Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20250831 - 004

TLP:CLEAR

Resumen Ejecutivo

En la última semana se han identificado vulnerabilidades, las cuales requieren atención prioritaria debido a su potencial explotación en entornos sensibles. Paralelamente, se observa un incremento en la actividad de grupos de **ransomware**, que continúan enfocando sus campañas en sectores estratégicos, manteniendo esta amenaza como una de las principales a nivel global y local. A nivel de fraude digital, se ha detectado un **aumento en la creación de sitios de suplantación dirigidos a entidades oficiales**, lo que representa un riesgo significativo para los ciudadanos y organizaciones.

Adicionalmente, se registra un **repunte en la actividad del grupo hacktivista Deface Perú, motivado por tensiones políticas y territoriales.** Finalmente, en Colombia los sectores, financiero, gubernamental, salud y telecomunicaciones se posicionan como los más afectados por incidentes de ciberseguridad, siendo prioritario fortalecer sus estrategias de prevención, detección y respuesta.

Tendencias nacionales observadas

- En los últimos días se ha identificado la circulación de **sitios fraudulentos** diseñados para suplantar portales oficiales, con el objetivo de recolectar información sensible y credenciales bancarias de los usuarios. Estas páginas imitan procesos de gestión digital y trámites en línea, representando un riesgo significativo para la ciudadanía y las organizaciones.
- De igual manera, se ha observado un incremento en la actividad de **grupos hacktivistas** como Deface Perú, lo que coincide con las tensiones políticas y territoriales que se presentan actualmente en la región. *Dicho grupo continúa enfocando sus campañas en la exposición de información confidencial.*

- En el contexto nacional, los sectores más impactados por incidentes cibernéticos corresponden al **financiero**, **gubernamental** y de **telecomunicaciones**. Estos entornos han sido los más afectados por campañas de fraude digital en las últimas semanas.

Panorama nacional

La comparativa semanal de detecciones en Colombia muestra que el kit de phishing **Tycoon 2FA** continúa siendo el más predominante con un aumento notable, consolidándose como la amenaza más activa. También se observan crecimientos en **EvilProxy** y **Lumma** *stealer*, lo que evidencia un refuerzo en campañas de la captura de credenciales y datos sensibles.

Los troyanos de acceso remoto (RAT) como **AgentTesla** y **Remcos** tuvieron incrementos relevantes, mientras que otras amenazas como **XWorm** y **AsyncRAT** registraron leves variaciones sin cambios significativos. En contraste, algunos como **Rhadamanthys** *stealer* mostraron una disminución. En general, la tendencia refleja un repunte en familias orientadas al fraude, captura de información y control remoto de sistemas, lo que resalta la necesidad de fortalecer la vigilancia y las medidas de protección en el entorno local.

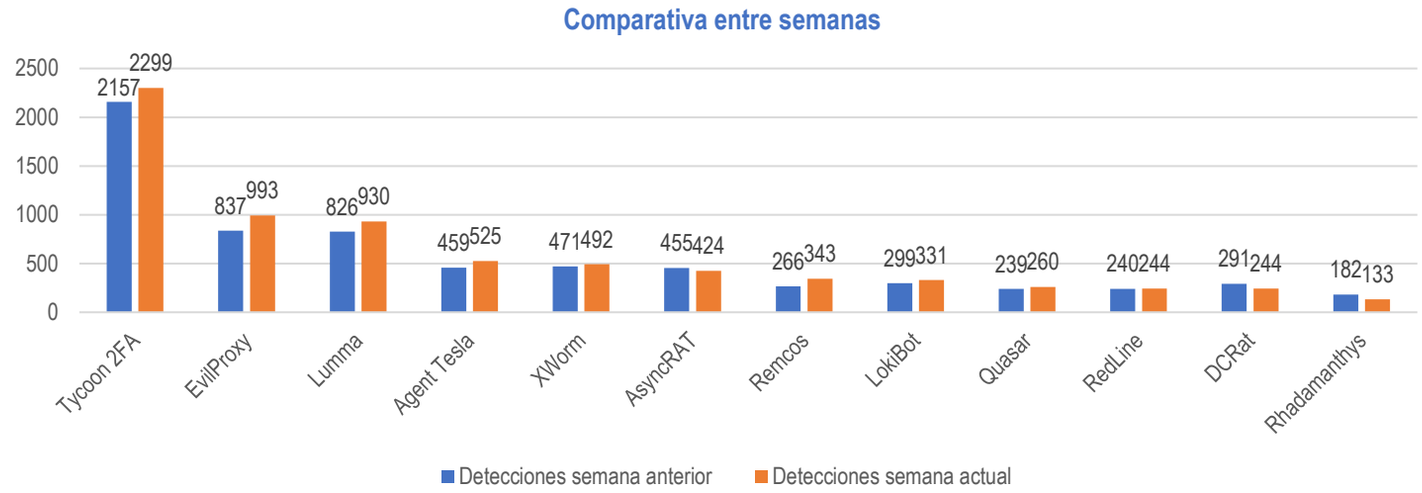


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Los grupos regionales de ransomware combinan fallas sin parche con phishing dirigido y exfiltración previa al cifrado, lo que exige parcheo inmediato y MFA resistente a phishing.

