Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20250914 - 006

TLP:CLEAR

Resumen Ejecutivo:

En la última semana se identificó una tendencia creciente de incidentes cibernéticos, reflejada en afectaciones tanto a organizaciones colombianas y también en Latinoamérica, evidenciando un interés creciente de los ciberdelincuentes en sectores estratégicos y gubernamentales. A nivel regional, los incidentes destacan la capacidad de los adversarios para realizar campañas disruptivas y de impacto mediático, lo que proyecta una intensificación futura de estos ataques.

En paralelo, se reportaron vulnerabilidades, como las asociadas a **BitLocker** y a la escalada de privilegios, que podrían ser aprovechadas para comprometer infraestructuras sensibles si no se aplican mitigaciones a tiempo. Asimismo, se observó actividad de *malware* dirigido, incluyendo variantes de ransomware y troyanos de acceso remoto, con técnicas de persistencia avanzadas para evadir defensas.

Finalmente, la presencia activa de actores de amenaza como **KillSec**, **TheGentlemen** y **Lynx** confirma la diversificación de tácticas y objetivos, lo que obliga a las organizaciones a fortalecer sus capacidades de detección temprana y respuesta proactiva, anticipando una mayor complejidad en el panorama de amenazas en el corto plazo.

Incidentes de la semana

En el siguiente cuadro se presentan los incidentes de ciberseguridad identificados en Colombia durante la última semana.

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Ransomware	06 - Sep - 2025	Una empresa del sector salud con sede en Barranquilla fue víctima de un ataque de ransomware.	KillSec
Ransomware	06 - Sep - 2025	Una empresa del sector salud con sede en Montería fue víctima de un ataque de ransomware.	KillSec
Defacement	05 - Sep - 2025	Entidad gubernamental identificó alteraciones en su portal web como resultado de un ataque de *defacement*.	Desconocido

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

Tendencias nacionales observadas

- En el país se han observado intentos de **explotación de vulnerabilidades** conocidas en servicios expuestos a internet, especialmente en plataformas de gestión empresarial y aplicaciones web. Los actores buscan aprovechar fallas sin parchear para obtener acceso no autorizado, instalar troyanos de acceso remoto o desplegar *ransomware*.

- Se ha detectado la evolución de **campañas de phishing** dirigidas a usuarios colombianos mediante el uso de **archivos SVG** con código embebido en HTML y JavaScript. Estos archivos, aparentemente inofensivos, buscan evadir los controles tradicionales de seguridad para redirigir a las víctimas hacia páginas fraudulentas de robo de credenciales bancarias y corporativas.

Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20250914 - 006

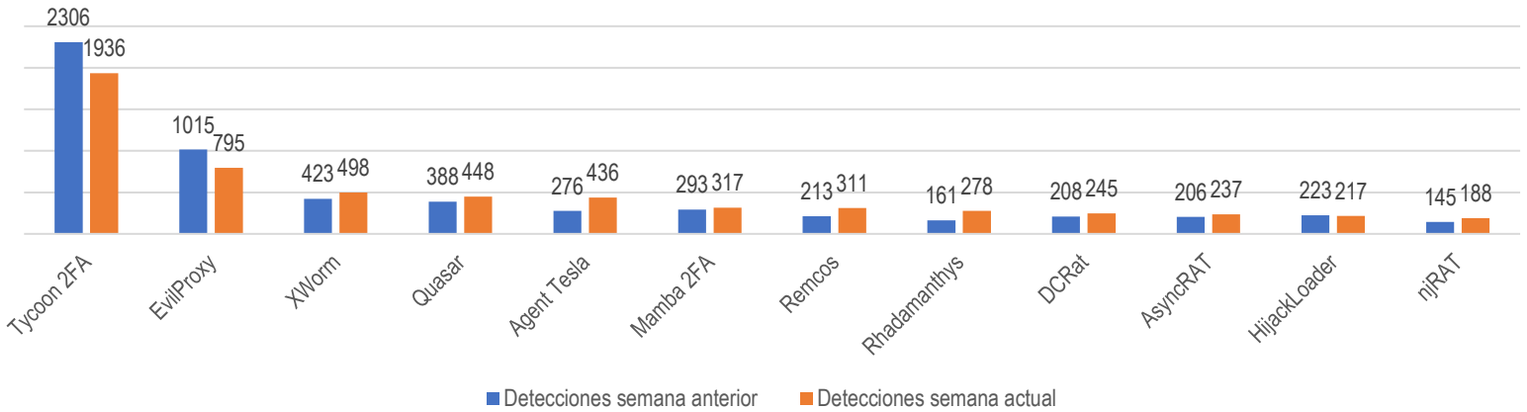
TLP:CLEAR

- Sitios web han sido blanco de **ataques de *defacement***, donde los ciberdelincuentes modifican la apariencia del sitio para difundir mensajes políticos, sociales o simplemente para demostrar capacidad de intrusión. Aunque el impacto técnico suele ser limitado, este tipo de incidentes afecta la reputación institucional y refleja fallas en la protección de servidores web y en la gestión de accesos.

