Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS –20260116-021

TLP:CLEAR

Resumen Ejecutivo

Durante la semana analizada, el panorama de ciberseguridad en Colombia evidencia una intensificación relevante de los vectores de ataque dirigidos a la identidad digital y al acceso remoto. Amenazas como **Tycoon 2FA**, **EvilProxy** y **Sneaky 2FA** se consolidan como los principales riesgos, registrando incrementos significativos en su actividad frente al periodo anterior. Este comportamiento refleja campañas agresivas y sostenidas orientadas a la evasión de mecanismos de autenticación multifactor (MFA), orientadas al compromiso de credenciales corporativas. A este escenario se suma la aparición abrupta de **XWorm**, lo que sugiere un entorno de amenazas altamente dinámico, con actores enfocados tanto en el acceso inicial como en el establecimiento de persistencia dentro de redes organizacionales.

A nivel regional, el contexto en Latinoamérica confirma la persistencia y madurez de operaciones de *ransomware* dirigidas contra infraestructuras críticas. Grupos como **Nova**, **Devman** y **Anubis** han materializado incidentes en Venezuela, Brasil y Chile. La dispersión geográfica de estos ataques, junto con la diversidad de tácticas empleadas, evidencia una amenaza transversal y regional, reforzando la necesidad de fortalecer controles de segmentación, respaldo y monitoreo continuo para mitigar escenarios de doble extorsión.

Adicionalmente, la identificación de vulnerabilidades críticas marca un punto de atención prioritario en la gestión de riesgos de la semana. Fallos de alta severidad en **Node.js** y **SAP S/4HANA**, junto con una vulnerabilidad de escalamiento de privilegios en **Windows Admin Center para Azure**, subrayan el riesgo de interrupción de servicios y compromiso de entornos empresariales y en la nube. En conjunto, este panorama refuerza la necesidad urgente de priorizar la aplicación de parches en componentes expuestos, así como de incrementar el control sobre identidades privilegiadas, con el fin de reducir la probabilidad de compromisos iniciales y movimientos laterales.

Tendencias observadas

❑ **Consolidación de la IA como habilitador transversal con impacto directo en ciberseguridad:**

Publicaciones recientes destacan que en 2026 la inteligencia artificial evoluciona hacia un rol estructural dentro de los procesos organizacionales, integrándose en flujos de trabajo, toma de decisiones y automatización avanzada. Esta adopción generalizada amplía la superficie de riesgo digital, ya que el uso extensivo de IA sin una adecuada gobernanza, supervisión humana y control de datos puede derivar en nuevas exposiciones, errores operativos y vectores de abuso, obligando a las organizaciones a fortalecer capacidades de seguridad, control y gestión responsable de estas tecnologías emergentes.

❑ **Desarrollo de *malware* modular y marcos de amenazas en entornos de nube y contenedores:**

Nuevos marcos y familias de *malware* dirigidos específicamente a servidores en la nube y entornos de contenedores han sido identificados, ofreciendo capacidades modulares. Esto indica una evolución en la sofisticación de las amenazas, orientándose a entornos dinámicos y modernos de operación, donde la superficie de ataque se diversifica más allá de sistemas tradicionales.

❑ **Incremento de fraudes y estafas en temporadas comerciales específicas:**

Con el auge del comercio electrónico asociado a eventos como las rebajas de enero, se han intensificado las estafas dirigidas a consumidores que buscan ofertas, utilizando dominios fraudulentos o técnicas de suplantación para capturar credenciales y datos financieros. Este patrón de uso oportunista de períodos de alta actividad de usuarios demuestra la persistencia del fraude digital como vector relevante de amenazas.

Panorama nacional

Durante el periodo analizado se observa un incremento generalizado y significativo en la actividad maliciosa, con un énfasis marcado en técnicas orientadas a la evasión de controles de identidad y mecanismos de autenticación. En este contexto, **Tycoon 2FA** se consolida como la amenaza crítica de la semana, al escalar de 732 a 2.704 eventos, liderando el panorama de riesgo y evidenciando una actividad intensiva dirigida a eludir esquemas de autenticación multifactor.

De forma paralela, plataformas como **EvilProxy** y **Sneaky 2FA** presentan un fortalecimiento notable, duplicando su volumen de actividad, lo que refuerza la tendencia hacia campañas cada vez más estructuradas y accesibles para la captura de credenciales corporativas. Asimismo, se destaca el incremento abrupto en los reportes de **XWorm**, que alcanza 590 detecciones, posicionándose como la cuarta amenaza más relevante de la semana en Colombia y sugiriendo la existencia de una campaña activa o en fase de expansión.

