halcyon | Ransomware Research Center

Forty-Four Percent and Rising: Ransomware Footprint is Expanding in the Automotive Industry

Summary:

Ransomware attacks targeting the automotive industry more than doubled in 2025, accounting for 44% of reported cyber incidents across the sector. The surge in attacks reflects a calculated shift by cybercriminals who increasingly view the automotive industry as a lucrative target, driven by its rapid adoption of connected technology, growing reliance on cloud services, and a sprawling network of third-party suppliers that broadens criminals' opportunities to strike. Given these escalating threats, companies across the automotive supply chain should prioritize understanding their exposure, strengthening their defenses, and ensuring they are prepared to respond when an attack occurs.

Background:

Since 2023, the automotive sector has seen a steady rise in cybersecurity incidents, with ransomware emerging as the fastest-growing and most disruptive threat. In 2025, industry insider Upstream ransomware accounted for nearly half of all incidents in the industry, more than doubling the volume recorded the previous year. This sharp increase is based on a variety of internal and external industry data, but even publicly-reported incidents alone show attacks against the automotive sector steadily increasing since 2022, including an almost 50% increase last year:

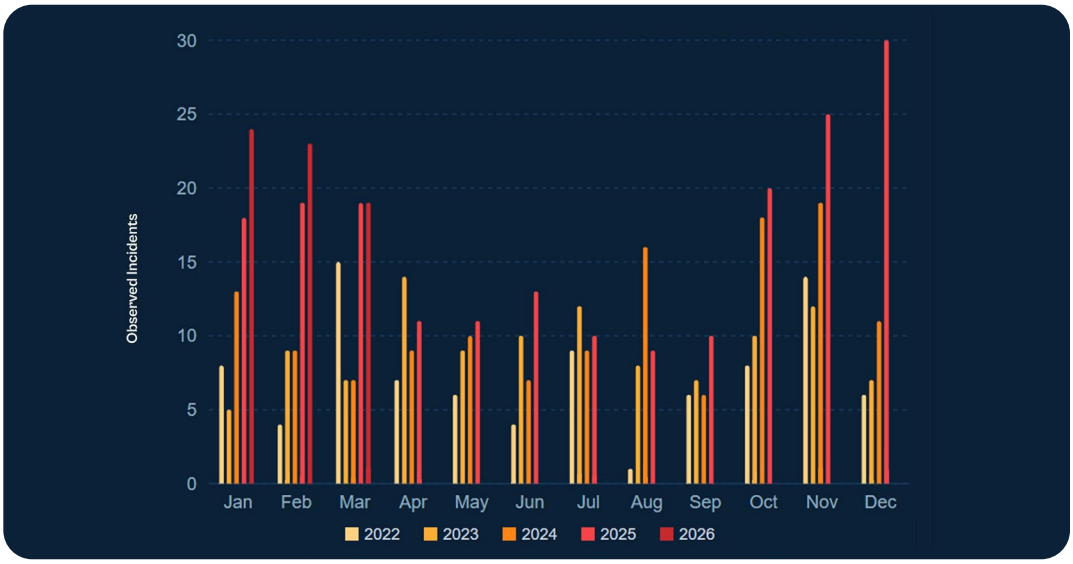

Figure 1: Public Ransomware Incidents in the Auto Sector Per Month

The automotive industry's vulnerability to ransomware stems from several converging factors:

- **Expanding Digital Attack Surface:** Connected vehicle platforms, over-the-air (OTA) update mechanisms, and cloud-based architectures have introduced new entry points across the industry. In 2025, adversaries used telematics systems, cloud platforms, and/or APIs as primary attack vectors in 67% of surveyed incidents.
- **Fragmented Supplier Ecosystem:** The majority of automotive cyber incidents in 2024 targeted suppliers and third-party providers rather than Original Equipment Manufacturers (OEMs) directly. Smaller suppliers often maintain privileged access to OEM systems while lacking the resources to implement robust cybersecurity measures.
- **Organized Threat Actors:** Well-resourced criminal groups—including BlackSuit, Everest, Qilin, Akira, and Scattered Spider—are targeting the sector through Ransomware-as-a-Service (RaaS) operations, using AI-enabled tools, established infrastructure, and a combination of data theft and encryption to maximize pressure on victims.
- **Low Tolerance for Downtime:** Automotive manufacturing and retail operations are tightly integrated and time sensitive. Production halts and system outages translate rapidly into substantial financial losses, making the sector an attractive extortion target.

Details:

Recent ransomware incidents have spanned the full automotive value chain—from vehicle manufacturers and Tier 1 suppliers to dealership platforms and connected vehicle systems—revealing an industry.

Repeated Compromises of Global OEM (January 2026)

Since 2024, criminal groups have reportedly compromised a global vehicle manufacturer and its subsidiaries at least four times. Most recently, in January, the Everest ransomware group claimed to have stolen approximately 900GB of internal data, including dealership records and internal reports. Other incidents include a December 2025 Red Hat GitLab compromise exposing 21,000 customer records, an August 2025 Qilin ransomware attack on a design subsidiary, and a 2024 Akira breach affecting 100,000 individuals in Australia and New Zealand.

