

Resumen Ejecutivo

Durante la última semana en Colombia se mantiene la tendencia de afectaciones y ataques cibernéticos que afectaron a entidades del sector privado y público, generando la inoperatividad de los servicios y minando la confianza de la ciudadanía. A nivel regional, se observó un incremento en la actividad de *ransomware* en Brasil y Ecuador, con impacto en sectores clave como comercio, industria y tecnología. Paralelamente, se identificaron vulnerabilidades críticas en plataformas ampliamente utilizadas (**Cisco**, **Fortinet**, **WordPress** y *frameworks* de servidores), con riesgo de comprometer infraestructuras críticas mediante la ejecución remota de código o denegación de servicio. El panorama evidencia un riesgo creciente para las organizaciones que no adopten medidas preventivas inmediatas, lo que exige fortalecer la gestión de vulnerabilidades (actualizaciones de seguridad), monitoreo y plan de respuesta a incidentes para mitigar impactos futuros.

Tendencias nacionales observadas

- ❑ Los kits de phishing como **Tycoon 2FA** continúan siendo protagonistas y se mantienen en la delantera en los reportes de amenazas detectadas en Colombia, mostrando sofisticación en técnicas para evadir controles de autenticación y comprometer usuarios en diversos sectores. Además se ha detectado un aumento en la actividad del *stealer* **Lumma** en Colombia, lo que refuerza la necesidad de mantener medidas de vigilancia y protección reforzadas.
- ❑ Los sectores más vulnerables a ciberataques en Colombia incluyen el sector gubernamental (impuestos), comunicaciones y financiero. Estos sectores manejan información sensible y servicios esenciales, lo que los convierte en objetivos preferentes para ataques como *phishing* y explotación de vulnerabilidades técnicas. Además, las infraestructuras críticas y los servicios públicos esenciales están especialmente expuestos debido a su importancia para la continuidad operativa y la seguridad nacional. La creciente sofisticación de los ataques y el aumento en la frecuencia de incidentes exigen una respuesta coordinada en estas áreas clave.



Panorama nacional

A nivel nacional, se observaron dos tendencias relevantes: por un lado, el uso persistente de defacement como vector de impacto reputacional contra un portal del sector educativo, evidenciando superficies web desactualizadas y controles débiles de cambio y autenticación. Por otro, un incidente en una entidad estatal derivó en inoperatividad de plataformas y generación de trámites erróneos hacia la ciudadanía, revelando brechas en segregación de funciones, validaciones de procesos y resiliencia operativa.

Sector	Número de casos	Amenazas	Posible actor involucrado	Nivel alerta
Gobierno	1	Compromiso de aplicaciones	Desconocido	Alto
Educación	1	Defacement	Hidden Cyber Crime	Alto

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

En la comparativa semanal de detecciones en Colombia se observa que el kit de phishing **Tycoon 2FA** mantiene la mayor actividad. **Lumma stealer** y **Quasar RAT** muestran un crecimiento notable. También se registra un ascenso en **AsyncRAT**, mientras que amenazas como **Agent Tesla**, **Mamba 2FA** y **LokiBot** presentan una disminución. Estos cambios reflejan una tendencia hacia el fortalecimiento de campañas que buscan eludir autenticación multifactor y el control remoto de sistemas.

