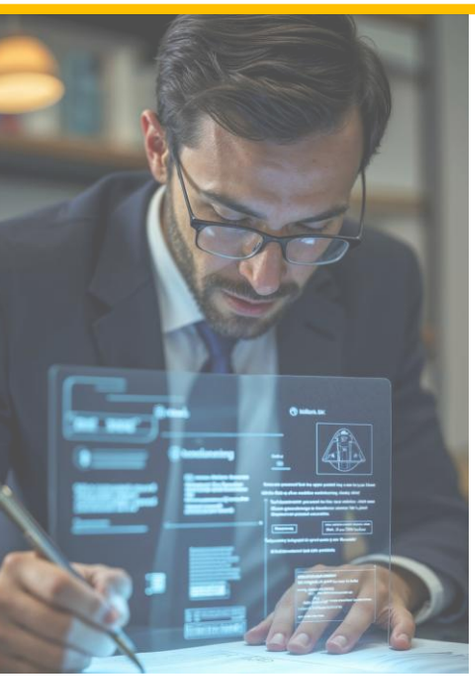
Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20251010 – 010

TLP:CLEAR



Resumen Ejecutivo

Durante la última semana se evidenció una actividad significativa en el panorama de ciberseguridad tanto a nivel nacional como regional, marcada por el incremento de incidentes de *ransomware* y la persistencia de amenazas basadas en accesos remotos (RAT) y campañas de *phishing* con suplantación de identidad. En Colombia, se registró un ataque de ransomware atribuido al grupo Sinobi, mientras que en Latinoamérica se identificaron incidentes similares dirigidos a sectores críticos como industria, transporte y finanzas, con participación de actores como INCRansom, Beast, Crypto24, DragonForce y Nova.

A nivel global, se reportaron vulnerabilidades críticas en plataformas ampliamente utilizadas (Oracle E-Business Suite, Redis, GoAnywhere MFT y WordPress) con puntajes CVSS superiores a 9.8, algunas ya explotadas activamente por grupos criminales. Estas tendencias reflejan una evolución constante de las amenazas y subrayan la necesidad de fortalecer las capacidades de detección, respuesta y concienciación, junto con la aplicación oportuna de parches y controles de seguridad en entornos corporativos.

Incidentes de la semana

Durante la última semana, en Colombia se registró un único incidente de *ransomware* atribuido al grupo **Sinobi**, el cual afectó a una empresa del sector energético. Este grupo, identificado recientemente por su rápida expansión y uso de técnicas de doble extorsión, continúa enfocando sus operaciones en organizaciones con infraestructura crítica, lo que refuerza la necesidad de mantener medidas de prevención y respuesta ante este tipo de amenazas.

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Ransomware	08/10/2025	Empresa del sector energético fue víctima de ransomware.	Sinobi

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

Tendencias nacionales observadas

- **Ataques de *ransomware***: se mantiene una alta actividad de grupos de ransomware en el país, con un incremento en los intentos de extorsión y filtración de información sensible en entidades públicas y privadas.
- **Phishing y estafas con identidad como vectores cada vez más usados**: las campañas de phishing siguen siendo el principal método de acceso inicial, aprovechando la suplantación de marcas y entidades gubernamentales para engañar a los usuarios y robar credenciales.
- **RAT como amenazas prevalentes**: continúan siendo utilizadas para el control y exfiltración de datos, destacando la presencia de familias como Remcos y AsyncRAT distribuidas mediante correos maliciosos.
- **Uso creciente de inteligencia artificial**: los ciberdelincuentes emplean IA para generar campañas más creíbles y automatizar ataques, mientras que las organizaciones comienzan a adoptar soluciones basadas en IA para detección temprana y respuesta ante incidentes.
- **Falta de talento especializado y baja inversión en seguridad limitan la capacidad de respuesta**: escasez de profesionales en ciberseguridad y los bajos presupuestos dificultan la gestión de incidentes, reduciendo la resiliencia de las organizaciones frente al incremento de amenazas.

Panorama nacional

En la última semana, las detecciones en Colombia evidenciaron una disminución general en las amenazas de tipo *stealer* y RAT, con excepción de algunos casos específicos. **EvilProxy** mantuvo una tendencia estable con un ligero aumento, consolidándose como una de las amenazas más persistentes. **DcRAT** y **Rhadamanthys** presentaron incrementos notables, lo que indica una posible reactivación de campañas dirigidas a la recolección de credenciales y control remoto de sistemas. Por su parte, **Tycoon 2FA**, aunque continúa liderando en volumen de detecciones, mostró una disminución considerable frente a la semana anterior. El surgimiento del kit de *phishing* **Sally 2FA** y del *loader* **PureCrypter** sugiere la aparición de nuevas variantes en el panorama local, enfocadas en el robo de autenticaciones y la ofuscación de cargas maliciosas.