Significant Ransomware Attack against Jaguar/Land Rover (October 2025)

Jaguar/Land Rover suffered a ransomware attack that halted all global production for more than three weeks. Estimated economic damage to the UK reached £1.9 billion ($2.5 billion), the disruption affected 104,000 supply chain workers, and the company's wholesale volumes fell 43% during the affected period.

Continued...

Vehicle-Level Ransoms (Mid-2025):

In June 2025, attackers hijacked accounts and seized remote control of vehicles in Russia, locking owners out, controlling windows, doors, and engine starts, and demanding ransoms to restore access. The attackers exploited weak app-registration practices tied to unofficial imports of a specific Chinese vehicle, gaining access through cloned SIMs, expired virtual numbers, and dealer-controlled logins that had since been revoked. This campaign demonstrates criminals' interest in now targeting vehicles themselves, with direct implications for physical safety.

Compromised IT Provider (February-March 2025):

Attackers maintained access for approximately one week, stealing data on 2.7 million vehicle owners including Social Security numbers. The same parent group's European operations had been separately targeted separately in 2024 by the Black Basta group, resulting in 3TB of exfiltrated data.

Supply Chain Attacks Japan, Italy, Australia (Early 2025):

Qilin stole over 500GB of engineering blueprints and supplier agreements from a Japanese precision parts manufacturer. Separate incidents hit suppliers in Italy and Australia during the same period.

Compromised Automotive Dealership Management Platform (June 2024):

BlackSuit attacked the leading software provider of dealership management systems in North America, taking down operations at approximately 15,000 dealerships for two weeks. Collective losses were estimated at $1 billion, including a reporter ransom payment of $25 million in Bitcoin. A second attack struck during initial recovery, extending the outage.

Mitigation:

- **Deploy Dedicated Anti-Ransomware Solution:** Deploy dedicated anti-ransomware defenses capable of detecting and stopping threats before encryption begins. Effective solutions should identify the behavioral patterns that precede a ransomware deployment–including reconnaissance, credential harvesting, lateral movement via RDP/SMB, privilege escalation, and data exfiltration–as well as late-stage indicators such as unauthorized GPO-deployed scheduled task creation, selective disabling of security tooling, and deletion of backup copies [M1038] [M1040].

- **Perimeter and Edge Device Hardening:** Prioritize patching of internet-facing assets, with immediate attention to VPN appliances (Fortinet, SonicWall), firewalls, file transfer platforms (Cleo, CrushFTP, MOVEit), RDP endpoints, and enterprise resource planning (ERP) systems (SAP, Oracle EBS). Refer to CISA's Known Exploited Vulnerabilities (KEV) Catalog for prioritization.
- **Credential Hygiene and Identity Controls:** Deploy phishing-resistant multi-factor authentication (MFA) across all systems, with particular emphasis on VPN, remote access, and privileged accounts [M1032]. Audit all third-party access and remove or rotate legacy credentials. The 2021 credentials exploited in the Jaguar/Land Rover breach illustrate how long-dormant access can remain a live risk. [M1018].
- **Endpoint Security Hardening:** Ensure endpoint detection and response (EDR) solutions are resilient against tampering techniques that attackers commonly use to disable or bypass security tooling, including Bring Your Own Vulnerable Driver (BYOVD) [M1038]. Validate that EDR agents generate alerts immediately upon any disruption to their operation [M1040].
- **Backup Resilience and Recovery Testing:** Maintain immutable, offline backups isolated from domain-joined systems, and test restoration procedures regularly [M1053]. Knowing a backup exists is not the same as knowing it works.
- **Supply Chain Risk Governance:** Establish baseline security requirements for critical vendors, software providers, and third-party service partners [M1013]. Actively monitor for breaches in third-party tools and platforms in use across organization [M1047].

References:

- Upstream Security - 2026 Global Automotive and Smart Mobility Cybersecurity Report
- Bitsight - Automotive Cyber Threats: Ransomware Trends in 2026
- Dragos - Industrial Ransomware Analysis Q3 2025
- Breached.company - The Automotive Industry Under Siege (2024–2025)
- Hackread - Everest Ransomware Claims Breach at Nissan
- Cybernews - Nissan 900GB Data Leak
- SecurityWeek - Nissan Confirms Impact From Red Hat Data Breach
- CNBC - Jaguar Land Rover Cyberattack
- BleepingComputer - Jaguar Land Rover Extends Shutdown
- CYFIRMA - Investigation Report on Jaguar Land Rover Cyberattack

- VicOne - Ransomware Attacks Target Automotive Industry in Early 2025
- CNN - CDK Global Ransom Payment
- TechTarget - CDK Global Outage Explained
- Canadian Auto Dealer - Ransomware Surges as Auto Cyberattacks Double
- WardsAuto - AI Doubled Auto Industry Cyberattacks
- CISA - Known Exploited Vulnerabilities Catalog

Source Summary:

This Alert is based on Halcyon observations, open-source information, and ongoing research. Findings reflect our current understanding of threat actor activity and may be updated as new evidence emerges. Assessments may be revised as additional evidence becomes available.

The Halcyon Ransomware Research Center unites experts, drives smart policies, and delivers actionable intelligence to detect, disrupt, and defeat ransomware. Explore the Center's latest reports, analysis, and resources here.