Reporte

Semanal

Inteligencia de amenaza cibernéticas

COLCERT -20260227- 026

TIC

TLP:CLEAR

Resumen Ejecutivo

Durante la semana, el panorama de amenazas evidenció una actividad sostenida de actores vinculados principalmente a campañas de *phishing*, capturas de credenciales y *malware* de acceso remoto, manteniendo una presión constante sobre organizaciones de distintos sectores. Aunque se observó una leve disminución en algunas familias predominantes como **Tycoon 2FA** y **EvilProxy**, el incremento en detecciones asociadas a herramientas como **AsyncRAT**, **XWorm**, **DCRat**, además de la reaparición de **Quasar** y **Stealc** reflejan una diversificación táctica orientada al compromiso de identidades y al acceso persistente a entornos corporativos.

A nivel regional, el *ransomware* continúa posicionándose como la amenaza de mayor impacto, con actividad atribuida a grupos como **Qilin** y **LockBit5**, además de actores emergentes como **Vect**, bajo esquemas de doble extorsión que combinan cifrado y filtración de datos. Asimismo, se identificaron incidentes de exfiltración y campañas de defacement, lo que confirma que la presión no se limita a la indisponibilidad operativa, sino también al daño reputacional y la exposición de información sensible.

En paralelo, la explotación activa de vulnerabilidades críticas y la evolución en la gestión de riesgos tecnológicos refuerzan la necesidad de adoptar enfoques preventivos y estratégicos de ciberseguridad. El entorno actual exige fortalecer controles de identidad, monitoreo continuo, segmentación de red y capacidad de respuesta ante incidentes, considerando que la amenaza se mantiene dinámica, distribuida y con creciente grado de especialización.

Tendencias observadas

- **Consolidación del almacenamiento en la nube como objetivo creciente del fraude digital:** el uso del almacenamiento en la nube se ha masificado en Colombia hasta convertirse en el repositorio principal de información personal y corporativa, donde ya no solo se guardan fotografías o archivos básicos, sino documentos sensibles, credenciales y datos financieros. Se estima que cerca del 67 % de los usuarios respalda la información de sus dispositivos en servicios online, lo que evidencia una creciente dependencia de estos entornos digitales. Esta adopción acelerada ha incrementado su atractivo para los ciberdelincuentes, quienes explotan configuraciones inseguras, contraseñas débiles y campañas de *phishing* para comprometer cuentas y acceder a grandes volúmenes de información.

- **Evolución en la gestión de vulnerabilidades:** el aumento exponencial de vulnerabilidades y la velocidad con la que estas son explotadas está impulsando una transformación en su gestión, expertos prevén que en 2026 evolucionará hacia modelos automatizados e inteligentes orientados al riesgo, integrando capacidades para evaluar el impacto real de las vulnerabilidades, priorizar su remediación, desplegar parches de forma automática y verificar su eficacia, reduciendo significativamente el tiempo de exposición. En este contexto, la gestión de vulnerabilidades se consolida como un proceso continuo y estratégico, enfocado en anticipar la explotación y fortalecer la resiliencia operativa frente a amenazas cada vez más dinámicas.

Panorama nacional

Durante la semana evaluada se observó un comportamiento mixto en el volumen de detecciones frente al periodo anterior. Si bien **Tycoon 2FA** y **EvilProxy** continúan liderando el panorama, ambos registraron una ligera disminución en sus cifras, lo que podría indicar una estabilización temporal de su actividad. En contraste, amenazas como **Sneaky 2FA**, **DCRat**, **XWorm** y **AsyncRAT** presentaron incrementos moderados, evidenciando una mayor diversificación en las técnicas de acceso inicial y control remoto. Llama especialmente la atención la reaparición de **Quasar** y **Stealc**, que no habían mostrado actividad la semana anterior y ahora registran un número significativo de detecciones, lo que sugiere posibles nuevas campañas en curso. En términos generales, aunque se reduce levemente la presión de los principales kits de *phishing*, se mantiene una dinámica activa en el ecosistema de *malware* y herramientas de acceso remoto.

