Reporte

Semanal

Inteligencia de amenaza cibernéticas

COLCERT -20260320- 028

TIC

TLP:CLEAR

Resumen Ejecutivo

Durante la semana analizada, el panorama de amenazas en Colombia y la región mostró una dinámica intensa, a nivel técnico, se evidenció una evolución en las herramientas de acceso remoto y exfiltración; mientras que vectores de evasión de **MFA** como **Tycoon 2FA** mostraron fluctuaciones, familias de malware como **Agent Tesla**, **Remcos** y **AsyncRAT** mantuvieron una tendencia al alza.

El ámbito regional refleja que se encuentra bajo una presión cibernética sin precedentes en donde grupos de ransomware están realizando explotación de brechas estructurales dada la digitalización acelerada de los países. Es así como reportes recientes muestran actores como Qilin y TheGentleman que vienen operando en paralelo en el cono sur realizando afectaciones en sectores de salud, energía y agroindustria respecto a ataques de ransomware de gran escala en lo que va de 2026.

Finalmente, durante la semana se destacaron vulnerabilidades críticas con un alto potencial de compromiso sistémico. Sobresale el CVE-2025-68613 en n8n, con un puntaje CVSS de 9.9, que permite la ejecución remota de código (RCE) y el control total de la instancia debido a fallos en la evaluación de expresiones. Asimismo, se reportaron fallas de alta severidad (CVSS 8.8) incluidas en el catálogo de CISA, como el CVE-2026-3909 en Google Chrome, relacionado con escritura fuera de límites en el componente Skia, y el CVE-2026-20963 en Microsoft Office SharePoint, que facilita la ejecución remota mediante la deserialización de datos no confiables. Estos hallazgos refuerzan la importancia de aplicar parches de seguridad de forma inmediata, restringir el acceso a interfaces críticas y fortalecer los mecanismos de monitoreo para neutralizar posibles intentos de explotación en entornos corporativos y de usuario final.

Tendencias observadas

Copa América de Ciberseguridad de la OEA: Colombia consolida su liderazgo regional tras participar en la Copa América de Ciberseguridad 2026 de la OEA, celebrada este 18 de marzo. El país, representado por expertos de sus equipos de respuesta (CSIRT), enfrentó desafíos técnicos en áreas críticas como forense digital y criptografía durante una sesión intensiva de ocho horas. Esta participación, que ocurre en el marco de la reciente gestión de incidentes en entidades públicas nacionales, no solo valida las capacidades tácticas del talento local frente a amenazas transnacionales, sino que abre una etapa de cooperación técnica reforzada con otros Estados miembros para fortalecer la resiliencia digital en todo el continente.

Panorama nacional

El monitoreo de esta semana revela una dinámica de amenazas en constante transformación. Aunque **Tycoon 2FA** se mantiene como el vector con mayor volumen de registros pese a una ligera contracción, el panorama general muestra un repunte significativo en la mayoría de las herramientas analizadas. Destaca especialmente el crecimiento de **EvilProxy**, que junto con **Sneaky 2FA**, refuerza la persistencia de tácticas diseñadas para comprometer entornos con autenticación de doble factor. Por otro lado, se hace evidente una tendencia al alza en el uso de troyanos y recolectores de información. El incremento en las detecciones de **AsyncRAT**, **XWorm**, **Agent Tesla** y **Stealc** sugiere que los atacantes están intensificando sus esfuerzos en campañas de acceso remoto y exfiltración de datos sensibles. En conclusión, mientras que herramientas específicas como **DCRat** mostraron un leve retroceso, el fortalecimiento de las familias de malware **infostealer** y **RATs** mantiene el nivel de riesgo en una zona crítica, obligando a una vigilancia constante sobre estos vectores de intrusión.

