Nro. Alerta:	AL-2025-051	CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS DEL ECUADOR **ALERTAS DE SEGURIDAD**	ecucert V 1.1
TLP:	TLP:CLEAR		
Fecha:	8-sep-2025	Ataque a la cadena de Suministro Drift	Pág.: **1** of **6**

I. DATOS GENERALES:

Clase de alerta: Ingeniería Social / Abuso de confianza
Tipo de Incidente: Suplantación de soporte técnico – Acceso no autorizado vía "Salesforce Data Loader"
Nivel de riesgo: Alta

II. ALERTA

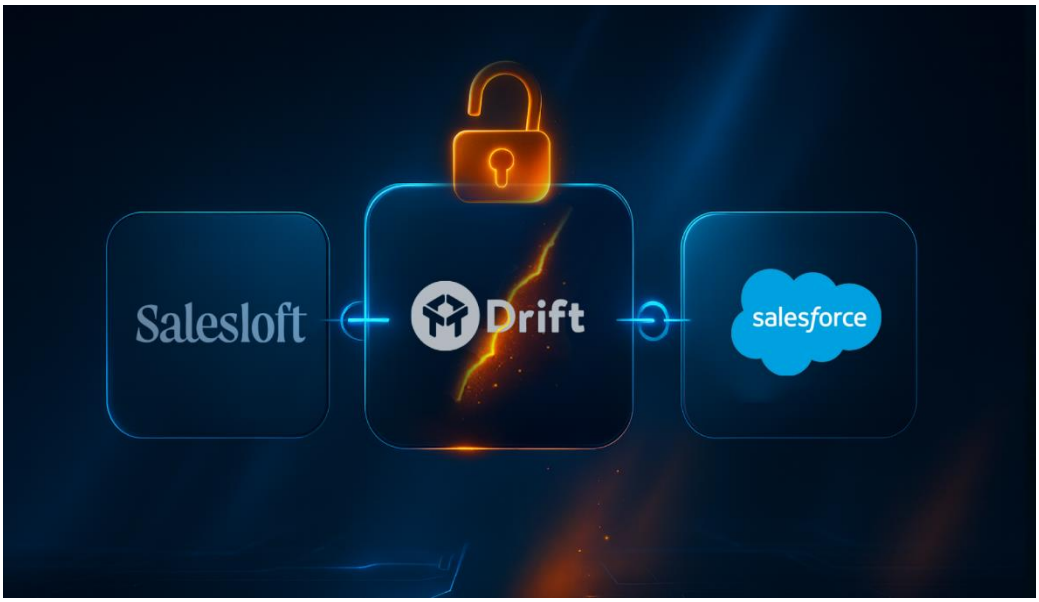

Figura 1.- Ataque a la cadena de Suministro Drift - Figura referencial

El servicio de chatbot Drift basado en IA de Salesloft se convirtió en el principal objetivo de ataque cibernético como cadena de Suministro de grandes empresas como Salesforce, Cloudflare, Zscaler, Palo Alto Networks, Google Worskspace, Stack y PagerDutyde. Mediante el uso de Ingeniería Social Phishing, Vishing actores de amenazas ganaron acceso a los sistemas de las víctimas para robar credenciales y exfiltrar de datos de estas empresas de alto nivel.

III. INTRODUCCIÓN

Drift IA está siendo el objetivo de actores de amenaza bajo el concepto de ataque a la cadena de suministro, esto significa que mediante Drift IA aprovechan su integración con SaaS de Salesforce, Slack y Google Workspace, para realizar el robo de tokens OAuth y para tener acceso a entornos de clientes con el fin de hacer una exfiltración masiva de datos sensibles como registros de cuentas, contactos de clientes, contenido

de casos de soporte, registros de peticiones, oportunidades y secretos potencialmente incrustados como claves de API o credenciales en la nube.

Si bien se pensaba que esta violación se limitaba a Salesforce, Salesloft realizo una revocación de todos los tokens activos de Drift IA y eliminaron la aplicación del mercado Salesforce. Sin embargo, Google Threat Intelligence Group (GTIG) revelo que tokens OAuth para otras integraciones de Drift también fueron robadas para Google Workspace (Email), Stack y Cloud Storage.