Comparativa entre semanas

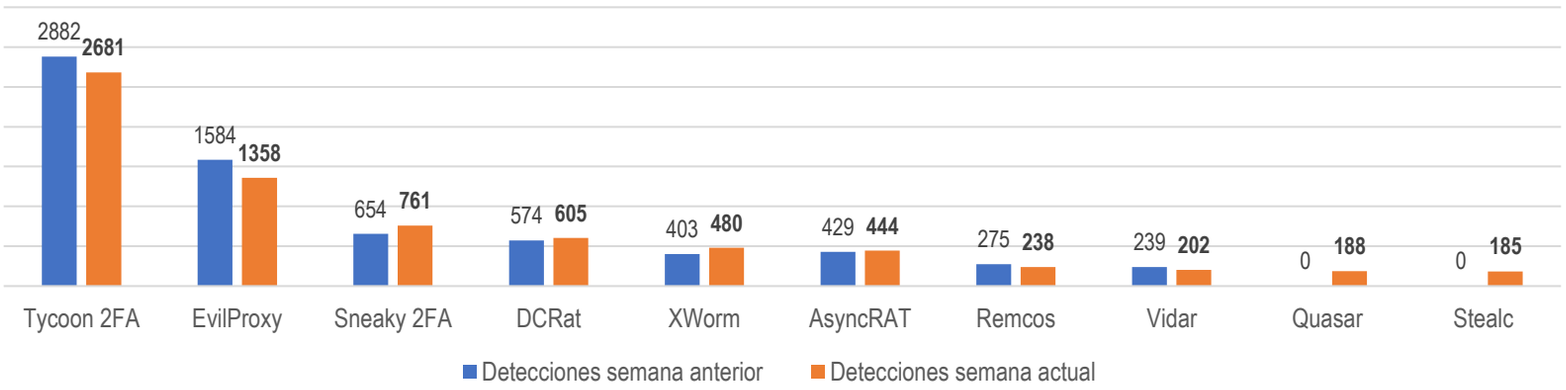

Gráfico 1. *Detecciones visualizadas. Fuente AnyRun.*

Panorama regional

Durante el periodo analizado, el panorama regional confirmó la persistencia del *ransomware* como la amenaza predominante en América Latina, impactando sectores estratégicos para la estabilidad económica y social. Los incidentes se concentraron principalmente en **Alimentación y Agricultura**, **Comercio**, **Industria y Turismo**, **Salud y Protección Social, Educación** y **Recursos Minero-Energéticos**, con eventos registrados en Brasil, Chile, Argentina, República Dominicana y México. Se destacó la actividad del grupo **Thegentlemen**, que mostró una fuerte focalización en la región, junto con operaciones atribuidas a **Lynx**, **Qilin** y **Lockbit5**, evidenciando un ecosistema criminal diverso y activo.

Adicionalmente, se identificaron incidentes de exfiltración de datos del sector financiero y educación que afectó a usuarios en Venezuela, atribuidos al actor **malconguerra2**, así como una campaña de defacement dirigida al sector gubernamental en Uruguay, vinculada al grupo **CyberTeam**. Estos eventos reflejan que, además del *ransomware*, persisten amenazas orientadas a la captura de información sensible y a la afectación reputacional de entidades públicas.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Alimentación y Agricultura	Ransomware	**Brasil**	Thegentlemen
Tecnologías de la información y comunicaciones	Ransomware	**Brasil**	Vect
Financiero	Ransomware	**Brasil**	Vect
Alimentación y Agricultura	Ransomware	**Chile**	Qilin
Comercio, Industria y Turismo	Ransomware	**Chile**	Lynx
Salud y Protección Social	Ransomware	**Chile**	Lockbit5