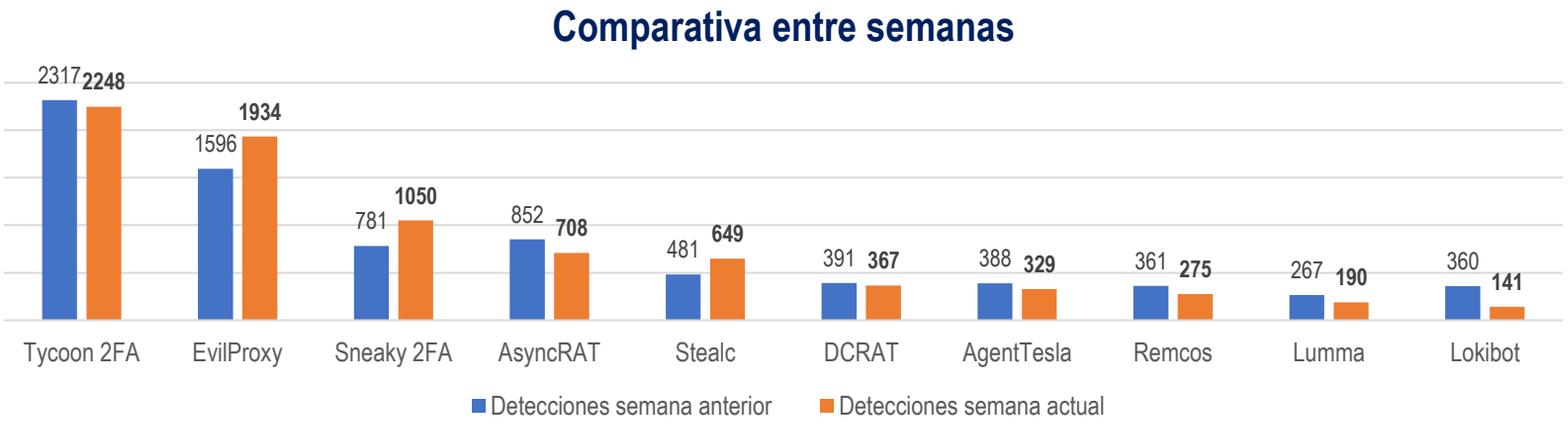

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante el periodo evaluado, el ecosistema de ciberamenazas en América Latina **se caracterizó por la poca información disponible de incidentes de Ransomware a nivel regional,** donde destaca nuevamente Qilin como uno de los actores de amenaza involucrado con una entidad colombiana. Por otro lado, Killsec y Payload han atacado a sectores de salud y gobierno en Brasil y México.

En Colombia nuevamente el actor de amenaza NixarGroup ha generado múltiples publicaciones de datos con millones de registros que pueden ser sensibles ya que contienen información de entidades de salud.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Salud	Ransomware	Brasil	Killsec
Gobierno	Ransomware	Colombia	Qilin
Gobierno	Ransomware	México	Payload
Salud	Data Leak	Colombia	Nyxar Group

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS
N8N	CVE-2025-68613	Vulnerabilidad crítica de ejecución remota de código (RCE) en n8n que permite a usuarios autenticados ejecutar código arbitrario debido a un aislamiento insuficiente en el sistema de evaluación de expresiones de flujos de trabajo (CWE-94). La explotación requiere autenticación previa y puede ser desencadenada durante la configuración de flujos de trabajo, otorgando al atacante los mismos privilegios del proceso n8n para comprometer totalmente la instancia, acceder a datos sensibles y ejecutar operaciones a nivel de sistema.	**9.9 (Crítica)**
Google Chrome	CVE-2026-3909	Vulnerabilidad de escritura fuera de límites en el componente Skia de Google Chrome que permite a un atacante remoto ejecutar código arbitrario mediante una página HTML manipulada. La explotación requiere interacción del usuario (visitar la página maliciosa) y puede comprometer totalmente la confidencialidad, integridad y disponibilidad del sistema. Catalogada como de alta severidad (CVSS 8.8) e incluida en el catálogo de vulnerabilidades explotadas conocidas de CISA.	**8.8 (Crítica)**
Microsoft Office SharePoint	CVE-2026-20963	Vulnerabilidad de deserialización de datos no confiables en Microsoft Office SharePoint que permite a un atacante autenticado ejecutar código de forma remota en la red. La explotación requiere autenticación previa en el sistema y puede comprometer totalmente la confidencialidad, integridad y disponibilidad de los datos. Catalogada como de alta severidad (CVSS 8.8) e incluida en el catálogo de vulnerabilidades explotadas conocidas de CISA.	**8.8 (Crítica)**

