Qualys, Tenable últimas vítimas do hack Salesloft Drift - Against Invaders

Data: 2025-09-09 19:06:58

Autor: Inteligência Against Invaders

Os provedores de segurança cibernética Tenable e Qualys são os mais recentes de uma lista

crescente de empresas afetadas por um ataque significativo à cadeia de suprimentos direcionado

aos dados dos clientes da Salesforce.

A campanha envolveu o roubo de tokens de autenticação OAuth conectados ao Salesloft Drift, um aplicativo de terceiros integrado ao Salesforce usado para automatizar fluxos de trabalho e gerenciar leads e informações de contato.

Em Um alerta de segurança em 3 de setembro, a empresa de avaliação de vulnerabilidades Tenable disse que um usuário não autorizado obteve acesso a uma parte das informações de seus clientes armazenadas na instância do Salesforce da empresa.

Esses dados incluíam linhas de assunto e descrições iniciais fornecidas pelos clientes ao abrir um caso de suporte da Tenable, bem como informações de contato comercial comumente disponíveis, como nomes, endereços de e-mail comercial, números de telefone e referências de localização.

“Neste momento, não temos evidências de que qualquer uma dessas informações tenha sido mal utilizada”, observou o provedor de segurança. Os produtos e dados da Tenable dentro do conjunto de produtos da Tenable não foram afetados.

Três dias depois, a empresa de gerenciamento de risco Qualys emitiu Um alerta semelhante, afirmando que as credenciais roubadas durante a campanha de roubo de tokens OAuth permitiram aos invasores “acesso limitado a algumas informações do Qualys Salesforce”.

Assim como a Tenable, a Qualys confirmou que seus produtos e serviços não foram afetados e ainda estavam totalmente operacionais.

Ambas as empresas disseram que desativaram o aplicativo Salesloft Drift e revogaram as integrações associadas com seus sistemas e/ou credenciais de integração alternadas.

A Tenable também fortaleceu seu ambiente Salesforce e outros sistemas conectados para reduzir a probabilidade de exploração futura.

A Qualys disse que trabalhou para conter qualquer possível acesso não autorizado. O provedor de gerenciamento de risco também está colaborando com a Salesforce e com a Mandiant do Google Cloud para investigar o incidente.

Hack ‘SalesDrift’: uma lista crescente de vítimas

O ataque à cadeia de suprimentos Salesloft Drift (também conhecido como hack ‘SalesDrift’) foi identificado pela primeira vez pelo Grupo de Inteligência de Ameaças do Google (GTIG), que compartilhou suas descobertas em 26 de agosto.

O próprio Google estava entre os alvos, já que um invasor explorou tokens de autenticação roubados para se infiltrar em contas de e-mail em um número limitado de usuários do Google Workspace em 9 de agosto.

Desde então, uma enxurrada de empresas confirmou que foram afetadas, incluindo Além da confiança, Bugcrowd, Redes Cato, Cloudflare, CyberArk, Elástico, JFrog, Nutanix, PagerDuty, Redes de Palo Alto, Rubrik, SpyCloud, Tanium e Zscaler.

A Okta revelou em 2 de setembro que havia bloqueado com sucesso uma tentativa de ataque ligada à campanha Salesloft Drift.

A empresa de segurança de identidade afirmou que controles de segurança aprimorados implementados após violações anteriores em 2022 e 2023 ajudaram a prevenir o ataque.

Essas medidas incluíram restringir o acesso IP de entrada ao Salesforce, o que, segundo a Okta, interrompeu a tentativa de acesso não autorizado antes que pudesse ser bem-sucedida.

A Nudge Security criou um painel que rastreia todas as empresas afetadas pelo hack ‘SalesDrift’ e inclui as datas dos comprometimentos e links para os avisos de segurança.

Compromisso inicial de deriva da Salesloft em março

Segundo para uma atualização de 7 de setembro pela Salesloft, os hackers violaram a plataforma de automação de vendas pela primeira vez em março.

Os invasores permaneceram inativos enquanto mapeavam os sistemas internos da empresa antes de roubar tokens OAuth dos clientes da Salesloft em junho.

Eles então começaram a aproveitar esses tokens para atingir redes de clientes a partir do final de agosto.

Em uma atualização posterior, também publicada em 7 de setembro, a Salesloft indicou que a integração entre a plataforma Salesloft e o Salesforce agora está restaurada.