Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20251114 – 015

TLP:CLEAR

Resumen Ejecutivo

Durante la última semana se registraron incidentes de filtración y extorsión contra entidades gubernamentales en Colombia, atribuidos al actor **Kazu**, y ataques de *ransomware* en Latinoamérica por grupos como **Tekir APT**, **Incransom** y **DragonForce**. Se identificaron vulnerabilidades críticas en Microsoft, Cisco y SAP con potencial de ejecución remota, y un aumento de campañas de *phishing*. Además, se resalta el impulso de iniciativas como el CSIRT Salud y la cooperación Colombia - Brasil para fortalecer la ciberseguridad regional.

Incidentes de la semana

Durante la última semana se registraron dos incidentes de filtración y extorsión dirigidos a entidades del sector gubernamental en Colombia, donde se evidenció la exfiltración y publicación de información sensible en plataformas de la web oscura. Estos hechos fueron atribuidos al actor **Kazu**, conocido por sus campañas de exposición de datos como mecanismo de presión y afectación reputacional. La recurrencia de estos eventos refuerza la necesidad de fortalecer las medidas de protección de datos y gestión de incidentes en el sector público.

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Filtración y extorsión	10 de noviembre de 2025	Dos entidades del sector gubernamental en Colombia fueron afectadas por la exfiltración y divulgación no autorizada de información sensible y confidencial.	**Kazu**

Tendencias observadas

- **Brechas de datos en el sector público:** se ha evidenciado un aumento de brechas de datos y ciberataques dirigidos a entidades públicas en la región, afectando ministerios, alcaldías y universidades. En Colombia y otros países latinoamericanos se han registrado intentos de intrusión y filtración de información sensible, lo que refuerza la necesidad de fortalecer la detección temprana y la respuesta coordinada en el sector público.

- **Distribución de múltiples malware mediante *phishing***: se ha identificado una campaña de phishing que distribuye simultáneamente AsyncRAT y Remcos RAT, ambos con funciones de control remoto y robo de información. Este tipo de ataques busca aumentar el impacto y evadir detección combinando varias amenazas en un mismo vector de infección.

- **Incremento de malware para dispositivos móviles**: se ha registrado un crecimiento sostenido de código malicioso dirigido a dispositivos Android, especialmente en aplicaciones falsas que suplantan entidades financieras y servicios de mensajería. Los troyanos móviles muestran mayor sofisticación y capacidad de evasión, afectando a usuarios y organizaciones que dependen de estos dispositivos para sus operaciones.

- **Iniciativas sectoriales para fortalecer la ciberseguridad**: Colombia propuso la creación del CSIRT Salud para mejorar la gestión de incidentes en el ámbito sanitario. Además, Colombia y Brasil firmaron un anexo de cooperación en ciberseguridad para proteger infraestructuras críticas y compartir buenas prácticas entre ambos países.

Panorama nacional

En el gráfico se observa un aumento general en las detecciones de amenazas en Colombia respecto a la semana anterior, destacándose **Tycoon 2FA** con el mayor número de registros y un crecimiento sostenido, seguido por **EvilProxy** y **XWorm**, que también muestran incrementos significativos. Se evidencia además la aparición de **Lumma**, que no había sido detectado en semanas pasadas, y el incremento de **Sneaky 2FA**, lo que refleja una tendencia de actores maliciosos orientados la captura de credenciales y autenticaciones multifactor. Por otro lado, **AsyncRAT** y **Remcos** mantienen niveles similares de actividad, indicando persistencia en campañas de control remoto. En conjunto, los datos reflejan una intensificación de las amenazas dirigidas a comprometer accesos y credenciales en entornos locales.