Comparativa entre semanas

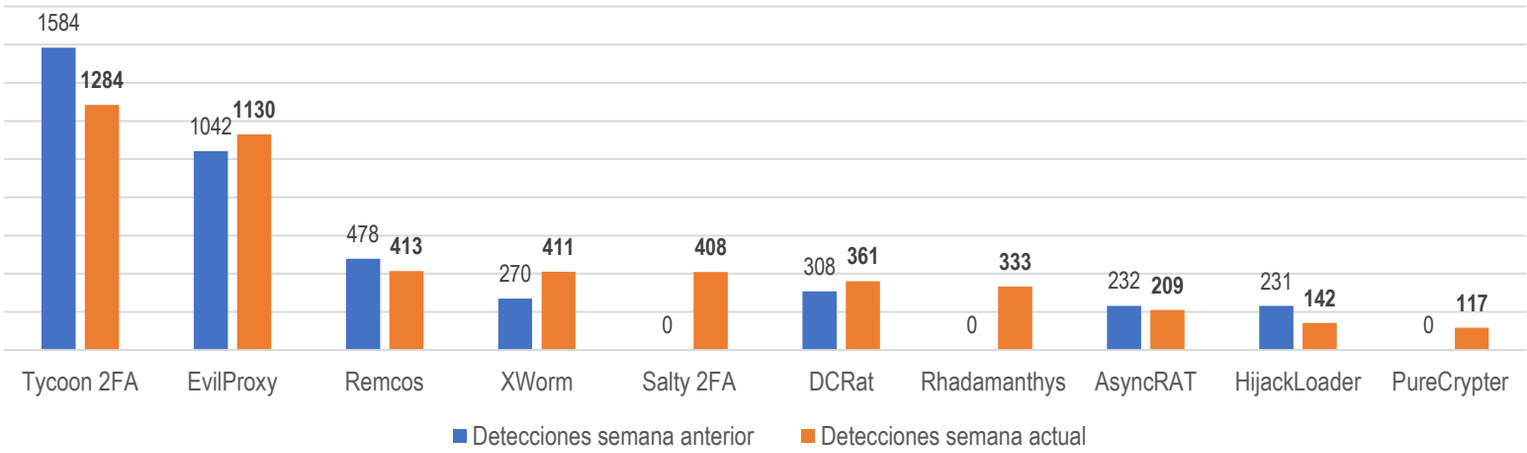


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

En la región se continúa evidenciando una actividad constante de *ransomware* dirigida a distintos sectores estratégicos, lo que demuestra la persistencia y diversificación de los grupos delincuenciales en Latinoamérica. Estos incidentes reflejan cómo los actores de amenaza continúan enfocándose en organizaciones con alto impacto operativo, manteniendo un nivel de riesgo elevado y reforzando la necesidad de fortalecer las capacidades de prevención y respuesta en la región.

Sector	Técnica / Vector predominante	Locación	Posible actor involucrado
Industria	Ransomware	Brasil	INCRansom
Industrial	Ransomware	Argentina	Beast
Financiero	Ransomware	Uruguay	Crypto24
Transporte	Ransomware	Costa Rica	DragonForce
Comercio	Ransomware	Mexico	Nova