Comparativa entre semanas

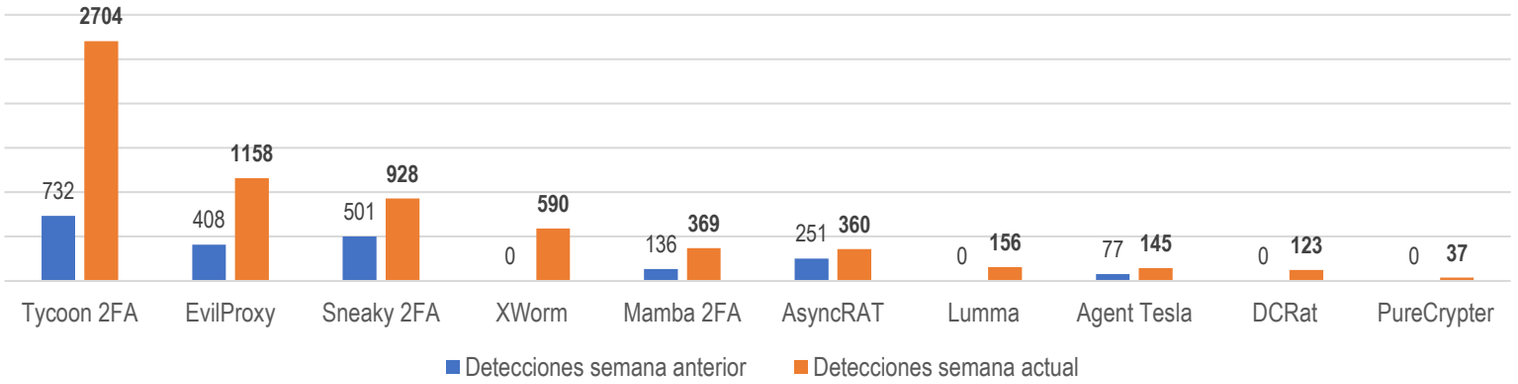


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

La siguiente tabla presenta una consolidación de incidentes de seguridad reportados en países de Latinoamérica durante el periodo analizado, a partir de información obtenida de fuentes abiertas. Los casos identificados a ataques de *ransomware*, con una afectación predominante en el sector de Recursos Minero-Energéticos, el cual ha sido impactado en Brasil y Chile por los actores **Devman** y **Anubis**, respectivamente. De igual forma, se registran incidentes en el sector de Tecnologías de la Información en Venezuela, atribuido al grupo **Nova**, y en el sector Educación en Perú, vinculado a **Qilin**. Esta dispersión geográfica y la variedad de actores involucrados evidencian una amenaza persistente y diversificada sobre infraestructuras críticas y servicios esenciales en la región, reforzando la necesidad de robustecer los controles de seguridad en industrias estratégicas frente a campañas de extorsión digital.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Tecnologías de la información y comunicaciones	Ransomware	Venezuela	Nova
Recursos Minero-Energéticos	Ransomware	Brasil	Devman
Recursos Minero-Energéticos	Ransomware	Chile	Anubis
Educación	Ransomware	Perú	Qilin

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS
Node.js	**CVE-2025-59466**	Problema con el modulo async_hooks que causa que errores de desbordamiento de pila no sean capturables, provocando un desbordamiento y denegación de servicio en servidores Node.js cuando se reciben entradas recursivas, afectando a múltiples *frameworks*.	**7.5 (Alto)**
SAP S/4HANA	**CVE-2026-0501**	Permite a un usuario autenticado ejecutar consultas SQL manipuladas para leer, modificar o borrar información alojada en la base de datos, comprometiendo confidencialidad, integridad y disponibilidad de la información.	**9.9 (Crítica)**
Windows Admin Center (Azure)	**CVE-2026-20965**	Permite que un atacante que ya ha accedido a una máquina virtual salte a otras partes de la red en la nube, con el potencial de tomar control de todo el entorno de Azure y suplantar a administradores para extraer datos sensibles.	**Aún sin publicar**

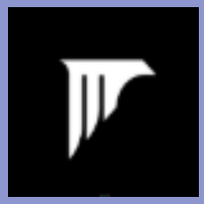
Tabla 2. Vulnerabilidades relevantes de la semana. Fuente: COLCERT.