Investigadores estiman que esta brecha ha comprometido a más de 700 organizaciones a nivel global, afectando a sectores claves como, computación en la nube, ciberseguridad, SaaS, tecnología empresarial y proveedores de seguridad como Cloudflare, Zscaler, Palo Alto Networks y PagerDuty, lo que la convierte en una de las mayores violaciones de seguridad en la Cadena de Suministro de servicios SaaS en los últimos años.

IV. VECTOR DE ATAQUE

Campaña de Ingeniería Social

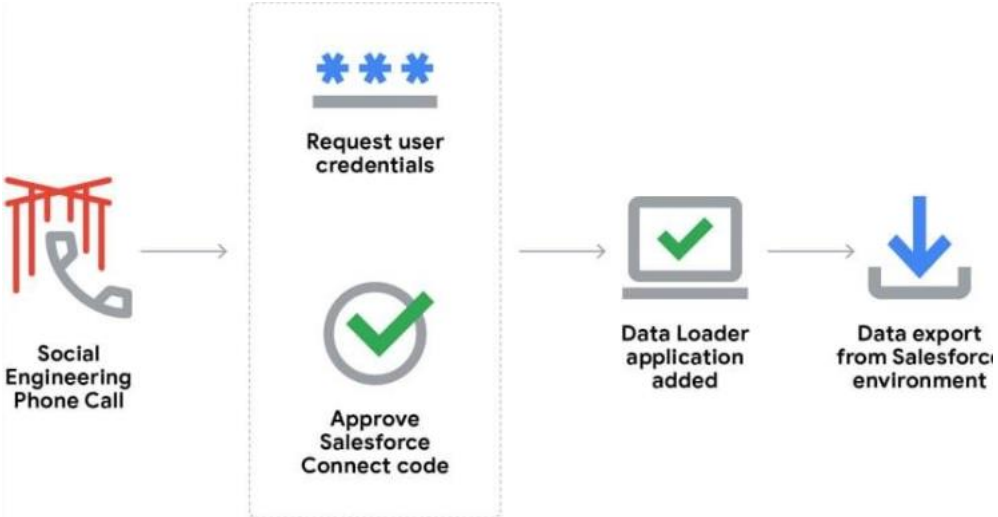

Figura 2.- Ataque a la Cadena de Suministro Drift - Figura referencial

El grupo GTIG de Google detecto varios actores de amenazas, uno de ellos se hace pasar por un grupo de extorsión llamado ShinyHunters, quienes usando Ingeniería Social (Phising, Vishing) realizaron ataques contra empresas conectadas a las plataformas Salesforce para robar datos.

En el rastreo de clúster de amenaza denominado UNC6040 los ataques se dirigen a empleados mediante Vishing, al actor de amenaza se hace pasar como personal de soporte técnico vía telefónica y solicitan al cliente objetivo que abra la página de configuración de Salesforce Connect e introduzca un "código de conexión", vinculando a Salesforce Data Loader (una aplicación cliente que permite a los usuarios importar, exportar, actualizar o eliminar datos dentro de los entornos de Salesforce) que es controlada por el actor de amenaza con el entorno de la víctima.

Con esto los atacantes pudieron:

- Exfiltrar datos de clientes afectados en el entorno de Salesforce.
- Para que el bot de IA Drift exportara grandes cantidades de datos de instancias corporativos de SalesForce para la recolección de credenciales