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

Vulnerabilidades relevantes de la semana

Durante la última semana se identificaron **múltiples vulnerabilidades críticas** que afectan tanto plataformas empresariales como entornos de infraestructura y servicios web ampliamente utilizados. Estas fallas, con puntajes CVSS entre 9.8 y 10, representan un riesgo elevado de **ejecución remota de código** (RCE) y comprometen directamente la confidencialidad, integridad y disponibilidad de los sistemas afectados. Se destaca que algunas ya están siendo aprovechadas por grupos delictivos en campañas activas, lo que refuerza la necesidad de aplicar con urgencia los parches de seguridad y reforzar los controles de exposición en los entornos corporativos.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Oracle E-Business Suite	**CVE-2025-61882**	Permite ejecutar código arbitrario de forma remota sin autenticación, comprometiendo confidencialidad, integridad y disponibilidad. Si se explota con éxito, un atacante puede tomar control del componente afectado, exfiltrar datos o manipular el sistema.	**9.8 (Critical)**
GoAnywhere Managed File Transfer	**CVE-2025-10035**	Deserialización en el servlet de licencias permite RCE (ejecución remota de comandos) sin necesidad de privilegios. Ya ha sido explotada en campañas de ransomware. Grupo vinculado: Medusa. Afecta instalaciones expuestas a Internet del producto MFT empresarial.	**10 (Critical)**
Redis (motor de datos en memoria)	**CVE-2025-49844**	Vulnerabilidad que permite, si el atacante tiene acceso autenticado, lograr RCE sobre el host (riesgo alto en despliegues sin autenticación o expuestos). Afecta versiones con scripting Lua hasta 8.2.1; parche en 8.2.2.	**9.9 (Critical)**
WP Travel Engine — Tour Booking Plugin (WordPress)	**CVE-2025-7634**	Inclusión local de archivos (LFI) sin autenticación en ciertas versiones del plugin. Permite a un atacante no autenticado incluir o ejecutar archivos PHP arbitrarios en servidores WordPress que usan ese plugin.	**9.8 (Critical)**

Tabla 3. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de Actores y campañas Activas

- **Sinobi:** es un actor relativamente nuevo en el ecosistema ransomware, que emergió a fines de junio de 2025, y está prácticamente identificado como un rebranding de Lynx o al menos como estrechamente relacionado en cuanto a código y sitios de filtraciones.

- **INCRansom**: es otro grupo emergente con actividad agresiva. Se identificó ya en 2024, y ha crecido bastante para 2025. Su modus operandi incluye doble extorsión, priorizando objetivos pequeños a medianos mal defendidos, con falta de parches y servicios expuestos. A diferencia de grupos más grandes, el objetivo no es tanto prestigio sino rapidez y efectividad monetaria.

- **Beast**: es un grupo que opera con modelo RaaS, ofreciendo afiliados la posibilidad de usar su infraestructura, y apunta a sistemas Windows, Linux, y en algunos casos VMware ESXi. Técnicamente han avanzado en capacidad de cifrado, terminación de servicios que obstaculizan el cifrado, eliminación de shadow copies, etc. Existe variante llamada “Boramae” que comparte mucho código con Beast, pero con mayor complejidad técnica.

- **Crypto24**: es un grupo más sofisticado, mezcla *malware* personalizado con herramientas legítimas que ya están presentes en sistemas (living-off-the-land) para evadir detección, escalar privilegios, permanecer latente, y luego lanzar la extorsión. Tácticas recientes incluyen deshabilitar agentes EDR, crear persistencia vía tareas programadas, servicios maliciosos, abuso de utilidades administrativas estándar como PSExec, net.exe, etc. También exfiltración de datos usando servicios como Google Drive.

- **DragonForce**: DragonForce es uno de los actores más visibles en 2025 que está intentando cambiar la estructura clásica del RaaS. Permite que afiliados operen con su propia marca, usando infraestructura compartida, sitios de filtraciones, paneles de backend y soporte técnico.

- **Nova**: actor emergente de RaaS que comenzó a figurar a partir de marzo-abril de 2025. Tiene un estilo agresivo en las filtraciones de datos, comunicación pública directa hacia víctimas y doble extorsión.

Recomendaciones

- **Mantener los dispositivos actualizados**: ante las recientes vulnerabilidades críticas detectadas en plataformas como Oracle E-Business Suite, GoAnywhere MFT, Redis y WordPress, se recomienda aplicar de manera prioritaria los parches oficiales publicados por los fabricantes. Es fundamental implementar una política de gestión de vulnerabilidades continua que contemple la evaluación, priorización y remediación según el nivel de criticidad y exposición del activo.

- **Proteger las contraseñas y activar la verificación en dos pasos**: los ataques que utilizan herramientas como EvilProxy o Tycoon 2FA demuestran la importancia de robustecer los mecanismos de autenticación. Se recomienda implementar autenticación multifactor (MFA) en todos los servicios críticos, especialmente en accesos remotos, portales administrativos y sistemas de terceros. Además, se deben revisar las configuraciones de autenticación para evitar métodos inseguros o sin cifrado, y establecer políticas de rotación y complejidad de contraseñas que minimicen el riesgo de compromiso.

- **Fortalecer la detección y respuesta ante amenazas**: los datos comparativos de detecciones semanales evidencian la actividad constante de amenazas como Remcos, DcRAT, AsyncRAT y Rhadamanthys, por lo que se recomienda mantener actualizados los sistemas de detección y respuesta (EDR, XDR, IDS/IPS). Es importante establecer alertas basadas en comportamiento y correlaciones en los SIEM para identificar patrones asociados a accesos remotos no autorizados, cifrado de archivos o ejecución de procesos sospechosos.

