

Weekly Intelligence Summary

Report Date: 24.11.2025

Intelligence Cut-off Date: 21.11.2025

Weekly Focus: Salesforce investigates data theft via Gainsight breach as ShinyHunters expands extortion capability through new ShinySp1d3r RaaS

Salesforce investigates a data-theft incident involving refresh tokens issued to the integrated third-party Gainsight, following unauthorised access to customer information.

The incident follows a series of high-profile data theft and extortion operations linked to the Scattered LAPSUS\$ Hunters threat actor, who has recently claimed access to multiple Salesforce customer datasets, including contact information, harvested from integrated third-party tools such as Gainsight.

Parallel to this disclosure, ShinyHunters has this week unveiled an in-development Ransomware-as-a-Service (RaaS) program known as ShinySp1d3r. Early builds of the malware observed by security researchers suggest that the service is being designed to target Windows systems and VMware ESXi environments, in line with prior targeting.

The new platform is reported to integrate tooling associated with affiliated threat actors such as Scattered Spider, reflecting the increased overlap and lack of meaningful distinction between the groups that were previously tracked separately, following the increased use of common infrastructure, codebases, and, most recently, a shared data leak site.

Why It Matters...

The introduction of ShinySp1d3r suggests that ShinyHunters and associated threat actors are moving towards an Extortion-as-a-Service (EaaS) and Ransomware-as-a-Service (RaaS) extortion model to monetise their breaches.

Previously, Orpheus reported on groups such as Crimson Collective and Scattered LAPSUS\$ Hunters leveraging shared leak sites and infrastructure to broaden the reach of extortion campaigns. By adding ransomware tooling to its portfolio, the threat actor is positioned to escalate existing data-theft operations into double extortion operations that also encrypt compromised systems.

Organisations using Salesforce or other cloud CRM platforms should prioritise the auditing of connected applications, token scopes, and integration privileges, while also monitoring for anomalous Workday/CRM activity that may indicate abuse of access tokens.

Entities across all sectors should incorporate emerging indicators associated with ShinySp1d3r into detection pipelines, particularly those operating ESXi virtualised infrastructure.

Intelligence Overview

Vulnerabilities

A critical FortiWeb zero-day tracked as CVE-2025-64446 (OVSS: 90 | CVSS: 9.8) is being actively exploited to create unauthorised admin accounts on internet-exposed appliances. Fortinet has issued patches across all supported branches, and CISA has added the flaw to its KEV list.

Google patched a high-severity Chrome zero-day (CVE-2025-13223, OVSS: 71 | CVSS: 8.8) actively exploited via a V8 type-confusion flaw, enabling potential remote code execution. Fixes are included in Chrome 142.0.7444.175/176.

Cybercrime

Princeton University reported a phishing-led breach exposing personal data for alumni, students, donors, and faculty, with no financial data affected. The incident follows a similar UPenn breach and highlights the continued targeting of the education sector.

A threat actor claims to have stolen Samsung Medison data via a third-party contractor and is selling it on dark-web forums. The claim is unverified, underscoring ongoing third-party risk.

China

A Dragon Breath campaign targeting Chinese-speaking users is distributing fake installers that deploy the RONINGLOADER malware, which disables security tools and delivers a tailored Gh0st RAT for espionage. The loaders impersonate apps like Chrome and Teams to evade detection.