Reporte

Semanal

Inteligencia de amenaza cibernéticas

COLCERT RS -20260220 - 025

TLP:CLEAR

Resumen Ejecutivo

Durante la semana, el panorama de ciberseguridad en Colombia y la región mostró un incremento en la actividad maliciosa orientada al compromiso de identidades digitales y al acceso inicial a entornos corporativos. A nivel nacional, **Tycoon 2FA** y **EvilProxy** nuevamente lideraron las detecciones, consolidando la tendencia de campañas de *phishing* avanzado y técnicas de para evadir la autenticación multifactor, mientras el repunte de **DCRat** y la aparición de **Vidar** y **Mamba 2FA** evidencian diversificación en herramientas de acceso remoto y robo de credenciales.

En el ámbito regional, el *ransomware* continúa siendo la principal amenaza para sectores estratégicos, con actividad atribuida a grupos emergentes como **Payload** y **SpaceBears**, además de grupos altamente activos como **Qilin,** Quienes se orientan a la interrupción operativa y extorsión financiera. Paralelamente, incidentes de *defacement* contra entidades gubernamentales y educativas reflejan la persistencia de actores enfocados en impacto reputacional.

Adicionalmente, se destacaron vulnerabilidades críticas con potencial de compromiso total de sistemas, incluyendo fallas en integraciones de mensajería empresarial, plataformas de recuperación de datos y aplicaciones de uso cotidiano, lo que refuerza la necesidad de una gestión de parches oportuna y controles de acceso robustos. En conjunto, el entorno de amenazas evidencia una convergencia entre motivaciones económicas, espionaje y presión reputacional, con foco creciente en la explotación de identidades y servicios expuestos.

Tendencias observadas

- **Formación especializada en IA y ciberseguridad como prioridad nacional**: la creación de un centro de excelencia en IA en Colombia orientado a certificar arquitectos de IA, científicos de datos y especialistas en ciberseguridad refleja una tendencia creciente hacia el fortalecimiento del talento avanzado y la cooperación academia-empresa para cerrar brechas de capacidades y preparar profesionales frente a amenazas digitales cada vez más sofisticadas.

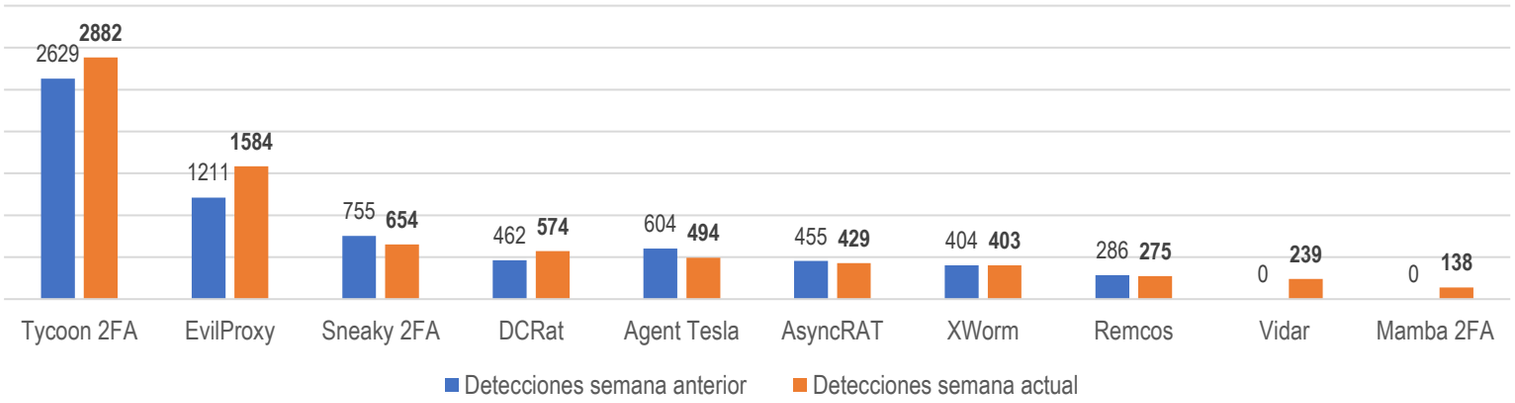
- **Expansión de la superficie de ataque y cambio hacia modelos Zero Trust:** la acelerada digitalización y la interconexión de infraestructuras críticas en Latinoamérica están ampliando los vectores de ataque, impulsando la adopción de enfoques como Zero Trust, automatización con IA y resiliencia organizacional para enfrentar amenazas cada vez más sofisticadas y persistentes.