Panorama nacional

En Colombia, la comparativa entre semanas muestra que los kit de *phishing* **Tycoon 2FA** y **EvilProxy** siguen siendo las amenazas más detectadas, aunque con una leve disminución frente a la semana anterior. En contraste, troyanos como **AgentTesla**, **Rhadamanthys** y **Quasar** evidenciaron un aumento en sus detecciones, lo que refleja una diversificación en las familias activas en el país. Otros como **Mamba 2FA**, **Remcos** y **AsyncRAT** mantienen niveles de actividad similares, consolidándose como amenazas persistentes en el entorno corporativo y ciudadano. Estos datos sugieren que, si bien algunas campañas pierden fuerza, surgen variantes con mayor alcance, lo que exige mantener medidas de protección actualizadas y estrategias de monitoreo constantes.

Comparativo entre semanas



Panorama regional

El panorama regional evidencia un incremento sostenido de ataques de ransomware dirigidos a sectores críticos como el minero-energético, salud, TIC y financiero en América Latina. En Perú se han registrado múltiples incidentes que afectan tanto al sector energético como al sanitario, atribuidos a los grupos **Lynx** y **KillSec**, mientras que en Brasil este último también ha estado activo contra empresas de tecnología. En el ámbito financiero, destaca la participación del grupo **Thegentlemen**, con operaciones que impactan a organizaciones en Venezuela, México, Colombia, Ecuador y Perú. La reiteración de estos incidentes con nivel de alerta alto refleja una presión creciente sobre la resiliencia de los sectores estratégicos de la región y subraya la necesidad de fortalecer capacidades de prevención, monitoreo y respuesta coordinada.

Sector	Técnica / Vector predominante	Locación	Posible actor involucrado	Nivel alerta
Minero-energético	Ransomware	Perú	Lynx	**Alto**
Salud	Ransomware	Perú	KillSec	**Alto**
TIC	Ransomware	Brasil	KillSec	**Alto**
Financiero	Ransomware	Venezuela	Thegentlemen	**Alto**
Financiero	Ransomware	México Colombia Ecuador, Perú	Thegentlemen	**Alto**

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

Vulnerabilidades críticas

Durante la última semana, las vulnerabilidades más relevantes identificadas impactaron a Microsoft Windows 10, Windows 11 y Windows Server, destacándose tres fallos de escalamiento de privilegios con altos puntajes CVSS. **Estas vulnerabilidades representan un riesgo significativo para entornos corporativos y requieren una pronta aplicación de parches de seguridad.**

Plataforma afectada	CVE	Impacto principal	Score CVSS
Microsoft Windows 10. Microsoft Windows 11. Microsoft Windows Server.	CVE-2025-54911	Permite a un atacante con credenciales locales de bajo privilegio y cierta interacción del usuario elevar privilegios hasta nivel SYSTEM.	**7.3**
Microsoft Windows 10. Microsoft Windows 11. Microsoft Windows Server.	CVE-2025-54912	Permite escalamiento de privilegios, posiblemente con menor necesidad de interacción del usuario, facilitando un control completo del sistema afectado.	**7.8**
Microsoft Windows 10. Microsoft Windows 11. Microsoft Windows Server.	CVE-2025-55234	Elevación de privilegios remota sin autenticación a través de explotación de fallos en mecanismos de autenticación del SMB, posibilidad de ataques de retransmisión.	**8.8**

Tabla 3. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de actores y campañas activas

- **KillSec**: Comenzó como un colectivo hacktivista con motivaciones geopolíticas (anti-Occidente, pro-Rusia), haciendo uso frecuente de DDoS, defacements y filtraciones de datos. Se ha transformado también en un actor con fines de lucro: ha lanzado un modelo de Ransomware-as-a-Service (RaaS), ofreciendo lockers, panel de afiliados y capacidades de personalización del ransomware. Su campaña reciente incluye ataques al sector salud en Colombia y Perú, así como a proveedores de software, con amenazas de exfiltrar datos sensibles si no se paga rescate.

