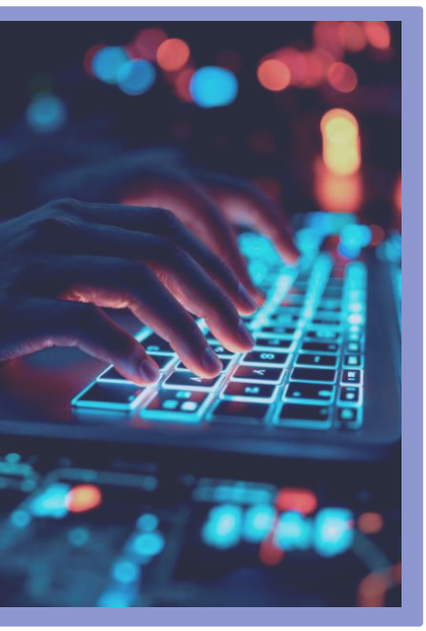
Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS -20251128- 017

TLP:CLEAR



Resumen Ejecutivo

Durante la semana se registraron diversos incidentes cibernéticos en Colombia, dirigidos principalmente a entidades del sector salud y organismos gubernamentales. Entre las técnicas empleadas se identificaron defacements, SEO poisoning y campañas de ransomware con exfiltración de datos. Los grupos responsables incluyen a Adl3r, KingSkrupellos y KillSec. Asimismo, se detectaron campañas de fraude y phishing relacionadas con eventos comerciales como Black Friday, y se observó el uso de inteligencia artificial tanto como vector de ataque como herramienta de defensa en el ámbito cibernético.

A nivel regional, *ransomware* y *defacements* afectaron sectores críticos en Brasil, México, Argentina y Uruguay, vinculados a grupos como Direwolf, Dragonforce, Qilin y Clop. Además, se identificaron vulnerabilidades críticas en **Microsoft Azure Bastion** y **Fluent Bit** que requieren aplicación urgente de parches.

La semana evidencia la necesidad de fortalecer la ciberresiliencia institucional, combinando prevención, detección y respuesta rápida a incidentes.

Incidentes de la semana

Estos incidentes reflejan una tendencia creciente de ataques dirigidos a instituciones públicas y sectores críticos, aprovechando vulnerabilidades en la infraestructura web y la falta de controles de seguridad robustos. El patrón observado demuestra que los atacantes continúan enfocándose en comprometer sitios oficiales para manipular información, dañar la reputación institucional y obtener acceso a datos sensibles, lo que subraya la necesidad urgente de fortalecer las medidas de ciberseguridad en el país.

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Defacement	22/11/2025	Institución de salud sufrió un ataque de defacement en su sitio web	Adl3r
SEO Poisoning	24/11/2025	Dominios gubernamentales fueron comprometidos y utilizados para realizar ataques de SEO poisoning mediante la carga de PDF ilegitimos.	Desconocido
Defacement	27/11/2025	Entidad gubernamental sufrió defacement en su sitio web.	KingSkrupellos
Ransomware	27/11/2025	Entidad gubernamental sufrió exfiltración de datos.	KillSec

Tabla 1. Incidentes detectados a nivel local. Fuente: COLCERT.

Tendencias observadas

- **Campañas de fraude y suplantación digital asociadas al Black Friday**: En el marco del evento comercial Black Friday 2025 en Colombia, se han identificado campañas de suplantación digital, phishing y estafas que buscan aprovechar el interés de los usuarios por obtener promociones, utilizando señuelos que simulan sitios legítimos o comunicaciones oficiales.

- **Uso de la inteligencia artificial (IA) como vector y como herramienta de defensa**: Se ha detectado la utilización de IA para potenciar ataques, mediante la creación de contenido malicioso más convincente o la imitación de plataformas legítimas. Al mismo tiempo, organizaciones en Colombia están integrando soluciones basadas en IA para fortalecer sus capacidades de detección, respuesta automatizada y monitoreo continuo como parte de sus estrategias de ciberseguridad.

