Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20251229 – 020

TLP:CLEAR

Resumen Ejecutivo

Durante la semana analizada, el panorama de amenazas cibernéticas en Colombia y la región evidenció una actividad sostenida y diversificada, con énfasis en campañas de ingeniería social, compromiso de credenciales, *ransomware* y explotación de vulnerabilidades críticas en infraestructura corporativa. Las detecciones registradas muestran que, aunque algunas familias de malware redujeron su volumen frente a la semana anterior, persiste un riesgo elevado asociado a herramientas diseñadas para evadir controles de autenticación multifactor y facilitar el acceso inicial a las organizaciones, lo que refuerza la relevancia del phishing como principal vector de ataque.

A nivel regional, los incidentes observados en Latinoamérica reflejan una concentración de ataques de ransomware en sectores estratégicos con especial afectación en países como Brasil, Argentina y Perú. Grupos como Thegentlemen, Qilin, BlackShrantac y LockBit 5.0 mantienen campañas activas bajo modelos de doble extorsión, combinando cifrado de información con exfiltración y amenaza de publicación, lo que incrementa el impacto operativo, legal y reputacional para las organizaciones afectadas.

En conjunto, el escenario observado confirma un entorno de amenazas activo y en evolución, donde los atacantes priorizan el acceso inicial mediante ingeniería social, el abuso de tecnologías legítimas y la explotación de vulnerabilidades críticas, consolidando la importancia de fortalecer las capacidades de prevención, detección temprana y respuesta a incidentes, especialmente en sectores estratégicos y durante periodos de alta exposición como el cierre de año.

Tendencias observadas

- **Phishing dirigido y amenazas avanzadas en Colombia:** Durante las últimas semanas, se ha identificado una campaña de *spearphishing* sofisticada contra instituciones gubernamentales colombianas atribuida al grupo de amenazas **BlindEagle**. El vector inicial consistió en correos con temas legales que dirigían a los destinatarios a un portal fraudulento y desencadenaban la ejecución de scripts que descargaban *malware* lo cual demuestra cómo la ingeniería social bien elaborada continúa siendo una de las amenazas más eficaces contra organizaciones en Colombia.

- **Malware oculto en paquetes de software compromete WhatsApp Web**: En el ámbito del desarrollo de software, se detectó un paquete malicioso alojado en el repositorio de npm que suplanta una librería legítima para interactuar con la API de WhatsApp Web. Esta biblioteca, con más de 56.000 descargas, permite a actores maliciosos interceptar mensajes, credenciales y archivos multimedia, además de generar enlaces automáticos para vincular dispositivos del atacante a las cuentas de las víctimas sin notificación visible.

- **Aumento de fraudes digitales en temporada de fin de año**: La temporada de fin de año ha traído consigo un incremento en las alertas de fraudes digitales dirigidos tanto a usuarios como a organizaciones, vinculados a compras navideñas, servicios de pagos y banca digital. Expertos señalan que las campañas de **ingeniería social**, como ***smishing*** y ***phishing***, se intensifican en esta época aprovechando el aumento de transacciones y promociones online. Además, la modernización de infraestructuras y la integración de datos entre instituciones se destacan como prioridades para reducir brechas de seguridad, mientras que la educación de los usuarios se muestra como un elemento clave para mitigar la efectividad de estas estafas.

Panorama nacional

Durante la semana analizada se mantiene una alta actividad de amenazas asociadas a campañas de captura de credenciales y control remoto, destacándose especialmente **Tycoon 2FA** y **EvilProxy**, que continúan liderando las detecciones a pesar de una reducción frente a la semana anterior, lo que sugiere campañas aún activas pero con menor intensidad. Se observa también una disminución generalizada en familias como **XWorm**, **AsyncRAT** y **Remcos**, lo que podría estar relacionado con ajustes en las infraestructuras de los actores o cambios en los vectores de distribución. No obstante, la persistencia de amenazas orientadas a la evasión de mecanismos de autenticación multifactor y al compromiso de credenciales refuerza la tendencia de ataques centrados en la ingeniería social y el acceso inicial, manteniendo un riesgo relevante para organizaciones públicas y privadas en Colombia.

