Resumen Ejecutivo

Durante la primera semana de agosto de 2025, se evidenció un aumento en las tendencias de ciberataques registrados. Grupos de ransomware como Qilin y Sarcoma intensificaron sus campañas, del mismo modo, el grupo hacktivista DefacePerú lanzó una serie de ataques contra el Estado colombiano en medio de la actual coyuntura política, es probable que los objetivos de los atacantes se centren en entidades públicas. Acorde con esta situación de amenaza identificada por estos actores principalmente, se insta a las organizaciones a que prioricen la aplicación de parches de seguridad, refuercen sus respaldos y controles de acceso, y mantengan una vigilancia proactiva para reducir el riesgo de interrupciones operativas, pérdida de información sensible y afectaciones a la reputación institucional.

Tendencias nacionales

- El **phishing** sigue siendo una de las amenazas más relevantes, las campañas de ingeniería social representan un vector de entrada para todo tipo de ataques contra entidades públicas y privadas. Se evidencia una necesidad para fortalecer planes recuperación y respaldo ante ataques de tipo *ransomware*, especialmente en sectores críticos como salud y gobierno.
- Se observó un incremento en detecciones de ataques mediante troyanos de acceso remoto (RAT) como **AsyncRAT** y **Remcos RAT**, distribuidos a través de campañas de phishing.

Los sectores más vulnerables ante este tipo de ataques son gobierno, financiero y servicios públicos críticos, pues para los ciberdelincuentes representan objetivos de alto valor tanto por la confidencialidad de los datos manejados, como por su rol estratégico en la prestación de servicios a los colombianos.

Panorama nacional

Durante la última semana se observaron detecciones de **Tycoon 2FA** y **EvilProxy,** los cuales siguen destacándose como los kits de phishing más activos, representando la mayor parte de los incidentes detectados. Herramientas como **Agent Tesla** y **AsyncRAT** mantienen una presencia sostenida, aunque con fluctuaciones leves frente a la semana anterior. Se mantiene activa la distribución de troyanos de acceso remoto (RAT) y malware de captura de credenciales (Stealer), afectando principalmente sectores que dependen de autenticación remota o servicios en la nube. En síntesis, el panorama evidencia una diversificación de vectores y una continuidad en campañas dirigidas, con énfasis en el abuso de mecanismos de autenticación multifactor y técnicas avanzadas de phishing.

