Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20251219 – 019

TLP:CLEAR

Resumen Ejecutivo

Durante esta semana se evidenció un panorama de riesgo cibernético activo en Colombia y la región, con incidentes relevantes que afectaron tanto a entidades gubernamentales como a empresas privadas, y un claro predominio del *ransomware* como principal amenaza en Latinoamérica. Actores como **Qilin**, **Safepay**, **Killsec**, **MintEye** e **INCransom** continúan desarrollando campañas activas contra sectores estratégicos empleando tácticas de doble extorsión y explotación de accesos remotos, mientras que ataques de *defacement* de menor sofisticación mantienen impacto reputacional sobre plataformas institucionales.

De manera complementaria, se identificaron tendencias estacionales y estratégicas que elevan el nivel de riesgo, destacándose el incremento de estafas y campañas de *phishing* con temática navideña, orientadas al fraude financiero y la captura de credenciales. En respuesta, las organizaciones colombianas comienzan a priorizar la ciberresiliencia y la continuidad del negocio como ejes estratégicos, fortaleciendo capacidades de prevención, detección y respuesta ante incidentes.

Incidentes de la semana

Durante la última semana se registraron dos incidentes cibernéticos relevantes a nivel nacional. El primero correspondió a un ataque de *defacement* contra el sitio web institucional de una entidad gubernamental, atribuido de forma preliminar al actor **We Boyz**, evidenciando afectación a la imagen y presencia digital de la entidad. El segundo incidente involucró un ataque de *ransomware* contra una empresa de servicios privados, presuntamente asociado al actor **Safepay**, con impacto potencial en la disponibilidad de los sistemas y la continuidad operativa de la organización.

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Defacement	**17/DIC/2025**	Una entidad gubernamental fue víctima de un ataque de *defacement* en su sitio web institucional.	We Boyz
Ransomware	**17/DIC/2025**	Una empresa de servicios privados fue afectada por un ataque de *ransomware*.	Safepay

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

Tendencias observadas

- **Explotación de la temporada navideña para fraudes digitales:** durante la temporada navideña se ha observado un incremento en campañas de estafas y phishing que utilizan temáticas festivas para engañar a usuarios y organizaciones. Estas campañas incluyen fraudes silenciosos asociados a tarjetas regalo y promociones falsas, aprovechando el aumento de transacciones y la menor percepción de riesgo en esta época.

- **Ciberresiliencia como prioridad estratégica empresarial:** las empresas colombianas están priorizando la ciberseguridad y la continuidad del negocio como ejes estratégicos, reforzando inversiones y adoptando nuevas soluciones orientadas a la ciberresiliencia, con el fin de mitigar el impacto de ciberataques e interrupciones operativas en un entorno de riesgo creciente.

COLCERT

Panorama nacional

El siguiente gráfico evidencia una disminución general en el volumen de detecciones frente a la semana anterior, aunque persisten amenazas con alta actividad en el entorno nacional. **Tycoon 2FA** continúa liderando como la amenaza más detectada, pese a una reducción significativa respecto a la semana previa, seguido por **EvilProxy** y **XWorm**, que mantienen una presencia relevante, aunque con tendencia a la baja. En contraste, se observa la aparición o incremento de familias como **Quasar**, **Vidar** y **Lumma**, que no registraban detecciones la semana anterior, lo que sugiere dinamismo en las campañas activas y rotación de herramientas por parte de los actores de amenaza. Este comportamiento refuerza la necesidad de mantener capacidades de monitoreo continuo y ajustes periódicos en los controles de detección.

