Your IT Company

Relatório Técnico - Ataques Exploram Salesloft Drift para Roubar Dados de Instâncias Salesforce

Sumário

1. Resumo Geral da Ameaça

Em agosto de 2025, o Google Threat Intelligence Group (GTIG) e a Mandiant identificaram uma campanha de roubo massivo de dados corporativos conduzida pelo grupo rastreado como UNC6395. O ataque teve como principal vetor o abuso de tokens OAuth comprometidos associados à integração do aplicativo de terceiros Salesloft Drift com Salesforce e outras plataformas conectadas.

A campanha teve início em 8 de agosto de 2025 e se estendeu até pelo menos 18 de agosto de 2025, quando foi detectada. O ator explorou os tokens para exportar grandes volumes de dados de instâncias corporativas de Salesforce, incluindo credenciais sensíveis (chaves de acesso AWS, senhas, tokens do Snowflake) e informações corporativas críticas (contas, usuários, oportunidades e casos).

Embora inicialmente acreditasse-se que a campanha fosse restrita às integrações entre Salesforce e Salesloft Drift, em 28 de agosto de 2025 o GTIG confirmou que o escopo era maior, afetando também outras integrações da plataforma Drift, incluindo o Drift Email, que foi usado para acessar um número limitado de contas do Google Workspace.

Este ataque não resulta de uma vulnerabilidade no núcleo do Salesforce, mas sim do abuso de integrações OAuth mal protegidas, evidenciando a fragilidade do ecossistema de terceiros e a importância da governança de APIs e credenciais.

2. Modus Operandi.

Fluxo do ataque:

- **Comprometimento de tokens OAuth:**
  - O ator obteve tokens associados ao Salesloft Drift.
  - Estes tokens concediam acesso privilegiado a dados armazenados no Salesforce.
- **Extração sistemática de dados:**
  - O grupo executou consultas SOQL (Salesforce Object Query Language) para extrair informações de objetos críticos (Conta, Oportunidade, Usuário, Caso).
- **Exemplo de query observada:**

```
SELECT Id, Username, Email, FirstName, Lastname, Title, CompanyName,
Department, Phone, IsActive, LastLoginDate
From User
Where IsActive – true
Order By LastLoginDate DESC
LIMIT 20;
```

3. MITRE ATT&CK

Fase Técnica (MITRE)	ID	Descrição Técnica	Aplicação no Ataque
Acesso Inicial: Valid Accounts (OAuth Abuse)	T1078.004	Uso de tokens OAuth comprometidos	Comprometimento de tokens Drift/Salesforce
Coleta: Automated Collection	T1119	Execução de consultas automatizadas para coleta	Consultas SOQL para exportar informações
Coleta: Data from Information Repositories	T1213.003	Extração de dados de repositórios SaaS	Extração de objetos Salesforce
Credenciais: Unsecured Credentials	T1552	Busca por credenciais e segredos expostos	Identificação de AKIA, tokens Snowflake, senhas
Evasão: Indicator Removal on Host	T1070	Exclusão de registros de atividades	Exclusão de query jobs após execução
Exfiltração: Exfiltration Over Web Services	T1567.002	Exportação de dados por APIs legítimas	Exfiltração via API Salesforce

4. Diamond Model

O Diamond Model é fundamental para estruturar o entendimento de campanhas de ameaça, permitindo identificar quem é o adversário, qual sua capacidade técnica, qual infraestrutura utiliza e quem são as vítimas. Esse modelo conecta indicadores técnicos a contextos estratégicos, facilitando respostas coordenadas e atribuição de responsabilidade.

- **Adversário:** UNC6395, focado em exfiltração de dados e credenciais.
- **Capacidade:** Exploração de integrações OAuth, consultas SOQL, evasão por logs.
- **Infraestrutura:** Tokens Drift, API Salesforce, IPs cloud e Tor.
- **Vítima:** Organizações usando Salesforce integrado ao Drift (milhares de clientes).

5. IoCs e Artefatos

- **User-Agents maliciosos**
  - Salesforce-Multi-Org-Fetcher/1.0
  - Salesforce-CLI/1.0
  - python-requests/2.32.4
  - Python/3.11 aiohttp/3.12.15

- **Endereços IP associados:**

  Infraestrutura cloud
  - 208.68.36.90 (DigitalOcean)
  - 44.215.108.109 (AWS)

  Tor exit nodes observados
  - 154.41.95.2, 176.65.149.100, 179.43.159.198
  - 185.130.47.58, 185.207.107.130, 185.220.101.133
  - 185.220.101.143, 185.220.101.164, 185.220.101.167
  - 185.220.101.169, 185.220.101.180, 185.220.101.185
  - 185.220.101.33, 192.42.116.179, 192.42.116.20
  - 194.15.36.117, 195.47.238.178, 195.47.238.83

6. Impacto e Potenciais Consequências

- Exposição de dados sensíveis: informações corporativas estratégicas (clientes, oportunidades, tickets).
- Roubo de credenciais: chaves AWS, tokens Snowflake e senhas reaproveitadas.
- Acesso a e-mails em contas do Google Workspace integradas via Drift.
- Risco de movimentação lateral: credenciais roubadas podem ser utilizadas para expandir o comprometimento.
- Danos reputacionais e regulatórios: empresas afetadas podem ser responsabilizadas por vazamento de dados de clientes.

7. Recomendações de Mitigação e Detecção

- **Investigar e detectar comprometimento:**
  - Revisar integrações no Drift Admin Settings.
  - Buscar nos logs do Salesforce
  - Event Monitoring e UniqueQuery events.
  - Atividade suspeita do usuário Drift Connected App.
  - Buscar IOCs (IPs e User-Agents maliciosos).
  - Executar ferramentas como Trufflehog para identificar segredos expostos.

- **Revogar e rotacionar credenciais**
  - Revogar e alterar tokens OAuth, chaves de API e senhas associados às integrações Drift.
  - Resetar senhas de contas associadas.
  - Configurar timeouts de sessão no Salesforce.
- **Controles de acesso:**
  - Minimizar escopos OAuth (evitar permissões como *fullaccess*).
  - Aplicar restrições de IP no Connected App.
  - Definir ranges de IP confiáveis nos perfis de usuários.
  - Remover o privilégio API Enabled de perfis não essenciais.

8. Considerações Finais

Este caso demonstra como tokens OAuth comprometidos representam um risco crítico em ecossistemas SaaS. Mesmo sem explorar falhas no núcleo do Salesforce, o atacante conseguiu acesso privilegiado a dados corporativos estratégicos, reforçando a necessidade de:

- Governança rigorosa de integrações com outros fabricantes.
- Monitoramento ativo de logs de API.
- Rotação contínua de credenciais.

A investigação conjunta entre a Google, Salesforce, Salesloft e Mandiant resultou em mitigação rápida, mas o risco persiste para organizações que não revisarem suas integrações.

9. Referências Técnicas

1. Google Cloud Blog — Data Theft Salesforce Instances via Salesloft Drift: https://cloud.google.com/blog/topics/threat-intelligence/data-theft-salesforce-instances-via-salesloft-drift

Esta publicação tem como objetivo orientar a equipe interna e os nossos clientes sobre ameaças emergentes no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

Produzido por: Equipe de Threat Intelligence