Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS -20251109- 014

TLP:CLEAR

Resumen Ejecutivo

Durante la última semana, el equipo de análisis situacional continuó con el seguimiento y monitoreo de las principales ciberamenazas que afectan tanto a Colombia como a la región. Se identificó un incremento sostenido en la actividad de grupos de *ransomware* como **Nightspire**, **Warlock**, **Blacknevas** y **Qilin**, los cuales impactaron sectores estratégicos en países latinoamericanos como Brasil, Bolivia, Argentina y México. En el ámbito de vulnerabilidades, se destacaron tres fallas críticas que podrían permitir la ejecución remota de código y la exposición de información sensible. Estas vulnerabilidades representan un riesgo relevante para entornos corporativos y requieren acciones inmediatas de actualización y mitigación por parte de los equipos técnicos. Asimismo, entre las tendencias observadas se resalta el impulso a la formación en ciberseguridad, con la apertura de 2.500 cupos gratuitos; el incremento en los ciberataques dirigidos a entidades colombianas, que posicionan al país como uno de los más afectados en Latinoamérica; y la persistencia del *ransomware* como una de las amenazas más activas y con mayor impacto operativo y económico en la región.

En cuanto al panorama de malware, se evidenció un comportamiento dinámico con familias como, **XWorm** y **Quasar RAT**, que mantienen una alta tasa de propagación. El análisis comparativo semanal muestra una evolución en las tácticas y técnicas de propagación utilizadas por los atacantes, reforzando la necesidad de mantener una vigilancia continua sobre indicadores de compromiso (IoC) y comportamientos anómalos.

Tendencias observadas

- **Formación y fortalecimiento del talento en ciberseguridad**: se destaca el impulso a la formación en competencias digitales y ciberseguridad, particularmente con la iniciativa desarrollada en Medellín en colaboración con Oracle, la cual ofrece 2.500 cupos gratuitos para capacitación en esta área. Este tipo de programas refuerza la estrategia nacional de desarrollo del talento tecnológico, promoviendo la creación de capacidades locales y la profesionalización del sector. La formación de nuevos especialistas no solo contribuye a reducir la brecha de talento en ciberseguridad, sino que también fortalece la capacidad del país para responder de manera más efectiva a las crecientes amenazas digitales y apoyar los procesos de transformación digital en entornos corporativos y gubernamentales.

- **Aumento en el volumen de ciberataques en Colombia**: Colombia continúa enfrentando un alto número de incidentes cibernéticos, posicionándose como uno de los países de la región con mayor actividad maliciosa reportada. Este incremento se atribuye al crecimiento en la superficie de ataque derivada de la digitalización acelerada y la adopción de servicios en la nube, así como a la sofisticación de las técnicas utilizadas por los actores de amenaza. Los ataques se dirigen principalmente a sectores financieros, gubernamentales y de salud, buscando la exfiltración de datos sensibles, interrupción de servicios o la obtención de beneficios económicos. Este panorama resalta la necesidad de fortalecer las capacidades de detección temprana, respuesta a incidentes y resiliencia tecnológica en las organizaciones.

- **Persistencia del *ransomware* como amenaza crítica**: el ransomware continúa siendo una de las amenazas más persistentes y con mayor impacto operativo y económico a nivel nacional e internacional. Las campañas recientes evidencian una evolución en los métodos de distribución y en los modelos de negocio de los grupos delictivos, adoptando esquemas de *Ransomware-as-a-Service* (RaaS) y técnicas de doble extorsión. Este tipo de ataques afecta tanto a entidades públicas como privadas, comprometiendo la disponibilidad de los servicios críticos y generando pérdidas significativas. Ante este escenario, se hace indispensable la implementación de estrategias de respaldo y recuperación efectivas, la actualización constante de controles de seguridad y la sensibilización del personal frente a tácticas de ingeniería social utilizadas para la propagación inicial del ataque.