Comparativa entre semanas

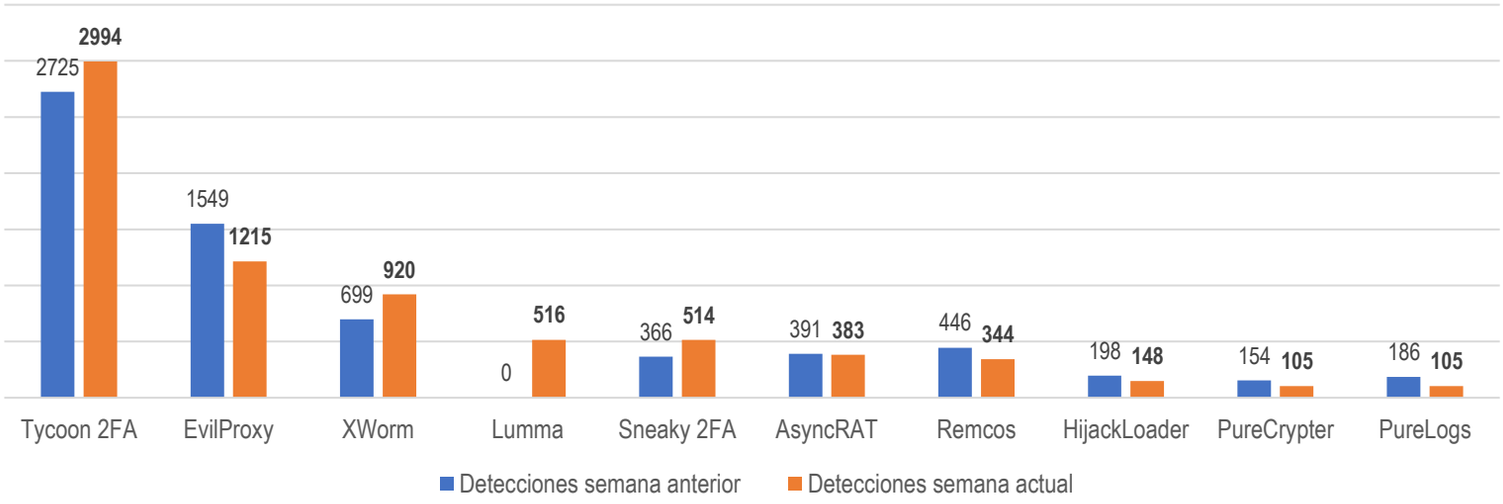

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la última semana se identificaron múltiples incidentes relacionados con *ransomware* en la región de Latinoamérica, afectando principalmente a los sectores comercio y gobierno. Los países con mayor número de reportes fueron **Argentina** y **México.** Entre los posibles actores involucrados se destacan **INCransom**, **Dragonforce** y **Tekir APT**, además de nuevos grupos como **Nightspire** y **Blackshrantac**, lo que sugiere una diversificación de actores con intereses regionales. Este panorama refleja una tendencia sostenida de ataques a sectores estratégicos, especialmente aquellos con alta dependencia tecnológica y valor en la información que manejan.

Sector	Amenaza	Locación	Posible actor involucrado
Alimentación y Agricultura	Ransomware	Perú	**Blackshrantac**
Comercio	Ransomware	Argentina	**DragonForce**
Comercio	Ransomware	Argentina	**INCransom**
Comercio	Ransomware	Costa Rica	**INCransom**
Minero-energético	Ransomware	México	**Nightspire**
Gobierno	Ransomware	Argentina	**Desconocido**
Gobierno	Ransomware	México	**Tekir APT**

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

Vulnerabilidades relevantes de la semana

Durante la última semana se identificaron vulnerabilidades críticas en plataformas ampliamente utilizadas a nivel corporativo, destacándose fallas que permiten ejecución remota de código y acceso no autorizado en entornos de bases de datos, aplicaciones empresariales y componentes de Windows. Las más relevantes afectan a Microsoft, Cisco y SAP, con puntajes CVSS entre 8.8 y 10, lo que refleja un riesgo elevado de compromiso en infraestructuras públicas y privadas si no se aplican las actualizaciones de seguridad publicadas por los proveedores.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Microsoft Graphics Component	**CVE-2025-60724**	Ejecución remota de código (RCE) mediante desbordamiento de búfer en heap, vía archivo malicioso. Afecta procesamiento de imágenes en aplicaciones Windows/Office usadas.	**9.8 (Crítico)**
Cisco Unified Contact Center Express	**CVE-2025-20354**	Permite subir archivos arbitrarios y ejecutar comandos como root. RCE en entornos Unified CCX.	**9.8 (Crítico)**
SAP SQL Anywhere Monitor	**CVE-2025-42890**	Gestión insegura de claves y secretos, permitiendo acceso no autorizado a información sensible en entornos de monitoreo de bases de datos corporativas.	**10.0 (Crítico)**
Microsoft SQL Server	**CVE-2025-59499**	Vulnerabilidad crítica en servidor de bases de datos, potencialmente permitiendo RCE o escalada de privilegios en entornos empresariales de gestión de datos.	**8.8 (Alto)**

Tabla 3. Vulnerabilidades relevantes de la semana. Fuente: COLCERT.

Análisis de actores y campañas activas

- **Kazu:** este actor ha mantenido actividad focalizada en Latinoamérica, principalmente mediante campañas de filtración de información y extorsión digital dirigidas a entidades públicas. Se caracteriza por divulgar supuestos datos exfiltrados en canales de mensajería y plataformas de la web oscura, con el objetivo de generar presión mediática y reputacional sobre sus víctimas

- **Tekir APT**: actor estatal (presuntamente turco), especializado en espionaje cibernético. En noviembre 2025 reclama ataques a fiscalías mexicanas, exfiltrando 250 GB de expedientes judiciales.
- **Blackshrantac**: actor emergente enfocado en ataques de *ransomware* dirigidos a sectores industriales y de alimentación, con actividad confirmada en Perú. Sus tácticas incluyen el cifrado de sistemas críticos y la posterior extorsión mediante la publicación de datos en sitios de filtración. Su perfil sugiere una orientación financiera con un nivel técnico intermedio.

