Reporte

Semanal

Inteligencia Amenaza Cibernéticas

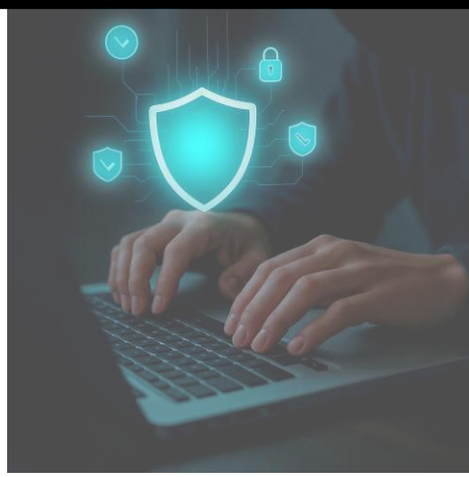
COLCERT RS – 20251018 – 011

TLP:CLEAR

Resumen Ejecutivo

Durante la última semana se identificaron vulnerabilidades críticas en plataformas como Microsoft Windows y Adobe AEM, con impactos que incluyen ejecución remota de código y escalamiento de privilegios, lo que incrementa el riesgo para entornos corporativos públicos y privados.

Asimismo, se observó actividad de grupos de amenaza como **Medusa**, **Sarcoma**, **SafePay**, **AlphaLocker**, **Nova**, **Sinobi y Black Shrantac**, enfocados en extorsión, captura de información y ataques de cifrado. En Colombia, las tendencias recientes muestran un aumento de campañas de *phishing* y explotación de sistemas desactualizados, especialmente contra sectores financiero, gubernamental y educativo.



Tendencias observadas

- **Altos intentos de ransomware en Colombia**: Kaspersky reportó que solo en Colombia los intentos de ataques con ransomware superaron los 35 millones en el último año, lo que pone de manifiesto la persistencia de esta modalidad como riesgo principal para empresas, entidades públicas y privadas. Aunque el informe indica una ligera caída regional respecto al año anterior, sigue siendo una amenaza de primer orden en la región.
- **Frecuencia y volumen creciente de intentos de *malware* y *phishing***: reportes regionales muestran que Colombia es uno de los países más afectados por *malware*, intentos de suplantación (*phishing*) y aplicaciones móviles fraudulentas. El phishing sigue estando muy presente contra entidades gubernamentales, educativas y del sector salud.
- **Continuación de escaneos automatizados y reconocimiento de superficie de ataque**: se observa que los actores de amenazas están invirtiendo en escaneo de redes e identificación de servicios vulnerables, lo que les permite encontrar puntos de acceso rápidamente y planear ataques más dirigidos.
- **Importancia de la institución pública como objetivo frecuente**: gobiernos locales, ministerios, hospitales y servicios públicos continúan siendo blanco de ataques. No solo por el valor de los datos que manejan, sino también por su posible debilidad en controles de seguridad.
- **Reputación, datos personales y privacidad bajo riesgo**: con la captura de datos personales, suplantaciones y fugas cada vez más frecuentes, existe una creciente preocupación por la privacidad y la protección de información de usuarios. Casos recientes, aunque más generales, reflejan exposición de correo electrónico, nombres, números de teléfono, etc.

Panorama nacional

En la última semana se observó un incremento general en las detecciones de amenazas en Colombia, con un crecimiento notable en familias orientadas a la captura de credenciales y eludir autenticaciones multifactor (2FA). Destaca **Tycoon 2FA**, consolidándose como la campaña más activa del periodo. También se registraron aumentos en **EvilProxy**, asociado la captura de tokens de sesión, y en **XWorm** y **Sally 2FA**, ambos vinculados a la distribución de troyanos y técnicas de *phishing* avanzado.

Por otra parte, se identificó la reaparición de **Lumma** y nuevas detecciones de **Quasar**, **Vidar** y **Mamba 2FA**, lo que evidencia una diversificación de las familias activas en el país. En contraste, las detecciones de **Rhadamanthys** disminuyeron levemente respecto a la semana anterior, lo que podría indicar una rotación o desplazamiento de vectores por parte de los actores de amenaza. En conjunto, la tendencia refleja una mayor actividad de campañas enfocadas en robo de información y bypass de autenticación, especialmente dirigidas a usuarios corporativos y servicios en línea.

