Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

CIBERATAQUE A LA CADENA DE SUMINISTRO: GRUPO UNC6395 FILTRA INFORMACIÓN A TRAVÉS DE SALESLOFT DRIFT

02/ 09 / 2025

CONTENIDO

INTRODUCCIÓN

El grupo UNC6395 llevó a cabo una sofisticada campaña de ataque dirigida a explotar integraciones de terceros. En este caso, el blanco fue Salesloft Drift, un asistente de IA que interactúa con Salesforce. Los atacantes lograron robar tokens OAuth válidos, lo que les permitió conectarse a instancias de Salesforce de múltiples compañías sin necesidad de contraseñas ni autenticación multifactor (MFA).

CIBERATAQUE A LA CADENA DE SUMINISTRO: GRUPO UNC6395 FILTRA INFORMACIÓN A TRAVÉS DE SALESLOFT DRIFT

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_09_02_2
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	02/09/2025
Es día cero (0 day):	No

RESUMEN

El grupo UNC6395 llevó a cabo una sofisticada campaña de ataque dirigida a explotar integraciones de terceros. En este caso, el blanco fue Salesloft Drift, un asistente de IA que interactúa con Salesforce. Los atacantes lograron robar tokens OAuth válidos, lo que les permitió conectarse a instancias de Salesforce de múltiples compañías sin necesidad de contraseñas ni autenticación multifactor (MFA).

Una vez dentro, extrajeron grandes volúmenes de datos empresariales, ejecutando consultas sobre objetos como Accounts, Contacts, Opportunities y Cases. Para ocultar sus huellas, eliminaron los registros de las consultas realizadas, lo que demuestra un conocimiento avanzado en técnicas de anti-forense.

Impacto en Palo Alto Networks

Palo Alto Networks fue una de las empresas afectadas. Es importante aclarar que no hubo intrusión directa en su infraestructura ni en sus productos de ciberseguridad. Lo comprometido fue únicamente su instancia de Salesforce, a través de la integración con Drift.

Los datos expuestos fueron principalmente información de contacto comercial y registros de ventas, sin incluir archivos adjuntos, código fuente ni datos técnicos críticos.

Como respuesta inmediata, la empresa revocó los tokens OAuth comprometidos, deshabilitó la integración con Drift y desplegó a su equipo de investigación Unit 42 para un análisis exhaustivo.

Este caso demuestra que el ataque no fue contra Palo Alto Networks como objetivo principal, sino que la compañía se vio afectada por la cadena de suministro digital al depender de un servicio externo que fue comprometido.

El alcance más amplio del ataque

- Además de Palo Alto Networks, el ataque impactó a Zscaler, PagerDuty, Tanium, SpyCloud y más de 700 organizaciones que usaban integraciones similares.
- Google Threat Intelligence confirmó que el grupo UNC6395 fue el responsable y que esta campaña forma parte de una tendencia creciente de ataques a la cadena de suministro SaaS.
- El hecho de que los atacantes borraran la evidencia en Salesforce dificulta que las organizaciones tengan plena certeza de qué datos fueron exfiltrados.

Este caso no representa una falla interna de Palo Alto Networks, sino un claro ejemplo de cómo los atacantes buscan el eslabón más débil en la cadena de confianza digital. Aunque los sistemas de Palo Alto permanecieron seguros, la filtración de información de ventas y contactos comerciales podría ser utilizada en el futuro para campañas de phishing dirigido o ataques de ingeniería social contra sus clientes y socios.

RECOMENDACIONES

- Revoca inmediatamente los tokens de aplicaciones de terceros que no sean críticas.
- Limita los permisos de cada aplicación con el principio de mínimo privilegio.
- Implementa procesos de auditoría periódica de todas las aplicaciones que tienen acceso a Salesforce, Microsoft 365, Google Workspace u otros SaaS.
- Revisa los logs de acceso en busca de conexiones desde ubicaciones o dispositivos anómalos.

INDICADORES DE COMPROMISO

https://github.com/develgroup/SOC_IOCs/tree/15ee1befe825bb8af63387d2a3e10508bbf87f02/20250901_01_UNC6395

NOTICIA COMPLETA

https://devel.group/blog/ciberataque-a-la-cadena-de-suministro-grupo-unc6395-filtra-informacion-a-traves-de-salesloft-drift/

CONTACTOS DE SOPORTE

Correo electrónico: cti@develsecurity.com

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group