Panorama regional

En el panorama regional reciente se ha evidenciado una intensificación de la actividad de distintos grupos de ransomware, entre ellos **Direwolf**, **Safepay** y **Dragonforce**. Estos actores han centrado sus campañas en sectores estratégicos como comercio, industria y turismo.

La recurrencia de estas operaciones refleja no solo el interés de los grupos criminales por explotar infraestructuras críticas y de alto valor económico, sino también la necesidad de reforzar medidas de prevención, monitoreo y respuesta ante incidentes cibernéticos en la región.

Sector	Técnica / Vector predominante	Locación	Posible actor involucrado	Nivel alerta
Comercio e Industria	Ransomware	Brasil	Direwolf	**Alta**
Comercio	Ransomware	México	Safepay	**Alta**
Turismo	Ransomware	Costa Rica	Dragonforce	**Alta**
Gobierno	Filtración de datos	Ecuador	Gatito_FBI_Nz	**Alta**

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

Vulnerabilidades críticas

Durante esta semana se identificaron vulnerabilidades críticas que afectan a infraestructuras ampliamente utilizadas en entornos empresariales y de desarrollo. En primer lugar, se reportó la CVE-2025-7775 en **Citrix NetScaler ADC/Gateway**, la cual permite ejecución remota de código (RCE) y denegación de servicio (DoS) bajo configuraciones específicas de IPv6/HDX.

La vulnerabilidad CVE-2025-9074 en **Docker Desktop** expone la posibilidad de escape de contenedores maliciosos, comprometiendo el motor Docker, accediendo a archivos del host y tomando control total de la máquina.

Finalmente, la CVE-2025-54988 afecta a **Apache Tika** en el módulo tika-parser-pdf, permitiendo ataques XXE que pueden derivar en la exfiltración de información sensible o en el envío de solicitudes maliciosas desde archivos PDF manipulados.

Estas vulnerabilidades resaltan la necesidad urgente de aplicar parches de seguridad y medidas de mitigación, ya que comprometen directamente la confidencialidad, integridad y disponibilidad de sistemas críticos en múltiples sectores.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Citrix NetScaler ADC/Gateway	CVE-2025-7775	RCE y/o DoS en NetScaler ADC y Gateway bajo ciertas configuraciones IPv6/HDX.	9.8
Docker Desktop – Container escape / acceso API	CVE-2025-9074	Contenedores maliciosos pueden escapar (escape), controlar el motor Docker, montar archivos del host, y potencialmente comprometer completamente el host.	9.3
Apache Tika – XXE en PDF (módulo tika-parser-pdf)	CVE-2025-54988	XXE permite leer datos sensibles o realizar solicitudes maliciosas desde archivos PDF.	9.8

Tabla 2. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de Actores y Campañas Activas

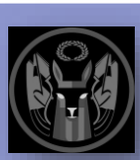
Deface Perú es un colectivo hacktivista que ejecuta desfiguraciones de sitios web institucionales y privados. Su objetivo principal es la protesta digital y la propaganda, afectando la reputación de las entidades comprometidas.

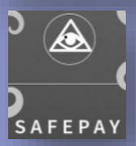
Direwolf es un ransomware que opera con técnicas de cifrado y doble extorsión. Infiltra redes, cifra sistemas y exfiltra datos para exigir rescate y extorsionar a víctimas en múltiples países y sectores.

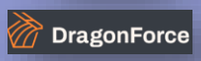
Safepay es un grupo y cepa de ransomware de rápido crecimiento detectado en 2025. Ataca principalmente MSPs y empresas, combina acceso a redes, cifrado de archivos y captura de información para realizar extorsión y afectar cadenas de servicio.

Dragonforce es un operador de ransomware as a service (RaaS) con variantes derivadas de familias conocidas. Ha sido ligado a incidentes de alto impacto donde compromete entornos empresariales, despliega cifrado y exfiltración, y coordina campañas que han causado interrupciones significativas en retail y otros sectores.

Gatito_FBI_Nz es un actor emergente con presencia en foros y redes sociales. Se centra en campañas de propaganda, publicación de supuestos accesos a infraestructuras y generación de ruido mediático, con impacto reputacional en sus objetivos.