Comparativa entre semanas

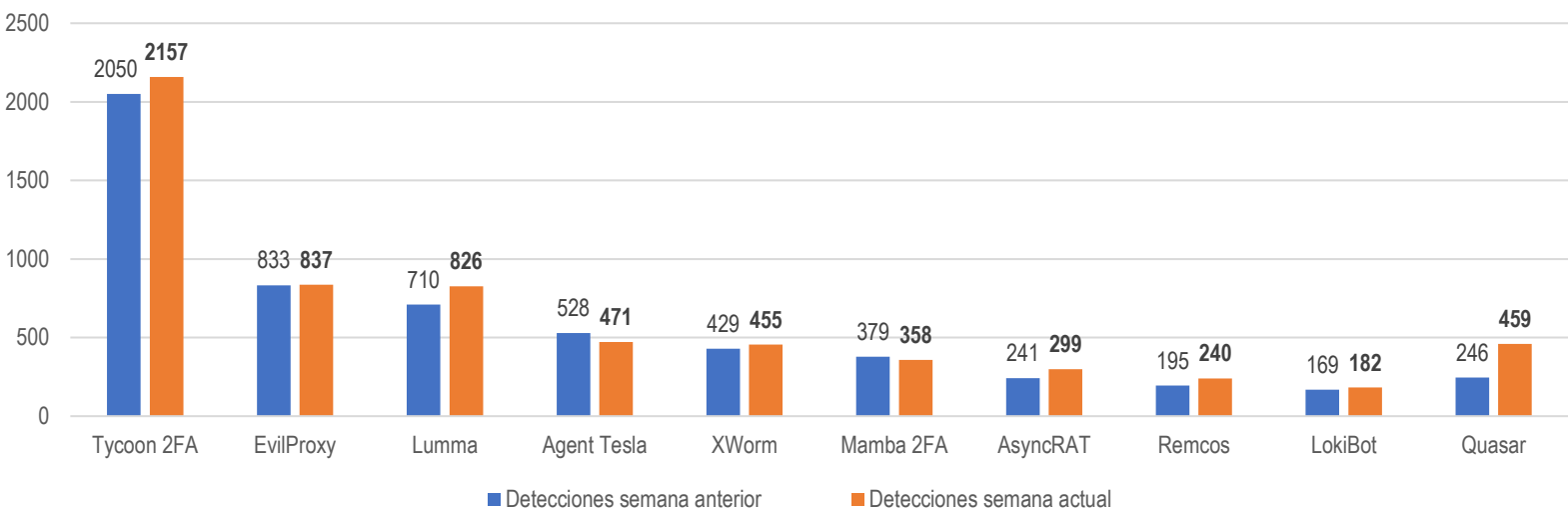


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.



Panorama regional

En el panorama regional se ha identificado un aumento de ataques con *ransomware*, los cuales bloquean la información de las víctimas para luego exigir un pago a cambio de recuperarla. En la última semana, se observaron incidentes en Brasil y Ecuador dirigidos a sectores como comercio, industria y tecnología. Estos ataques han sido atribuidos a grupos de ciberdelincuentes como **Medusa**, **Beast** y **Warlock**, que buscan afectar tanto a empresas como a servicios esenciales. Dado que estas amenazas no reconocen fronteras, resulta fundamental mantener la alerta, ya que estos grupos podrían expandir sus operaciones y llegar a impactar a organizaciones y ciudadanos en Colombia.

Sector	Técnica / Vector predominante	Locación	Posible actor involucrado	Nivel alerta
Comercio	Ransomware	Brasil	Medusa	Alta
Industria	Ransomware	Brasil	Beast	Alta
Tecnológico	Ransomware	Ecuador	Warlock	Alta

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

Vulnerabilidades críticas

Durante la semana se identificaron vulnerabilidades críticas que afectan a plataformas ampliamente utilizadas en entornos corporativos y de uso cotidiano. Entre ellas destacan fallas en **Cisco** y **Fortinet**, que permiten la ejecución remota de código sin autenticación; en **Google Chrome**, que posibilita la manipulación de memoria para ejecutar acciones maliciosas al visitar páginas web; en implementaciones de **HTTP/2**, expuestas a ataques de denegación de servicio; y en un plugin de **WordPress**, con riesgo de inyección de comandos remotos. Todas presentan altos puntajes de severidad, lo que resalta la urgencia de aplicar actualizaciones y parches de seguridad para evitar compromisos masivos.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Cisco Secure Firewall Management Center (FMC)	CVE-2025-20265	Ejecución remota de comandos/código sin autenticación si FMC usa RADIUS para GUI o SSH.	10.0
Fortinet FortiSIEM	CVE-2025-25256	Ejecución remota de código sin autenticación.	9.8
Google Chrome	CVE-2025-9132	permitir a un atacante corromper memoria y ejecutar código arbitrario de forma remota al visitar una página HTML especialmente diseñada	8.8
Plataformas y servidores como Apache Tomcat, Netty, F5 BIG-IP, Fastly, Varnish, así como otros frameworks que integran HTTP/2.	CVE-2025-8671	Vulnerabilidad de denegación de servicio (DoS) en implementaciones de HTTP/2.	7.5
Plugin Cloudflare Image Resizing de WordPress	CVE-2025-8723	Inyección de comandos remota sin autenticación.	9.8

Tabla 3. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de actores y campañas activas

Medusa es un grupo de ransomware operando bajo el modelo Ransomware-as-a-Service (RaaS), activo desde 2021. Utiliza un doble esquema de extorsión: cifra datos de sus víctimas y amenaza con filtrarlos públicamente si no se paga el rescate. Desde 2025, ha escalado su alcance en América Latina, impactando especialmente sectores como salud, educación, tecnología, manufactura, legal y aseguradoras, con más de 300 víctimas identificadas, lo que generó alertas de entidades como el FBI y CISA.



Beast funciona también como RaaS desde 2022 y ofrece a sus afiliados la posibilidad de generar versiones personalizadas para Windows, Linux y sistemas ESXi, adaptándose así a entornos diversos. Cuenta con una plataforma dinámica de desarrollo con soporte técnico para cambios frecuentes en sus binaries. Sus capacidades técnicas incluyen cifrado avanzado (Elliptic-curve y ChaCha20), eliminación de copias de respaldo y escaneo de subredes para realizar movimiento lateral.



