Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20251215 – 018

TLP:CLEAR

Resumen Ejecutivo:

Durante esta semana se observaron varias tendencias relevantes en el panorama de ciberamenazas que mantienen en alerta tanto a organizaciones públicas como privadas en Colombia y la región. Persisten los incidentes asociados a **contraseñas débiles**, que siguen siendo una puerta de entrada frecuente para los atacantes, así como un aumento de **campañas maliciosas con temática navideña** orientadas a engañar a usuarios y capturar información sensible. Continuaron también las campañas que distribuyen troyanos de acceso remoto suplantando entidades gubernamentales colombianas, lo que evidencia un interés sostenido de los actores maliciosos en técnicas de ingeniería social localizadas.

En el ámbito regional, sobresale la actividad de grupos de *ransomware* como **Worldleaks** y **LockBit 5.0**, que focalizaron ataques contra sectores productivos y estratégicos en Brasil, México y Bolivia, afectando industrias como agricultura, comercio y energía. A nivel corporativo, hubo fluctuaciones en la detección de familias de código malicioso respecto a la semana anterior, destacándose movimientos en troyanos, backdoor y herramientas de acceso remoto.

Esta semana dejó ver un entorno activo y dinámico, donde los ciberdelincuentes combinan tácticas tradicionales con campañas focalizadas y oportunistas. Las organizaciones deben mantener controles básicos fortalecidos, mejorar la gestión de vulnerabilidades, reforzar la autenticación y elevar la capacidad de detección temprana para reducir el impacto de estas amenazas emergentes.

Tendencias observadas

- **Persistencia de uso de contraseñas débiles**: se evidenció que muchas personas, tanto usuarios comunes como en entornos corporativos, siguen utilizando contraseñas muy simples y fáciles de adivinar, como “123456”, pese a las advertencias de expertos en ciberseguridad. Esto significa que el riesgo de accesos no autorizados, compromiso de cuentas y filtración de datos personales o corporativos se mantiene elevado, porque los ciberdelincuentes pueden comprometer cuentas sin técnicas complejas si la contraseña es predecible.

- **Aumento de ciberataques dirigidos a usuarios en temporada navideña**: la temporada navideña trae consigo una oleada de ciberataques dirigidos a cuentas de correo, redes sociales, servicios bancarios y dispositivos personales, donde técnicas como ***phishing*** y ***credential stuffing*** se disparan. Además, estos ataques no solo se limitan a hurtos de credenciales o datos personales, sino que también pueden derivar en **pérdidas económicas directas** o la suplantación de identidad para **extorsionar a familiares de las víctimas**. La intensificación de estas amenazas durante un periodo de alta actividad en línea deja en evidencia que los actores maliciosos adaptan sus métodos para maximizar resultados aprovechando hábitos de consumo y menor conciencia sobre los riesgos.

- **Continuación de campañas de *malware* con suplantación de entidades oficiales**: durante esta temporada decembrina los ciberataques han mostrado un incremento significativo que afecta a personas y dispositivos móviles en Colombia. Los ataques incluyen ***phishing***, ***credential stuffing***, ***malware*** y otros métodos automatizados. Esto se intensifica en épocas con alto uso de compras en línea, uso de redes públicas, y descargas de aplicaciones.

Panorama nacional

El comparativo semanal muestra un aumento notable en las amenazas orientadas a la capturade credenciales y el compromiso de autenticación, con los kit de *phishing* **Tycoon 2FA** y **EvilProxy** manteniéndose como las familias más activas. Destaca la aparición repentina de **Sneaky 2FA** tras no tener actividad en semanas anteriores. Aunque Troyanos de acceso remoto (RAT) como **AsyncRAT**, **Remcos** y **AgentTesla** presentan variaciones menores, su presencia constante confirma que siguen siendo ampliamente utilizadas en campañas de acceso remoto y exfiltración. En general, las cifras muestran un incremento en la diversidad y volumen de amenazas dirigidas a comprometer cuentas y tomar control remoto de los equipos esta semana.