Recomendaciones

Frente a ransomware se debe aplicar una estrategia de copias de seguridad 3-2-1 (3 copias, 2 medios distintos, 1 fuera de línea) con pruebas de restauración periódicas. Implementar segmentación de red y controles de privilegios mínimos (PAM) para reducir la superficie de propagación. Activar controles de aislamiento automático en EDR/EDX cuando se detecten procesos de cifrado masivo o uso indebido de utilidades legítimas (ej. vssadmin.exe, bcdedit.exe).

Reforzar la seguridad de portales web y CMS: parches actualizados, WAF con reglas antidefacement, control de integridad de archivos (File Integrity Monitoring).

Para la identificación de troyanos de acceso remoto (RAT) y stealers se debe activar detección de procesos living-off-the-land (ej. uso anómalo de MSBuild.exe, csc.exe, PowerShell). Monitorizar tráfico C2 en puertos poco comunes y uso de protocolos cifrados no estándar. Aplicar control de aplicaciones (AppLocker / WDAC) para evitar ejecución de binarios no firmados.

- Usar contraseñas robustas y habilitar el doble factor de autenticación (2FA) en todas las cuentas. **No reutilizar la misma contraseña en varios servicios.** Validar siempre la fuente oficial antes de compartir información sensible o documentos de interés público.
- Adoptar un ciclo de gestión de parches continuo con priorización basada en CVSS y explotación. Desinstalar software que ya no se utilice. **Usar un firewall personal para reducir la exposición de puertos y servicios innecesarios.**
- **Implementar un plan de búsqueda proactiva de amenazas (Threat Hunting) para identificar de forma temprana indicios de ransomware y programas de robo de información.** Este plan debe usar fuentes de inteligencia (OSINT/CTI), correlación en las herramientas de monitoreo (SIEM/EDR) y apoyarse en el marco de MITRE ATT&CK. Con esto se pueden detectar accesos iniciales sospechosos antes de que se conviertan en incidentes graves.

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

Las fuentes utilizadas son de OSINT, las cuales combinan repositorios oficiales (NVD, alta confiabilidad), reportes de empresas de ciberseguridad, medios periodísticos y fuentes internas. En conjunto, ofrecen un nivel de confianza medio-alto, con fortalezas en la diversidad de perspectivas. Sin embargo, el documento tiene imitaciones por vacíos técnicos y la dinámica cambiante de las amenazas.

- **Ransomware.live, 28/08/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración.** https://www.ransomware.live/
- **Any Run, 28 de agosto de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.** https://any.run/malware-trends/
- **NVD (National Vulnerability Database), publicada el 26 de agosto de 2025, información actualizada el 27 de agosto de 2025, CVE-2025-7775, Fuente gubernamental (sitio oficial .gov).** https://nvd.nist.gov/vuln/detail/CVE-2025-7775
- **NVD (National Vulnerability Database), publicada el 20 de agosto de 2025, información actualizada el 25 de agosto de 2025, CVE-2025-9074, Fuente gubernamental (sitio oficial .gov).** https://nvd.nist.gov/vuln/detail/CVE-2025-9074
- **NVD (National Vulnerability Database), publicada el 20 de agosto de 2025, información actualizada el 25 de agosto de 2025, CVE-2025-54988, Fuente gubernamental (sitio oficial .gov).** https://nvd.nist.gov/vuln/detail/CVE-2025-54988
- **Trustwave SpiderLabs Blog, publicada el 24 de junio de 2025, información actualizada en la misma fecha, Dire Wolf Strikes: New Ransomware Group Targeting Global Sectors, Blog especializado en seguridad informática (empresa privada).** https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/dire-wolf-strikes-new-ransomware-group-targeting-global-sectors/
- **Group-IB Blog, publicada el 25 de septiembre de 2024, información actualizada en la misma fecha, Inside the Dragon: DragonForce Ransomware Group, Blog especializado en seguridad informática (empresa privada).** https://www.group-ib.com/blog/dragonforce-ransomware/
- **Check Point Cyber-Hub, publicada en 2025, información actualizada en la misma fecha, SafePay Ransomware: An Emerging Threat in 2025, Blog especializado en seguridad informática (empresa privada).** https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/safepay-ransomware/
- **Infobae, publicada el 4 de agosto de 2025, información actualizada en la misma fecha, Hackeo masivo a la PNP al descubierto: así operó 'Gatito FBI' para acceder y vender datos de miles de peruanos en la dark web, Medio de comunicación general (prensa digital).** https://www.infobae.com/peru/2025/08/04/hackeo-masivo-a-la-pnp-al-descubierto-asi-opero-gatito-fbi-para-acceder-y-vender-datos-de- miles-de-peruanos-en-la-dark-web/