- **Soberanía digital y reducción de dependencia tecnológica:** expertos advierten sobre los riesgos de privacidad, jurisdicción y acceso a datos asociados al uso de plataformas como WhatsApp y Gmail, impulsando el debate sobre migrar hacia soluciones que garanticen mayor control sobre la información, cumplimiento normativo y resiliencia frente a presiones geopolíticas.

Panorama nacional

Durante la semana, el panorama de detecciones en Colombia muestra un incremento general en la actividad maliciosa, liderado nuevamente por **Tycoon 2FA**, que aumentó de 2.629 a 2.882 detecciones y se mantiene como la principal amenaza asociada a campañas de phishing y evasión de autenticación multifactor. También se observa un crecimiento relevante de **EvilProxy**, que pasó de 1.211 a 1.584 eventos. En contraste, amenazas como **Sneaky 2FA** y **Agent Tesla** registraron una disminución moderada, mientras **DCRat** mostró un aumento. Se destaca además la aparición de **Vidar** y **Mamba 2FA** en el panorama actual, lo que sugiere diversificación en herramientas. En conjunto, los datos reflejan una persistente priorización de ataques contra identidades digitales y acceso a servicios corporativos.

Comparativa entre semanas



Panorama regional

El panorama regional durante la semana evidenció una alta prevalencia del ransomware como principal amenaza en América Latina, afectando sectores estratégicos como comercio, transporte y TIC en México, Brasil y Chile, lo que confirma la continuidad de campañas orientadas a la interrupción operativa y la extorsión financiera. La presencia de grupos emergentes como **Payload**, además de actores como **SpaceBears** y **Qilin** sugiere una actividad diversificada de actores criminales que aprovechan vulnerabilidades y accesos expuestos en infraestructuras críticas y servicios digitales. Paralelamente, los incidentes de defacement en entidades gubernamentales y del sector educativo en Perú y Brasil, atribuidos a **chinahfans**, reflejan un componente orientado al impacto reputacional y simbólico. En conjunto, la región enfrenta un entorno de amenazas mixtas donde convergen motivaciones económicas y de influencia, con impactos potenciales en la continuidad operativa y la confianza institucional.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Comercio, industria y turismo	Ransomware	**México**	Payload
Transporte	Ransomware	**Brasil**	Spacebears
Tecnologías de la información y comunicaciones (TIC)	Ransomware	**Chile**	Qilin
Gobierno/Estado	Defacement	**Perú**	chinafans
Educación	Defacement	**Brasil**	chinafans

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS
WhatsApp bridge de Nanobot	CVE-2026-2577	Vulnerabilidad causada por la falta de autenticación del componente WhatsApp bridge de Nanobot. Un atacante remoto con acceso a la red puede conectarse al servidor WebSocket expuesto y secuestrar la sesión de WhatsApp, lo que le permitirá enviar mensajes suplantando al usuario e interceptar conversaciones y archivos adjuntos en tiempo real.	**10.0 (Crítico)**
Dell RecoverPoint for Virtual Machines	CVE-2026-22769	Vulnerabilidad de credenciales embebidas, un atacante remoto no autenticado puede usar estas credenciales para obtener acceso total al sistema operativo subyacente y persistencia con privilegios.	**10.0 (Crítico)**
Aplicación de bloc de notas de Windows.	CVE-2026-20841	Afecta al Bloc de notas al procesar archivos Markdown (.md) especialmente manipulados. Permite la Ejecución Remota de Código (RCE) si el usuario hace clic en un enlace malicioso dentro del archivo, ejecutando comandos con los privilegios del usuario	**7.8 (Alto)**

