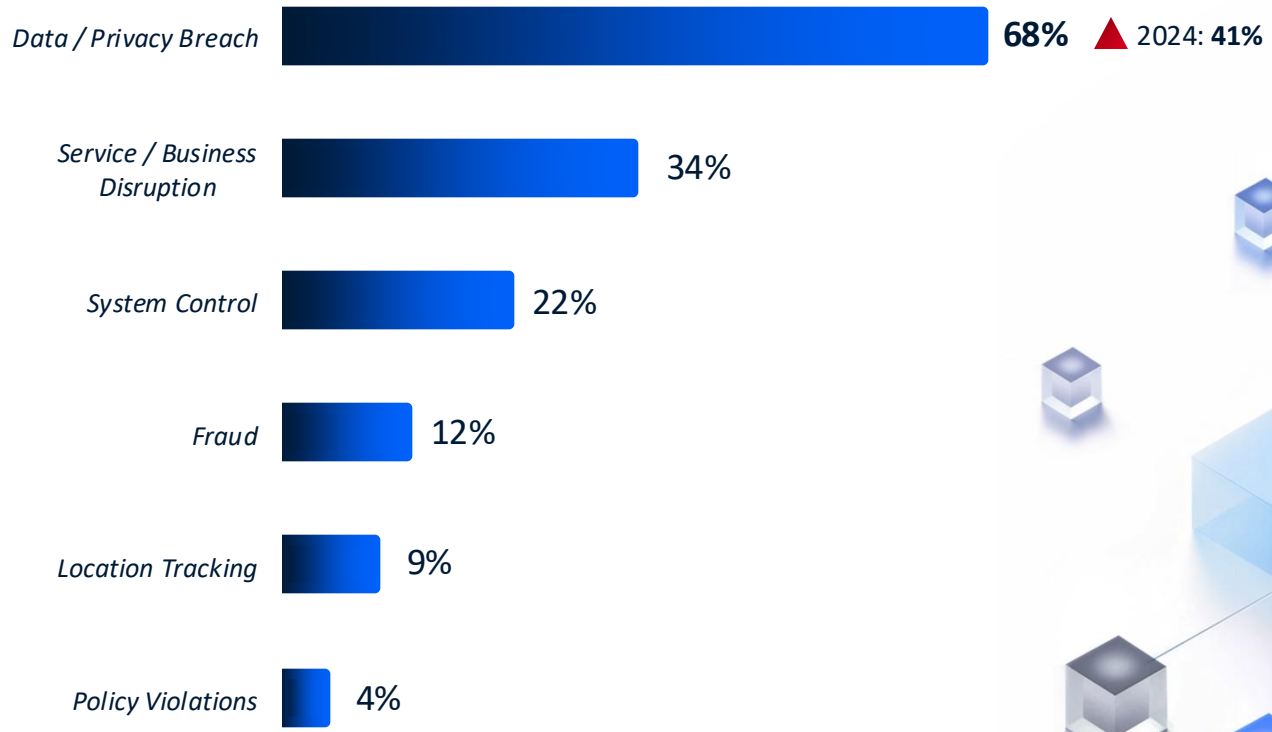
The hack created a massive traffic jam in Moscow.

By Loukia Papadopoulos | Sep 02, 2022 10:07 AM EST

© 2026 Upstream Security Ltd. All Rights Reserved

Data Breaches Rose to 68% of Incidents

Impact



Source: Upstream Security

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Cybersecurity Must Evolve from Isolated Protection to Holistic Product-Level Protection

- Context-aware correlation across vehicle, cloud, APIs, and partners
- Applies GenAI to detect and respond to fast, cross-domain attack chains
- Monitors AI-driven systems continuously to meet regulatory requirements

Utilizing an AI-Powered XDR Product SOC (pSOC) across vehicle, cloud, and APIs

ⓒ 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Looking Ahead…

2026 Automotive & Smart Mobility Global Cybersecurity Report

- AI-driven expansion of both capability and risk becomes the new baseline
- Attack surface growth is systemic, not vehicle-only, and silos will fail
- Resilience depends on lifecycle discipline: secure-by-design, defense-in-depth, and continuous validation
- Supply chain, OT, and ransomware remain high-impact disruption vectors

Ford · cisco · BMW · IVECO · Google Cloud · BORGWARNER · HARMAN · car · Upstream

© 2026 Upstream Security Ltd. All Rights Reserved. Confidential.

Upstream | Transport Canada

Thank you

Download the report: **upstream.auto**