Panorama nacional

En la comparativa semanal se evidencia un incremento notable en las detecciones del kit de *phishing* **Tycoon 2FA**, que continúa siendo la familia más activa. Le siguen **EvilProxy** y el troyano **XWorm**, que también registran un crecimiento significativo, lo que sugiere una intensificación en las campañas orientadas a la captura de credenciales y la propagación de troyanos de acceso remoto. Otras familias como **Quasar**, **Rhadamanthys** y **Remcos** mantienen una presencia constante, reflejando la persistencia de amenazas vinculadas al control remoto y la exfiltración de información. En conjunto, el gráfico evidencia un incremento generalizado en la actividad maliciosa, destacando la necesidad de fortalecer los mecanismos de detección temprana y las medidas de protección frente a ataques basados en robo de información y compromisos de autenticación multifactor.

Comparativa entre semanas

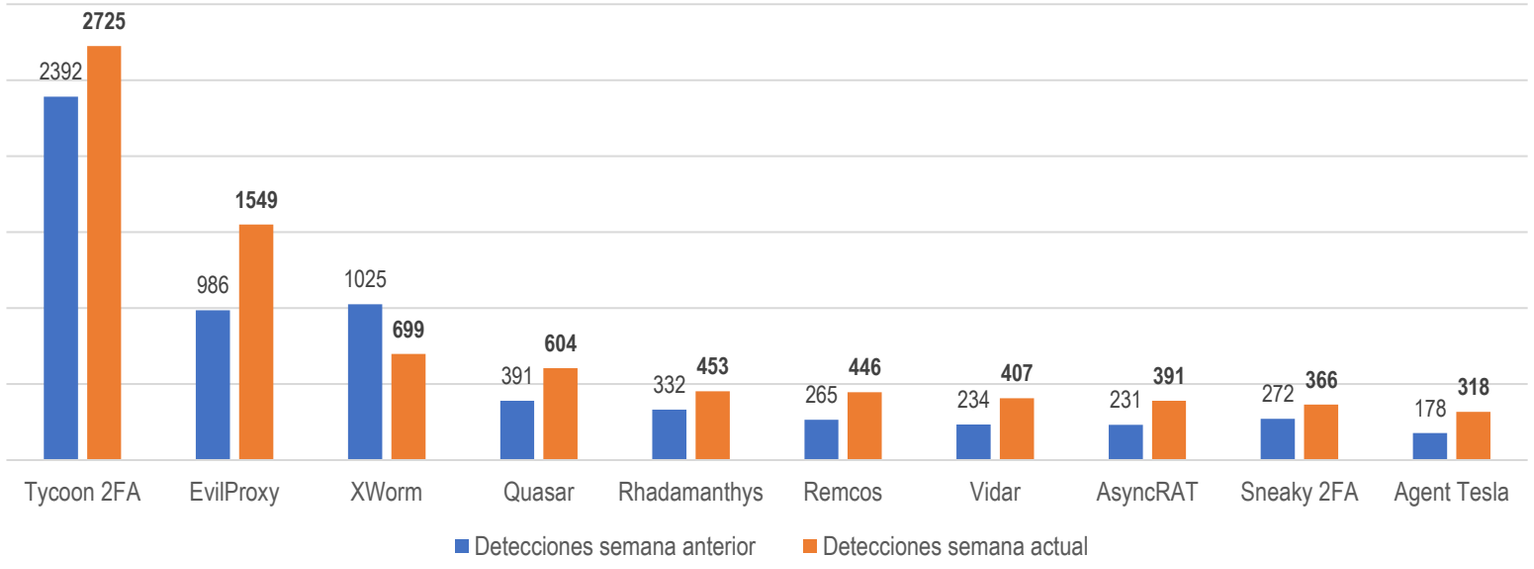

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la última semana, en el panorama regional se identificaron cuatro incidentes relevantes asociados principalmente a campañas de *ransomware* dirigidas a distintos sectores estratégicos de América Latina. Estos hallazgos reflejan una tendencia sostenida de ataques de *ransomware* en la región, orientados a sectores con alto valor estratégico y económico, lo que resalta la necesidad de mantener una vigilancia constante y estrategias de resiliencia cibernética fortalecidas.