- **The Gentlemen:** Es un grupo relativamente nuevo que ha irrumpido con fuerza en el panorama del ransomware. Se caracteriza por afectar a sectores con fuerte componente de OT (operational technology), construcción, manufactura, salud y seguros, y ha extendido su actividad por América del Sur, Asia-Pacífico, Estados Unidos y Medio Oriente. Utilizan tácticas avanzadas de evasión —como uso de drivers legítimos, abuso de GPOs (Group Policy Objects) para comprometer dominios enteros—, lo que eleva el riesgo para infraestructuras corporativas con redes amplias.

Análisis de actores y campañas activas

- **Lynx: E**s un grupo de ransomware bajo modelo RaaS, identificado alrededor de julio de 2024. Su modus operandi incluye phishing para acceso inicial, explotación de vulnerabilidades en soluciones de acceso remoto como VPN, recopilación de credenciales, movimiento lateral, eliminación de defensas de seguridad y doble extorsión.

Recomendaciones

- **Aplicar de inmediato los parches de seguridad oficiales** publicados por Microsoft y, en paralelo, habilitar políticas de control de cuentas de usuario (UAC) estrictas para reducir el riesgo de escalamiento no autorizado. Además, es aconsejable **implementar reglas en EDR/XDR** para la detección de procesos anómalos asociados a inyección de código y abuso de cifrado, de manera que la mitigación sea tanto preventiva como reactiva. Esta medida aplica específicamente para sistemas Windows en infraestructuras críticas.

- **Debe reforzarse** la supervisión de directorios críticos en Windows como *Startup* y *AppData/Roaming*, ya que allí suelen alojarse scripts y ejecutables diseñados para mantener persistencia. Se aconseja **integrar reglas YARA o Sigma** que identifiquen patrones asociados a la creación de archivos por lotes y ejecutables maliciosos. Esta recomendación aplica en escenarios donde se ha evidenciado el uso de **loader** y **RAT** que abusan de procesos legítimos para evadir controles.

- **Fortalecer las copias de seguridad** bajo esquemas 3-2-1 (tres copias en dos medios distintos, con una aislada fuera de línea) y realizar pruebas periódicas de recuperación. Asimismo, se recomienda **segmentar la red** para limitar la propagación lateral y establecer alertas tempranas sobre la creación de procesos masivos de cifrado. Esta práctica aplica especialmente en organizaciones de salud, entidades de gobierno y empresas del sector privado que han sido objetivos recientes de estas campañas.

- **Fortalecer los sistemas de monitoreo** de superficie de ataque externa (attack surface management) y contar con servicios de **inteligencia de amenazas** (Threat Intelligence) que permitan anticipar campañas de *defacement*, extorsión o captura de información. En este caso, resulta clave también aplicar controles en WAF y sistemas de detección de intrusos (IDS/IPS) para bloquear intentos de explotación de vulnerabilidades web, dado que estos actores han demostrado capacidad para generar alto impacto mediático y reputacional.

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

Las referencias utilizadas combinan fuentes oficiales y medios abiertos especializados en ciberseguridad, lo que aporta solidez y contraste en la multiplicidad de las fuentes de análisis. Mientras NVD de NIST ofrece alta credibilidad técnica, los portales especializados permiten comprender tendencias y actores emergentes. No obstante, algunos reportes presentan limitaciones en cuanto a la información publicada, por lo que se requiere complementar estos vacíos. Por lo anterior la información presentada cuenta con un nivel de credibilidad medio-alto.

Ransomware.live, 11/09/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 11 de septiembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
Microsoft Security Response Center (MSRC), 9 septiembre 2025, CVE-2025-54911 | BitLocker Elevation of Privilege Vulnerability, Fuente oficial del fabricante.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54911
Microsoft Security Response Center (MSRC), 9 septiembre 2025, CVE-2025-54912 | BitLocker Elevation of Privilege Vulnerability, Fuente oficial del fabricante.
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-54912
NIST, 09/09/2025, fecha de información 11/09/2025, "CVE-2025-55234: SMB Server might be susceptible to relay attacks …", fuente oficial / base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-55234
Daily Security Review, 29/07/2025, "Lynx Ransomware: INC Ransomware Reincarnated", blog / recurso de actores de amenazas.
https://dailysecurityreview.com/resources/threat-actors-resources/lynx-ransomware-inc-ransomware-reincarnated/
CSO Online, 10/09/2025, "Ransomware upstart 'The Gentlemen' raises the stakes for OT-heavy sectors", medio especializado en seguridad.
https://www.csoonline.com/article/4054790/ransomware-upstart-the-gentlemen-raises-the-stakes-for-ot%E2%80%91heavy-sectors.html
Cyber-Defence.io, 07/04/2025, "KillSec – Threat Actor Profile", informe / perfil de actor de amenaza.
https://cyber-defence.io/insights/killsec/