Uso de credenciales robadas

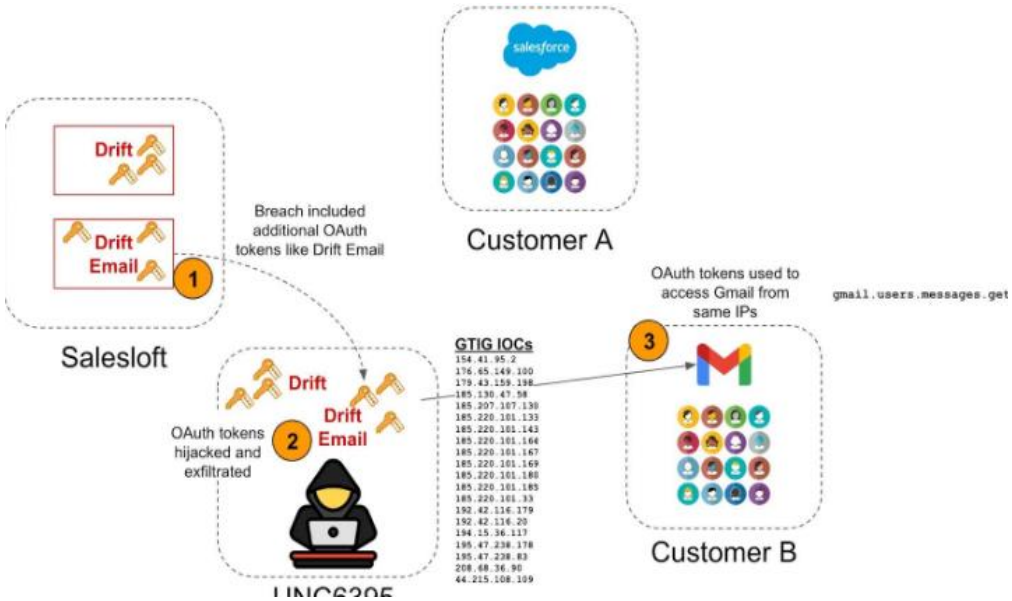

Figura 3.- Uso de credenciales robadas - Ataque a la cadena de Suministro Drift

GTIG y Mandiant detectaron a otro actor de amenaza llamado UNC6395 obteniendo acceso no autorizado a los tokens emitidos por Drift, estos tokens de OAuth permitieron a Drift conectarse con los sistemas de clientes en su nombre, especialmente a Salesforce.

Estos tokens les permitieron acceder a instancias de Salesforce sin explotar ninguna vulnerabilidad en la plataforma de Salesforce en sí. El ataque se basó en:

- Abuso de Token de OAuth, actores de amenaza obtuvieron credenciales válidas de OAuth, probablemente mediante Phishing o Ingeniería Social, para autenticarse como usuarios legítimos de la integración de Drift.
- Automatización en Python, utilizando una herramienta en Python con bibliotecas asíncronas (como aiohttp) y la API Bulk de Salesforce extrayeron rápidamente grandes volúmenes de datos, como cuentas, contactos, casos y oportunidades.
- Técnicas Antiforenses, fue usada para eliminar los trabajos de consulta (query jobs) para cubrir sus huellas, aunque los registros (logs) permanecieron intactos para su detección.

V. IMPACTO

En relación con el reciente incidente de seguridad en el que se vieron involucrados diversos SaaS de organizaciones de alto perfil, algunos confirmaron públicamente haber sufrido exposición de datos sensibles. La información comprometida incluye desde detalles de contacto de clientes hasta tokens de autenticación y registros de soporte, lo que evidencia el alcance y la gravedad del ataque.

Organización	Exposición Reportada
Zscaler	Se robó una parte importante de los registros de clientes: nombres, correos electrónicos, cargos, teléfonos, región e información de soporte.
Cloudflare	Acceso a registros de soporte y extracción de contactos y tokens de API. Rotación de 104 tokens internos.
Palo Alto Networks	Exposición de datos de Salesforce CRM: cuentas de ventas, contactos y contenidos confidenciales de soporte.
PagerDuty	Acceso a nombres, correos electrónicos y números de teléfono en Salesforce.
SpyCloud	Datos de su instancia de Salesforce expuestos pese a no ser cliente activo de Drift.
Google	Acceso a un número reducido de cuentas de Gmail vinculadas a Drift Email. Google revocó tokens y deshabilitó integración.
Tanium	Acceso limitado a Salesforce: nombres, correos electrónicos, teléfonos y ubicación. Sin acceso a la plataforma principal.

Tabla 1.- Organizaciones afectadas - Ataque a la Cadena de Suministro Drift

VI. INDICADORES DE COMPROMISO

Estos indicadores permiten a las organizaciones analizar sus registros y sistemas en busca de señales de compromiso asociadas a la vulnerabilidad vinculada con Drift.

