Reporte

Semanal

Inteligencia de amenaza cibernéticas

COLCERT RS -20260130 - 023

TIC

TLP:CLEAR

Resumen Ejecutivo

Durante el periodo analizado, el entorno de ciberseguridad en Colombia muestra una presión sostenida y diversificada de amenazas digitales, con un claro énfasis en ataques enfocados en el compromiso de identidad y los accesos remotos. Las detecciones recientes reflejan campañas agresivas que explotan tanto vectores de *phishing* y evasión de autenticación como herramientas de acceso remoto no autorizadas, lo cual es consistente con tendencias más amplias observadas en América Latina donde las organizaciones enfrentan miles de intentos de ataque semanales y un crecimiento de riesgos asociados a la sofisticación tecnológica.

En paralelo, el contexto regional confirma la continuidad de operaciones de *ransomware* con impacto transversal en múltiples sectores. Grupos como **Incransom**, **Morpheus** y **Safepay** han mantenido actividad reciente en Latinoamérica, con campañas orientadas a la doble extorsión mediante cifrado de sistemas y exfiltración de información sensible. La diversidad geográfica y sectorial de estas operaciones refuerza la madurez del ecosistema de extorsión digital y su capacidad para adaptarse rápidamente a distintos entornos, incrementando el riesgo operativo para organizaciones en la región.

Adicionalmente, la identificación de vulnerabilidades críticas en productos ampliamente utilizados representa un habilitador clave para ataques de mayor impacto. Destacan fallos de alta severidad que afectan a soluciones **Fortinet** (incluyendo FortiOS, FortiManager y FortiAnalyzer), la plataforma de automatización **n8n**, y componentes del ecosistema **Node.js**, como la biblioteca **vm2**, los cuales pueden permitir omisión de autenticación, ejecución remota de código o escape de *sandbox* bajo determinadas condiciones.

La explotación de estas debilidades podría facilitar accesos iniciales, escalamiento de privilegios y compromisos persistentes en infraestructuras empresariales.

En conjunto, el panorama observado en la última semana refuerza la importancia de estrategias de ciberseguridad integrales y dinámicas. Desde la protección de identidades y la resiliencia operacional hasta la respuesta activa ante incidentes y la remediación de vulnerabilidades críticas, con el fin de reducir la probabilidad y el impacto de compromisos en entornos corporativos y de servicios esenciales.

Tendencias observadas

- **Brecha entre percepción y preparación ante ciberataques:** en el contexto latinoamericano y que impacta a Colombia, estudios recientes señalan que, aunque una proporción significativa de organizaciones cree estar preparada contra ciberataques, existe una brecha crítica entre esa percepción y la implementación continua de estrategias de ciberseguridad. Este desbalance se traduce en riesgos operativos sostenidos y en una exposición mayor a incidentes recurrentes, especialmente en sectores dependientes de digitalización acelerada.

- **Incremento sostenido de ataques cibernéticos en la región, con impacto en Colombia:** estudios recientes revelan que las organizaciones en América Latina, incluida Colombia, enfrentan un promedio de más de 2.800 ataques cibernéticos por semana, superando con creces los promedios globales y reflejando un crecimiento sostenido de la presión ofensiva contra entornos empresariales y gubernamentales. Este aumento expone brechas de madurez en ciberseguridad y subraya la necesidad de mecanismos de defensa adaptativos que combinen capacitación, tecnología y cooperación intersectorial.

COLCERT

Panorama nacional

Durante el periodo analizado se presenta un cambio en la dinámica de las detecciones, con cuatro familias registrando incrementos y una reconfiguración clara del panorama observado la semana anterior. **Tycoon 2FA** vuelve a destacar con un aumento significativo (de 2.309 a 3.336 detecciones), retomando una tendencia claramente ascendente y reafirmándose como la amenaza predominante a nivel nacional, especialmente asociada a la evasión de controles de identidad y el compromiso de autenticación multifactor. En paralelo, **EvilProxy** mantiene su crecimiento sostenido y **AsyncRAT** muestra un aumento moderado, mientras que **DCRat** registra un incremento proporcional relevante pese a su menor volumen absoluto, lo que sugiere mayor actividad de campañas de acceso remoto en fases iniciales. Por el contrario, se observan descensos en familias previamente destacadas como **Sneaky 2FA**, **XWorm**, **Mamba 2FA** y **Remcos**, lo que apunta a una posible rotación táctica o a la priorización de infraestructuras de phishing más efectivas durante la semana analizada. En conjunto, el comportamiento refuerza un escenario dinámico, con énfasis renovado en plataformas de phishing avanzado y malware orientado al acceso persistente.

