Google confirma que violação de dados expôs informações de clientes em

Data: 2025-08-09 19:16:51

Autor: Inteligência Against Invaders

O Google confirmou que um Violação de dados divulgada recentemente de uma de suas instâncias do Salesforce CRM envolvia as informações de potenciais clientes do Google Ads.

“Estamos escrevendo para informá-lo sobre um evento que afetou um conjunto limitado de dados em uma das instâncias corporativas do Salesforce do Google usadas para se comunicar com clientes em potencial do Ads”, diz uma notificação de violação de dados compartilhada com o BleepingComputer.

“Nossos registros indicam que informações básicas de contato comercial e notas relacionadas foram afetadas por este evento.”

O Google diz que as informações expostas incluem nomes comerciais, números de telefone e “notas relacionadas” para um agente de vendas do Google contatá-los novamente.

A empresa diz que as informações de pagamento não foram expostas e que não há impacto nos dados do Google Ads na conta do Google Ads, no Merchant Center, no Google Analytics e em outros produtos do Google Ads.

A violação foi conduzida por agentes de ameaças conhecidos como ShinyHunters, que estão por trás de uma onda contínua de ataques de roubo de dados direcionados aos clientes da Salesforce.

ShinyHunters disse ao BleepingComputer que também está trabalhando com agentes de ameaças associados ao “Scatter Spider”, que são responsáveis por obter acesso inicial aos sistemas visados.

“Como já dissemos repetidamente, ShinyHunters e Scatter Spider são a mesma coisa”, disse ShinyHunters ao BleepingComputer.

“Eles nos fornecem acesso inicial e conduzimos o despejo e a exfiltração das instâncias do Salesforce CRM. Assim como fizemos com o Snowflake.”

Os agentes de ameaças agora estão se referindo a si mesmos como “Sp1d3rHunters”, para ilustrar o grupo sobreposto de pessoas envolvidas nesses ataques.

Como parte desses ataques, os agentes de ameaças realizam ataques de engenharia social contra funcionários para obter acesso a credenciais ou induzi-los a vincular uma versão maliciosa do aplicativo Data Loader OAuth do Salesforce ao ambiente Salesforce do alvo.

Os agentes de ameaças baixam todo o banco de dados do Salesforce e extorquem as empresas por e-mail, ameaçando liberar os dados roubados se o resgate não for pago.

Esses ataques do Salesforce foram relatado pela primeira vez pelo Grupo de Inteligência de Ameaças do Google (GTIG) em junho, com a empresa sofrendo o mesmo destino um mês depois.

Databreaches.net relatou que os agentes de ameaças já enviou uma demanda de extorsão ao Google. No entanto, se não for pago, não seria surpreendente que os agentes de ameaças vazassem os dados gratuitamente como forma de provocar a empresa.

ShinyHunters também disse ao BleepingComputer que, desde então, mudou para uma nova ferramenta personalizada que torna mais fácil e rápido roubar dados de instâncias comprometidas do Salesforce.

Em uma atualização, O Google reconheceu recentemente as novas ferramentas, afirmando que viram scripts Python usados nos ataques em vez do Salesforce Data Loader.

[IMAGEM REMOVIDA]