Reporte

Semanal

Inteligencia de Amenazas Cibernéticas

COLCERT RS-20250725-001

TLP:CLEAR

Resumen Ejecutivo:

Durante la semana del 17 al 25 de julio se observaron varios incidentes cibernéticos en Colombia y la región. En el país, se registró un ataque de *defacement* al sitio web de un partido político, atribuido al grupo CyberTeam, y dos casos de ransomware: uno contra una empresa barranquillera del sector comercial, llevado a cabo por el grupo **Arcus Media**, y otro contra otra empresa de soluciones tecnológicas , atribuido por el grupo **INC Ransom**.

En países vecinos como Brasil, Argentina y Chile también se reportaron ataques de ransomware por parte de grupos como **Handala**, **Cicada3301** y **Direwolf**. Además, se identificaron vulnerabilidades críticas en plataformas ampliamente utilizadas como Microsoft SharePoint, Citrix, Cisco, Fortinet y VMware, lo que eleva el riesgo de explotación si no se aplican las actualizaciones correspondientes.

Incidentes de la semana

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Defacement	15 de julio de 2025	El sitio web oficial de un partido político Colombiano fue víctima de un ataque de *defacement*, una técnica utilizada por ciberdelincuentes para alterar la apariencia de una página web sin autorización. En este caso, los atacantes reemplazaron el contenido legítimo del sitio con un mensaje de burla e imágenes ajenas a la organización.	El grupo que se atribuyó el ataque se hace llamar **CyberTeam**, conocido en entornos digitales por acciones similares en otras regiones.
Ransomware	21 de julio de 2025	Una empresa barranquillera del sector comercial y dedicada al sector de servicios especiales de comida, fue víctima de un ataque de ransomware.	El grupo de ransomware **Arcus Media** afirma haber realizado el ataque
Ransomware	24 de Julio de 2025	Una empresa del sector comercio, dedicada a la distribución mayorista de soluciones tecnológicas especializadas en seguridad electrónica, redes y comunicaciones, fue víctima de un ataque de ransomware.	El grupo **INC Ransom** se atribuyó el ataque contra la empresa colombiana a través de la publicación de información relacionada en su sitio de filtraciones.

Panorama nacional:

En Colombia, se ha identificado actividad maliciosa asociada a diversas amenazas cibernéticas, tanto en forma de troyanos de acceso remoto (RAT), *stealers* y kits diseñados para evadir la autenticación en dos pasos (2FA). Entre las amenazas más detectadas se encuentran los kits de phishing **Tycoon 2FA**, **Lumma** y **EvilProxy**, que lideran el ranking con cifras superiores a mil detecciones, siendo **Tycoon 2FA** el más reportado.

Estas herramientas representan un alto riesgo al permitir que los ciberdelincuentes evadan medidas de seguridad como el doble factor de autenticación, accediendo a cuentas personales y corporativas. Asimismo, se han observado altos niveles de circulación de *malware* como **Xworm**, **AgentTesla**, **AsyncRAT** y **Remcos**, que permiten el control remoto de dispositivos comprometidos.

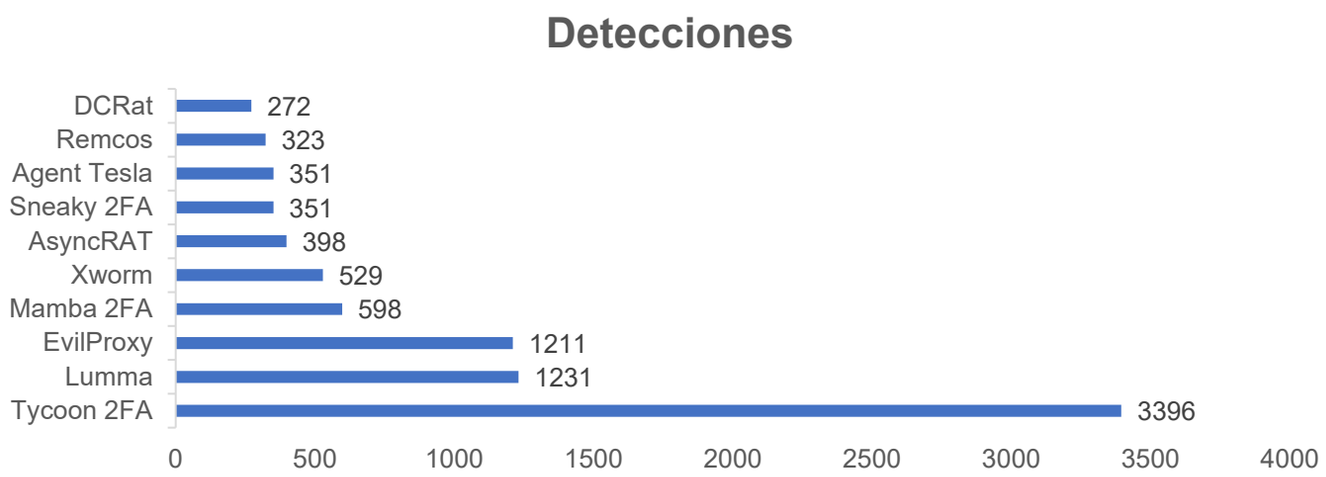


Gráfico 1. Detección visualizadas. Fuente: ANY RUN.

