Salesforce se recusa a pagar resgate por ataques generalizados de roubo

Data: 2025-10-08 07:43:25

Autor: Inteligência Against Invaders

A Salesforce confirmou que não negociará ou pagará um resgate aos agentes de ameaças por trás

de uma onda massiva de ataques de roubo de dados que afetou os clientes da empresa este ano.

Conforme relatado pela primeira vez por Bloomberg, a Salesforce enviou um e-mail aos clientes na terça-feira para dizer que não pagaria um resgate e alertou que a “inteligência de ameaças confiável” indica que os agentes de ameaças planejavam vazar os dados roubados.

“Posso confirmar que a Salesforce não se envolverá, negociará ou pagará qualquer demanda de extorsão”, confirmou a Salesforce também ao BleepingComputer.

Esta declaração segue o lançamento de um site de vazamento de dados por agentes de ameaças conhecidos como “Scattered Lapsus$ Hunters”, que estão tentando extorquir 39 empresas cujos dados foram roubados do Salesforce. O site foi localizado nos fóruns de violação[.]hn, que leva o nome do notório site BreachForums, um fórum de hackers conhecido por vender e vazar dados roubados.

As empresas que estão sendo extorquidas no site de vazamento de dados incluem marcas e organizações conhecidas, incluindo FedEx, Disney/Hulu, Home Depot, Marriott, Google, Cisco, Toyota, Gap, Kering, McDonald’s, Walgreens, Instacart, Cartier, Adidas, Sake Fifth Avenue, Air France & KLM, Transunion, HBO MAX, UPS, Chanel e IKEA.

No total, os agentes de ameaças alegaram ter roubado quase 1 bilhão de registros de dados, que seriam divulgados publicamente se uma demanda de extorsão fosse paga por empresas individuais ou como um pagamento único da Salesforce que cobriria todos os clientes afetados listados no site.

[IMAGEM REMOVIDA]realizar ataques de engenharia social se passando pela equipe de suporte de TI para induzir os funcionários a conectar um aplicativo OAuth malicioso à instância do Salesforce de sua empresa.

Uma vez vinculados, os agentes de ameaças usaram a conexão para baixar e roubar os bancos de dados, que foram usados para extorquir a empresa por e-mail.

Esses ataques de engenharia social impactaram Pesquise no Google, Cisco, Qantas, Adidas, Allianz Life, Seguro de Agricultores, Dia de trabalho, Kering e subsidiárias da LVMH, como Dior, Louis Vuittone Tiffany & Co.

Uma segunda campanha de roubo de dados do Salesforce começou no início de agosto de 2025,

quando os agentes de ameaças usaram tokens roubados SalesLoft Drift OAuth para migrar para os ambientes de CRM dos clientes e exfiltrar dados.

Os ataques de roubo de dados da Salesloft se concentraram principalmente no roubo de dados de tíquetes de suporte para verificar credenciais, tokens de API, tokens de autenticação e outras informações confidenciais que permitiriam aos invasores violar a infraestrutura e os serviços em nuvem da empresa.

Um dos agentes de ameaças por trás dos ataques da Salesloft, conhecido como ShinyHunters, disse ao BleepingComputer que eles roubaram aproximadamente 1,5 bilhão de registros de dados para mais de 760 empresas durante esta campanha.

Muitas empresas já confirmaram que foram afetadas pelo ataque à cadeia de suprimentos da Salesloft, incluindo Pesquise no Google, Cloudflare, Zscaler, Sustentável, CyberArk, Elástico, Além da confiança, Ponto de prova, JFrog, Nutanix, Qualys, Rubrik, Redes Cato, Redes de Palo Altoe muitos mais.

O site de vazamento de dados lançado recentemente foi usado principalmente para extorquir clientes nos ataques originais de engenharia social, com os agentes de ameaças afirmando que começariam a extorquir publicamente os afetados pelos ataques da Salesloft após 10 de outubro.

No entanto, o site de vazamento de dados agora está encerrado, com o domínio agora usando servidores de nomes de surina.ns.cloudflare.com e hans.ns.cloudflare.com, que têm ambos foi usado pelo FBI no passado ao apreender domínios.

O BleepingComputer entrou em contato com o FBI para saber se eles apreenderam o domínio, mas não recebeu uma resposta no momento.

[IMAGEM REMOVIDA]