Reporte

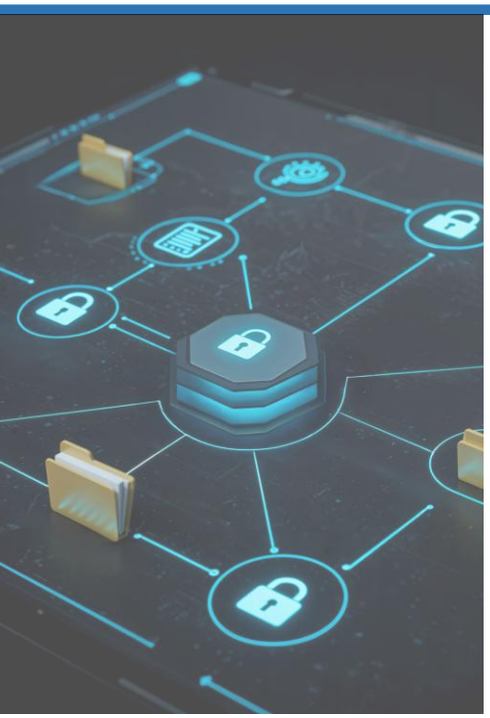
Semanal

Inteligencia de amenaza cibernéticas

COLCERT RS – 20260213 - 024

TIC

TLP:CLEAR



Resumen Ejecutivo

En el transcurso de la semana se evidenció que en Colombia hubo una disminución general en el volumen de detecciones frente a la semana anterior; sin embargo, persiste una alta concentración en amenazas orientadas a la evasión de mecanismos de autenticación multifactor (MFA), acceso inicial y control remoto. **Tycoon 2FA** continúa liderando la actividad, seguido por **EvilProxy** y **Sneaky 2FA**, mientras que familias como **AsyncRAT**, **XWorm**, **Remcos** y **LokiBot** mantienen presencia sostenida. Se destaca el incremento de **DCRat** y la reaparición de **Amadey**, lo que sugiere ajustes tácticos y posibles nuevas campañas dirigidas.

A nivel regional, el *ransomware* continúa siendo la principal amenaza, con incidentes concentrados en Chile, Brasil y México, impactando sectores estratégicos como gobierno, tecnologías de la información, comercio, industria y salud. Se identificó actividad atribuida a grupos como **Cl0p**, **LockBit5**, **Qilin**, **TheGentlemen** y **WorldLeaks**, reflejando la consolidación de modelos de extorsión basados en filtración de datos y esquemas de “extorsión como servicio” (EaaS), con menor dependencia del cifrado tradicional.

En materia de vulnerabilidades, se destacan fallas críticas y de alta severidad en productos ampliamente utilizados. incluyendo soluciones empresariales y componentes del sistema operativo, que podrían facilitar ejecución remota de código, inyección de comandos sin autenticación y elevación de privilegios, aumentando el riesgo de explotación oportunista.

Se evidencia una creciente presión sobre infraestructuras críticas y una tendencia hacia la adopción de enfoques preventivos basados en inteligencia artificial y mayores inversiones en ciberseguridad. En conjunto, el escenario descrito mantiene un nivel de riesgo significativo para entidades públicas y organizaciones privadas, requiriendo fortalecimiento continuo de capacidades de detección, gestión de vulnerabilidades y respuesta ante incidentes.

Tendencias observadas

Infraestructuras críticas como blanco prioritario:

- analistas de seguridad han destacado que variedad de sectores enfrentan una frecuencia de ataque equivalente a un incidente cada 49 segundos. Las defensas tradicionales gradualmente obligan a la integración de modelos de IA predictiva.