Ransomware en la región:

Durante esta semana se confirmaron varios ataques de *ransomware* en América Latina, afectando a organizaciones en Brasil, Argentina y Chile. Estos incidentes, atribuidos a variantes como **Cicada3301**, **Handala** y **Direwolf**, evidencian una evolución en la diversificación de grupos y técnicas usadas por los ciberdelincuentes en la región.

La presencia de estos ataques en distintos países sugiere una estrategia regional dirigida, que podría ampliarse hacia otros sectores o territorios, incluida Colombia. Este comportamiento debe interpretarse como una alerta para reforzar los planes de respuesta a incidentes y la protección de infraestructuras críticas.

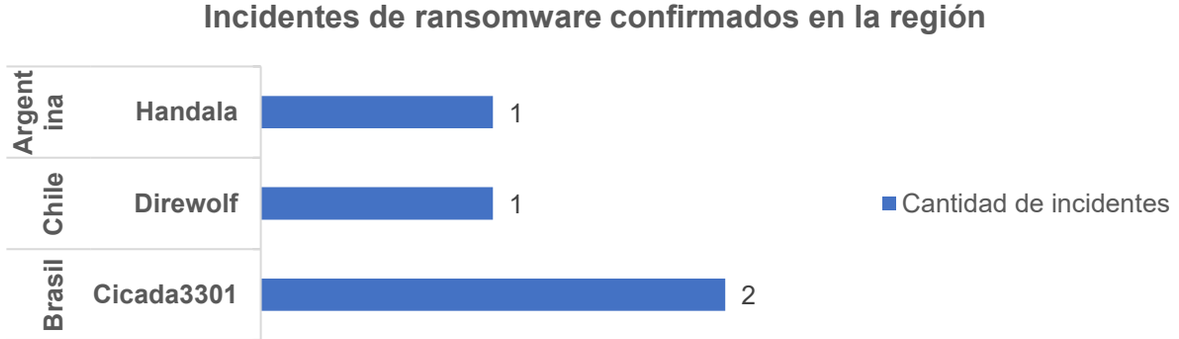


Gráfico 2. Incidentes de ransomware a nivel regional. Fuente: foros deep y dark web, ransomware.live

Vulnerabilidades críticas:

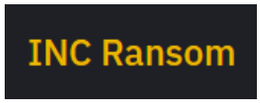
Durante la semana se identificaron vulnerabilidades críticas en plataformas tecnológicas ampliamente utilizadas, estas debilidades permiten que los ciberdelincuentes accedan sin autorización a servidores, capturen información, suplanten identidades o tomen el control de sistemas. Algunas de las plataformas afectadas incluyen Microsoft **SharePoint**, **Citrix** (NetScaler), **Cisco**, **Fortinet** y **VMware**, todas herramientas claves en entornos corporativos y gubernamentales.

El impacto de estas fallas puede ser grave, ya que habilitan ataques remotos sin necesidad de contraseñas y con privilegios elevados, incluso desde internet. Si estas vulnerabilidades no se corrigen a tiempo mediante actualizaciones, podrían ser aprovechadas por actores de amenaza para lanzar ataques dirigidos, comprometer datos confidenciales o paralizar servicios esenciales. Por eso es clave que las organizaciones apliquen los parches de seguridad recomendados cuanto antes.

Vulnerabilidad / Plataforma	CVE(s)	Impacto principal	CVSS
Microsoft SharePoint “ToolShell”	CVE-2025-53770	Ejecución remota de código (RCE)	9,8
CitrixBleed 2 (NetScaler ADC/Gateway)	CVE-2025-5777	Captura de información sin necesidad de autenticación	9,3
Cisco ISE / ISE-PIC	CVE-2025-20337	Ejecución remota de código como usuario root sin autenticarse	10
FortiWeb (Fortinet)	CVE-2025-25257	Inyección SQL sin autenticación que permite ejecución remota de código (RCE)	9,8
VMware (ESXi/Workstation/Fusion + Tools)	Varios (41236-39)	Ejecución remota de código en el host, fuga de información y evasión	9,8

Análisis de Actores y Campañas Activas:

Se identificó actividad del grupo hacktivista **CyberTeam**, conocido por realizar ataques de defacement con motivaciones políticas y sociales. En esta ocasión, se atribuyeron la modificación del sitio web del Partido Liberal Colombiano, evidenciando su interés en objetivos simbólicos con alta visibilidad. Por otro lado, el ransomware **Arcus Media** ha sido vinculado a campañas recientes en América Latina, aunque aún no se ha identificado con claridad un actor específico detrás de su operación, lo que podría indicar un grupo nuevo o en evolución. Finalmente, el grupo **INC Ransom**, activo desde 2023, continúa ejecutando ataques dirigidos a empresas medianas del sector tecnológico y comercial, como en el caso reciente de Lince Colombia, enfocándose en la exfiltración y cifrado de datos para extorsión. La actividad de estos actores refuerza la necesidad de monitorear tanto amenazas motivadas políticamente como aquellas orientadas al lucro económico.