- **Fortalecimiento de la ciberresiliencia institucional:** Ante un entorno persistente de intentos de intrusión y exposición a vulnerabilidades, se destaca la necesidad de que las organizaciones consoliden su postura de ciberresiliencia. Esto implica no solo la prevención, sino también la preparación frente a incidentes mediante controles técnicos, monitoreo permanente, gestión de incidentes, planes de continuidad operativa y una cultura organizacional centrada en la seguridad.

Panorama nacional

La gráfica refleja un incremento en la detección de diversas amenazas, con especial énfasis en **Tycoon 2FA**, que registró la mayor actividad durante la semana. También se observaron aumentos en **EvilProxy**, **Sneaky 2FA**, **AsyncRAT** y **Mamba 2FA**, lo que refuerza la tendencia de ataques orientados a la captura de credenciales y evasión de mecanismos de autenticación.

Destaca además el reingreso de **Lumma**, ausente en el periodo anterior, mientras que **Remcos**, **AgentTesla** y **HijackLoader** mantienen una actividad estable. En conjunto, los datos evidencian una mayor circulación de herramientas utilizadas para el acceso no autorizado y el compromiso de cuentas corporativas.

Comparativa entre semanas

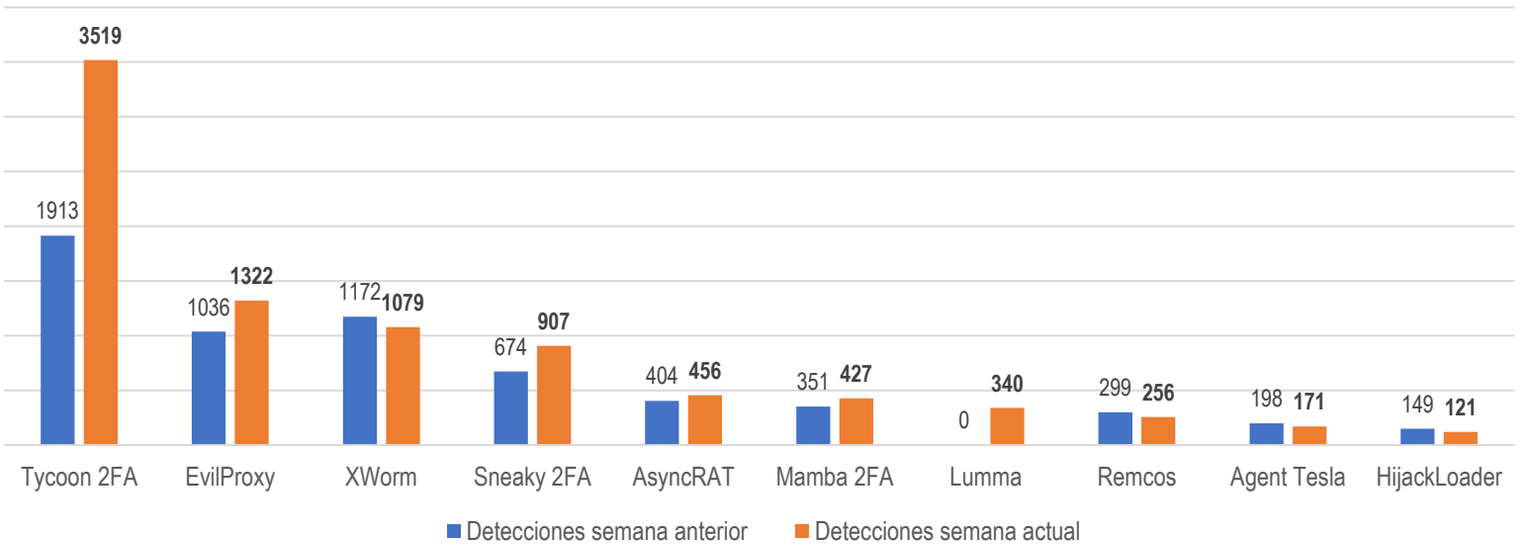


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la semana se reportaron múltiples incidentes en América Latina, principalmente ataques de ransomware dirigidos a sectores críticos en Brasil, México, Argentina y Uruguay, asociados a grupos como **Direwolf**, **Dragonforce**, **Qilin** y **Clop**.

