Reporte

Semanal

Inteligencia de amenaza cibernéticas

COLCERT RS-20260123-022

TLP:CLEAR

Resumen Ejecutivo

Durante la semana analizada, el panorama de ciberseguridad en Colombia muestra una actividad sostenida y altamente concentrada en amenazas orientadas a la evasión de controles de identidad y campañas de *phishing* avanzado, con **Tycoon 2FA** manteniéndose como la principal amenaza a nivel nacional, pese a una leve reducción en su volumen de detecciones frente a la semana anterior. En paralelo, **Sneaky 2FA** y **EvilProxy** registran incrementos relevantes, consolidando la tendencia hacia el uso de plataformas de *phishing-as-a-service* altamente escalables para la captura de credenciales corporativas. Asimismo, se observa una presencia creciente de malware de acceso remoto, como **XWorm**, **AsyncRAT** y **Remcos**, lo que sugiere campañas activas orientadas a persistencia, control remoto y potencial movimiento lateral dentro de entornos empresariales.

A nivel regional, los incidentes reportados en Latinoamérica continúan evidenciando la persistencia del *ransomware* como una de las principales amenazas, con afectación recurrente a sectores estratégicos como comercio, industria, servicios financieros y salud. Grupos como **TheGentlemen, Sinobi y LockBit 5** mantienen campañas activas bajo esquemas de doble extorsión, combinando cifrado de información con exfiltración de datos sensibles.

De manera complementaria, se identificó la divulgación de vulnerabilidades críticas y de alta severidad, las cuales afectan plataformas de comunicaciones empresariales, componentes de *software* ampliamente utilizados y servicios de colaboración. Estas fallas, en algunos casos explotables de forma remota, representan habilitadores clave para compromisos de mayor alcance, facilitando la ejecución de código, el acceso no autorizado y la interrupción de servicios. En conjunto, el escenario observado confirma un entorno de amenazas activo y en evolución, en el que los atacantes priorizan el acceso inicial, la explotación de identidades y servicios expuestos, reforzando la necesidad de fortalecer la gestión de vulnerabilidades, la protección de identidades y las capacidades de detección y respuesta, especialmente en sectores críticos y entornos corporativos.

Tendencias observadas

- **Automatización y sofisticación del cibercrimen impulsada por IA:**Expertos de seguridad y reportes globales destacan que en 2026 la inteligencia artificial dejará de ser solo herramienta defensiva para convertirse en un vector clave de ataque. Los ciberdelincuentes están utilizando IA para generar campañas de *phishing* personalizadas, *deepfakes* y contenido sintético que facilita la evasión de detección y la expansión de ataques automatizados. Esto supone una presión adicional sobre organizaciones y usuarios digitales en Colombia y la región.

- **Ransomware y extorsiones siguen como principal riesgo operativo:** El *ransomware* mantiene su presencia como una de las amenazas más disruptivas, con ataques que evolucionan en sofisticación y técnicas de evasión. En algunos casos, estas campañas incorporan automatización e inteligencia artificial para optimizar la selección de víctimas, maximizar el impacto operativo y acelerar los procesos de negociación y monetización.

- **Ciberseguridad empresarial y redes corporativas en la mira:**Especialistas plantean que la automatización ofensiva y el uso de inteligencia artificial están transformando los vectores de ataque contra entornos corporativos, desplazando el foco desde el malware tradicional hacia la identidad, el acceso y las configuraciones de infraestructura. Este escenario obliga a las organizaciones a replantear sus estrategias de defensa, fortaleciendo la gobernanza de datos, la gestión de identidades y accesos, la segmentación de redes y las capacidades de detección y respuesta, con un énfasis creciente en resiliencia operativa y continuidad del negocio.

Panorama nacional

Durante el periodo analizado se evidencia una actividad maliciosa sostenida y diversificada, con incrementos relevantes en múltiples familias asociadas a evasión de controles de identidad, phishing avanzado y malware de acceso remoto. **Tycoon 2FA** se mantiene como la amenaza predominante a nivel nacional, si bien registra una leve disminución frente a la semana anterior (de 2.704 a 2.309 detecciones), continúa liderando ampliamente el volumen de eventos y consolidándose como el principal habilitador de compromisos de credenciales y elusión de esquemas de autenticación multifactor.

De manera paralela, se observa un crecimiento significativo en plataformas como **Sneaky 2FA** y **EvilProxy**, que incrementan sus detecciones, reforzando la tendencia hacia el uso de infraestructuras de phishing como servicio (PhaaS) altamente escalables. Asimismo, destacan los aumentos en **XWorm** y **Mamba 2FA**, así como la aparición de actividad relevante en **Remcos** y la continuidad de detecciones de **AsyncRAT**, lo que sugiere campañas activas de malware orientadas al acceso remoto persistente y al movimiento lateral dentro de entornos corporativos en Colombia.