Comparativa entre semanas

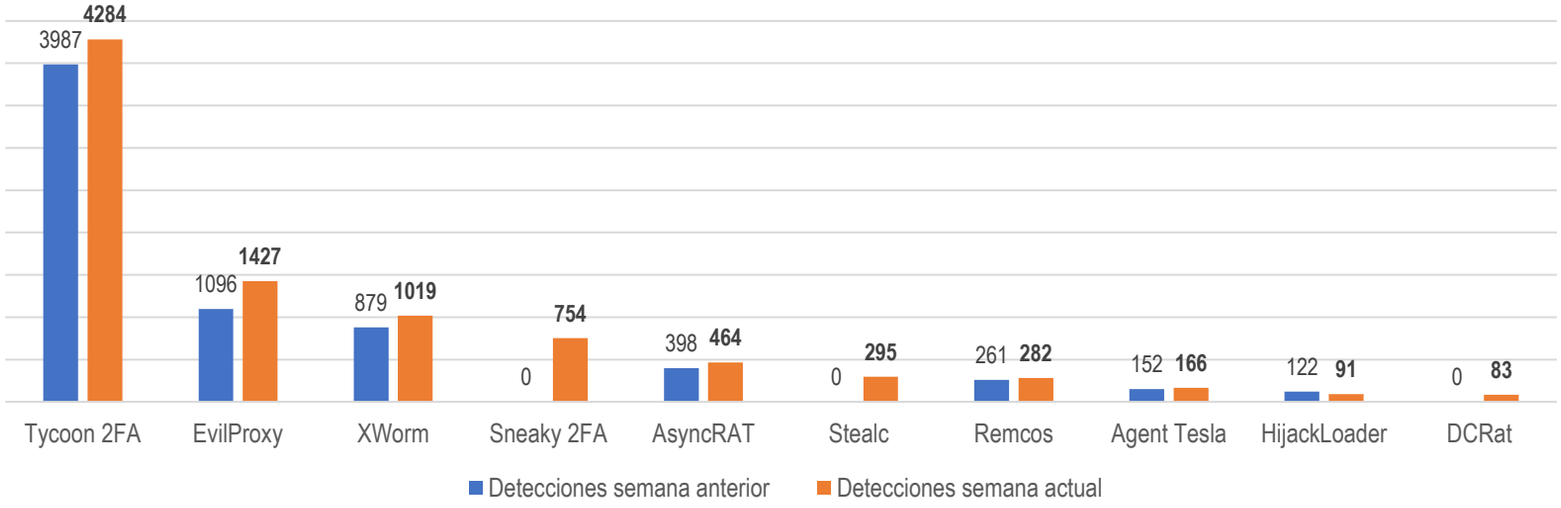

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la última semana, los incidentes registrados en LATAM evidencian una marcada concentración de ataques de *ransomware* dirigidos principalmente a sectores productivos y estratégicos de la región. **Brasil** aparece como el país más afectado, con compromisos en los sectores de **Alimentación y Agricultura**, y **Comercio, Industria y Turismo**, atribuidos al grupo **Worldleaks**, lo que sugiere un interés creciente en industrias con alta dependencia operativa y baja tolerancia a interrupciones. Paralelamente, **LockBit 5.0** mantiene actividad relevante en **México** y **Bolivia**, apuntando a sectores críticos como **Comercio** y **Recursos Minero-Energéticos.** En conjunto, los datos reflejan un panorama regional donde **el *ransomware* continúa siendo la principal amenaza** disruptiva, con grupos consolidados enfocando sus esfuerzos en industrias clave para la estabilidad económica y logística de la región.

Sector afectado	Amenaza	Locación	Posible actor involucrado
Alimentación y Agricultura	Ransomware	Brasil	Worldleaks
Comercio, Industria y Turismo	Ransomware	Brasil	Worldleaks
Comercio, Industria y Turismo	Ransomware	México	LockBit 5.0
Recursos Minero-Energéticos	Ransomware	Bolivia	LockBit 5.0

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

Vulnerabilidades críticas

Plataforma afectada	CVE	Impacto principal	Score CVSS	CISA KEV
React Server Components (RSC)	**CVE-2025-55182**	Ejecución remota de código (RCE) no autenticada debido a deserialización insegura permitiendo a atacantes comprometer servidores y ejecutar comandos arbitrarios.	**10.0 (Crítico)**	**TRUE**
Windows Cloud Files Mini Filter Driver	**CVE-2025-62221**	Un atacante con acceso local de bajo privilegio puede escalar a SYSTEM, se reportó explotación activa en entornos reales.	**7.8 (Alto)**	**TRUE**
Apache Tika	**CVE-2025-66516**	Permite que un archivo PDF malicioso pueda hacer que los sistemas que procesan ese documento accedan y envíen información interna sin autorización.	**10.0 (Crítico)**	**FALSE**
SAP Solution Manager	**CVE-2025-42880**	Permite a un atacante autenticado inyectar código malicioso, otorgando control total del sistema (alto impacto en confidencialidad, integridad y disponibilidad).	**9.9 (Crítico)**	**FALSE**
Ivanti Endpoint Manager	**CVE-2025-10573**	Permite a un atacante no autenticado ejecutar JavaScript arbitrario en el contexto de una sesión de administrador (requiere interacción del usuario).	**9.6 (Crítico)**	**FALSE**
Microsoft Exchange Server	**CVE-2025-64666**	Un actor autenticado podría escalar privilegios sobre la organización. Parche incluido en el ciclo de actualizaciones de diciembre.	**7.5 (Alto)**	**FALSE**

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

Análisis de Actores y Campañas Activas

- **Worldleaks**: es una operación de extorsión y filtrado de datos que emergió en 2025, vinculada como sucesora de operadores previos como **Hunters International** y con un modelo que prioriza la publicación y venta de datos capturados. en la última semana se le atribuyeron compromisos contra empresas en Brasil, Estados Unidos, Canadá y Suiza.

