Google confirma violação do Salesforce CRM e enfrenta ameaça de extors

Data: 2025-08-10 19:04:58

Autor: Inteligência Against Invaders

Google confirma violação do Salesforce CRM e enfrenta ameaça de extorsão

O Google divulgou uma violação do Salesforce Customer Relationship Management (CRM) expondo dados de alguns clientes em potencial do Google Ads.

O Google confirmou uma violação em uma instância do Salesforce CRM que afeta os dados de possíveis clientes do Google Ads. O site Databreaches.net informou que os invasores enviaram um extorsão demanda para a gigante da tecnologia.

O Google Threat Intelligence Group confirmou que um de seus sistemas de banco de dados Salesforce, usado para armazenar informações de contato e notas relacionadas para pequenas e médias empresas, foi violado pelo agente da ameaça Caçadores brilhantes (também conhecido como UNC6040).

“Em junho, uma das instâncias corporativas do Salesforce do Google foi afetada por atividades de UNC6040 semelhantes descritas neste post. O Google respondeu à atividade, realizou uma análise de impacto e iniciou as mitigações. A instância foi usada para armazenar informações de contato e notas relacionadas para pequenas e médias empresas.” lê o declaração publicado pelo Google. “A análise revelou que os dados foram recuperados pelo agente da ameaça durante uma pequena janela de tempo antes que o acesso fosse cortado. Os dados recuperados pelo agente da ameaça foram confinados a informações comerciais básicas e amplamente disponíveis publicamente, como nomes comerciais e detalhes de contato.

A gigante da tecnologia já notificou os indivíduos afetados.

As informações expostas incluem nomes comerciais, números de telefone e “notas relacionadas” para que um agente de vendas do Google entre em contato com eles novamente. Os dados financeiros não foram afetados, o incidente não afetou os dados do Google Ads na conta do Google Ads, no Merchant Center, no Google Analytics e em outros produtos do Google Ads.

A ShinyHunters alegou que a violação do Google envolveu cerca de 2,55 milhões de registros, com os quais o agente da ameaça está trabalhando Aranha Dispersa que lhes fornecem acesso inicial aos alvos, e agora chamam essa colaboração de “Sp1d3rHunters” de acordo com o Bleeping Computer.

ShinyHunters supostamente exigiu 20 BTC (~ $ 2,3 milhões) do Google, mas depois alegou que era uma brincadeira. Eles agora usam uma ferramenta personalizada para exfiltrar mais rapidamente

dados de sistemas Salesforce comprometidos.

O Grupo de Inteligência de Ameaças do Google está rastreando UNC6040, um grupo com motivação financeira que usa phishing de voz para direcionar os sistemas Salesforce para roubo e extorsão de dados em larga escala. Fingindo ser suporte de TI, eles ligam para os funcionários, muitas vezes em filiais de empresas globais que falam inglês, para induzi-los a conceder acesso ou compartilhar credenciais. Uma tática comum é fazer com que as vítimas aprovem um aplicativo Salesforce Data Loader falso, dando aos invasores a capacidade de roubar dados confidenciais. Em alguns casos, meses se passam antes que a extorsão comece, às vezes sob o nome ShinyHunters para aumentar a intimidação.

Os agentes de ameaças usaram engenharia social para roubar credenciais ou vincular aplicativos OAuth maliciosos do Salesforce Data Loader, baixaram bancos de dados inteiros e extorquiram vítimas.

Siga-me no Twitter:@securityaffairseLinkedineMastodonte

PierluigiPaganini

(Assuntos de Segurança–hacking,Google)