Comparativa entre semanas

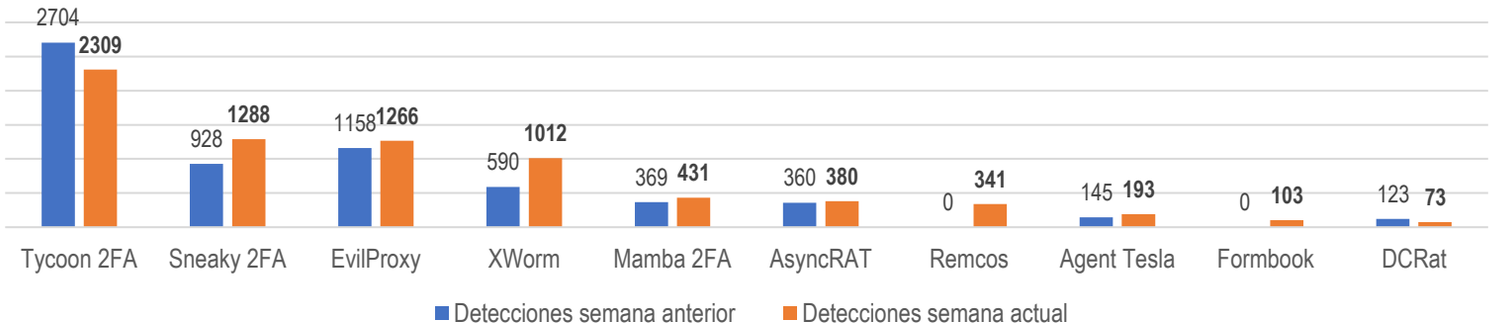

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante el periodo analizado se consolida un conjunto de incidentes de seguridad reportados en países de Latinoamérica, a partir de información obtenida de fuentes abiertas, evidenciando una actividad persistente de *ransomware* en la región. Los casos identificados muestran una afectación recurrente en los sectores de Comercio, Industria y Turismo, así como en los sectores Financiero y de Salud y protección social, con incidentes registrados en México, Brasil y Ecuador. En este contexto, se identifican múltiples actores de amenaza con presencia activa, entre ellos **Qilin**, **TheGentlemen**, **Tengu**, **Sinobi** y **LockBit**, lo que refleja un ecosistema de extorsión digital diverso y descentralizado. La recurrencia de ataques contra sectores económicos y de servicios esenciales refuerza la persistencia del *ransomware* como una de las principales amenazas para la región y subraya la necesidad de fortalecer las capacidades de prevención, detección y respuesta ante este tipo de campañas en el entorno latinoamericano.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Salud y protección social	Ransomware	**México**	Qilin
Comercio, Industria, Turismo	Ransomware	**México**	Thegentlemen
Financiero	Ransomware	**México**	Qilin
Comercio, Industria, Turismo	Ransomware	**Ecuador**	Tengu
Comercio, Industria, Turismo	Ransomware	**Brasil**	Sinobi
Salud y protección social	Ransomware	**Brasil**	Thegentlemen
Financiero	Ransomware	**Brasil**	Lockbit5

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS
Cisco Unified Communications Manager (Unified CM)	**CVE-2026-20045**	Permite a un atacante remoto no autenticado enviar solicitudes HTTP especialmente diseñadas al interfaz de gestión web de varios componentes de Cisco Unified Communications, lo que puede desencadenar la ejecución de comandos arbitrarios en el sistema operativo subyacente y permitir la elevación de privilegios.	**8.2 (Alto)**
Librería binary-parser para Node.js	**CVE-2026-1245**	Permite a un atacante remoto aprovechar una falla de code injection en la librería binary-parser utilizada en entornos Node.js, donde los valores no confiables usados para construir definiciones de parsers se interpolan directamente en código JavaScript generado dinámicamente sin validación. Esta debilidad permite la ejecución de código arbitrario con los mismos privilegios que el proceso Node.js	**6.5 (Medio)**
Zoom Node Multimedia Routers (MMR)	**CVE-2026-22844**	Permite a un participante de una reunión explotar una falla de inyección de comandos presente en los Node Multimedia Routers (MMRs) de Zoom para ejecutar código arbitrario de forma remota en los sistemas afectados con acceso de red y sin interacción adicional del usuario.	**9.9 (Crítica)**

Actores y campañas activas

- **TheGentlemen:** es un actor de *ransomware* activo desde 2025 que ha ganado visibilidad por su enfoque oportunista sobre organizaciones medianas y grandes, especialmente en los sectores de comercio, manufactura y servicios. Opera bajo un modelo de doble extorsión, combinando el cifrado de sistemas con la exfiltración previa de información sensible. **TheGentlemen** se caracteriza por el uso recurrente de accesos iniciales mediante credenciales comprometidas y servicios RDP expuestos, así como por la rápida publicación de víctimas en su sitio de filtraciones, lo que evidencia una estrategia orientada a acelerar la presión y reducir los tiempos de negociación.