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

Actores y campañas activas

- **0APT:** el grupo emergente **0APT** se presenta como una operación *Ransomware-as-a-Service* (RaaS) con sitio de filtraciones y listas masivas de víctimas, pero múltiples análisis indican que publica datos falsos o generados artificialmente y evidencia manipulada para aparentar brechas reales. Su estrategia consiste en crear presión reputacional y psicológica mediante la amenaza pública de filtraciones, archivos "prueba" corruptos o con datos aleatorios y listados inflados de organizaciones, buscando pagos sin haber comprometido sistemas.

- **Payload:** el *ransomware* **Payload** ha sido identificado como una operación que emerge en febrero de 2026, que combina cifrado de sistemas con extracción previa de información para extorsión doble, apoyándose en accesos iniciales mediante credenciales comprometidas, explotación de servicios expuestos y herramientas legítimas del sistema para evadir detección. Su modelo operativo refleja la evolución del ecosistema RaaS, priorizando rapidez de despliegue, presión reputacional y monetización mediante filtración de datos.

Recomendaciones

- Implementar FIDO2/passkeys o autenticación resistente al phishing para accesos críticos. Restringir accesos desde dispositivos no gestionados y aplicar evaluación continua de sesión.
- Deshabilitar almacenamiento de contraseñas en navegadores corporativos.
- Forzar reautenticación y revocación de sesiones ante indicios de compromiso.
- Verificar que los respaldos estén aislados, inmutables y probados periódicamente.
- Evaluar el uso seguro de IA en procesos internos y definir controles de protección de datos.
- Fortalecer capacidades internas mediante capacitación especializada y ejercicios prácticos.

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

Ransomware.live, 19 de enero de 2026, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/.

Any Run, 19 de enero de 2026, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/.

Infobae, 17 de febrero de 2026, "Crean centro de inteligencia artificial para formar expertos en ciberseguridad, arquitectos en IA y más en Colombia", Portal de noticias de latino américa.
https://www.infobae.com/tecno/2026/02/17/crean-centro-de-inteligencia-artificial-para-formar-expertos-en-ciberseguridad-arquitectos-de-ia-y-mas-en-colombia/.

Noticias RCN, 17 de febrero de 2026, "Asi pinta la ciberseguridad en Latinoamérica para 2026", Portal de noticias colombiano.
https://www.noticiasrcn.com/opinion/enrique-fenollosa-1987/asi-pinta-la-ciberseguridad-en-latinoamerica-para-2026-992590.

El Economista, 17 de febrero de 2026, "Adiós a WhatsApp y Gmail: por qué este experto en ciberseguridad dice que es crucial pasarnos a opciones europeas", Portal de noticias.
https://www.eleconomista.es/tecnologia/noticias/13781898/02/26/adios-a-whatsapp-y-gmail-por-que-este-experto-en-ciberseguridad-dice-que-es-crucial-pasarnos-a-opciones-europeas.html.

The Hacker News, 18 de febrero de 2026, "Dell RecoveryPoint for VMs Zero-day CVE", Portal de noticias de ciberseguridad.
https://thehackernews.com/2026/02/dell-recoverpoint-for-vms-zero-day-cve.html.

NIST, 17 de febrero de 2026, CVE-2026-22769, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-22769.

NIST, 17 de febrero de 2026, CVE-2026-20841, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-2577.

NIST, 12 de febrero de 2026, CVE-2026-20841, Base de datos oficial de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2026-20841.