Sector afectado	Amenaza	Locación	Posible actor involucrado
Financiero	Exfiltración	**Venezuela**	malconguerra2
Educación	Exfiltración	**Venezuela**	malconguerra2
Gobierno	Defacement	**Uruguay**	CyberTeam
Comercio, Industria y Turismo	Ransomware	**Argentina**	Thegentlemen
Educación	Ransomware	**Argentina**	ShadowByt3$
Comercio, Industria y Turismo	Ransomware	**República Dominicana**	Thegentlemen
Recursos Minero-Energéticos	Ransomware	**México**	Qilin

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS
Cisco Catalyst SD-WAN Controller	**CVE-2026-20127**	Vulnerabilidad actualmente explotada que provoca una autenticación inadecuada y permite a un atacante remoto eludir los mecanismos de verificación y obtener privilegios administrativos sobre los sistemas **Cisco Catalyst SD-WAN** afectados.	**10.0 (Crítica)**

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

Actores y campañas activas

- **ShadowByt3$:** el actor **ShadowByt3$** es un grupo emergente vinculado a operaciones de *ransomware* y filtración de datos que ha comenzado a aparecer en plataformas de monitoreo de incidentes durante febrero de 2026. Su actividad se caracteriza por un modelo de doble extorsión. Por medio de su blog de exfiltraciones se atribuyeron el ataque contra la Universidad del Museo Social Argentino (UMSA), donde el grupo habría divulgado información extraída como mecanismo de presión, evidenciando su interés en objetivos de américa latina.

ShadowByt3$

- **Vect:** Se trata de un grupo emergente de *ransomware* que opera bajo el modelo *Ransomware-as-a-Service* (RaaS) y ha ganado visibilidad desde finales del 2025, apoyándose en la red de Tor para exfiltrar la información sensible antes del cifrado y así generar presión en las víctimas. Sus campañas a nivel global han afectado organizaciones en distintos sectores, evidenciando un enfoque oportunista orientado a entidades con alta dependencia operativa y exposición de datos.

VECT RANSOMWARE

Recomendaciones

- Endurecer políticas de autenticación reforzando controles y revisando configuraciones de proveedores de identidad.
- Implementar listas de control de aplicaciones (application whitelisting) para limitar la ejecución de herramientas no autorizadas como RATs y *stealers*.
- Supervisar activamente conexiones salientes hacia dominios y direcciones IP recién creadas o de baja reputación.
- Bloquear la descarga y ejecución automática de archivos adjuntos en correos electrónicos con macros o scripts embebidos.
- Realizar ejercicios de simulación de *phishing* enfocados en técnicas de adversary-in-the-middle (AiTM).
- Asegurar que las soluciones EDR cuenten con políticas específicas para detectar comportamiento asociado a *loaders* y troyanos bancarios.
- Mantener inventarios actualizados de activos expuestos a internet y verificar que no existan servicios innecesarios publicados.

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

Ransomware.live, 26 de enero de 2026, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 26 de enero de 2026, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
Noticias RCN, 20 de febrero de 2026, "La nube domina el almacenamiento en Colombia", Portal de noticias colombiano.
https://www.noticiasrcn.com/tendencias/nube-almacenamiento-claves-evitar-fraudes-993964.
IT User, 26 de febrero de 2026, "Cinco tendencias que transformarán la gestión de vulnerabilidades en 2026", Portal de noticias de tecnología.
https://www.ituser.es/seguridad/2026/02/cinco-tendencias-que-transformaran-la-gestion-de-vulnerabilidades-en-2026.
Halcyon, 3 de febrero de 2026, "Emerging Ransomware Group: Vect", Blog de proveedor de ciberseguridad.
https://www.halcyon.ai/ransomware-alerts/emerging-ransomware-group-vect
Hookphish 25 de febrero de 2026, "Ransomware Group ShadowByt3$ Hits: UMSA", Blog de proveedor de ciberseguridad.
https://www.hookphish.com/blog/ransomware-group-shadowbyt3-hits-umsa/
Cisco, 25 de febrero de 2026, "Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability" , Comunicado sobre vulnerabilidad oficial de Cisco.
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
CVE, 25 de febrero de 2026, CVE-2026-20127, Base de datos oficial de vulnerabilidades.
https://www.cve.org/CVERecord?id=CVE-2026-20127