Comparativa entre semanas

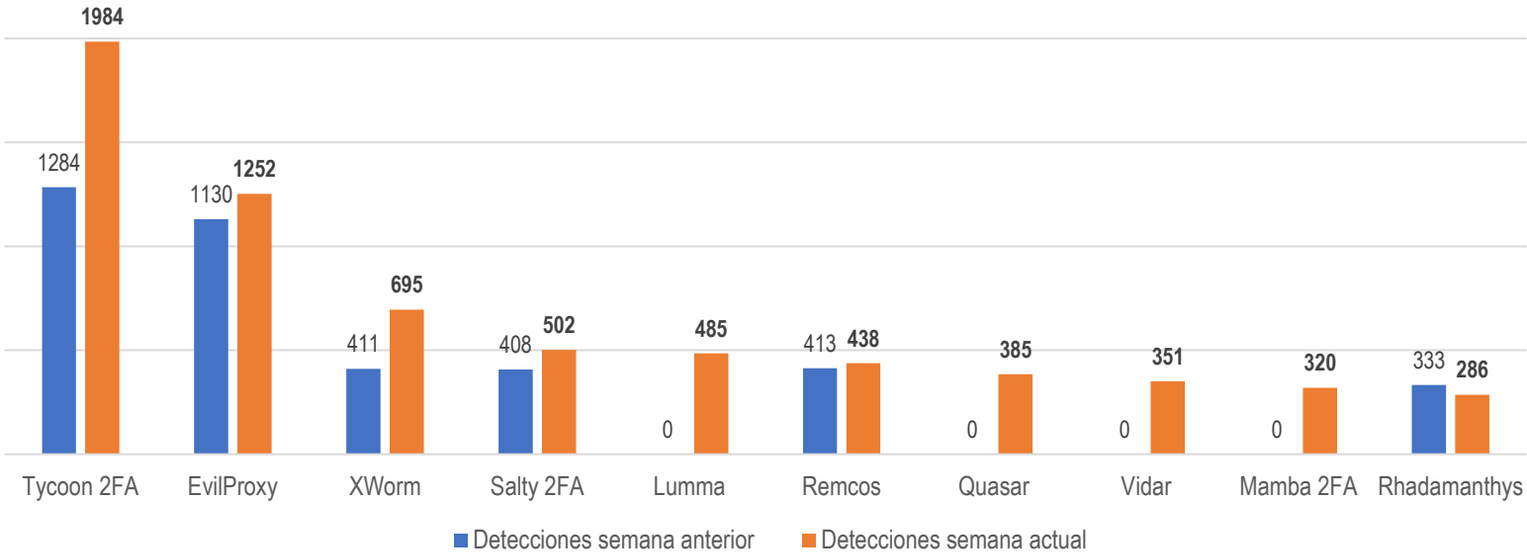


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la última semana, la actividad de *ransomware* en la región latinoamericana se mantuvo activa y diversificada, afectando principalmente a los sectores industrial, salud y protección social, gubernamental y de recursos minero-energéticos. Se observa una distribución geográfica amplia, con incidentes reportados en Brasil, Argentina, México y República Dominicana, lo que evidencia una tendencia sostenida de los actores de amenaza a dirigirse contra infraestructuras críticas y sectores estratégicos.

Sector	Técnica / Vector predominante	Locación	Posible actor involucrado
Recursos Minero-Energéticos	Ransomware	Republica Dominicana	**Medusa**
Industria	Ransomware	Brasil	**Alphalocker**
Salud y Protección Social	Ransomware	Brasil	**Sarcoma**
Turismo	Ransomware	Argentina	**Safepay**
Gobierno	Ransomware	Argentina	**Nova**
Salud y Protección Social	Ransomware	Argentina	**Sinobi**
Industria	Ransomware	México	**Black Shrantac**

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

Vulnerabilidades relevantes de la semana

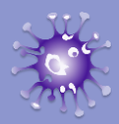
Durante la última semana se identificaron vulnerabilidades con alto impacto en entornos corporativos, afectando principalmente a Microsoft Windows y Adobe Experience Manager (AEM). En conjunto, estas fallas reflejan la necesidad de aplicar de forma prioritaria los parches de seguridad liberados durante la semana para reducir el riesgo de compromiso en infraestructuras críticas.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Microsoft Windows	**CVE-2021-43226**	Vulnerabilidad de escalación de privilegios locales. Un atacante autenticado podría ejecutar código arbitrario con privilegios SYSTEM, permitiendo el control total del equipo afectado. Está siendo explotada activamente.	**7.8**
Adobe Experience Manager Forms / Adobe AEM	**CVE-2025-54253**	En Adobe Experience Manager (AEM) Forms, esta vulnerabilidad de mala configuración permite que un atacante ejecute código arbitrario sin interacción del usuario, al evadir mecanismos de seguridad del producto.	**10.0**
Microsoft Windows	**CVE-2025-59230**	Falla de control de acceso en el servicio Remote Access Connection Manager (RasMan) de Windows, que permite a un atacante local (con acceso al sistema) escalar privilegios a nivel SYSTEM.	**7.8**
Microsoft Windows	**CVE-2025-24990**	Vulnerabilidad de escalamiento de privilegios en el controlador Agere Modem (ltmdm64.sys) de Windows.	**7.8**

Tabla 2. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de Actores y campañas Activas