- **Hacer copias de seguridad periódicas:** guardar una copia de tus archivos importantes en un disco externo o en la nube puede evitar pérdidas si sufres un ataque de ransomware. Asegúrate de que esas copias no estén conectadas permanentemente al computador para que no se vean afectadas.

- **Ser cuidadoso con la información personal en línea:** los ciberdelincuentes usan datos públicos para crear mensajes o páginas falsas más creíbles. No compartas información sensible (como números de documento, contraseñas o datos financieros) en redes sociales o formularios no verificados.

- **Supervisar la exposición en Internet y el uso de servicios externos:** muchas intrusiones comienzan por activos expuestos sin control, como interfaces administrativas, APIs o servidores mal configurados. Se recomienda realizar evaluaciones periódicas de superficie de ataque externa mediante herramientas OSINT o escáneres de exposición (como Shodan, Censys, Attack Surface Management) para identificar servicios abiertos, versiones obsoletas o configuraciones inseguras accesibles desde la red pública.

- **Auditar el uso de cuentas privilegiadas:** el abuso de cuentas con altos privilegios sigue siendo un vector común en intrusiones avanzadas. Es recomendable implementar soluciones de gestión de accesos privilegiados (PAM) y activar alertas cuando se realicen inicios de sesión fuera del horario laboral, desde ubicaciones inusuales o en sistemas sensibles.

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

Ransomware.live, 02/10/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 02 de octubre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
SOCRadar, 19 ago 2025, Dark Web Profile: Beast Ransomware, Perfil o inteligencia de actor.
https://socradar.io/dark-web-profile-beast-ransomware/?
Hendry Adrian, 12 octubre 2025, Sinobi rebrand of the Lynx ransomware gang, Blog / análisis.
https://www.hendryadrian.com/sinobi-rebrand-of-the-lynx-ransomware-gang/
DeXpose, 22 sept 2025, Incransom Targets Pennsylvania Office of Attorney General, Informe / alerta de incidente.
https://www.dexpose.io/incransom-targets-pennsylvania-office-of-attorney-general/
Hendry Adrian, 14 octubre 2025, Crypto24 ransomware group blends legitimate tools with custom malware for stealth attacks, Blog / análisis.
https://www.hendryadrian.com/crypto24-ransomware-group-blends-legitimate-tools-with-custom-malware-for-stealth-attacks/
Undercode News, — (sin fecha visible públicamente), Nova ransomware group hits municipality of Pisa in latest dark web breach, Noticias / medio especializado.
https://undercodenews.com/nova-ransomware-group-hits-municipality-of-pisa-in-latest-dark-web-breach/
Undercode News, — (sin fecha visible públicamente), Beast ransomware strikes again: Acheson Doyle Acmark targeted in coordinated attack, Noticias / medio especializado
https://undercodenews.com/beast-ransomware-strikes-again-acheson-doyle-acmark-targeted-in-coordinated-attack/
Quorum Cyber, — (sin fecha visible públicamente), Threat Assessment: DragonForce calls for ransomware cartel with LockBit and Qilin, Análisis / inteligencia.
https://www.quorumcyber.com/threat-intelligence/threat-assessment-dragonforce-calls-for-ransomware-cartel-with-lockbit-and-qilin/
Microsoft Security Blog, 6 oct 2025, Investigating active exploitation of CVE-2025-10035 GoAnywhere Managed File Transfer vulnerability, Blog técnico / alerta.
https://www.microsoft.com/en-us/security/blog/2025/10/06/investigating-active-exploitation-of-cve-2025-10035-goanywhere-managed-file-transfer-vulnerability/
Redis (oficial), 3 oct 2025, Security Advisory: CVE-2025-49844, Boletín técnico.
https://redis.io/blog/security-advisory-cve-2025-49844/
Oracle, 4 oct 2025, Oracle Security Alerts: CVE-2025-61882, Alerta de seguridad / boletín.
https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
Wordfence, 8 oct 2025, WP Travel Engine Tour Booking Plugin: unauthenticated local file inclusion vulnerability, Blog / inteligencia de vulnerabilidades.
https://www.wordfence.com/threat-intel/vulnerabilities/wordpress-plugins/wp-travel-engine/wp-travel-engine-tour-booking-plugin-tour-operator-software-667-unauthenticated-local-file-inclusion