Adicionalmente, se identificaron casos de **defacement** en varios gobiernos de la región, atribuidos a actores como **Mizun0** y **KingSkrupellos**. Estos eventos reflejan una actividad persistente de amenazas dirigidas a sectores estratégicos, con implicaciones en la seguridad operativa y reputacional de las entidades afectadas.

Sector	Amenaza	Locación	Posible actor involucrado
Transporte	Ransomware	Brasil	**Direwolf**
Tecnologías de la Información y Comunicaciones	Ransomware	Brasil	**Dragonforce**
Financiero	Ransomware	Uruguay	**Ransomhouse**
Alimentación Y Agricultura	Ransomware	Argentina	**Dragonforce**
Energia	Ransomware	Argentina	**Direwolf**
Educación	Ransomware	Mexico	**Qilin**
Turismo	Ransomware	Mexico	**Tengu**
Alimentación y Agricultura	Ransomware	Mexico	**Clop**
Gobierno	Defacement	Brasil	**Mizun0**
Gobierno	Defacement	Argentina	**KingSkrupellos**
Gobierno	Defacement	Honduras	**KingSkrupellos**
Gobierno	Defacement	Ecuador	**KingSkrupellos**

Tabla 2. Incidentes detectados a nivel regional. Fuente: COLCERT.

Vulnerabilidades relevantes de la semana

Esta semana se identificaron vulnerabilidades críticas que afectan a **Microsoft Azure Bastion** y **Fluent Bit**, exponiendo riesgos de ejecución remota de código, elevación de privilegios y manipulación de registros. La más grave, **CVE-2025-49752** (CVSS 10.0), permite a atacantes obtener acceso administrativo sin autenticación en entornos Azure.

En el caso de **Fluent Bit**, múltiples CVE habilitan la inyección de etiquetas, corrupción de memoria y transmisión de datos no autorizados, lo que representa un rango de impactos que va desde **denegación de servicio (DoS)** hasta compromisos severos en la integridad del registro. Estas vulnerabilidades requieren **atención inmediata** y la aplicación **prioritaria de parches**.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Microsoft Azure Bastion	**CVE-2025-49752**	Vulnerabilidad de bypass de autenticación y elevación de privilegios que permite a un atacante remoto sin autenticación válida obtener acceso administrativo a máquinas virtuales gestionadas por Bastion.	**10.0 (Crítico)**
Fluent Bit	**CVE-2025-12972**	Permite inyectar en el tag valores con ../ y escribir archivos arbitrarios fuera del directorio previsto. Permite RCE si Fluent Bit corre con permisos elevados.	5.3 (Medio)
	CVE-2025-12970	Un nombre de contenedor demasiado largo puede corromper memoria, con posibilidad de Denegación de Servicio (DoS) o ejecución remota de código (RCE).	8.8 (Alto)
	CVE-2025-12969	Permite a atacantes remotos enviar datos sin credenciales si la configuración no es correcta. Pueden inyectar logs falsos, saturar alertas, manipular flujos.	6.5 (Medio)
	CVE-2025-12977	Permite inyección de etiquetas maliciosas (tags con nuevos saltos de línea, ../, etc.), *log tampering*, redirección o manipulación de logs.	**9.1 (Crítico)**
	CVE-2025-12978	Permite *spoofing* parcial de etiquetas, manipulación de *routing* de *logs*, posible redirección a destinos no autorizados o filtración.	5.4 (Medio)

Tabla 3. Vulnerabilidades relevantes de la semana. Fuente: COLCERT.

Análisis de Actores y Campañas Activas

- **Adl3r**: actor identificado en reportes de *defacement* dirigidos a organizaciones en la región; perfil típico de "*website defacer*" más que de operador de ransomware.
- **KingSkrupellos**: actor observado públicamente reivindicando múltiples *defacements* en gobiernos de LATAM en recientes listados de incidentes.
- **KillSec**: grupo vinculado a operaciones de *ransomware* y exfiltración de datos, con incidentes reportados contra instituciones de salud.
- **Direwolf**: *Ransomware* emergente observado en 2025 con capacidades de exfiltración y cifrado.
- **Dragonforce**: Operador de RaaS en rápido crecimiento, vinculado a ataques a grandes empresas (retail, servicios).
- **RansonHouse**: Grupo de extorsión con sitio de filtración activo y trayectorias de víctimas en múltiples países, lleva años operando.
- **Qilin**: *Ransomware* de alta actividad en 2025, con cientos de víctimas. Opera como RaaS con gran volumen de campañas.
- **Tengu**: grupo de ransomware con actividad reportada recientemente en LATAM y otras regiones; reclamos públicos de víctimas recientes.
- **Clop**: operador de *ransomware* conocido por grandes campañas de extorsión y explotación de vulnerabilidades en *supply-chain*.