Comparativa entre semanas

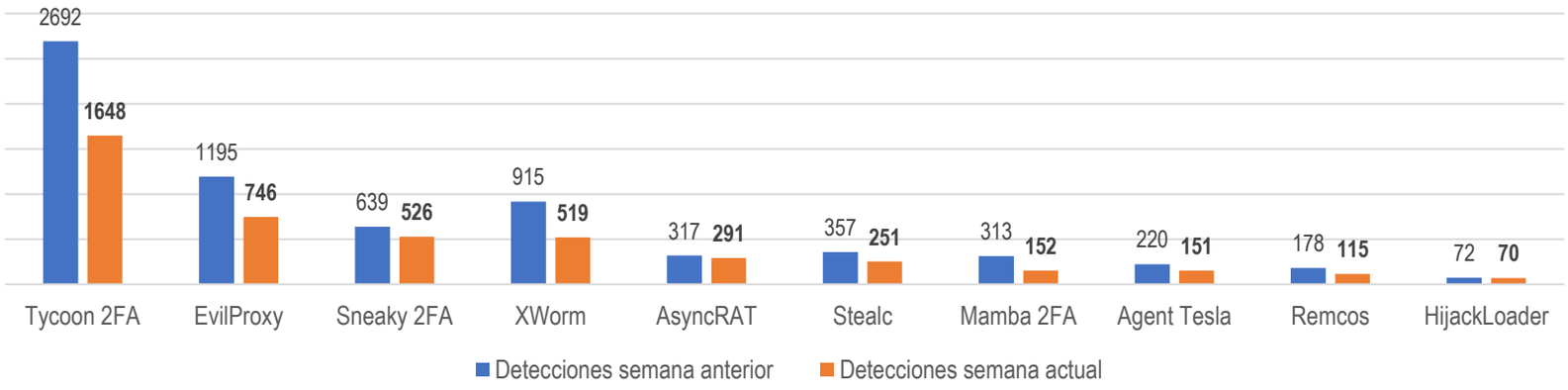

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la semana se evidenció una concentración de incidentes de *ransomware* en sectores estratégicos de Latinoamérica, con un impacto recurrente en Tecnologías de la Información y Comunicaciones, Comercio, Industria y Turismo, así como Salud y Alimentación, lo que refleja el interés de los actores de amenaza por organizaciones con alta dependencia operativa y capacidad de pago. Brasil y Argentina se posicionan como los países con mayor número de eventos reportados, mientras que Perú también presenta afectaciones relevantes.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Tecnologías de la Información y Comunicaciones	Ransomware	**Perú**	Qilin
Alimentación y Agricultura	Ransomware	**Perú**	Black Shrantac
Educación	Ransomware	**Brasil**	LockBit 5.0
Tecnologías de la Información y Comunicaciones	Ransomware	**Brasil**	TheGentlemen
Salud y Protección Social	Ransomware	**Brasil**	TheGentlemen
Comercio, Industria y Turismo	Ransomware	**Brasil**	TheGentlemen
Alimentación y Agricultura	Ransomware	**Brasil**	TheGentlemen
Comercio, Industria y Turismo	Ransomware	**Argentina**	Qilin
Comercio, Industria y Turismo	Ransomware	**Argentina**	Qilin

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS	CISA KEV
WatchGuard Firebox - Fireware OS	**CVE-2025-14733**	Ejecución remota de código (RCE) sin autenticación mediante una condición de escritura fuera de límites en el proceso iked, afectando VPNs IKEv2. Permite comprometer dispositivos de seguridad perimetral.	**9.8 (Crítico)**	**TRUE**
n8n	**CVE-2025-68613**	Permite a usuarios autenticados ejecutar código arbitrario en el servidor mediante inyección de expresiones, lo que podría comprometer completamente el sistema y exponer datos sensibles en entornos corporativos con automatizaciones integradas.	**9.9 (Crítico)**	**FALSE**

Tabla 2. Vulnerabilidades relevantes de la semana. Fuente: COLCERT.

Actores y campañas activas

- **BlindEagle**: también rastreado como APT-C-36, es un grupo de amenazas de larga data (activo desde al menos 2018) que ha centrado sus operaciones principalmente en objetivos en Colombia y Latinoamérica, especialmente instituciones gubernamentales y grandes organizaciones de sectores como financiero, energía, manufactura y servicios públicos.
- **Qilin**: se ha consolidado como uno de los grupos de *ransomware* más prolíficos en 2025, liderando frecuentemente el volumen de incidentes reportados a nivel mundial. Diversos análisis señalan que este actor representa el mayor porcentaje de víctimas de ransomware, a veces superando a otras bandas consolidadas y eclipsando a muchos grupos medianos.
- **Black Shrantac**: es un actor cibercriminal recientemente identificado (desde septiembre 2025), caracterizado por operar en el modelo de doble extorsión, enfocándose en maximizar la presión al amenazar la publicación de datos sensibles si no se paga el rescate.
- **LockBit 5.0**: ha sido históricamente una de las familias de *ransomware* más activas, y su versión 5.0, lanzada en 2025, representa una actualización significativa de capacidades técnicas, incluyendo cifrado mejorado, técnicas antianálisis, ejecución sin archivos y soporte multiplataforma (Windows, Linux y ESXi).
- **TheGentlemen**: es una amenaza emergente de *ransomware* identificada a mediados de 2025, ganando visibilidad rápidamente por su modelo de doble extorsión y enfoque metódico para la infiltración y evasión. Su infraestructura ha listado decenas de víctimas en múltiples regiones, incluyendo industrias como manufactura, construcción, salud e incluso servicios financieros.