- **LockBit 5.0**: es una de las operaciones RaaS (ransomware-as-a-service) históricamente más dañinas. La versión 5.0 es la evolución más reciente que resurgió con capacidades aumentadas tras interrupciones previas del ecosistema. Ésta está diseñada para atacar entonos **Windows**, **Linux** y **ESXi**. Desde su reaparición se le ha observado activo en múltiples campañas globales y con víctimas en diferentes sectores. Reportes técnicos y diarios de inteligencia durante la última semana indican el compromiso más de 30 empresas alrededor del mundo.

Recomendaciones

- **Fortalecer el sistema de autenticación** mediante el uso obligatorio de contraseñas complejas, dobles factores de autenticación no basados en SMS y controles de rotación periódica, reduciendo riesgos asociados a credenciales débiles o comprometidas.
- **Restringir la ejecución de archivos provenientes de correos electrónicos o descargas no verificadas** mediante políticas de AppLocker o WDAC, mitigando tácticas de infección usadas en campañas que suplantan entidades gubernamentales colombianas.
- **Segmentar la red interna** para evitar la propagación lateral en caso de infección por *ransomware* o RAT, aplicando controles estrictos de acceso por rol, VLAN y microsegmentación en sistemas críticos.
- **Implementar copias de seguridad cifradas, aisladas y con validaciones automáticas**, asegurando que los respaldos no queden accesibles desde redes productivas, lo cual limita el impacto de ataques de doble extorsión.
- **Configurar alertas para detectar comportamientos asociados a evasión y persistencia**, como creación de tareas programadas, modificación de claves de registro de Windows (Run/RunOnce), uso de procesos legítimos del sistema (living-off-the-land) y cambios inesperados en políticas de seguridad.
- **Parchar de manera prioritaria todas las vulnerabilidades críticas identificadas** en la semana, especialmente aquellas con explotación activa y con impacto directo en plataformas corporativas, estableciendo un ciclo de actualización acelerado que incluya inventario de activos, clasificación de riesgos, pruebas controladas y despliegue automatizado de parches, asegurando además la verificación posterior para confirmar que la corrección quedó aplicada correctamente en todos los sistemas afectados.

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

Ransomware.live, 11 de diciembre de 2025, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 11 de diciembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
National Vulnerability Database (NVD), 04-dic-2025, CVE-2025-66516 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-66516
National Vulnerability Database (NVD), 05-dic-2025, CVE-2025-55182 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-55182
National Vulnerability Database (NVD), 09-dic-2025, CVE-2025-62221 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-62221
National Vulnerability Database (NVD), 09-dic-2025, CVE-2025-42880 Detail, base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-42880
Semana.com, 10-dic-2025, Nunca utilice esta contraseña en sus cuentas, agencia de ciberseguridad demostró que es la más insegura de todas, medio de comunicación.
https://www.semana.com/amp/tecnologia/articulo/nunca-utilice-esta-contrasena-en-sus-cuentas-agencia-de-ciberseguridad-demostro-que-es-la-mas-insegura-de-todas/202539/
ACIS.org.co, 09-dic-2025, Oleada de ciberataques sacude la Navidad: delincuentes digitales ponen en la mira cuentas y móviles de usuarios en Colombia, organización/boletín institucional.
https://www.acis.org.co/blog/noticias-2/oleada-de-ciberataques-sacude-la-navidad-delincuentes-digitales-ponen-en-la-mira-cuentas-y-moviles-de-usuarios-en-colombia-4790
ESET Latinoamérica (X/Twitter), 09-dic-2025, Publicación sobre campañas de malware y suplantación detectadas por ESET, red social / fuente de seguridad privada.
https://x.com/ESETLA/status/1998429635319586881
WatchGuard Technologies, Ransomware – World Leaks, Ransomware Tracker / Inteligencia de amenazas.
https://www.watchguard.com/es/wgrd-security-hub/ransomware-tracker/world-leaks
Trend Micro, 25-sep-2025, New LockBit 5.0 Targets Windows, Linux, ESXi, Investigación técnica / Inteligencia de amenazas.
https://www.trendmicro.com/en_us/research/25/i/lockbit-5-targets-windows-linux-esxi.html