Inversión estratégica en ciberseguridad corporativa:

- se confirmó que una de las principales empresas de telecomunicaciones en el país destinó más de 15.000 millones de pesos para fortalecer la infraestructura de ciberseguridad en Colombia, marcando un cambio de modelo reactivo a preventivo en las telecomunicaciones del país. Esta inversión busca proteger infraestructuras críticas de comunicación ante el incremento del 23% en ciberataques registrados en 2025

COLCERT

Panorama nacional

Durante la semana analizada, el panorama nacional de detecciones evidencia una tendencia general a la disminución frente a la semana anterior, especialmente en amenazas asociadas a evasión de autenticación y acceso inicial. **Tycoon 2FA** continúa liderando el volumen de actividad, aunque registra una reducción relevante (de 3.060 a 2.629 detecciones), patrón que también se observa en **EvilProxy** (1.566 a 1.211) y **Sneaky 2FA** (1.061 a 755). De igual forma, familias como **AsyncRAT**, **XWorm**, **Remcos** y **LokiBot** presentan descensos sostenidos. No obstante, se identifican incrementos puntuales en **DCRat**, que pasa de 306 a 462 detecciones, y la aparición de **Amadey**, que no registraba actividad la semana anterior y ahora reporta 117 eventos, lo que podría indicar reactivación o nuevas campañas focalizadas. En conjunto, aunque el volumen total muestra una contracción, persiste una alta concentración en herramientas orientadas al acceso remoto, captura de credenciales y control remoto, manteniendo un nivel de riesgo significativo para organizaciones y usuarios en Colombia.

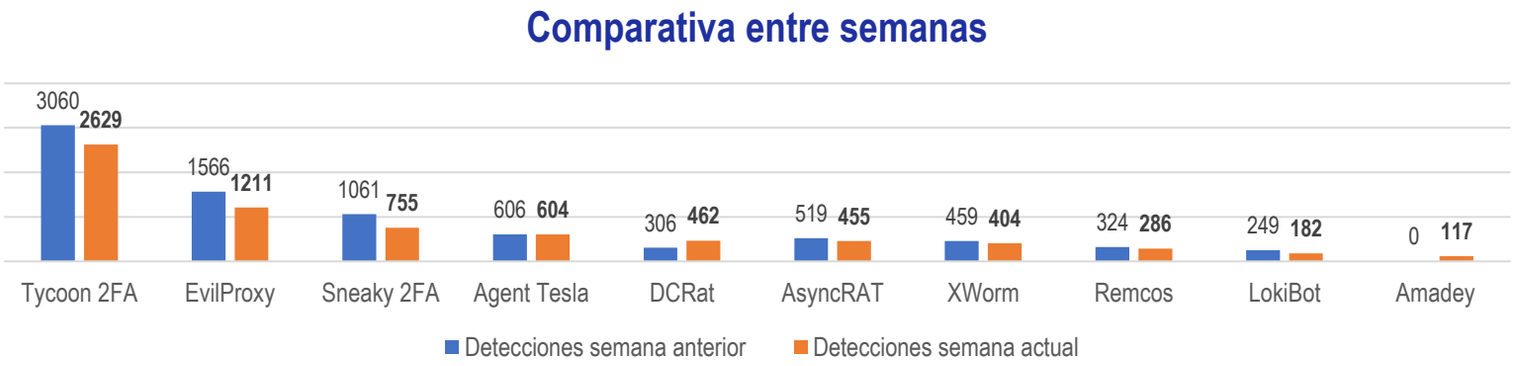


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Por otro lado, se ha detectado un ataque de **Ransomware** dirigido al sector de **Energía y servicios públicos en Colombia**, vinculada al grupo cibercriminal **TheGentlemen**. Este actor opera bajo un modelo de **doble extorsión**, donde primero exfiltran información sensible y luego cifran los sistemas para paralizar la operación y exigir un rescate. Su estrategia se basa en ganar acceso inicial explotando vulnerabilidades en VPN o firewalls, para luego moverse lateralmente de forma sigilosa, desactivando herramientas de seguridad y comprometiendo la infraestructura crítica de la organización.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Energía y servicios públicos	Ransomware	**Colombia**	TheGentlemen

