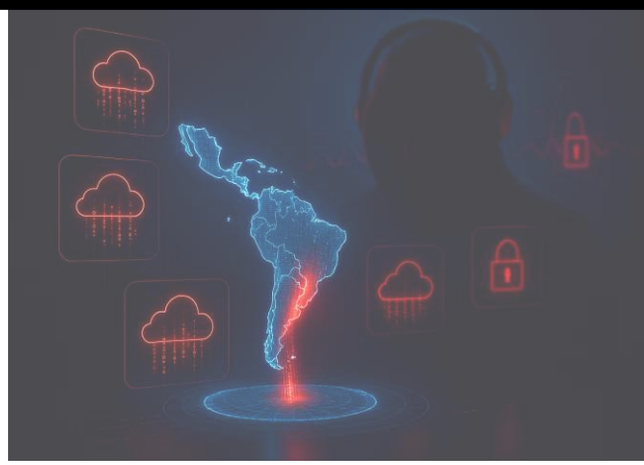
Advertencia

Técnica

ShinyHunters Operaciones en (Colombia y LATAM)

COLCERT AD-20260403 - 033

TLP:CLEAR



Resumen Ejecutivo

El grupo de amenazas ShinyHunters ha intensificado sus operaciones contra Latinoamérica durante el primer trimestre de 2026. Aprovechando accesos persistentes obtenidos en infraestructuras regionales a finales de 2025, el grupo ejecuta actualmente campañas de vishing asistidas por inteligencia artificial dirigidas contra plataformas de gestión pública en Colombia, con el objetivo de comprometer credenciales de inicio de sesión único (SSO). La finalidad de la operación es la exfiltración masiva de información confidencial alojada en entornos SaaS — incluyendo Salesforce, Google Workspace y Snowflake — para monetizarla mediante esquemas de extorsión financiera directa a las entidades afectadas.

NIVEL DE RIESGO

ALTO

Contexto de la amenaza

A partir de marzo de 2026, el grupo de amenazas ShinyHunters ha consolidado una nueva fase de operaciones denominada "Chaos Trinity". Esta fase se caracteriza por la convergencia de tres vectores de ataque: el uso de inteligencia artificial para vishing, la explotación de configuraciones en entornos SaaS en la nube y el despliegue de su propio ransomware, SHINYSPIDER.

Tras el compromiso masivo de Aeroméxico y otras entidades de la región a finales de 2025, se ha detectado infraestructura de escaneo activa dirigida específicamente a redes corporativas colombianas que utilizan Salesforce Experience Cloud y Snowflake. El grupo no solo busca el cifrado de archivos; su objetivo principal es la exfiltración de bases de datos de clientes para extorsión pública a través de su sitio de filtraciones, "Scattered LAPSUS$ Hunters".

Perfil técnico y comportamiento (TTPs)

ShinyHunters opera bajo un modelo de intrusión híbrida:

- **Ingeniería social de nueva generación (Vishing con IA):** El grupo utiliza modelos de lenguaje (LLM) y clonación de voz para contactar a empleados de mesas de ayuda (Helpdesk) en español. Simulan ser personal técnico de nivel superior para solicitar la aprobación de nuevos dispositivos MFA o la desactivación temporal de condicionales de acceso.
- **Abuso de aplicaciones conectadas (OAuth):** Explotan aplicaciones legítimas de terceros (como Gainsight o Data Loader) vinculadas a Salesforce para obtener tokens de acceso persistentes sin necesidad de contraseñas de usuario final.
- **Escaneo automatizado (AuraInspector):** Utilizan versiones modificadas de herramientas de seguridad para identificar sitios de Salesforce con perfiles de usuarios invitados que permiten consultas SQL excesivas.
- **Extorsión por múltiples canales:** Una vez exfiltrados los datos, contactan a los ejecutivos de la organización utilizando canales cifrados fuera de banda, como correos electrónicos seguros y el protocolo P2P Tox, tipicamente imponen una ventana critica de 72 horas para el pago del rescate, bajo la coacción de hacer públicos los activos de información comprometidos.

