

# Weekly Intelligence Summary

Report Date: 08.09.2025

Intelligence Cut-off Date: 05.09.2025

## Weekly Focus: Jaguar Land Rover cyber incident severely disrupts global operations

**Researchers have reported a significant breach at Jaguar Land Rover (JLR), with three prolific threat actor groups claiming collaboration in the attack, resulting in major disruption to both manufacturing and retail operations.**

The threat actors Scattered Spider, Shiny Hunters, and LAPSUS\$, now styling themselves as “Scattered LAPSUS\$ Hunters”, claim to have exploited a flaw in JLR’s SAP NetWeaver environment. Disruption has been most visible at the Halewood plant, where staff were instructed not to attend work, suggesting halted production schedules and delays across the wider supply chain. Retail systems were also taken offline, limiting JLR’s ability to process vehicle orders during a critical UK sales window.

JLR maintains that there is currently no evidence of customer data theft, though external researchers observed malicious network traffic consistent with ransomware or destructive malware. The decision to proactively shut down core systems aligns with containment measures typically applied in high-severity incidents.

This marks JLR’s second significant breach in 2025, following the Hellcat ransomware breach of 350GB of sensitive company data in March. The recurrence highlights persistent targeting of JLR and its Tata Group partner, reinforcing perceptions of the company as a high-value target for organised cybercrime groups.

### Why It Matters...

The collaboration of Scattered Spider, ShinyHunters, and LAPSUS\$ is notable, bringing together three prolific cybercriminal groups. Such coordination increases both the sophistication and impact of operations, complicating attribution and response efforts.

The operational consequences for JLR have already been severe, with manufacturing halted and sales channels disrupted. This demonstrates the tangible financial and reputational risks posed by ransomware and destructive campaigns against the automotive sector.

Although JLR continues to state there is no evidence of theft, the claimed exploitation of SAP systems raises concerns over the compromise of sensitive corporate data, intellectual property, and customer information. Organisations linked to JLR or Tata Group should remain alert to potential secondary targeting and possible data leaks.

This incident highlights the growing trend of adversarial collaboration and the exploitation of trusted enterprise platforms. Urgent patching of SAP NetWeaver, strict identity controls, and heightened monitoring for anomalous administrative or bulk data activity are strongly recommended.

## Intelligence Overview

### Data Breach

TransUnion experienced a data breach exposing the sensitive personal data of about 4.46 million US customers following the compromise of a third-party application used in consumer support operations.

The Dutch Clinical Diagnostics laboratory suffered a data breach affecting over 850,000 cervical cancer screening patients. Threat actors published a 100 MB sample of the total 300GB of stolen data on a dark web forum.

### Malware

Threat actors leveraged HexStrike AI, a legitimate open-source red teaming tool, to exploit recently disclosed Citrix NetScaler vulnerabilities, effectively accelerating the exploitation timeline of critical vulnerabilities.

Threat actors used AnyDesk installer and a Windows File Explorer ClickFix variant to deliver the MetaStealer infostealer through SMB shares and disguised MSI packages. The malware enables login credentials, sensitive files and cryptocurrency wallet data theft.

### Cybercrime

Black Nevas ransomware group claimed to have exfiltrated about 4TB of sensitive corporate data from Toyota Kirloskar Motor including employee, corporate, supplier and customer information.

Cloudflare, Palo Alto Networks, and Zscaler disclosed data breaches related to the Salesloft Drift data-theft campaigns. Threat actors obtained access to Cloudflare API tokens, Palo Alto business information and Zscaler personal Salesforce information.