

# Weekly Intelligence Summary

Report Date: 13.10.2025

Intelligence Cut-off Date: 10.10.2025

## Weekly Focus: Scattered LAPSUS\$ Hunters data leak site continues listing organisations as Salesforce data deadline approaches

**On 8 October 2025, threat actors operating under the Scattered LAPSUS\$ Hunters data leak site (DLS) listed more global entities, including Dell, Telstra, Kuwait Airways, Lycamobile, Verizon, and Thai telecom providers True Corporation and dtac.**

Samples of exfiltrated data were published to the DLS to substantiate the claims. The leaked material reportedly includes personally identifiable information (PII), as well as technical and corporate datasets, including device serial numbers, network logs, and customer records. Data from the Salesforce campaigns is set to be released at 11:59 PM New York time on October 10, 2025.

This latest activity builds upon Scattered LAPSUS\$ Hunters' earlier compromise of Jaguar Land Rover, which caused significant operational disruption. It also coincides with the emergence of cross-group collaboration between Crimson Collective and Scattered LAPSUS\$ Hunters, following the Red Hat Consulting breach in early October 2025.

That intrusion, which exfiltrated almost 570 GB of development data from Red Hat's self-managed GitLab instance, marked what appears to be a new Extortion-as-a-Service (EaaS) model, with Crimson Collective leveraging the newly launched Scattered LAPSUS\$ Hunters' DLS to coordinate extortion attempts alongside affiliated threat actors.

## Why It Matters...

The activities of Scattered LAPSUS\$ Hunters and allied collectives such as Crimson Collective and ShinyHunters demonstrate a greater level of sophistication and coordination of data-extortion operations, in line with prior trends of greater specialisation amongst groups within the cybercriminal ecosystem.

The adoption of an EaaS model is likely to enable even less sophisticated actors to participate to a greater degree in large-scale breaches through shared infrastructure, creating a realistic possibility that both the scale and frequency of incidents will escalate.

To secure infrastructure, the threat from Scattered LAPSUS\$ Hunters' should be viewed collectively rather than as isolated actors and integrate the latest threat intelligence from all affiliated groups into threat-detection and monitoring workflows.

Orpheus advises entities with ties to the listed organisations to ingest technical and behavioural indicators of compromise all linked threat actors, whilst proactively monitoring extortion sites for potential disclosures.

## Intelligence Overview

### Qilin Ransomware

Qilin has claimed the compromise of Asahi, which forced the Japanese company to suspend its domestic operations. The group alleged it had exfiltrated 27GB of data, including financial documents, contracts, employee details, and development forecasts.

Qilin also disclosed its role in a recent ransomware incident impacting Mecklenburg County Public Schools. The group claims to have exfiltrated 305GB of sensitive data, including financial records, grants, budgets, and medical files, and has published a sample to support their claim.

### Targeted Extortion

Threat actors linked to C10p ransomware are attempting to extort executives after claiming to have stolen sensitive data from Oracle's E-Business Suite. Screenshots and file trees have been distributed as proof of compromise, with the actors demanding, in one instance, up to USD 50 million.

KaruHunters has claimed responsibility for breaching Huawei Technologies, offering alleged stolen data for sale on DarkForums. In the post, published on 3 October 2025, the actor claims to have exfiltrated sensitive intellectual property, including source code, internal development tools and scripts, build files, and configuration data.

### Nation State

US law firm Williams & Connolly confirmed a compromise of several attorney email accounts caused by the exploitation of an undisclosed zero-day vulnerability. The FBI is investigating the incident, which is suspected to be part of a broader Chinese state-linked cyber-espionage campaign.