Comparativa entre semanas

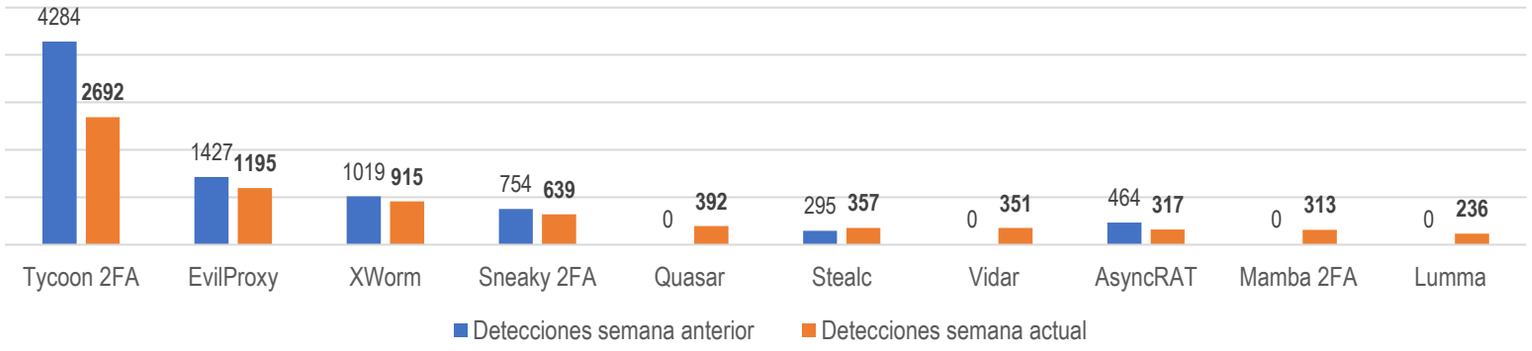


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

La información recopilada evidencia que, a nivel Latinoamérica, el *ransomware* continúa siendo la principal amenaza, afectando de manera transversal a múltiples sectores estratégicos, con especial impacto en gobierno, transporte, agua y comercio, industria y turismo. Se observa una alta concentración de incidentes en países como Argentina, Brasil, México y Chile, lo que sugiere una focalización regional por parte de actores conocidos como **Qilin**, **Safepay**, **Killsec**, **MintEye** e **INCransom**, los cuales mantienen campañas activas contra infraestructuras críticas y servicios esenciales. Adicionalmente, se reporta un incidente en el sector minero-energético en Venezuela con amenaza y actor aún no identificados, lo que refleja limitaciones en la atribución temprana y refuerza la necesidad de mejorar las capacidades regionales de detección, análisis y cooperación frente a este tipo de amenazas.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Recursos Minero-Energéticos	Desconocido	Venezuela	Desconocido
Gobierno	Ransomware	Brasil	Killsec
Transporte	Ransomware	Chile	MintEye
Agua	Ransomware	Argentina	Safepay
Comercio, Industria y Turismo	Ransomware	Argentina	Qilin
Comercio, Industria y Turismo	Ransomware	Costa Rica	INCransom
Transporte	Ransomware	Mexico	Qilin

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

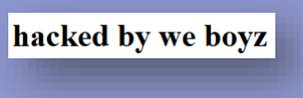
Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS	CISA KEV
FortiOS FortiProxy FortiSwitchManager	CVE-2025-59718	Permite a un atacante no autenticado eludir la autenticación de inicio de sesión de FortiCloud SSO mediante un mensaje SAML manipulado, logrando así acceso administrativo sin credenciales válidas si la función FortiCloud SSO está habilitada.	**9.8 (Crítico)**	TRUE
FortiWeb	CVE-2025-59719	Similar a CVE-2025-59718, permite a un atacante no autenticado evitar la autenticación mediante un mensaje SAML creado maliciosamente, resultando en acceso administrativo sin necesidad de credenciales cuando el FortiCloud SSO está activado.	**9.8 (Crítico)**	FALSE
Google Chrome	CVE-2025-14174	Puede llevar a ejecución remota de código vía contenido web malicioso. Explotado en el ciberespacio, se publicaron parches de emergencia para Chrome y para WebKit (Apple).	8.8 (Alto)	TRUE
ASUS Live Update	CVE-2025-59374	Puede permitir la ejecución no intencionada en máquinas objetivo. CISA lo añadió al catálogo de KEV por evidencia de explotación.	**9.8 (Crítico)**	TRUE
Cisco Secure Email Gateway, Secure Email y AsyncOS	CVE-2025-20393	Ejecución arbitraria de comandos con privilegios *root* en el sistema operativo subyacente.	**10.0 (Crítico)**	TRUE
SonicWall SMA1000	CVE-2025-40602	Escalación de privilegios por falta de autorización en la consola de administración.	6.6 (Medio)	TRUE

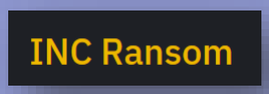
Tabla 3. Vulnerabilidades relevantes de la semana. Fuente: COLCERT.

Actores y campañas activas

- **We Boyz**: es un actor de amenaza al que se le han atribuido múltiples ataques de *defacement* contra entidades gubernamentales en diversos países a nivel global, principalmente orientados a la alteración de sitios web institucionales con fines de exposición pública y afectación reputacional.
- **KillSec**: evolucionó de hacktivismo a Ransomware-as-a-Service (RaaS). Incorpora herramientas como DDoS, llamadas sociales y stealers avanzados para maximizar impacto global en sectores vulnerables.
- **MintEye**: es un actor nuevo, activo desde diciembre de 2025, con al menos cinco víctimas en su Data Leak Site (DLS). Sus campañas usan extorsión doble y se centran en empresas industriales y legales de EE.UU., mostrando rápida escalada.