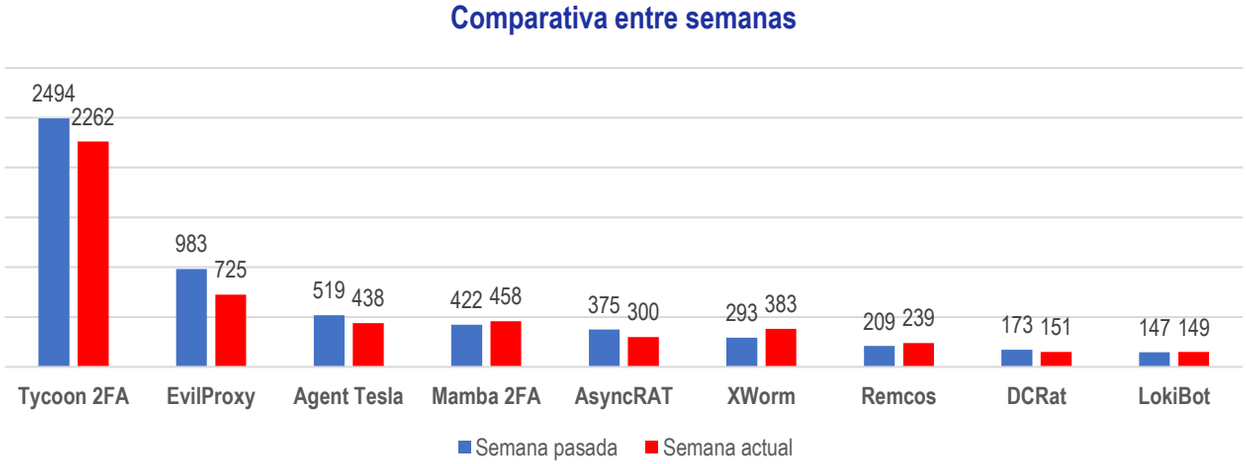

Gráfico 1. Detecciones visualizadas. Fuente AnyRun

Se identificaron incidentes de ciberseguridad relevantes a nivel nacional que afectaron a sectores estratégicos del país. En particular, se registraron dos casos de ataques tipo ransomware dirigidos a las industrias de Alimentación y Agricultura y Sector Industrial. Los análisis preliminares señalan como posibles actores involucrados a los grupos Sarcoma y Qilin, conocidos por su actividad maliciosa contra infraestructuras críticas y empresariales.

Sector	Número de casos	Amenazas	Posible actor involucrado	Nivel alerta
Alimentación Y Agricultura	1	Ransomware	Sarcoma	Alto
Industrial	1	Ransomware	Qilin	Alto

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

Panorama regional y global

Durante la última semana, diversos incidentes relevantes a nivel regional han afectado principalmente a sectores de gobierno, energético y financiero en países latinoamericanos. Los ataques identificados incluyen desde la exfiltración de información confidencial mediante compromisos en organismos públicos, hasta sofisticadas campañas de *ransomware* dirigidas contra instituciones financieras y empresas clave en la distribución de combustibles. Esto resalta la necesidad de fortalecer las medidas de prevención y reacción ante este tipo de incidentes en toda la región. A continuación, se presenta una tabla que resume los sectores más afectados, las amenazas detectadas y los posibles responsables de los incidentes identificados.

Sector	Técnica/Vector predominante	Locación	Posible actor involucrado	Nivel de alerta
Gubernamental	Exfiltración de datos confidenciales	Perú	DeadManPE	Medio
Energético	Ransomware	Brasil	Devman	Alto
Financiero	Ransomware	Brasil	DragonForce	Alto

Tabla 2. Incidentes detectados a nivel regional. Fuente: COLCERT.

Vulnerabilidades críticas

Durante la primera semana de agosto de 2025, se identificaron varias vulnerabilidades críticas en plataformas tecnológicas de uso extendido en entornos empresariales y de infraestructura crítica, elevando el nivel de alerta para organizaciones públicas y privadas en Colombia. Estas fallas tienen potencial para la ejecución remota de código, explotación activa de consolas de gestión y carga arbitraria de archivos, facilitando posibles campañas de *ransomware*, manipulación de información confidencial e interrupciones operacionales. Resulta especialmente relevante para Colombia la presencia de vulnerabilidades que afectan tanto a sistemas de seguridad empresarial como a dispositivos de acceso remoto, áreas fundamentales en sectores como salud, servicios públicos críticos y entidades gubernamentales.

Vulnerabilidad / Plataforma	CVE	Impacto principal	CVSS
NVIDIA Triton Inference Server	CVE-2025-23319	Ejecución de código, denegación del servicio, manipulación y filtrado de información	9.8
Trend Micro Apex One (on-premise)	CVE-2025-54987	Ejecución remota de comandos	9.4
Trend Micro Apex One (on-premise)	CVE-2025-54948	Explotación activa en la consola de gestión	9.4

Tabla 3. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Ante este panorama, se recomienda la aplicación inmediata de parches, la revisión de los controles de acceso y la segmentación de entornos administrativos para prevenir que estos vectores sean explotados en la región por actores de amenaza con capacidad global o local.

Análisis de Actores y Campañas Activas

Se identificó nueva actividad del grupo **Qilin.** El cual es reconocido por operar bajo el modelo de **Ransomware como Servicio** (RaaS). Qilin recluta afiliados en todo el mundo y les proporciona herramientas para llevar a cabo ataques sofisticados que combinan el cifrado de archivos críticos con la amenaza de publicar información confidencial, ejerciendo así una presión doble sobre las víctimas. Este grupo se adapta rápidamente a nuevas vulnerabilidades y contextos regionales, manteniendo campañas activas constantes que afectan tanto a grandes corporativos como a sectores estratégicos en América Latina.