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

Panorama regional

Durante la semana analizada, el panorama regional evidencia una concentración predominante de incidentes de *ransomware* en Chile, Brasil y México, con impactos distribuidos principalmente en los sectores de gobierno, comercio, industria, turismo y tecnologías de la información. En Chile se observa actividad atribuida a los grupos **TheGentlemen** y **Qilin**, afectando tanto entidades gubernamentales como organizaciones del sector productivo y tecnológico. Brasil destaca por una mayor recurrencia de eventos vinculados al actor LockBit5, con múltiples afectaciones en comercio e industria, además de presencia del grupo **Clop** en el sector TI. En México, las detecciones se asocian a **TheGentlemen**, **WorldLeaks** y **Tengu**, impactando gobierno y salud, lo que evidencia una diversificación sectorial relevante. Adicionalmente, se reporta un incidente de *defacement* en Ecuador atribuido a Tex7ure, dirigido a una página web gubernamental. En conjunto, el comportamiento regional mantiene una actividad sostenida de grupos de *ransomware* consolidados, con una marcada focalización en sectores estratégicos y de alto valor operativo.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Gobierno	Ransomware	**Chile**	TheGentlemen
Comercio, industria y turismo	Ransomware	**Chile**	Qilin
Tecnologías de la información	Ransomware	**Chile**	Qilin
Manufactura	Ransomware	**Chile**	LockBit5
Tecnologías de la información	Ransomware	**Brasil**	Clop
Tecnologías de la información	Ransomware	**Brasil**	LockBit5
Comercio, industria y turismo	Ransomware	**Brasil**	LockBit5
Automotor	Ransomware	**Brasil**	LockBit5
Educación	Ransomware	**Brasil**	TheGentlemen
Construcción e ingeniería	Ransomware	**Brasil**	TheGentlemen
Servicios Legales y profesionales	Ransomware	**Brasil**	Insomnia
Salud y protección social	Ransomware	**Brasil**	Beast
Comercio, industria y turismo	Ransomware	**México**	Thegentlemen
Salud y protección social	Ransomware	**México**	WorldLeaks
Gobierno	Ransomware	**México**	Qilin
Energía y Servicios Públicos	Ransomware	**México**	Payouts King
Gobierno	Ransomware	**México**	Tengu
Gobierno	Defacement	**Ecuador**	Tex7ure

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS
Microsoft Office Word	**CVE-2026-21514**	Vulnerabilidad de bypass de características de seguridad que permite eludir las mitigaciones OLE debido a la dependencia en entradas no confiables en decisiones de seguridad. Un atacante puede inducir a la víctima a abrir un archivo malicioso especialmente diseñado para evadir los controles de seguridad, lo que puede facilitar posteriormente la ejecución de código malicioso.	**7.8 (Alto)**
FortiClientEMS 7.4.4	**CVE-2026-21643**	Falla crítica que permite inyección de comandos debido a una validación insuficiente de entradas en la interfaz de gestión. Un atacante remoto podría enviar solicitudes especialmente diseñadas al servidor EMS y ejecutar comandos a nivel del sistema operativo, distribuyendo configuraciones maliciosas o deshabilitando controles de seguridad.	**9.8 (Crítico)**
Windows Shell	**CVE-2026-21510**	Vulnerabilidad de elevación de privilegios causada por un manejo incorrecto de permisos o validación insuficiente de procesos dentro del entorno del Shell de Windows. Un atacante con acceso local previo podría explotar la falla para escalar privilegios hasta SYSTEM, facilitando la persistencia, evasión de controles y despliegue de cargas maliciosas adicionales dentro del equipo comprometido.	**8.8 (Alto)**
Microsoft Windows	**CVE-2026-21533**	Los Servicios de Escritorio Remoto de Microsoft Windows se ven afectados por una vulnerabilidad de administración incorrecta de privilegios que permite la escalada de privilegios locales. Esta falla permite que un usuario autenticado obtenga permisos de nivel superior al previsto en el sistema host.	**7.8 (Alto)**

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

Actores y campañas activas

- **Cl0p:** es un actor de amenazas prolífico de origen ruso que ha evolucionado en 2025 hacia un modelo de "extorsión pura" (encryption-less), abandonando frecuentemente el cifrado para centrarse exclusivamente en la extracción y publicación de datos. Este grupo se especializa en la explotación masiva de vulnerabilidades, lo que le permite comprometer cientos de organizaciones simultáneamente en ataques de "cadena de suministro". Su operativa se caracteriza por olas de alta intensidad, priorizando sectores financieros y gubernamentales en América y Europa, y utilizando portales de filtración en la Dark Web diseñados para maximizar el daño reputacional mediante una navegación estructurada de la información robada.