Black Shrantac

- **INCransom**: grupo con presencia consolidada en campañas recientes de ransomware doble extorsión, afectando sectores comerciales y de servicios en Argentina y Costa Rica. Este actor combina cifrado de archivos con la amenaza de divulgar información confidencial, y se le ha vinculado con infraestructura y técnicas compartidas con otros grupos de habla rusa.

INC Ransom

- **DragonForce**: actor ransomware conocido por ataques a gobiernos locales. En noviembre reclama filtraciones de datos de alcaldías peruanas y paraguayas. Usa tácticas de triple extorsión.

Recomendaciones

- Implementar un proceso continuo de identificación, evaluación y corrección de vulnerabilidades en sistemas, aplicaciones y servicios expuestos a internet, asegurando la aplicación oportuna de parches de seguridad y configuraciones seguras en infraestructura crítica.
- Adoptar mecanismos de autenticación multifactor (MFA) en todas las cuentas administrativas y de usuarios con acceso sensible, junto con políticas de contraseñas robustas y una revisión periódica de privilegios para evitar accesos indebidos o uso indebido de credenciales comprometidas.
- Actualizar y probar regularmente los procedimientos de respuesta a incidentes, incluyendo la notificación, contención, análisis forense y comunicación interna y externa, garantizando una gestión oportuna ante ataques de exfiltración o filtración de información.
- Implementar herramientas de Data Loss Prevention (DLP) que supervisen el flujo de datos sensibles dentro y fuera de la red, aplicando cifrado de información crítica en tránsito y en reposo, además de establecer controles estrictos de salida hacia servicios en la nube o medios extraíbles.
- Desarrollar programas de concientización que incluyan buenas prácticas en el manejo de información confidencial, detección de intentos de ingeniería social, uso seguro del correo institucional y reporte inmediato de incidentes o comportamientos sospechosos.

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

Ransomware.live, 13 de noviembre de 2025, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/

Any Run, 13 de noviembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/

Pulzo, 13 de noviembre de 2025, Cómo los ciberataques afectan a clientes de Bancolombia, Davivienda y otros bancos, Medio de comunicación.
https://www.pulzo.com/economia/como-ciberataques-clientes-bancolombia-davivienda-bancos-2025-PP4893201

ConsultorSalud, 10 de noviembre de 2025, 13 de noviembre de 2025, CSIRT Salud: una iniciativa para enfrentar los ciberataques al sistema de salud, Medio especializado.
https://consultorsalud.com/csirt-salud-equip-ciberataques-sistema-de-salud/

ComputerWeekly, 7 de noviembre de 2025, 13 de noviembre de 2025, Fiscalía del Estado de Guanajuato sufre presunto ataque de ransomware, Medio especializado.
https://www.computerweekly.com/es/noticias/366634284/Fiscalia-del-Estado-de-Guanajuato-sufre-presunto-ataque-de-ransomware

Aerocivil Colombia (X), 8 de noviembre de 2025, Anuncio sobre cooperación en ciberseguridad entre Colombia y Brasil en el sector aeronáutico, Fuente institucional.
https://x.com/AerocivilCol/status/1987643842141512132

NIST NVD, 11 de noviembre de 2025, CVE-2025-60724 - Vulnerabilidad crítica en Microsoft Windows, Fuente técnica oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-60724

NIST NVD, 11 de noviembre de 2025, CVE-2025-20354 - Vulnerabilidad crítica en Cisco ASA y FTD, Fuente técnica oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-20354

NIST NVD, 10 de noviembre de 2025, CVE-2025-42890 - Vulnerabilidad en SAP BusinessObjects BI Platform, Fuente técnica oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-42890

NIST NVD, 9 de noviembre de 2025, CVE-2025-59499 - Vulnerabilidad en componentes de Oracle Fusion Middleware, Fuente técnica oficial.
https://nvd.nist.gov/vuln/detail/CVE-2025-59499

Cyber Intelligence House, 8 de noviembre de 2025, Leak of the Week – July 21st (Updated dataset on current breaches), Fuente de inteligencia de amenazas.
https://cyberintelligencehouse.com/leak-of-the-week-july-21st/

Cyfirma, 24 de octubre de 2025, Weekly Intelligence Report – 24 October 2025, Fuente de inteligencia de amenazas.
https://www.cyfirma.com/news/weekly-intelligence-report-24-october-2025