Cadenas de agente de usuario maliciosas
Buscador de organizaciones múltiples de Salesforce/1.0
Salesforce-CLI/1.0
solicitudes de Python/2.32.4
Python/3.11 aiohttp/3.12.15

Tabla 2.- Organizaciones afectadas - Ataque a la Cadena de Suministro Drift

Direcciones IPs sospechosas
208[.]68[.]36[.]90 (Océano Digital)
44[.]215[.]108[.]109 (Servicios web de Amazon)
154[.]41[.]95[.]2 (nodo de salida TOR)
176[.]65[.]149[.]100 (nodo de salida TOR)
179[.]43[.]159[.]198 (nodo de salida TOR)
185[.]130[.]47[.]58 (nodo de salida TOR)
185[.]207[.]107[.]130 (nodo de salida TOR)
185[.]220[.]101[.]133 (nodo de salida TOR)
185[.]220[.]101[.]143 (nodo de salida TOR)
185[.]220[.]101[.]164 (nodo de salida TOR)
185[.]220[.]101[.]167 (nodo de salida TOR)
185[.]220[.]101[.]169 (nodo de salida TOR)
185[.]220[.]101[.]180 (nodo de salida TOR)
185[.]220[.]101[.]185 (nodo de salida TOR)
185[.]220[.]101[.]33 (nodo de salida TOR)
192[.]42[.]116[.]179 (nodo de salida TOR)
192[.]42[.]116[.]20 (nodo de salida TOR)
194[.]15[.]36[.]117 (nodo de salida TOR)
195[.]47[.]238[.]178 (nodo de salida TOR)
195[.]47[.]238[.]83 (nodo de salida TOR)

Tabla 3.- Direcciones IPs sospechosas - Ataque a la Cadena de Suministro Drift

VII. RECOMENDACIONES:

- Revocar y regenerar todos los tokens de acceso OAuth asociados a integraciones de terceros en Salesforce.
- Auditar las integraciones actuales con aplicaciones de terceros y eliminar aquellas que no sean esenciales.
- Implementar autenticación multifactor (MFA) para todas las cuentas con acceso a Salesforce.
- Monitorear actividades inusuales en las instancias de Salesforce, especialmente accesos desde ubicaciones geográficas atípicas.
- Actualizar y aplicar parches de seguridad a todas las aplicaciones y servicios integrados con Salesforce.
- Establecer políticas de acceso con privilegios mínimos para integraciones de terceros.

VIII. DESCARGO DE RESPONSABILIDAD

- La información en la presente alerta se proporciona con fines informativos.

- Cualquier referencia a productos, procesos o servicios comerciales específicos, no constituye respaldo o recomendación por parte del EcuCERT a los mismos.
- La presente alerta no debe utilizarse con fines publicitarios o de patrocinio de productos.

IX. REFERENCIAS:

UNIT42 (2025). Threat Brief: Compromised Salesforce Instances. https://unit42.paloaltonetworks.com/threat-brief-compromised-salesforce-instances/

PALO ALTO NETWORKS (2025). Salesforce Third-Party Application Incident Response. https://www.paloaltonetworks.com/blog/2025/09/salesforce-third-party-application-incident-response/

SOCRADAR (2025). Salesloft-Drift Breach: Everything You Need to Know. https://socradar.io/salesloft-drift-breach-everything-you-need-to-know/

SEGU-INFO (2025). Sigue la sangría de ataques a Sales Force. https://blog.segu-info.com.ar/2025/09/sigue-la-sangria-de-ataques-sales-force.html

REDHOTCYBER (2025). Palo Alto Networks also compromised via Salesforce and Drift. https://www.redhotcyber.com/en/post/palo-alto-networks-also-compromised-via-salesforce-and-drift

TECHRADAR (2025). Even Cloudflare isn't safe from Salesloft & Drift data breaches. https://www.techradar.com/pro/security/even-cloudflare-isnt-safe-from-salesloft-drift-data-breaches

SALESFORCEBEN (2025). Salesforce Customers Targeted in New Data Hacks Through Salesloft & Drift. https://www.salesforceben.com/salesforce-customers-targeted-in-new-data-hacks-through-salesloft-drift/