Por otro lado, el grupo **Sarcoma** ha destacado por sus ataques rápidos y selectivos, ejecutados con una precisión que busca maximizar el impacto y la visibilidad mediática. Sarcoma enfoca sus campañas en explotar accesos remotos inseguros y vulnerabilidades emergentes, empleando estrategias de exfiltración y cifrado de datos para aumentar la presión extorsiva. Su capacidad de modificar continuamente sus técnicas, junto con la agilidad operativa, los convierte en un actor relevante y desafiante para los equipos de ciberseguridad de la región.

En conjunto, la actividad de **Qilin** y **Sarcoma** evidencia el alto nivel de especialización y persistencia de los grupos de ransomware activos en el entorno latinoamericano.

Recomendaciones

- Capacitar periódicamente a todo el personal sobre cómo identificar correos electrónicos sospechosos, evitar hacer clic en enlaces o descargar archivos de remitentes desconocidos, y habilite la autenticación multifactor (MFA) para reducir el impacto en caso de que las credenciales sean comprometidas.
- Implementar copias de seguridad regulares, segmentación de red y actualizaciones frecuentes de sistemas; combinar estas acciones con detección proactiva de amenazas, reduciendo significativamente el riesgo e impacto del ransomware.
- Limitar el acceso de usuarios y procesos exclusivamente a los recursos indispensables para su función. Implementar notificaciones automáticas que alerten sobre accesos anómalos o manipulación de archivos sensibles en tiempo real.
- Establecer un programa continuo de gestión de vulnerabilidades que incluya escaneos periódicos, priorización de riesgos, aplicación oportuna de parches y monitoreo de amenazas emergentes, para reducir la superficie de ataque y prevenir compromisos de seguridad.

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

Las fuentes utilizadas para respaldar este informe provienen principalmente de informes de seguridad oficiales, bases de datos internacionales especializadas como NIST/NVD, portales especializados en inteligencia de amenazas y servicios de monitoreo de *ransomware* en tiempo real. La confianza en las fuentes es alta, dado que incluyen información oficial, así como la validación de los analistas de múltiples fuentes de OSINT. Sin embargo, existen limitaciones inherentes, como la eventual ausencia de detalles técnicos completos para incidentes recientes, principalmente en los primeros días de exposición pública, o el uso de fuentes de inteligencia abiertas que, aunque útiles para el análisis situacional, pueden contener lagunas o falta de corroboración independiente en su etapa inicial. A pesar de estas limitaciones, el nivel de credibilidad de la información utilizada se considera medio-alto, dado el cruce de múltiples fuentes OSINT confiables, repositorios oficiales y evidencia técnica observable.

1. Any Run, 6 de agosto de 2025, "Malware Trends", Plataforma de inteligencia de amenazas. https://any.run/malware-trends/.
2. Grupo ASD, 26 de mayo de 2025, "Ciberseguridad en Colombia: Un gran desafio en 2025", Blog de proveedor de ciberseguridad https://www.grupoasd.com/ciberseguridad-en-colombia-un-gran-desafio-en-2025/
3. Dark Web Informer, 5 de agosto de 2025, "Peru's SANIPES Hit by Document Leak, Thousands of Internal Files Exposed", Blog de inteligencia de amenazas. https://darkwebinformer.com/perus-sanipes-hit-by-document-leak-thousands-of-internal-files-exposed/
4. Ransomware.live, 01/07/2025, 07/08/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración, https://www.ransomware.live/
5. NVIDIA, 4 de agosto de 2025, "Security Bulletin: NVIDIA Triton Inference Server - August 2025", Boletín sobre vulnerabilidad detectada en hardware de NVIDIA. https://nvidia.custhelp.com/app/answers/detail/a_id/5687
6. NIST, 5 de agostp de2025, "CVE-2025-54987 Detail", Fuente oficial de vulnerabilidades https://nvd.nist.gov/vuln/detail/CVE-2025-54987
7. NIST, 5 de agostp de2025, "CVE-2025-54948 Detail", Fuente oficial de vulnerabilidades https://nvd.nist.gov/vuln/detail/CVE-2025-54948
8. PC Risk, 10 de abril de 2025, "Sarcome Group Ransomware", Blog de ciberseguridad. https://www.pcrisk.es/guias-de-desinfeccion/13711-sarcoma-group-ransomware