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

Actores y campañas activas

Durante las últimas dos semanas de marzo de 2026, el ecosistema de ciberamenazas en Colombia ha registrado el surgimiento y rápida consolidación de NyxarGroup. Este actor de amenazas se ha posicionado como una pieza crítica en el panorama de la exfiltración de datos tras ejecutar una serie de ataques dirigidos contra la infraestructura digital de múltiples entidades de salud, logrando un impacto mediático y técnico sin precedentes en foros clandestinos.

El actor no solo se limita a la extracción de datos, sino que gestiona una estrategia de comercialización activa en XSSF y XForums, dos de los mercados negros (underground) con mayor reputación en la comunidad de habla hispana y global. En estos espacios, el grupo publica "muestras" de las bases de datos para validar la autenticidad de la información ante posibles compradores. Los precios de venta, que oscilan entre 100 y 500 dólares (generalmente transaccionados en criptoactivos como Monero o Bitcoin), sugieren un modelo de negocio de "volumen", donde buscan ventas rápidas múltiples de sets de datos específicos en lugar de una única subasta masiva.

Recomendaciones

- Prioriza el uso de llaves físicas de seguridad (estándar FIDO2) o autenticación biométrica, ya que son mucho más resistentes a los ataques de interceptación que los códigos por SMS o notificaciones push tradicionales.
- Implementar planes de trabajo para gestionar las vulnerabilidades de la infraestructura tecnológica, con el fin de garantizar el cierre oportuno de brechas y prevenir la explotación de vulnerabilidades conocidas por parte de actores maliciosos.
- Aplicar de forma inmediata los parches de seguridad para navegadores y plataformas de colaboración. En el caso de Microsoft SharePoint, asegurar de restringir los privilegios de usuarios autenticados para minimizar el radio de impacto de una posible ejecución remota de código (RCE).
- Verificar la configuración de las plataformas que exponen servicios hacia internet, con el fin de identificar malas prácticas de gestión o configuraciones técnicas inadecuadas que puedan facilitar el acceso no autorizado a información sensible o ser utilizadas como punto de entrada para alcanzar servicios críticos.
- Ejecutar simulacros de phishing que imiten las tácticas actuales (como el uso de información de citas médicas reales filtradas) para entrenar a los empleados y ciudadanos en la identificación de comunicaciones fraudulentas altamente personalizadas.

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

Ransomware.live, 6 de marzo de 2026, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/.
Any Run, 6 de marzo de 2026, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/.
Segurilatam, 23 de febrero de 2026, La OEA presenta la primera edición de la Copa América de Ciberseguridad, Prensa especializada en seguridad.
https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/la-oea-presenta-la-primera-edicion-de-la-copa-america-de-ciberseguridad_20260223.html
Organización de los Estados Americanos (OEA), 18 de marzo de 2026, Calendario de Eventos: OAS Cyber Americas Cup, Organismo internacional oficial.
https://www.oas.org/ext/es/principal/calendario/evento/id/1465
Tenable, Marzo 2026, 19 de Marzo de 2026, CVE-2025-68613: n8n Remote Code Execution Vulnerability, Base de datos técnica de vulnerabilidades.
https://www.tenable.com/cve/CVE-2025-68613
Google Chrome Releases, 12 de marzo de 2026, Stable Channel Update for Desktop (CVE-2026-3909), Blog oficial de actualizaciones de software.
https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_12.html
Enigma Security, 19 de marzo de 2026, La CISA alerta sobre la explotación activa de una vulnerabilidad en Microsoft SharePoint (CVE-2026-20963), Blog de investigación y análisis de seguridad.
https://enigmasecurity.cl/cve-632/