Recomendaciones estratégicas:

- Crear contraseñas que combinen letras, números y símbolos, y que no sean fáciles de adivinar. Es importante no utilizar la misma contraseña en varias cuentas. Cuando una plataforma lo permita, se debe activar la verificación en dos pasos, pero siempre con precaución frente a mensajes o enlaces que intenten engañar para robar ese segundo código.
- Evitar abrir archivos o hacer clic en enlaces desconocidos sin confirmar su origen, incluso si parecen venir de personas conocidas. La verificación antes de abrir cualquier contenido es clave para evitar riesgos como el robo de información o el secuestro de archivos.
- Revisar con frecuencia que los equipos, dispositivos móviles, aplicaciones y software de protección estén al día. Esta acción sencilla ayuda a prevenir ataques que pueden afectar tanto a personas como a empresas.
- Guardar copias de seguridad de la información importante. En caso de un ataque que cifre los archivos del equipo, tener una copia de seguridad guardada en otro lugar puede marcar la diferencia. Esta medida permite recuperar la información sin depender de los atacantes ni ceder ante sus exigencias económicas.

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

La información contenida en este informe fue recopilada a partir de fuentes abiertas (OSINT) y bases de datos reconocidas internacionalmente, permitiendo un análisis de contexto sobre los incidentes de ciberseguridad observados.

Se utilizó información técnica de alta fiabilidad proveniente de la National Vulnerability Database (NVD) del NIST para identificar y caracterizar vulnerabilidades críticas reportadas en diversas plataformas. Así mismo, se incluyeron datos de plataformas especializadas como ransomware.live y ANY.RUN, las cuales recopilan, respectivamente, reportes en tiempo real sobre campañas activas de malware a partir de sitios de filtración en la dark web y análisis dinámicos de archivos en entornos controlados. Estas plataformas son comúnmente utilizadas por analistas de amenazas, pero pueden tener limitaciones debido a la naturaleza cambiante y anónima de los grupos criminales.

Se incorporó además información proveniente de la cuenta oficial del grupo hacktivista CyberTeam en la plataforma X. Si bien la credibilidad de las publicaciones en redes sociales puede variar, en este caso, los mensajes fueron consistentes con otras fuentes técnicas y de contexto. Las principales limitaciones encontradas incluyen vacíos de información sobre los actores detrás de Arcus Media e INC Ransom, lo que obliga a depender parcialmente de la atribución por comportamiento y de las publicaciones en foros no oficiales. A pesar de estas limitaciones, el nivel de confianza general de la información utilizada se considera medio-alto, dado el cruce de múltiples fuentes OSINT confiables y evidencia técnica observable.

1. NIST NVD, 19/07/2025, 19/07/2025, "CVE-2025-53770", Fuente oficial técnica, https://nvd.nist.gov/vuln/detail/CVE-2025-53770

2. NIST NVD, 19/07/2025, 19/07/2025, "CVE-2025-5777", Fuente oficial técnica, https://nvd.nist.gov/vuln/detail/CVE-2025-5777

3. NIST NVD, 19/07/2025, 19/07/2025, "CVE-2025-20337", Fuente oficial técnica, https://nvd.nist.gov/vuln/detail/CVE-2025-20337

4. NIST NVD, 19/07/2025, 19/07/2025, "CVE-2025-25257", Fuente oficial técnica, https://nvd.nist.gov/vuln/detail/CVE-2025-25257

5. NIST NVD, 20/07/2025, 20/07/2025, "CVE-2025-41236", Fuente oficial técnica, https://nvd.nist.gov/vuln/detail/CVE-2025-41236

6. NIST NVD, 20/07/2025, 20/07/2025, "CVE-2025-41237", Fuente oficial técnica, https://nvd.nist.gov/vuln/detail/CVE-2025-41237

7. NIST NVD, 20/07/2025, 20/07/2025, "CVE-2025-41238", Fuente oficial técnica, https://nvd.nist.gov/vuln/detail/CVE-2025-41238

8. NIST NVD, 20/07/2025, 20/07/2025, "CVE-2025-41239", Fuente oficial técnica, https://nvd.nist.gov/vuln/detail/CVE-2025-41239

9. X (CyberTeam), 14/07/2025, 14/07/2025, “Ataque de defacement contra sitios colombianos”, Fuente OSINT – redes sociales, https://x.com/cyberteam2009/status/1944971190977593822

10. Ransomware.live, 14-24/07/2025, 24/07/2025, "Seguimiento de campañas ransomware de Arcus Media, INC Ransom, Handala, Direwolf y Cicada3301", Plataforma OSINT – foros y sitios de filtración, https://www.ransomware.live/

11. ANY.RUN, 14-24/07/2025, 24-24/07/2025, "Análisis dinámico de muestras asociadas a campañas de ransomware en la región", Plataforma OSINT – entornos controlados, https://any.run/

Elaboración: ColCERT