CYXCEL®
TRACE

September 2025

The TRACE Brief

Welcome to the TRACE Brief,
CyXcel's monthly Cyber Threat Intelligence briefing.

In Focus: Jaguar Land Rover Cyberattack

What Happened?

Jaguar Land Rover (JLR) was subjected to a cyberattack on September 1 2025 in one of the most significant recent cyber incidents to hit the UK automotive industry. The attack, attributed to the group "Scattered Lapsus$ Hunters", has resulted in a complete shutdown of JLR's global production operations, affecting over 33,000 employees and causing estimated daily losses of £5-10 million.

Upon detection of the incident, JLR shutdown IT systems to contain the breach, halting production across facilities in the UK, Slovakia, China and India. Whilst initially optimistic about a swift recovery, JLR has since extended the production shutdown multiple times, with the latest extension running until September 24, though industry sources warn that the impact could last until November.

Who is Behind the Attack?

The attack has been claimed by "Scattered Lapsus$ Hunters", a cybercriminal collective that represents a merger of three notorious hacking groups: Scattered Spider, Lapsus$, and ShinyHunters. This alliance, combines the sophisticated social engineering capabilities of Scattered Spider, the brazen extortion tactics of Lapsus$ and the data theft expertise of ShinyHunters

Scattered Spider gained notoriety earlier this year after a wave of attacks against UK retailers, notably M&S, the Co-Op and Harrods, and in September 2024 an attack on Transport for London (TfL) which caused service disruption and the accessing of customer data. Two teenagers from the UK were charged on September 18 with Computer Misuse Act offences in connection with the TfL attack following an operation by officers from the National Crime Agency (NCA) and City of London Police.

The group's tactics in the JLR attack appear to align with their established methods, including social engineering campaigns and the deployment of ransomware with data exfiltration capabilities.

Production Disruption

JLR's production capabilities have been inoperational since September 1. The company typically manufactures approximately 1,000 vehicles daily across its UK facilities in Solihull, Halewood and Wolverhampton, with additional production sites in Slovakia, China and India. Over 33,000 JLR employees have been instructed to remain at home while production lines remain offline, and an extended shutdown may create uncertainty about long-term job security and operational continuity.

In Focus: Jaguar Land Rover Cyberattack

Data Compromise

On September 10, JLR confirmed that "some data has been affected" as a result of the cyberattack.” While the company has not disclosed the specific nature or scope of the compromised data, it has notified relevant regulators, including the UK's Information Commissioner's Office (ICO).

Impact on Supply Chain

The impact of the attack extends far beyond JLR's direct operations, creating a cascading crisis throughout the company's extensive supply chain network. JLR supports approximately 104,000 jobs across its UK supply chain, with many small and medium-sized enterprises (SMEs) particularly vulnerable to the extended halt in operations, with reports that some may face potential bankruptcy, lacking the financial resilience awaiting operations to resume.

The incident also highlights potential risks associated with a “just-in-time” logistics model which, unlike more resilient supply chain models, relies on real-time data feeds and interconnected systems that become single points of failure during cyberattacks.

In conclusion, the JLR cyberattack demonstrates how a single breach can paralyse global business operations, creating cascading efforts throughout an entire supply chain ecosystem.

Key Takeaways

- Financially motivated threat actors are joining forces, creating larger groups with the capability to successfully infiltrate some of the world's largest global brands, causing operational disruption and extensive financial losses.
- JLR is two years into an £800m deal to accelerate digital transformation across its business. In addition to the hardening of IT infrastructure, organizations must ensure policies are adopted which counter attacks initiated through social engineering, both in human form, and through increased capabilities in AI, where we have already seen “deepfake” videos successfully used in attacks causing significant financial losses.
- Significant cyberattacks ripple through an organization's supply chain. Suppliers have been forced to scale back production, and some risk bankruptcy, lacking the financial resources to cope with extended business interruption. In the UK, the government is facing calls for a furlough scheme to be set up to prevent widespread job losses.