Recomendaciones

- Implementar actualizaciones y parches de seguridad de manera prioritaria en todos los sistemas críticos, incluyendo servidores web, aplicaciones y servicios en la nube, para reducir la exposición a vulnerabilidades como las identificadas en **Azure Bastion** y **Fluent Bit**.
- Configurar monitoreo continuo de los sistemas y redes mediante SIEM, EDR o herramientas de detección avanzada, incluyendo alertas sobre actividades anómalas, ejecución de procesos sospechosos o cambios no autorizados en archivos y registros.
- Realizar auditorías y pruebas de seguridad periódicas, como escaneo de vulnerabilidades y pruebas de penetración, enfocadas en identificar brechas en aplicaciones web, servicios expuestos y configuraciones inseguras.
- Restringir el acceso a sistemas críticos mediante controles de identidad y acceso, utilizando autenticación multifactor, permisos mínimos necesarios y segmentación de redes para limitar el movimiento lateral de atacantes.
- Aplicar políticas de respaldo y recuperación de información de manera regular, asegurando que los datos críticos se puedan restaurar rápidamente ante un ataque de ransomware o pérdida de integridad.
- Capacitar al personal en ciberseguridad, *phishing* y buenas prácticas de manejo de información, para reducir la efectividad de campañas de ingeniería social y fraudes por suplantación digital.
- Revisar y limitar el uso de credenciales embebidas o hardcoded en scripts y configuraciones, muchas herramientas como Fluent Bit o integraciones en la nube almacenan claves o tokens en texto plano. Auditar y reemplazar estas prácticas con gestores seguros de secretos reduce el riesgo de filtración o abuso de credenciales.
- Aplicar control de integridad sobre binarios y archivos de configuración críticos, usar herramientas que verifiquen automáticamente la integridad de ejecutables y archivos sensibles permite detectar alteraciones maliciosas en componentes como agentes de log o servicios de administración remota.
- Desplegar autenticación basada en identidad federada o tokens temporales para acceso cloud, reducir el uso de claves estáticas en plataformas como Azure mediante el uso de Azure AD, tokens de corta duración y autenticación federada, disminuye la exposición frente a accesos persistentes y no autorizados.

Resumen de las fuentes y nivel de confianza en la información proporcionada

Ransomware.live, 27 de noviembre de 2025, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración. https://www.ransomware.live/

Any Run, 27 de noviembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/

CERT/CC (VU#761751), 24/11/2025, "Fluent Bit contains five vulnerabilities, including stack buffer overflow, authentication bypass, and path traversal", Advertencia de vulnerabilidad.
https://www.kb.cert.org/vuls/id/761751

NVD (National Vulnerability Database), 20/11/2025, "CVE-2025-49752 Detail – Azure Bastion Elevation of Privilege Vulnerability", base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-49752

Infobae, 26/11/2025, "La ciberresiliencia se convierte en la clave para enfrentar los 37.000 millones de ciberataques anuales en Colombia", artículo periodístico.
https://www.infobae.com/colombia/2025/11/26/la-ciberresiliencia-se-convierte-en-la-clave-para-enfrentar-los-37000-millones-de-ciberataques-anuales-en-colombia/

Infobae, 27/11/2025, "Aumentan estafas digitales por Black Friday 2025: expertos advierten cinco riesgos clave", artículo periodístico.
https://www.infobae.com/colombia/2025/11/27/aumentan-estafas-digitales-por-black-friday-2025-expertos-advierten-cinco-riesgos-clave/

CrowdStrike, 03/05/2023, "What Is SEO Poisoning? – SEO Poisoning (Social Engineering)", página de referencia técnica.
https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/seo-poisoning/