Técnicas, tácticas y procedimientos (TTPs)

ShinyHunters utiliza un árbol de ataques sofisticado centrado en la identidad y la nube:

Táctica (MITRE)	Técnica ID	Descripción del comportamiento
Acceso Inicial	T1566.004	Vishing: Llamadas de ingeniería social (IA-voz) a helpdesks para obtener tokens MFA.
Acceso Inicial	T1199	Compromiso de aplicaciones de terceros (OAuth) vinculadas a Salesforce .
Evasión de Defensa	T1027	Uso de empaquetadores y código reflectivo para ocultar malware como SHINYSPIDER .
Recopilación	T1560	Compresión de bases de datos robadas antes de la exfiltración.
Exfiltración	T1567.002	Exfiltración a la Nube: Uso de servicios como LimeWire o MEGA para hostear muestras de datos robados .
Impacto	T1486	Uso reciente de ransomware basado en Go (SHINYSPIDER) para inhabilitar sistemas locales .

Indicadores de Compromiso (IoCs)

DIRECCIONES IP

- **91.202.4.68**
- **95.129.232.236**

CUENTAS DE CONTACTO DEL ACTOR

- shinygroup@tuta[.]com
- shinycorp@tuta[.]com

HASHES DE ARCHIVO — SHINYSPIDER (SHA256)

- 670a269d935f1586d4f0e5bed685d15a38e6fa790f763e6ed5c9fdd72dce3cf2
- 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b
- aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121

ID DE NEGOCIACIÓN

- BD1B683FD3E6CB094341317A4C09923B7AE3E7903A6CDB90E5631EC7DC1452636FF35D9F5AF2

Medidas de protección y mitigación

Para prevenir el compromiso:

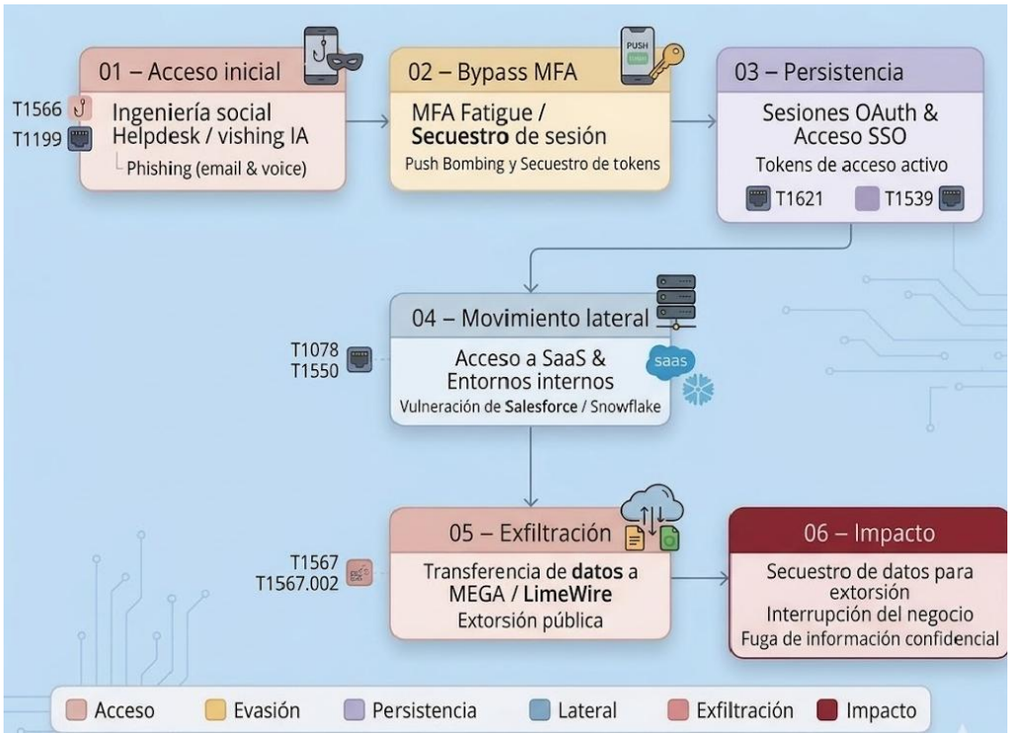
1. **Reforzar la autenticación multifactor (MFA):** Implementar MFA resistente a phishing (como llaves FIDO2) y prohibir la aprobación de notificaciones push de origen desconocido .
2. **Entrenamiento contra Vishing:** Capacitar al personal de soporte técnico (helpdesk) para verificar rigurosamente la identidad de los empleados antes de realizar un reset MFA o conceder accesos remotos .
3. **Auditoría de SaaS (Salesforce/Snowflake):** Revisar periódicamente las "Connected Apps" y revocar tokens OAuth inactivos o sospechosos. Desactivar el acceso público a APIs en perfiles de usuarios invitados .
4. **Segmentación de red:** Aislar infraestructuras críticas para evitar el movimiento lateral hacia entornos de nube si una estación de trabajo es comprometida .
5. **Hunting proactivo con los IoCs:** no basta con esperar; hay que buscar activamente las IPs y hashes en SIEM/EDR. Falta mencionar esto explícitamente como medida preventiva de detección temprana.
6. **Conditional Access / Zero Trust en SSO:** bloquear login desde IPs fuera de Colombia o desde ASNs asociados a VPN comerciales. ShinyHunters usa infraestructura de cloud pública para vishing; el geo-fencing es un freno real.
7. **Alertas sobre creación de nuevas Connected Apps en Salesforce:** no solo auditar las existentes, sino alertar en tiempo real cuando se autoriza una nueva OAuth app, especialmente en producción.
8. **Política de verificación por canal alterno (out-of-band:** antes de hacer reset MFA, el helpdesk debe confirmar por un segundo canal (Teams, correo corporativo) que no sea voz. Esto complementa el entrenamiento pero es una medida de proceso, no solo capacitación.

