FBI alerta sobre UNC6040, UNC6395 hackers roubam dados do Salesforce

Data: 2025-09-14 23:37:51

Autor: Inteligência Against Invaders

O FBI emitiu um alerta FLASH alertando que dois clusters de ameaças, rastreados como UNC6040

e UNC6395, estão comprometendo os ambientes Salesforce das organizações para roubar dados e

extorquir vítimas.

“O Federal Bureau of Investigation (FBI) está lançando este FLASH para disseminar Indicadores de Comprometimento (IOCs) associados a recentes atividades cibernéticas maliciosas por grupos criminosos cibernéticos UNC6040 e UNC6395, responsáveis por um número crescente de roubos de dados e invasões de extorsão”, diz o Aviso FLASH do FBI.

“Ambos os grupos foram observados recentemente visando as plataformas Salesforce das organizações por meio de diferentes mecanismos de acesso inicial. O FBI está divulgando essas informações para maximizar a conscientização e fornecer IOCs que podem ser usados pelos destinatários para pesquisa e defesa de rede.

UNC6040 foi divulgado pela primeira vez pela Google Threat Intelligence (Mandiant) em junho, que alertou que, desde o final de 2024, os agentes de ameaças estavam usando engenharia social e ataques de vishing para induzir os funcionários a conectar aplicativos maliciosos do Salesforce Data Loader OAuth às contas do Salesforce de suas empresas.

Em alguns casos, os agentes de ameaças se passaram por pessoal de suporte de TI corporativo, que usou versões renomeadas do aplicativo chamadas “My Ticket Portal”.

Uma vez conectados, os agentes de ameaças usaram o aplicativo OAuth para exfiltrar em massa dados corporativos do Salesforce, que foram usados em tentativas de extorsão pelo grupo de extorsão ShinyHunters.

Nesses primeiros ataques de roubo de dados, ShinyHunters disse ao BleepingComputer que eles visavam principalmente o “Contas” e “Contatos“, que são usadas para armazenar dados sobre os clientes de uma empresa.

Esses ataques de roubo de dados foram generalizados, impactando empresas grandes e conhecidas, como Pesquise no Google,Adidas,Qantas,Allianz Life,Cisco, Kering, Louis Vuitton,Dior eTiffany & Co.

Ataques posteriores de roubo de dados em agosto também visaram clientes do Salesforce, mas desta vez utilizaram tokens roubados do Salesloft Drift OAuth e de atualização para violar as instâncias do Salesforce dos clientes.

Essa atividade é rastreada como UNC6395 e acredita-se que tenha ocorrido entre 8 e 18 de agosto,

com os agentes de ameaças usando os tokens para direcionar as informações do caso de suporte da empresa que foram armazenadas no Salesforce.

Os dados exfiltrados foram então analisados para extrair segredos, credenciais e tokens de autenticação compartilhados em casos de suporte, incluindo chaves da AWS, senhas e tokens do Snowflake. Essas credenciais podem ser usadas para migrar para outros ambientes de nuvem para roubo de dados adicionais.

A Salesloft trabalhou com a Salesforce para revogar todos os tokens Drift e exigiu que os clientes se autenticassem novamente na plataforma.

Mais tarde, foi revelado que os agentes da ameaça também roubaram tokens do Drift Email, que foram usados para acessar e-mails de um pequeno número de contas do Google Workspace.

Uma investigação da Mandiant determinou que o ataque se originou em março, quando os repositórios GitHub da Salesloft foram comprometidos, permitindo que os invasores roubassem os tokens Drift OAuth.

Como os ataques anteriores, esses novos ataques de roubo de dados do Salesloft Drift afetaram várias empresas, incluindo Cloudflare,Zscaler,Sustentável,CyberArk,Elástico,Além da confiança, Ponto de prova,JFrog,Nutanix,Qualys,Rubrik,Redes Cato,Redes de Palo Altoe muitos mais.

Embora o FBI não tenha nomeado os grupos por trás dessas campanhas, o BleepingComputer foi informado pelo grupo de extorsão ShinyHunters que eles e outros agentes de ameaças que se autodenominam “Caçadores de Lapsus $ Dispersos, estavam por trás de ambos os grupos de atividade.

Esse grupo de hackers afirma ter se originado e se sobreposto aos grupos de extorsão Lapsus$, Scattered Spider e ShinyHunters.

Na quinta-feira, os agentes de ameaças anunciaram por meio de um domínio associado ao BreachForums que planejavam “escurecer” e parar de discutir operações no Telegram.

No entanto, em um post de despedida, os hackers alegaram ter obtido acesso à verificação de antecedentes do E-Check do FBIystem e o sistema de solicitação de aplicação da lei do Google, publicando capturas de tela como prova.

Se legítimo, esse acesso permitiria que eles se passassem por policiais e extraíssem registros confidenciais de indivíduos.

Quando contatado pelo BleepingComputer, o FBI se recusou a comentar e o Google não respondeu ao nosso e-mail.

[IMAGEM REMOVIDA]