- **Sinobi:** es un grupo de *ransomware* emergente observado desde finales de 2025, con actividad concentrada principalmente en América Latina. Este actor muestra un patrón de ataques dirigidos contra organizaciones con baja madurez en ciberseguridad, aprovechando configuraciones débiles, falta de segmentación de red y controles de acceso insuficientes. **Sinobi** emplea herramientas ampliamente disponibles para movimiento lateral y persistencia, priorizando la velocidad de ejecución sobre la sofisticación técnica, lo que le permite comprometer entornos completos en ventanas de tiempo reducidas y maximizar el impacto operativo de sus campañas.

- **LockBit 5:** representa la evolución más reciente del ecosistema **LockBit**, consolidándose como uno de los actores de ransomware más activos y sofisticados del panorama actual. Mantiene un modelo de Ransomware-as-a-Service (RaaS) altamente estructurado, con afiliados distribuidos globalmente y procesos estandarizados para la selección de objetivos, negociación y filtración de datos. LockBit 5 continúa enfocándose en sectores críticos como servicios financieros, industria y tecnología, incorporando mejoras en evasión, automatización del cifrado y explotación de identidades, lo que refuerza su capacidad para ejecutar campañas a gran escala con impacto significativo y sostenido.

Recomendaciones

- Fortalecer la protección de identidades y accesos privilegiados, implementando autenticación resistente al *phishing* (por ejemplo, llaves de seguridad físicas o autenticación basada en certificados) y monitoreo continuo de sesiones, con el fin de reducir la efectividad de plataformas de Phishing-as-a-Service como **Tycoon 2FA**, **Sneaky 2FA** y **EvilProxy**, enfocadas en la captura de credenciales y tokens de sesión.
- Priorizar la gestión y remediación de vulnerabilidades críticas y de alta severidad en servicios expuestos, aplicando de manera oportuna los parches de seguridad para plataformas de colaboración, componentes de *software* ampliamente utilizados y soluciones de comunicaciones empresariales, a fin de mitigar riesgos de ejecución remota de código, elevación de privilegios y compromiso inicial de infraestructura.
- Reforzar las capacidades de detección y respuesta en *endpoints* y servidores, ajustando reglas para identificar comportamientos asociados a *malware* de acceso remoto como **XWorm, AsyncRAT** y **Remcos**, incluyendo persistencia mediante claves de registro, ejecución desde rutas inusuales y comunicaciones salientes hacia infraestructuras externas no confiables.
- Robustecer las estrategias de respaldo, recuperación y resiliencia frente a *ransomware*, garantizando la inmutabilidad de los *backups*, la segregación de credenciales administrativas y la realización periódica de pruebas de restauración, especialmente en sectores críticos, con el objetivo de minimizar el impacto operativo y financiero de campañas de doble extorsión activas en la región.

Fuentes

Ransomware.live, 22 de enero de 2026, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/.

Any Run, 22 de enero de 2026, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/.

The Hacker News, 20 de enero de 2026, "CERT/CC advierte sobre fallo en binary-parser que permite ejecución remota de código (CVE-2026-1245)", Medio especializado en ciberseguridad.
https://thehackernews.com/2026/01/certcc-warns-binary-parser-bug-allows.html.

La FM, 20 de enero de 2026, "Inteligencia artificial y la desinformación encabezan los riesgos digitales para las empresas en 2026", Medio de comunicación colombiano – análisis de riesgos y tendencias.
https://www.lafm.com.co/sociedad/inteligencia-artifical-riesgos-informaticos-riesgos-de-seguridad-empresas-388246.

Xataka Colombia, 19 de diciembre de 2025, "IA, ransomware y regulación: las grandes tendencias de la ciberseguridad que marcarán el arranque de 2026", Medio tecnológico regional – tendencias de ciberseguridad.
https://www.xataka.com.co/seguridad/ia-ransomware-regulacion-grandes-tendencias-ciberseguridad-que-marcaran-arranque-2026.

NVD – NIST, 21 de enero de 2026, "CVE-2026-20045", Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-20045.

NVD – NIST, 20 de enero de 2026, "CVE-2026-1245", Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-1245.

NVD – NIST, 20 de enero de 2026, "CVE-2026-22844", Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-22844.