September 2025

Kering Luxury Brands Breach

In another attack attributed to the ShinyHunters group, luxury brand group Kering were targeted in April 2025, after unauthorized access was gained to their Salesforce CRM systems.

Data was stolen from several Kering owned brands, including Gucci, Balenciaga and Alexander McQueen.

The breach became public in September when attackers leaked information to the media, alleging to have stolen data containing up to 7.4million unique email addresses and multiple personal identifiers relating to customers, including names, dates of birth, email and home addresses and detailed purchase history.

The Salesforce attacks in April impacted several other high-profile organizations, including Google, Cisco, TransUnion, and other luxury brands including LVMH brands (Louis Vuitton, Dior and Tiffany & Co) and Chanel.

Salesforce were not directly breached in the attacks, instead attackers used social engineering techniques targeting Salesforce users, convincing them to grant third-party application Oauth permissions, which allowed long term access tokens to victims' accounts.

Key Takeaways

- Cyber incidents often result in not only a financial loss but brand trust erosion.
- The attack highlights the risks that luxury brands face in protecting often affluent clients' privacy and security.
- Impacted customers are at a heightened risk of targeting or potential identity theft, with a vast dataset of information stolen which could be used for financial fraud, impersonation or account takeovers.

Our Trace team monitors the dark web and digital communications platforms for client exposure and risk across three core areas.

Data, Credentials and Access

We monitor for threats which pose the greatest risks to your organisation, searching across stealer marketplaces or initial access brokers offering valid credentials or access to your business, identification of leaked credentials and the offering for sale or exposure of company data.

Organisational Risk

Monitoring for adversarial chat which could indicate an impending or future cyber attack, the registration of domains which may be intended to spoof legitimate company infrastructure.

Supply Chain and Vendor Risks

We dig deeper, monitoring your critical supply chain partners to identify risks which might expose your data or risk downtime, disrupt your business operations. If a breach does occur within your supply chain, we identify leaked data to allow you to assess the risks posed.

CYXCEL® TRACE

September 2025

Ransomware Causes Airport Chaos

On September 19-20 2025, a ransomware attack targeted Collins Aerospace's MUSE (Multi-User System Environment) platform, causing widespread disruption across major European airports.

The attack forced airports to revert to manual check-in procedures, resulting in extensive flight delays, cancellations and passenger backlogs.

The attack compromised Collins Aerospace's cloud-based MUSE system, which provides shared check-in and boarding infrastructure for multiple airlines across approximately 170 airports globally.

Collins Aerospace has been previously targeted by cybercriminals, most notably in July 2023 when the BianLian ransomware group successfully breached the company's systems. This earlier incident resulted in approximately 20GB of sensitive data being exfiltrated.

The attacks on Collins Aerospace must be viewed within the broader context of escalating cyber threats against aviation infrastructure providers. The sector has experienced a 600% increase in cyberattacks between 2024 and 2025, with threat actors increasingly recognizing the strategic value of targeting shared service providers rather than individual airlines or airports.

Key Takeaways

- The aviation industry is attractive to a range of threat actors, with financially motivated actors seeking to cause widespread disruption as a mechanism to get paid.
- In targeting the MUSE platform, attackers were able to disrupt the operations of multiple airlines through a third-party vendor, highlighting how a single cyber event can cascade across multiple critical infrastructure nodes and the need for robust fallback systems.

Disruption in Numbers

- 90% of flights from London Heathrow delayed by 15+ minutes on September 22.
- Brussels airport was severely affected, asking airlines to cancel half of all scheduled flights on September 21.
- More than 500 flights cancelled, with Brussels, Heathrow, Berlin and Dublin experiencing the majority of disruptions.