- **World Leaks:** es una plataforma de "Extorsión como Servicio" (EaaS) emergida a finales de 2024 que se diferencia por no operar su propio *ransomware*, sino por ofrecer infraestructura de exfiltración y negociación a afiliados y otros grupos criminales (como el ransomware Secp0). A diferencia de los modelos RaaS tradicionales, World Leaks se posiciona como un "broker" de datos robados, ofreciendo incluso un acceso diferenciado para periodistas ("Insider platform") con el fin de amplificar la cobertura mediática de sus filtraciones. Sus campañas recientes han afectado a organizaciones en sectores farmacéuticos e industriales a nivel global, utilizando herramientas personalizadas para la exfiltración silenciosa de datos sensibles y ejerciendo presión mediante la publicación selectiva de documentos corporativos críticos.

Recomendaciones

- ❑ Priorizar la gestión de vulnerabilidades críticas, aplicando de forma inmediata los parches asociados a CVE de severidad alta y crítica, especialmente en soluciones expuestas a Internet y sistemas de gestión centralizada.
- ❑ Dado que el grupo TheGentlemen explota vulnerabilidades en VPN y firewalls, es crítico mantener todos los dispositivos de red actualizados con los últimos parches de seguridad. Además, es importante configurar la Autenticación de Múltiple Factor (MFA) en todas las cuentas, especialmente aquellas con privilegios administrativos, para neutralizar el uso de credenciales robadas.
- ❑ Implementar monitoreo continuo de endpoints (EDR/XDR) con reglas específicas para detectar comportamientos asociados a RATs como DCRat, AsyncRAT, XWorm y Remcos, incluyendo conexiones salientes sospechosas y creación anómala de procesos.
- ❑ Fortalecer capacidades de respuesta a incidentes, incluyendo ejercicios de simulación enfocados en escenarios de extorsión y filtración masiva de datos.
- ❑ Capacitar continuamente al personal, especialmente en identificación de correos de phishing avanzado y manipulación segura de documentos adjuntos.
- ❑ Adoptar políticas de mínimo privilegio y segmentación de red para que un atacante no pueda saltar fácilmente de un equipo a otro.

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

Ransomware.live, 12 de enero de 2026, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/.
Any Run, 12 de enero de 2026, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/.
Ciberlatam, 10 de febrero de 2026, "Infraestructuras críticas, IA y soberanía del dato, los grandes retos de la ciberseguridad", Portal de noticias de ciberseguridad.
https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/infraestructuras-criticas-ia-y-soberania-del-dato-los-grandes-retos-de-la-ciberseguridad_20260210.html.
CheckPoint, 22 de abril de 2025, "The State of ransomware", Blog de tendencias de ciberseguridad donde analizan la actividad de actores de amenazas.
https://blog.checkpoint.com/research/the-state-of-ransomware-in-the-first-quarter-of-2025-a-126-increase-in-ransomware-yoy/.
Lexfo, 20 de mayo de 2025, WorldLeaks an extortion platform, Blog de inteligencia de amenazas.
https://blog.lexfo.fr/world-leaks-an-extortion-platform.html
La Republica, 6 de febrero de 2026, Claro invierte más de $15.000 millones para ciberseguridad de las empresas en el país, Portal de noticias colombiano.
https://www.larepublica.co/empresas/claro-invierte-mas-de-us-15-000-millones-para-la-ciberseguridad-de-las-empresas-en-el-pais-4321380.
NIST, 6 de febrero de 2026, CVE-2026-21643, Base oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-21643.
NIST, 10 de febrero de 2026, CVE-2026-21514, Base oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-21514.
NIST, 10 de febrero de 2026, CVE-2026-21510, Base oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-21510.
NIST, 11 de febrero de 2026, CVE-2026-21533 Base oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-21533.