Black Shrantac

Recomendaciones

- Fortalecer los controles contra phishing y suplantación de identidad, implementando filtros avanzados de correo electrónico, validaciones estrictas de SPF, DKIM y DMARC, así como monitoreo de cuentas internas para detectar envíos anómalos, con el fin de reducir el impacto de campañas dirigidas como las asociadas a BlindEagle y otros actores que abusan de relaciones de confianza dentro de las organizaciones.
- Reforzar la seguridad del acceso inicial a los sistemas corporativos, aplicando autenticación multifactor resistente al phishing, políticas de contraseñas robustas y restricciones de acceso basadas en contexto, con el objetivo de mitigar el impacto de herramientas orientadas la captura de credenciales y la evasión de mecanismos 2FA.
- Capacitar de forma continua al personal en la identificación de correos fraudulentos, enlaces sospechosos y archivos maliciosos, priorizando a usuarios con acceso a información sensible o funciones críticas, especialmente durante periodos de alta actividad como el cierre de año, cuando aumentan los fraudes digitales y los ataques de ingeniería social.
- Implementar una gestión rigurosa de parches y vulnerabilidades, priorizando la corrección inmediata de fallas críticas como CVE-2025-14733 y CVE-2025-68613, especialmente en dispositivos perimetrales, firewalls y soluciones de gestión de infraestructura.
- Realizar ejercicios periódicos de simulación de incidentes, incluyendo escenarios de *phishing*, *ransomware* y fuga de información, que permitan evaluar la efectividad de los controles existentes, mejorar los tiempos de respuesta y fortalecer la coordinación entre las áreas técnicas, legales y de gestión.

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

Ransomware.live, 25 de diciembre de 2025, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 25 de diciembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
NVD NIST, 18 dic 2025, CVE-2025-14733 Detail, Base de datos de vulnerabilidades NVD.
https://nvd.nist.gov/vuln/detail/CVE-2025-14733
NVD NIST, 19 dic 2025, CVE-2025-68613 Detail, Base de datos de vulnerabilidades NVD.
https://nvd.nist.gov/vuln/detail/CVE-2025-68613
Zscaler Blog (Security Research), 16 dic 2025, BlindEagle Targets Colombian Government Agency with Caminho and DCRAT, Blog de investigación de amenazas.
https://www.zscaler.com/blogs/security-research/blindeagle-targets-colombian-government-agency-caminho-and-dcrat
Semana.com, 23 dic 2025, Ciberataque silencioso: detectan paquete malicioso que permite robar mensajes y controlar cuentas de WhatsApp Web, Portal de noticias / Tecnología.
https://www.semana.com/tecnologia/articulo/ciberataque-silencioso-detectan-paquete-malicioso-que-permite-robar-mensajes-y-controlar-cuentas-de-whatsapp-web/202518/
Infobae (Tecno), 23 dic 2025, Ciberseguridad en Navidad y Año Nuevo: claves para evitar fraudes digitales en fiestas, Portal de noticias / Tecnología.
https://www.infobae.com/tecno/2025/12/23/ciberseguridad-en-navidad-y-ano-nuevo-claves-para-evitar-fraudes-digitales-en-fiestas/
Cyfirma (Weekly Intelligence Report), 26 dic 2025, Weekly Intelligence Report – 26 December 2025, Informe de inteligencia de seguridad.
https://www.cyfirma.com/news/weekly-intelligence-report-26-december-2025/
Red Piranha (Threat Intelligence Report), 8 dic 2025, Threat Intelligence Report – December 2 – December 8, 2025, Informe de inteligencia de amenazas.
https://redpiranha.net/news/threat-intelligence-report-december-2-december-8-2025
Dexpose.io, 15 dic 2025, BlackShrantac Targets VFM Systems & Services in Ransomware Attack, Blog de análisis de amenazas.
https://www.dexpose.io/blackshrantac-targets-vfm-systems-services-in-ransomware-attack/
AhnLab Security E-Center (ASEC), 11 dic 2025, The Gentlemen – The New Ransomware of Autumn 2025, Análisis de malware y amenazas.
https://asec.ahnlab.com/en/91545/