Sector	Amenaza	Locación	Posible actor involucrado
Tecnologías De La Información Y Comunicaciones	Ransomware	Brasil	**Nightspire**
Tecnologías De La Información Y Comunicaciones	Ransomware	Bolivia	**Warlock**
Comercio	Ransomware	Argentina	**Blacknevas**
Financiero	Ransomware	Mexico	**Qilin**

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

Vulnerabilidades relevantes de la semana

Durante el periodo analizado, se identificaron vulnerabilidades críticas de alta relevancia a nivel global, entre las que destacan las CVE-2025-11953, CVE-2025-12779 y CVE-2025-11833. Estas fallas impactan directamente en componentes ampliamente utilizados en entornos corporativos, representando un riesgo significativo de **ejecución remota de código**, **escalamiento de privilegios** o **exposición de información sensible**. La rápida divulgación de estas vulnerabilidades ha impulsado la emisión de alertas tempranas y la recomendación de aplicar parches de seguridad de manera prioritaria, contribuyendo a la reducción del riesgo operativo y al fortalecimiento de las medidas de ciberdefensa en las organizaciones.

Plataforma afectada	CVE	Impacto principal	Score CVSS
React Native Community CLI (Metro Development Server)	**CVE-2025-11953**	Ejecución remota de código (OS command injection) mediante un endpoint expuesto por el servidor de desarrollo. Un atacante no autenticado puede enviar una petición POST y ejecutar comandos en la máquina del servidor donde corre el Metro Dev Server. Alto riesgo para pipelines de desarrollo, entornos CI/CD y máquinas de desarrolladores que queden expuestas en red.	**9.8 (Crítico)**
Amazon WorkSpaces client para Linux	**CVE-2025-12779**	Manejo inapropiado de tokens de autenticación que puede permitir a usuarios locales no privilegiados en la misma máquina extraer tokens y acceder al WorkSpace de otro usuario. Riesgo para despliegues compartidos, salas de formación, equipos de escritorio virtuales en entornos corporativos y proveedores de servicios gestionados. AWS publicó aviso y versión corregida.	**8.8 (Alto)**
Plugin Post SMTP Mailer/Email Log para WordPress	**CVE-2025-11833**	La vulnerabilidad permite a un ciberdelincuente no autenticado acceder a los registros de correo electrónico del plugin debido a un control de acceso insuficiente en el manejo de los objetos de registro.	**9.8 (Crítico)**

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

Análisis de actores y campañas activas

- **Nightspire**: ransomware relativamente nuevo (emergida en 2025) que ha mostrado un enfoque de doble extorsión, poco *branding* público y ataques dirigidos a organizaciones de diversos sectores. Se ha observado cifrado de archivos en endpoints y en almacenamiento en la nube.
- **Warlock**: se ha identificado asociándose a campañas de *ransomware* que explotan vulnerabilidades críticas en Microsoft SharePoint y otros servicios empresariales expuestos. Informes lo relacionan con actores con vínculos a China en algunos análisis de Microsoft.
- **Blacknevas**: es una familia de *ransomware* que ha mostrado actividad global y técnicas de cifrado híbrido (AES + RSA). Investigaciones muestran similitudes técnicas con familias como Trigona y sugieren evolución con variantes más resistentes a recuperación. Se ha observado entrega vía *spearphishing* y explotación de vulnerabilidades.
- **Qilin**: también conocido en algunas fuentes como Agenda, es un ransomware con un historial muy activo desde 2022 que ha realizado ataques de alto impacto y campañas masivas durante los dos últimos años. En 2025 se reportó un uso innovador de técnicas como ejecución de payloads Linux vía WSL en máquinas Windows para evadir detección, y campañas con grandes volúmenes de víctimas.