Comparativa entre semanas

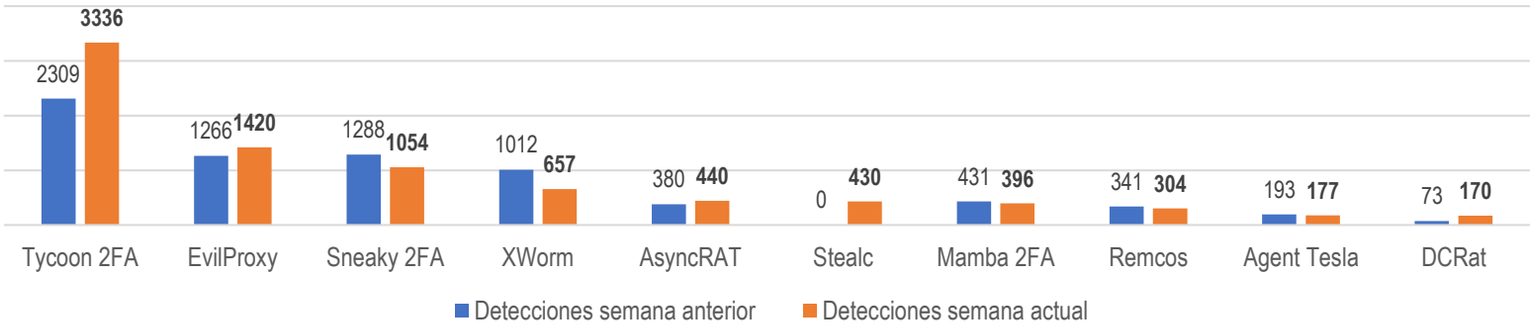

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la semana se registraron eventos relevantes de seguridad en distintos países de Latinoamérica, que confirman la continuidad del *ransomware* como amenaza dominante en la región, de acuerdo con reportes provenientes de fuentes abiertas. Los incidentes identificados evidencian una amplia diversidad de sectores impactados, incluyendo comercio, industria y turismo, educación, recursos minero-energéticos, alimentación y agricultura, así como transporte, con casos reportados en México, Brasil, Paraguay, Chile y Argentina. La dispersión geográfica y sectorial de los incidentes refuerza la tendencia de campañas oportunistas y dirigidas contra sectores clave para la economía regional, destacando la necesidad de mantener una postura de ciberseguridad reforzada y capacidades de respuesta alineadas con este tipo de amenazas de alto impacto.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Comercio, Industria, Turismo.	Ransomware	México	**Morpheus**
Educación	Ransomware	Brasil	**Incransom**
Recursos Minero-Energéticos	Ransomware	Paraguay	**Qilin**
Alimentacion y agricultura	Ransomware	Chile	**Qilin**
Transporte	Ransomware	Argentina	**Safepay**

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS
Fortinet FortiOS / FortiAnalyzer / FortiManager / FortiProxy / FortiWeb	**CVE-2026-24858**	Vulnerabilidad de omisión de autenticación que permite a un atacante con una cuenta FortiCloud válida y un dispositivo registrado iniciar sesión en otros dispositivos registrados sin pasar por los controles de autenticación esperados cuando FortiCloud SSO está habilitado, exponiendo múltiples productos Fortinet a accesos no autorizados.	**9.4 (Crítico)**
n8n	**CVE-2026-0863 / CVE-2026-1470**	Permite evasión de *sandbox* y ejecución remota de código en instancias de n8n debido a fallas en la validación de entrada y escape del entorno seguro, lo que puede conllevar al compromiso total de la instancia bajo condiciones específicas de ejecución de *workflows*.	**8.5-9.9 (Crítico)**
Biblioteca vm2 (Node.js)	**CVE-2026-22709**	Fallo de escape de *sandbox* en la biblioteca vm2 usada para ejecutar código JavaScript no confiable, que permite a un atacante evadir las restricciones del entorno *sandbox* y ejecutar código arbitrario en el sistema que lo aloja, representando un riesgo elevado para aplicaciones que dependen de esta biblioteca para aislamiento de código	**9.8 (Crítico)**