Warlock emergió en 2025 como un actor sofisticado que explota vulnerabilidades en Microsoft SharePoint. Su modus operandi inicia con un *exploit* en servidores expuestos, seguida de la instalación de *webshells*, escalamiento de privilegios, movimientos laterales, captura de credenciales y ejecución de *ransomware*. Además, combina cifrado de datos con exfiltración (double extortion) y uso de herramientas como RClone. **Warlock** ha afectado organizaciones en sectores tecnológicos, gubernamentales y de infraestructura crítica a nivel global, alcanzando múltiples víctimas en pocos días.



Recomendaciones

- ❑ Implementar **planes de respaldo seguros**, implementación de métodos de aislamiento de aire, segmentación de redes, actualización de sistemas críticos y monitoreo continuo de accesos remotos. Realizar simulaciones de respuesta para garantizar tiempos efectivos de recuperación. Todo esto para fortalecer las medidas en contra de ransomware.
- ❑ Para la prevención de **defacement** y ataques a portales web, se debe **mantener actualizados los CMS, plugins y servidores web**, además de aplicar configuraciones seguras de Apache/Nginx, implementar un Web Application Firewall (WAF) y sistemas de detección de intrusos (IDS/IPS) que permitan identificar accesos no autorizados.
- ❑ **Aplicar parches** de seguridad de manera prioritaria en plataformas como Cisco, Fortinet, navegadores y WordPress. Establecer un **procedimiento de gestión de vulnerabilidades** que permita reducir la ventana de exposición.
- ❑ Contar con un **plan de continuidad de negocio** y de recuperación ante desastres (BCP/DRP) que contemplen fallas en servicios tecnológicos y transaccionales, caídas de sistemas críticos. Además garantizar disponibilidad mediante **sistemas de respaldo eléctrico** (UPS, plantas de energía), enlaces de comunicaciones alternos y ambientes de contingencia para mantener la operación frente a incidentes.
- ❑ Dar seguimiento a actores como **Medusa, Beast y Warlock**, que han demostrado capacidad de expansión en América Latina, con la posibilidad de impactar organizaciones colombianas en el corto plazo.
- ❑ Reforzar la capacitación en detección de phishing, uso responsable de credenciales, higiene digital (contraseñas seguras, MFA) y procedimientos claros para escalar incidentes.

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

El presente documento procesa la información evaluando de manera crítica la credibilidad y confianza de las fuentes abiertas (OSINT), ya que de ellas depende la solidez de los argumentos expuestos y el nivel de investigación en el análisis. En este sentido, fuentes como NVD (National Vulnerability Database), ofrecen un alto grado de credibilidad y confiabilidad. Sin embargo, existen limitaciones, así como posibles vacíos de información en la cobertura de incidentes locales, dado el constante cambio de las amenazas cibernéticas y su impacto en las organizaciones.

Ransomware.live, 21/08/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración.

 <https://www.ransomware.live/>

Any Run, 21 de agosto de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.

 <https://any.run/malware-trends/>

NVD, 2025-08-14, 2025-08-21, Cisco Secure Firewall Management Center (FMC) RADIUS Authentication Remote Command Execution Vulnerability (CVE-2025-20265), Base de datos de vulnerabilidades oficial.

 <https://nvd.nist.gov/vuln/detail/CVE-2025-20265>

NVD, 2025-07-18, 2025-08-21, Fortinet FortiSIEM Remote Code Execution Vulnerability (CVE-2025-25256), Base de datos de vulnerabilidades oficial.

 <https://nvd.nist.gov/vuln/detail/CVE-2025-25256>

NVD, 2025-08-19, 2025-08-21, Google Chrome Heap Buffer Overflow in ANGLE Vulnerability (CVE-2025-9132), Base de datos de vulnerabilidades oficial.

 <https://nvd.nist.gov/vuln/detail/CVE-2025-9132>

NVD, 2025-08-15, 2025-08-21, HTTP/2 Multiple Implementations Denial of Service Vulnerability (CVE-2025-8671), Base de datos de vulnerabilidades oficial.

 <https://nvd.nist.gov/vuln/detail/CVE-2025-8671>

NVD, 2025-08-18, 2025-08-21, WordPress Plugin Cloudflare Image Resizing Remote Command Injection (CVE-2025-8723), Base de datos de vulnerabilidades oficial.

 <https://nvd.nist.gov/vuln/detail/CVE-2025-8723>

WeLiveSecurity, 2025-03-04, 2025-08-21, Medusa: cómo opera este ransomware en América Latina, Medio especializado en ciberseguridad.

 <https://www.welivesecurity.com/es/ransomware/medusa-como-opera-america-latina/>

Cybereason, 2023-01-17, 2025-08-21, Threat Analysis: Beast Ransomware, Blog técnico especializado.

 <https://www.cybereason.com/blog/threat-analysis-beast-ransomware>

Trend Micro Research, 2025-08-06, 2025-08-21, Warlock Ransomware: How a New Group is Weaponizing Unpatched SharePoint Servers, Informe de investigación en ciberseguridad.

 https://www.trendmicro.com/en_us/research/25/h/warlock-ransomware.html