Recomendaciones

- Mantener los sistemas operativos, aplicaciones y navegadores web siempre actualizados, aplicando los parches de seguridad emitidos por los fabricantes en el menor tiempo posible. Esto reduce la exposición a vulnerabilidades críticas como las identificadas recientemente (CVE-2025-11953, CVE-2025-12779 y CVE-2025-11833), las cuales podrían ser explotadas por actores maliciosos para comprometer equipos personales y corporativos.
- Evitar descargar o abrir archivos, enlaces o documentos provenientes de correos electrónicos no solicitados, mensajes en redes sociales o plataformas de mensajería instantánea, ya que son los principales canales utilizados para distribuir *malware*.
- Utilizar contraseñas robustas, únicas y diferentes para cada servicio en línea, combinando letras mayúsculas, minúsculas, números y caracteres especiales. Activar la autenticación multifactor (MFA) en todas las cuentas posibles, especialmente en servicios financieros, correos electrónicos y redes sociales.
- Realizar copias de seguridad periódicas (backups) de la información importante en dispositivos externos o servicios en la nube seguros. En caso de un ataque de *ransomware*, estas copias pueden facilitar la recuperación de los datos sin necesidad de pagar rescates.
- Evitar el uso de redes Wi-Fi públicas o abiertas para realizar transacciones financieras o ingresar a servicios sensibles. Si es necesario conectarse, utilizar una red privada virtual (VPN) que cifre la comunicación y proteja los datos transmitidos.
- Participar en programas de sensibilización o formación básica en ciberseguridad, como los promovidos recientemente en el país por entidades públicas y privadas. La capacitación continua ayuda a reconocer intentos de fraude digital y a adoptar buenas prácticas de seguridad digital en el día a día.

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

Ransomware.live, 06/11/2025, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 06 de noviembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
NVD (National Vulnerability Database), 2025-11-03, CVE-2025-11953 – Detail, Fuente oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-11953
NVD (National Vulnerability Database), 2025-11-05, CVE-2025-12779 – Detail, Fuente oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-12779
NVD (National Vulnerability Database), 2025-11-01, CVE-2025-11833 – Detail, Fuente oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-11833
Infobae, 2025-10-30, Medellín ofrece 2.500 cupos para formación en inteligencia artificial, ciberseguridad y desarrollo en la nube: así puede participar, Medio de comunicación.
https://www.infobae.com/colombia/2025/10/30/medellin-ofrece-2500-cupos-para-formacion-en-inteligencia-artificial-ciberseguridad-y-desarrollo-en-la-nube-asi-puede-participar/
Semana, 2025-10-28, Ciberataques en Colombia aumentan 23 %: ya es el cuarto país más afectado de Latinoamérica, Medio de comunicación.
https://www.semana.com/economia/empresas/articulo/ciberataques-en-colombia-aumentan-23-ya-es-el-cuarto-pais-mas-afectado-de-latinoamerica/202525/
Impacto TIC, 2025-10-30, Ciberseguridad en Colombia: riesgos a los que se enfrenta el país, Medio especializado en tecnología.
https://impactotic.co/ciber-seguridad/ciberseguridad-en-colombia-riesgos-a-los-que-se-enfrenta-el-pais/
SOCRadar® Cyber Intelligence Inc., 30 May 2025, Dark Web Profile: NightSpire Ransomware, blog.
https://socradar.io/dark-web-profile-nightspire-ransomware/
Trend Micro Inc., 20 Aug 2025, Warlock: From SharePoint Vulnerability Exploit to Enterprise Ransomware, investigación.
https://www.trendmicro.com/en_us/research/25/h/warlock-ransomware.html
SentinelOne Inc., 30 Apr 2025, BlackNevas Ransomware: In-Depth Analysis, Detection, and Mitigation, blog.
https://www.sentinelone.com/anthology/blacknevas/
Reuters, 8 Oct 2025, Japan's Asahi hack that halted beer production claimed by Qilin ransomware group, noticia.
https://www.reuters.com/world/asia-pacific/cybercriminals-claim-hack-japans-asahi-group-2025-10-07/