ShinyHunters lança vazamento de dados listando violação do Salesforce -

Data: 2025-10-05 03:32:45

Autor: Inteligência Against Invaders

O Trinity of Chaos, um grupo de ransomware vinculado a Lapsus$, Scattered Spider e ShinyHunters, criou um site de vazamento de dados na rede TOR. Este site inclui dados de 39 empresas, como Aeromexico, AirFrance, Google, Cisco, Stellantis e Qantas Airlines, afetadas por ataques a instâncias fracas do Salesforce e outras vulnerabilidades.

Trinity of Chaos, um coletivo de ransomware presumivelmente associado ao Lapsus$, Scattered Spider e ShinyHunters.O relatório anterior do Resecurity indica que o grupo continuará suas atividades, agora com foco no ransomware tradicional.

O Data Leak Site (DLS) lista vítimas recentes como Stellantis, que revelou uma violação de dados que afetou clientes norte-americanos em 21 de setembro de 2025. Isso se seguiu a um ataque à Jaguar Land Rover que interrompeu seu varejo e produção.

A maioria das amostras de dados vazadas não inclui senhas, mas tem muitas PII, sugerindo que provavelmente vêm de instâncias comprometidas do Salesforce devido a ataques de vishing e tokens OAuth roubados vinculados à integração de bate-papo Drift AI da Salesloft. Isso levou o FBI a emitir um aviso rápido com indicadores técnicos para as organizações verificarem possíveis invasões em seus sistemas Salesforce.

Um relatório da Resecurity revelou uma crescente campanha global de crimes cibernéticos liderada por LAPSUS$, ShinyHunters e Scattered Spider. Apesar das alegações de sua “aposentadoria”, este grupo continua a hackear e extorquir grandes empresas, with muitas violações de dados significativas ainda não divulgadas. O relatório indica um aumento nos esforços de extorsão privada, sugerindo que o impacto real desses hackers pode ser muito maior do que se sabe. Eles também afirmam ter atualizado o Data Leak Site (DLS) após 10 de outubro, que agora apresenta mais de 1,5 bilhão de registros.

Analistas de resegurança indicam que novas vítimas e incidentes estão surgindo. As atividades de extorsão em andamento e a reputação do grupo estão pressionando as empresas a permanecerem em silêncio, revelando a extensão dos dados comprometidos nos setores da Fortune 100, financeiro, tecnologia, aviação, varejo e automotivo.

Especialistas em segurança cibernética alertam que os cibercriminosos podem usar dados roubados para fins prejudiciais, inclusive em aplicativos de IA. Eles podem analisar as informações da vítima para obter insights e conectar conjuntos de dados, permitindo engenharia social sofisticada, phishing direcionado e roubo de identidade, principalmente contra grandes empresas e entidades governamentais.