ShinyHunters afirma que 1,5 bilhão de registros do Salesforce foram roubados

Data: 2025-09-17 21:40:15

Autor: Inteligência Against Invaders

O grupo de extorsão ShinyHunters afirma ter roubado mais de 1,5 bilhão de registros do Salesforce de 760 empresas usando tokens Salesloft Drift OAuth comprometidos.

No ano passado, os agentes de ameaças foram [visando clientes do Salesforce em ataques de roubo de dados](#) usando engenharia social e aplicativos OAuth maliciosos para violar instâncias do Salesforce e baixar dados. Os dados roubados são usados para extorquir as empresas a pagar um resgate para evitar que os dados vazem publicamente.

Esses ataques foram reivindicados por agentes de ameaças afirmando que fazem parte dos grupos de extorsão ShinyHunters, Scattered Spider e Lapsus\$, agora se autodenominando “Scattered Lapsus\$ Hunters”. O Google rastreia essa atividade como UNC6040 e UNC6395.

Em março, um dos agentes de ameaças [violou o repositório GitHub do Salesloft](#), que continha o código-fonte privado da empresa.

ShinyHunters disse ao BleepingComputer que os agentes de ameaças usaram o [Porco Trufado](#) ferramenta de segurança para escanear o código-fonte em busca de segredos, o que resultou na descoberta de tokens OAuth para as plataformas Salesloft Drift e Drift Email.

SalesloftDrift é uma plataforma de terceiros que conecta o agente de bate-papo Drift AI a uma instância do Salesforce, permitindo que as organizações sincronizem conversas, leads e casos de suporte em seu CRM. O Drift Email é usado para gerenciar respostas de e-mail e organizar bancos de dados de CRM e automação de marketing.

Usando esses tokens Drift OAuth roubados, ShinyHunters disse ao BleepingComputer que os agentes de ameaças roubaram aproximadamente 1,5 bilhão de registros de dados de 760 empresas do “[Conta](#)”, “[Contato](#)”, “[Caso](#)”, “[Oportunidade](#)”, e “[Utilizador](#)” Tabelas de objetos do Salesforce.

Desses registros, aproximadamente 250 milhões eram da Conta, 579 milhões do Contato, 171 milhões do Opportunity, 60 milhões do Usuário e cerca de 459 milhões de registros das tabelas Case Salesforce.

A tabela Case foi usada para armazenar informações e textos de tickets de suporte enviados por clientes dessas empresas, que, para empresas de tecnologia, podem incluir dados confidenciais.

Como prova de que eles estavam por trás do ataque, o agente da ameaça compartilhou um arquivo de texto listando as pastas de código-fonte no repositório GitHub do Salesloft violado.

O BleepingComputer entrou em contato com a Salesloft com perguntas sobre essas contagens de

registros e o número total de empresas afetadas, mas não recebeu uma resposta ao nosso e-mail. No entanto, uma fonte confirmou que os números são precisos.

O Google Threat Intelligence (Mandiant) informou que os dados roubados do caso foram analisados em busca de segredos ocultos, como credenciais, tokens de autenticação e chaves de acesso, para permitir que os invasores se voltassem para outros ambientes para novos ataques.

“Depois que os dados foram exfiltrados, o ator pesquisou os dados para procurar segredos que pudessem ser usados para comprometer os ambientes das vítimas”, [explicou o Google](#).

“O GTIG observou UNC6395 visando credenciais confidenciais, como chaves de acesso (AKIA) da Amazon Web Services (AWS), senhas e tokens de acesso relacionados ao Snowflake.”

Os tokens roubados Drift e Drift Email foram usados em campanhas de roubo de dados em larga escala que atingiram grandes empresas, incluindo [Pesquise no Google](#), [Cloudflare](#), [Zscaler](#), [Sustentável](#), [CyberArk](#), [Elástico](#), [Além da confiança](#), [Ponto de prova](#), [JFrog](#), [Nutanix](#), [Qualys](#), [Rubrik](#), [Redes Cato](#), [Redes de Palo Alto](#) e [muitos mais](#).

Devido ao grande volume desses ataques, o [O FBI divulgou recentemente um comunicado](#) alertando sobre o UNC6040 e Agentes de ameaças UNC6395, compartilhando IOCs descobertos durante os ataques.

Na quinta-feira passada, os agentes de ameaças que afirmam fazer parte do Scattered Spider afirmaram que planejavam “escurecer” e parar de discutir operações no Telegram.

Em uma postagem de despedida, os agentes de ameaças alegaram ter violado o sistema de solicitação de aplicação da lei (LERS) do Google, que é usado pela aplicação da lei para emitir solicitações de dados, e a plataforma eCheck do FBI, usada para realizar verificações de antecedentes.

Depois de entrar em contato com o Google sobre essas alegações, a empresa confirmou que [uma conta fraudulenta foi adicionada à sua plataforma LERS](#).

“Identificamos que uma conta fraudulenta foi criada em nosso sistema para solicitações de aplicação da lei e desativamos a conta”, disse o Google ao BleepingComputer.

“Nenhuma solicitação foi feita com esta conta fraudulenta e nenhum dado foi acessado.”

Embora os agentes de ameaças tenham indicado que estão se aposentando, pesquisadores de [ReliaQuest](#) relatam que os agentes de ameaças começaram a atacar instituições financeiras em julho de 2025 e provavelmente continuarão realizando ataques.

Para se proteger contra esses ataques de roubo de dados, [A Salesforce recomenda](#) que os clientes sigam as práticas recomendadas de segurança, incluindo a habilitação da autenticação multifator (MFA), a aplicação do princípio do menor privilégio e o gerenciamento cuidadoso dos aplicativos conectados.

[\[IMAGEM REMOVIDA\]](#)

-