- **Safepay:** surgió en septiembre de 2024 y alcanzó pico en 2025 como uno de los grupos más activos. Emplea código modificado de LockBit, extorsión doble y plazos de 24 horas para encriptación agresiva en sectores públicos y privados.
- **Qilin:** lidera en 2025 con más de 700 ataques confirmados hasta octubre, cuadruplicando víctimas de 2024 mediante RaaS. Campañas recientes incluyen brechas en MSP surcoreanos y clínicas israelíes (8 TB exfiltrados), priorizando disrupción en infraestructuras críticas.
- **INCransom:** usa tácticas sofisticadas como explotación de CVE-2023-3519 en Citrix, WMI para ejecución y RDP para movimiento lateral, enfocándose en salud, educación e industria. Opera extorsión descentralizada, con persistencia mediante cuentas comprometidas y desactivación de Defender.



Recomendaciones

- **Fortalecer la gestión de parches y actualizaciones**, priorizando la corrección inmediata de vulnerabilidades críticas y explotadas activamente (KEV), especialmente en dispositivos perimetrales, soluciones de seguridad, navegadores y software de actualización, con el fin de reducir la superficie de ataque frente a actores oportunistas y campañas masivas.
- **Endurecer los controles de autenticación y acceso**, implementando autenticación multifactor obligatoria en accesos administrativos, VPN, soluciones SSO y consolas de gestión, así como revisando configuraciones por defecto que puedan permitir bypass de autenticación o escalación de privilegios.
- **Reforzar la seguridad del correo electrónico y la navegación web**, desplegando controles avanzados contra *phishing*, enlaces maliciosos y archivos adjuntos, considerando el incremento de campañas de fraude y phishing temático estacional dirigidas a la captura de credenciales y distribución de amenazas.
- **Concientizar y capacitar de forma continua al personal**, enfocándose en la identificación de correos fraudulentos, estafas digitales, uso seguro de credenciales y reporte oportuno de incidentes, especialmente en periodos de alta actividad comercial o estacional.
- **Segmentar las redes y limitar privilegios**, reduciendo la propagación lateral de amenazas mediante la separación de entornos críticos, la aplicación del principio de mínimo privilegio y el control estricto de cuentas administrativas y de servicio.
- **Mantener respaldos seguros y aislados**, garantizando copias de seguridad periódicas, offline o inmutables, y realizando pruebas de restauración para asegurar la recuperación ante incidentes de cifrado o sabotaje de información.

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

Ransomware.live, 18 de diciembre de 2025, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración, https://www.ransomware.live/
Any Run, 18 de diciembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas. https://any.run/malware-trends/
Forbes Colombia, 17-dic-2025, Empresas colombianas van a priorizan ciberseguridad y continuidad este 2026, Medio de negocios, https://forbes.co/2025/12/17/negocios/empresas-colombianas-van-a-priorizan-ciberseguridad-y-continuidad-este-2026
Semana.com, 15-dic-2025, Alerta en Navidad: criminales aprovechan la temporada para relanzar extorsiones y fraudes silenciosos con tarjetas regalo, Medio generalista, https://www.semana.com/tecnologia/articulo/alerta-en-navidad-criminales-aprovechan-la-temporada-para-relanzar-extorsiones-y-fraudes-silenciosos-con-tarjetas-regalo/202538/
El Tiempo, 14-dic-2025, Navidad, la época favorita de los ciberdelincuentes en Colombia, Medio generalista, https://www.eltiempo.com/tecnosfera/novedades-tecnologia/navidad-la-epoca-favorita-de-los-ciberdelincuentes-en-colombia-3516825
National Vulnerability Database (NVD), 09-dic-2025, CVE-2025-59718 Detail, Base de datos de vulnerabilidades, https://nvd.nist.gov/vuln/detail/CVE-2025-59718
National Vulnerability Database (NVD), 09-dic-2025, CVE-2025-59719 Detail, Base de datos de vulnerabilidades, https://nvd.nist.gov/vuln/detail/CVE-2025-59719
National Vulnerability Database (NVD), 12-dic-2025, CVE-2025-14174 Detail, Base de datos de vulnerabilidades, https://nvd.nist.gov/vuln/detail/CVE-2025-14174
National Vulnerability Database (NVD), 17-dic-2025, CVE-2025-59374 Detail, Base de datos de vulnerabilidades, https://nvd.nist.gov/vuln/detail/CVE-2025-59374
National Vulnerability Database (NVD), 17-dic-2025, CVE-2025-20393 Detail, Base de datos de vulnerabilidades, https://nvd.nist.gov/vuln/detail/CVE-2025-20393
National Vulnerability Database (NVD), 18-dic-2025, CVE-2025-40602 Detail, Base de datos de vulnerabilidades, https://nvd.nist.gov/vuln/detail/CVE-2025-40602

COLCERT