- **Medusa:** Ransomware-as-a-Service (RaaS) muy activo desde 2021, con uso de modelo de doble extorsión. Sus afiliados aprovechan accesos iniciales comprados o phishing para entrar a redes corporativas.
- **Sarcoma:** grupo de ransomware que ha atacado el sector salud, explotando la urgencia operativa para aumentar presión de pago. Se le asocia al cifrado y exfiltración de datos para extorsión adicional.
- **Safepay:** actores con orientación a *ransomware* dirigidos al sector turismo o empresas con infraestructura en línea, con ataques de cifrado y exigencia de rescate a entidades de servicios.
- **AlphaLocker:** operador de *ransomware* que ha dirigido ataques en Brasil a entornos industriales, utilizando cifrado directo y amenazas de filtración como palanca para pagos.
- **Nova:** *Ransomware* orientado al sector gubernamental latinoamericano, aprovechando debilidades en infraestructura pública para ataques de cifrado e interrupción operativa.
- **Sinobi:** actor de amenazas que apunta al sector salud o servicios sensibles, con actividad de ransomware que busca doble extorsión y presión reputacional para forzar pagos.
- **Black Shrantac:** grupo de ransomware activo en México con enfoque en entornos industriales; combina técnicas de cifrado, exfiltración y presión para pago rápido.



Black Shrantac

Recomendaciones

- Fortalecer los procesos de **identificación, evaluación y priorización de vulnerabilidades conocidas**, aplicando parches de seguridad de forma oportuna, especialmente frente a las vulnerabilidades recientemente incluidas en el catálogo KEV de CISA, como las asociadas a Microsoft y componentes críticos del sistema. Esto reduce la superficie de ataque y previene la explotación por actores oportunistas o grupos especializados como Medusa y Sarcoma.
- Implementar **sistemas de monitoreo en tiempo real** que permitan detectar comportamientos anómalos, conexiones sospechosas y uso indebido de procesos legítimos del sistema (por ejemplo, MSBuild.exe o rundll32.exe). Estas prácticas ayudan a identificar la actividad temprana de troyanos y ransomware.
- Reforzar la **segmentación de redes internas** y aplicar el **principio de privilegio mínimo** para los usuarios y servicios, de modo que un compromiso inicial no permita la propagación lateral del atacante. Limitar los permisos de escritura en carpetas críticas y restringir el acceso administrativo solo a personal autorizado contribuye a mitigar ataques de cifrado y exfiltración de datos.
- Capacitar a los empleados en la identificación de campañas de phishing, mensajes sospechosos y tácticas de ingeniería social, dado que muchas campañas recientes en Colombia han iniciado mediante correos o enlaces fraudulentos que distribuyen cargas maliciosas. Un personal consciente y entrenado reduce drásticamente la probabilidad de intrusión.
- Realizar copias de seguridad periódicas de los datos críticos en medios aislados o en la nube con cifrado y autenticación robusta. Asegurarse de que las copias puedan restaurarse correctamente permite mantener la continuidad del negocio ante ataques de ransomware, que buscan extorsionar a las víctimas mediante el cifrado y la captura de información.
- Revisar los servicios publicados en Internet, especialmente aquellos asociados a aplicaciones web, VPN, y paneles administrativos, limitando el acceso mediante autenticación multifactor y listas de control de IP. Este control evita que grupos como Nova o Black Shrantac aprovechen configuraciones débiles o vulnerabilidades de día cero en servicios expuestos.

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

Ransomware.live, 06/10/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 16 de octubre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
Kaspersky, 6 octubre 2025, *Ataques de ransomware superan 1,1 millones de intentos en América Latina*, comunicado de prensa.
https://latam.kaspersky.com/about/press-releases/ataques-de-ransomware-superan-11-millones-de-intentos-en-america-latina
Check Point, *Medusa Ransomware Group: A Rising Threat in 2025*, artículo técnico / blog.
https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/medusa-ransomware-group/
Check Point, *What is Locker Ransomware?*, artículo técnico / blog.
https://www.checkpoint.com/es/cyber-hub/ransomware/what-is-locker-ransomware/
Lumu, *Sarcoma Ransomware: Double-Extortion Threat*, blog.
https://lumu.io/blog/sarcoma-ransomware-double-extortion-threat/
Bitdefender, 04 septiembre 2025, *SafePay Ransomware Attacks: TTPs*, blog / artículo de seguridad.
https://www.bitdefender.com/en-us/blog/businessinsights/safepay-ransomware-attacks-ttps
WatchGuard, *Black Shrantac*, tracker de ransomware / reporte.
https://www.watchguard.com/es/wgrd-security-hub/ransomware-tracker/black-shrantac
NVD (National Vulnerability Database), 15 diciembre 2021, *CVE-2021-43226*, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2021-43226
NVD (National Vulnerability Database), 05 agosto 2025, *CVE-2025-54253*, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-54253
NVD (National Vulnerability Database), 14 octubre 2025, *CVE-2025-59230*, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-59230
NVD (National Vulnerability Database), 14 octubre 2025, *CVE-2025-24990*, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-24990