ShinyHunters lança site de vazamento de dados: Trinity of Chaos anuncia

Data: 2025-10-03 23:03:13

Autor: Inteligência Against Invaders

ShinyHunters lança site de vazamento de dados: Trinity of Chaos anuncia novas vítimas de ransomware

Trinity of Chaos, vinculado a Lapsus$, Scatter Spider & ShinyHunters, atingiu 39 empresas por meio de falhas do Salesforce, lançando um site de vazamento de dados TOR.

O Trindade do Caos, um coletivo de ransomware presumivelmente associado a Lapsus$, Aranha Dispersae Caçadores brilhantes Grupos **Lançado** um site de vazamento de dados (DLS) na rede TOR contendo 39 empresas, incluindo, entre outras, Aeromexico, AirFrance, Google, Cisco, Stellantis, Qantas Airlines, afetadas pela atividade cibernética maliciosa direcionada a instâncias vulneráveis do Salesforce e outras vulnerabilidades. Como circunstanciado pelo Resecurity no relatório anterior de inteligência de ameaças, o grupo pretende continuar suas atividades e mudou para um modus operandi tradicional de ransomware.

A listagem no Data Leak Site (DLS) inclui referências às vítimas mais recentes, incluindo a Stellantis, gigante automotiva que divulgou uma violação de dados que afetou seus clientes norte-americanos há algumas semanas (21 de setembro de 2025). Este incidente ocorreu após um ataque à montadora britânica de luxo Jaguar Land Rover, que interrompeu severamente suas atividades de varejo e produção.

Notavelmente, a maioria das amostras de dados vazadas não tem senhas, mas contém quantidades substanciais de dados PII, o que pode confirmar que os registros roubados provavelmente se originam das instâncias afetadas do Salesforce por meio de ataques de vishing e tokens OAuth roubados usados para a integração de bate-papo Drift AI da Salesloft. Isso gerou um recente aviso rápido emitido pelo FBI, descrevendo indicadores técnicos que as organizações devem monitorar para determinar se os invasores se infiltraram em seus ambientes Salesforce.

Um relatório de segurança anterior descoberto uma campanha global de crimes cibernéticos em rápido desdobramento – e potencialmente muito maior – liderada pela notória aliança de LAPSUS$, ShinyHunters e Scattered Spider. Ao contrário das recentes alegações de “aposentadoria”, a chamada “Trindade do Caos” continua a conduzir hacks coordenados e operações de extorsão contra empresas líderes, com várias violações de dados importantes ainda a serem divulgadas ao público. Este relatório oportuno destaca uma onda de tentativas de extorsão privadas, sinalizando que o verdadeiro raio de explosão desses agentes de ameaças pode exceder em muito o que veio à tona até agora. O grupo afirma ter atualizado o Data Leak Site (DLS) após 10 de outubro em caso de falta de pagamento. Segundo eles, o novo DLS contará com mais de 1,5 bilhão de registros.

Analistas de segurança alertam que só agora novas vítimas e incidentes estão vindo à tona. Com a

atividade de extorsão confidencial em andamento – e o grupo aproveitando sua notoriedade para coagir as empresas ao silêncio – a extensão total dos dados comprometidos nos setores da Fortune 100, serviços financeiros, tecnologia, aviação, varejo e automotivo está apenas começando a surgir.

De acordo com especialistas em segurança cibernética, os cibercriminosos podem explorar dados roubados para fins maliciosos em grande escala, inclusive em aplicativos prejudiciais de inteligência artificial (IA). Ao ter contexto sobre as vítimas afetadas e seus setores, os agentes de ameaças podem realizar mineração de dados para extrair informações valiosas e correlacionar conjuntos de dados das vítimas com outras informações disponíveis. Isso pode levar a esquemas sofisticados de engenharia social, campanhas de phishing direcionadas e roubo de identidade, especialmente visando grandes empresas e setores governamentais.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,ShinyHunters)