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

Actores y campañas activas

- **Incransom**: es un actor de *ransomware* identificado desde 2023, con actividad reciente en América Latina y foco recurrente en el sector educativo y organizaciones con infraestructuras expuestas. Opera bajo un esquema de doble extorsión, combinando cifrado de sistemas con la exfiltración de información sensible para aumentar la presión sobre las víctimas. **Incransom** suele apoyarse en vectores de acceso inicial de baja complejidad, como servicios remotos mal configurados, credenciales comprometidas y vulnerabilidades sin parchear, lo que le permite comprometer rápidamente entornos con niveles limitados de madurez en ciberseguridad. Su operativa prioriza la rapidez y el impacto reputacional, con publicación temprana de víctimas en sitios de filtración.

- **Safepay**: es un grupo de *ransomware* que ha ganado visibilidad desde 2024 alejarse del modelo *ransomware-as-a-service* (RaaS) y por ataques dirigidos contra infraestructuras críticas y sectores estratégicos, incluyendo transporte y logística. Este actor presenta un enfoque más selectivo en la identificación de objetivos, priorizando organizaciones con alta dependencia operativa de sus sistemas tecnológicos. **Safepay** combina técnicas de cifrado robusto con amenazas de divulgación de información, alineándose con modelos de doble extorsión, y muestra una mayor disciplina operativa en las fases de reconocimiento y preparación del ataque, lo que sugiere campañas más planificadas y orientadas a maximizar el impacto financiero y operativo de sus víctimas.

Recomendaciones

- Realizar los procesos de gestión de vulnerabilidades críticas, priorizando la aplicación de parches y medidas de mitigación en servicios expuestos a Internet. La atención oportuna a fallas de alta severidad reduce de forma significativa los riesgos de ejecución remota de código, escalamiento de privilegios y accesos iniciales utilizados como punto de entrada en campañas recientes.
- Reforzar los controles de identidad y autenticación mediante la adopción de mecanismos resistentes al *phishing*, como autenticación basada en llaves físicas, certificados o MFA adaptativo. Es clave complementar estos controles con monitoreo continuo de intentos de acceso anómalos, con el fin de mitigar el impacto de plataformas de phishing avanzadas y campañas orientadas a la captura de credenciales y tokens de sesión observadas durante el periodo analizado.
- Implementar principios de mínimo privilegio y revisión continua de cuentas, especialmente para usuarios administrativos y cuentas de servicio. La rotación de credenciales, la eliminación de accesos obsoletos y la auditoría de privilegios reducen significativamente la efectividad de campañas que abusan de credenciales comprometidas para movimiento lateral y persistencia.

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

Ransomware.live, 29 de enero de 2026, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/.
Any Run, 29 de enero de 2026, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/.
Technocio, 27 de enero de 2026, "Empresas enfrentan más de 2.800 ciberataques semanales", Portal de noticias.
https://www.technocio.com/empresas-enfrentan-mas-de-2-800-ciberataques-semanales/.
Noticias.red, 22 de enero de 2026, "Ataques cibernéticos: un riesgo que preocupa a CEOs en México y el resto de Latinoamérica, señala Incode", Portal de noticias.
https://noticias.red/2026/01/22/ataques-ciberneticos-un-riesgo-que-preocupa-a-ceos-en-mexico-y-el-resto-de-latam-senala-incode/.
SOS Ransomware, 21 de agosto de 2025, "INC Ransom: anatomía y soluciones para una gran amenaza", Blog de proveedor de ciberseguridad.
https://sosransomware.com/es/grupos-de-ransomware/inc-ransom-anatomia-y-soluciones-para-una-gran-amenaza-en-2025/.
SentinelOne, 22 de enero de 2025, "HellCat and Morpheus: Two brands, one payload as ransomware affiliates drop identical code", Blog de proveedor de ciberseguridad.
https://www.sentinelone.com/blog/hellcat-and-morpheus-two-brands-one-payload-as-ransomware-affiliates-drop-identical-code/.
Check Point, 2025, "SafePay Ransomware", Blog de proveedor de ciberseguridad.
https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/safepay-ransomware/.
NIST, 27 de enero de 2026, CVE-2026-24858, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-24858.
NIST, 18 de enero de 2026, CVE-2026-0863, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-0863.
NIST, 27 de enero de 2026, CVE-2026-1470, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-1470.
NIST, 26 de enero de 2026, CVE-2026-22709, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-22709.