CYXCEL® TRACE

September 2025

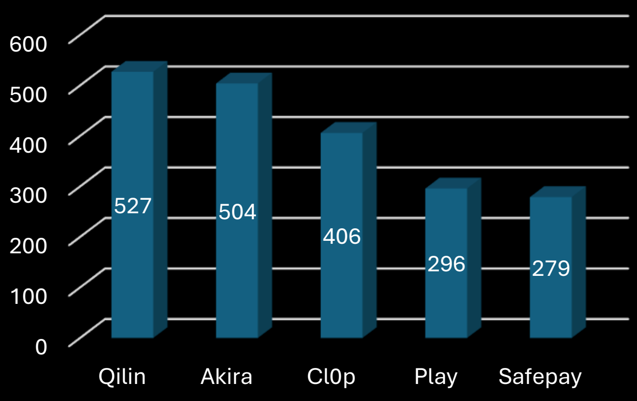
Ransomware Round-up

Ransomware remains the most serious risk to organizations from financially motivated attackers looking to both encrypt systems and exfiltrate data, with successful attacks leading to significant disruption and costs. 2025 is again showing year on year increase with over 5,500 published attacks this year to date (vs 4,201 at same time last year), and more groups than ever involved with the explosion of Ransomware as a Service (RaaS) lowering the bar for less skilled threat actors.

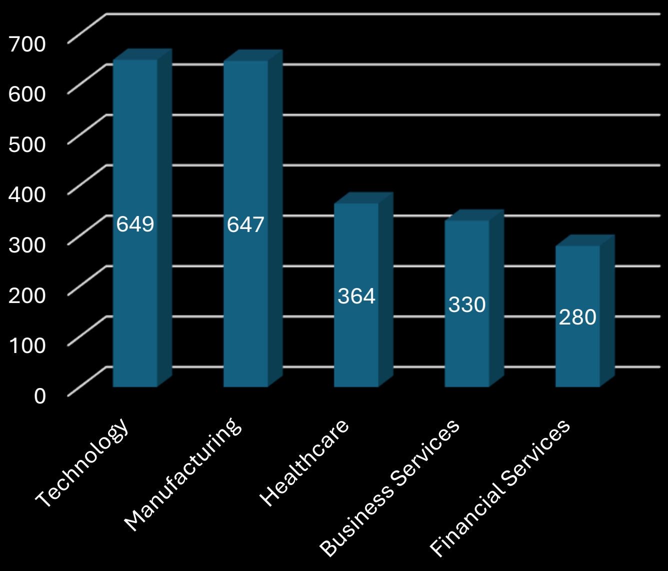
Qilin ransomware group is the most prolific by volume, publishing data from over 500 organizations this year to date, closely followed by Akira, with both groups operating a Ransomware as a Service model. Qilin were responsible for the cyber attack on Synnovis in June 2024, a pathology services provider for King's College Hospital and Guy's and St Thomas' NHS Foundation Trusts. This ransomware attack resulted in the postponement of 10,152 acute outpatient appointments and 1,710 elective procedures, with at least one confirmed patient death attributed to delayed blood test results during the cyber incident. The attack exposed nearly 400GB of sensitive NHS patient data, including names, NHS numbers, and blood test descriptions, published on the dark web when ransom demands were not met.

Technology and Manufacturing sectors have been the hardest hit, with their low tolerance for downtime making them a prime target for ransomware operators. Healthcare, Business and Financial Services are also prime targets, often with rich datasets of sensitive client or personal data being stolen as a means of pressuring organizations into paying.

Most prolific ransomware groups (by published attacks) in 2025



Most targeted sector (by published attacks) in 2025



CYXCEL® *We offer fully integrated, customizable solutions that combine expertise in technology, cybersecurity, law, and geopolitics.*

Rescue

All aspects of incident management and response, to ensure your business emerges from a breach swiftly, effectively, and more resilient.

Resolve

A full-spectrum suite of services to strengthen your business against disruption and threats, while protecting its rights and reputation.

Transform

A bespoke service to upgrade your digital and cybersecurity infrastructure, covering everything from design to delivery.

Operate

Hosted and managed security solutions, specialist industry services, and on-demand access to extra capacity and skills augmentation.