Actores y campañas activas

- **Nova (anteriormente conocido como RALord):** es un grupo de *ransomware* emergente identificado en 2024 que opera como una evolución de la variante RALord. Se distingue por un enfoque altamente selectivo en lugar de campañas masivas, priorizando objetivos que combinan capacidad financiera con vulnerabilidad operativa crítica, como el sector salud y tecnológico. Nova emplea tácticas de doble extorsión y ha demostrado una rápida expansión global, comprometiendo víctimas en múltiples continentes mediante el abuso de servicios remotos expuestos y credenciales comprometidas.

- **Devman:** es un actor de amenazas observado desde mediados de 2025, vinculado técnicamente al linaje de grupos como DragonForce y Conti, de quienes recicla componentes de código para su *malware*. A diferencia del modelo RaaS tradicional, **Devman** opera bajo una estructura más cerrada y centralizada, ejecutando ataques directos con herramientas propias. Su modus operandi se destaca por la capacidad de propagación lateral sin necesidad de tráfico constante hacia un servidor de comando y control (C2), lo que le permite evadir sistemas de detección perimetral mientras cifra recursos de red local.

- **Anubis:** es un grupo de *ransomware* activo desde finales de 2024 que ha ganado notoriedad en 2025 por incorporar capacidades destructivas de tipo *wiper* (borrado permanente) junto a sus rutinas de cifrado. Este actor se enfoca en sectores de infraestructura, ingeniería y construcción, operando bajo un esquema que combina la exfiltración de datos para la venta con la amenaza de destrucción irreversible de la información. Anubis utiliza tácticas de presión agresiva, publicando artículos detallados sobre sus víctimas en foros y redes sociales para maximizar el daño reputacional y forzar el pago.



Recomendaciones

- Implementar controles de autenticación resistentes al *phishing* y monitoreo de identidad, priorizando el uso de llaves de seguridad físicas o autenticación basada en certificados en lugar de códigos SMS o push, para neutralizar la efectividad de plataformas de Phishing-as-a-Service como Tycoon 2FA y EvilProxy que buscan interceptar tokens de sesión.
- Priorizar la remediación urgente de vulnerabilidades críticas en infraestructura expuesta, aplicando los parches de seguridad liberados para Node.js, SAPSAP S/4HANA y Windows Admin Center (Azure), dado su alto potencial para causar denegación de servicio o permitir la toma de control total de entornos en la nube sin necesidad de credenciales previas.
- Intensificar la detección conductual en *endpoints* para bloquear *malware* modular, ajustando las reglas de EDR para identificar patrones de ejecución asociados a troyanos de acceso remoto como XWorm, tales como la manipulación de registros para persistencia, inyección en procesos legítimos y conexiones inusuales a puertos no estándar, frenando así las campañas de acceso remoto detectadas.
- Robustecer las estrategias de respaldo y recuperación ante amenazas de *ransomware*, asegurando la inmutabilidad de los *backups* y realizando simulacros de restauración en sectores críticos, para garantizar la continuidad operativa frente a actores destructivos como que operan activamente en la región.

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

Ransomware.live, 15 de enero de 2026, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/.
Any Run, 8 de enero de 2026, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/.
CincoDias, 14 de enero de 2026, "Las ciberestafas más comunes en rebajas y cómo evitarlas". Portal de noticias.
https://cincodias.elpais.com/smartlife/lifestyle/2026-01-14/las-ciberestafas-mas-comunes-en-rebajas-y-como-evitarlas.html.
Cyware, 14 de enero de 2026, "Daily Threat Intelligence".
https://www.cyware.com/resources/threat-briefings/daily-threat-briefing/cyware-daily-threat-intelligence-january-14-2026.
El Tiempo, 11 de enero de 2026 "Las tendencias en IA para el 2026", Portal de noticias.
https://www.eltiempo.com/tecnosfera/novedades-tecnologia/las-tendencias-en-ia-para-el-2026-que-usted-debe-estudiar-y-aprender-3523555.
The Hacker News, 14 de enero de 2026, "Critical Node.Js Vulnerability Can Cause Server Crashes via async_hooks Stack Overflow".
https://thehackernews.com/2026/01/critical-nodejs-vulnerability-can-cause.html.
Node.js, 13 de enero de 2026, "Mitigatin denial-of-service vulnerability", Blog oficial de proveedor.
https://nodejs.org/en/blog/vulnerability/january-2026-dos-mitigation-async-hooks.
NIST, 12 de enero de 2026, CVE-2026-0501, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-0501.
NIST, 13 de enero de 2025, CVE-2026-20965, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-20965.