En caso de compromiso (Mitigación inmediata)

- ❑ **Revocación de sesiones:** Cerrar todas las sesiones activas en SSO y plataformas SaaS y forzar un cambio de credenciales global.
- ❑ **Aislamiento de aplicaciones:** Desvincular temporalmente aplicaciones de terceros (como Gainsight o Salesforce Data Loader) mientras se auditan los registros de acceso .
- ❑ **Monitoreo de logs de auditoría:** Buscar llamadas inusuales a métodos getConfigData o picos en el uso de la API /aura en Salesforce .
- ❑ **Preservación de evidencia forense antes de revocar sesiones:** exportar logs de auditoría de Salesforce (Event Monitoring) y Snowflake (QUERY_HISTORY) *antes* de cerrar sesiones, porque la revocación puede eliminar trazas activas.
- ❑ **Notificación a proveedores SaaS:** contactar a Salesforce Trust y Snowflake Security para correlacionar actividad sospechosa desde su lado; ellos tienen visibilidad de infraestructura que las entidades no tienen.
- ❑ **Búsqueda de persistencia en Oauth:** después del incidente, verificar si el actor creó apps OAuth propias que sobreviven al cambio de contraseña. Un reset de credenciales *no* revoca tokens OAuth activos si no se hace explícitamente.

Cadena de ataque — ShinyHunters (Chaos Trinity)

Modelo de intrusión basado en identidad y nube



Esta cadena de ataque destaca por su naturaleza centrada en identidad, donde el adversario elude la explotación de vulnerabilidades técnicas tradicionales y se apoya en la manipulación humanza y el abuso de credenciales legítimas.

A diferencia de los ataques clásicos de seguridad perimetral o de vulnerabilidades en software, ShinyHunters utiliza credenciales válidas (MFA y OAuth) para moverse lateralmente en entornos SaaS.

En este contexto, el riesgo principal no reside en fallos de software, sino en debilidades en los procesos de verificación de identidad (IAM), autenticación, y gobernanza de accesos, lo que incrementa la dificultad de detección y respuesta por parte de los equipos de seguridad.

Fuentes

BleepingComputer. (2026, 9 de marzo). ShinyHunters claims ongoing Salesforce Aura data theft attacks.
https://www.bleepingcomputer.com/news/security/shinyhunters-claims-ongoing-salesforce-aura-data-theft-attacks
Google Threat Intelligence. (2026). Threat Actor Profile: UNC6240 (ShinyHunters) [Base de datos interna].
Google Threat Intelligence. (2026, 23 de enero). Threat Actors Associated with the ShinyHunters Brand Expand Targeting of Cloud Applications for Extortion Operations (Report No. 26-10002301).
Mandiant. (2025, 3 de octubre). ShinyHunters Launches a Data Leak Site (Report No. 25-10047068).
Okta Security. (2026). Phishing kits adapt to the script of callers: Vishing attacks targeting Identity Providers.
https://www.okta.com/blog/threat-intelligence/phishing-kits-adapt-to-the-script-of-callers/
Salesforce Security. (2026, 7 de marzo). Warning: Threat actor scanning Experience Cloud sites.
https://www.theregister.com/2026/03/09/shinyhunters_claims_more_highprofile_victims