Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20250928 – 008

TLP:CLEAR

Resumen Ejecutivo

Durante la última semana, el panorama de ciberseguridad en Colombia y América Latina estuvo marcado por la persistencia de *ransomware* y campañas de *phishing* como principales amenazas, junto con un aumento de malware avanzado (Tycoon 2FA, EvilProxy, Agent Tesla, Remcos) dirigido a la captura de credenciales y control remoto.

Actores como **Qilin**, **Ciphbit** y **The Gentlemen** continúan desplegando operaciones con impacto en sectores estratégicos, confirmando el carácter transnacional de estas campañas. En paralelo, se identificaron vulnerabilidades críticas en Cisco, SolarWinds y Google Chrome, con puntajes CVSS altos que representan riesgos significativos para entornos corporativos.

Las PyMEs y usuarios finales se convierten en objetivos principales, mientras que los ciberdelincuentes integran IA y automatización para aumentar la efectividad de sus operaciones. Este contexto evidencia un nivel de riesgo elevado que exige fortalecer la capacidad defensiva, acelerar la gestión de parches y robustecer la concienciación de los usuarios para mitigar impactos futuros en la región.

Tendencias nacionales observadas

- **Ransomware como amenaza constante**: esta continúa siendo la amenaza más persistente para entidades públicas y organizaciones privadas. Los ciberdelincuentes mantienen la estrategia de "doble extorsión", que combina el cifrado de la información con la filtración de datos sensibles para aumentar la presión sobre las víctimas.

- **Ataques phishing como principal vector de ataque:** sigue consolidándose como la puerta de entrada más común de incidentes de seguridad digital en Colombia. A través de correos electrónicos falsos, mensajes instantáneos o sitios web fraudulentos, los ciberdelincuentes buscan engañar a colaboradores y ciudadanos para capturar credenciales y acceder a sistemas críticos. La facilidad de distribución y la baja inversión necesaria para ejecutar estas campañas convierten al phishing en una herramienta altamente rentable y peligrosa para los delincuentes.

- **PyMEs y usuarios finales como objetivos frecuentes**: las pequeñas y medianas empresas, así como los usuarios, son cada vez más el objetivo de ataques cibernéticos. Las pymes suelen contar con recursos limitados para implementar soluciones avanzadas de seguridad, lo que las hace vulnerables frente a ataques oportunistas. De igual forma, los ciudadanos pueden ser víctimas de fraudes en línea y captura de información personal, con impactos que van desde pérdidas económicas hasta suplantación de identidad.

- **Incremento del uso de malware con componentes de IA y automatización**: en el último año se ha evidenciado un crecimiento en el uso de *malware* que integra funciones de inteligencia artificial y automatización. Estas capacidades permiten a los ciberdelincuentes mejorar la evasión de defensas tradicionales, generar campañas de *phishing* más convincentes e incluso adaptar el código malicioso en tiempo real para dificultar su detección. La incorporación de estas tecnologías marca una evolución en la sofisticación de las amenazas que enfrentan las organizaciones colombianas.

Panorama nacional

Durante esta semana en Colombia se observó una alta actividad del kit de *phishing* **Tycoon 2FA**, que mantuvo la mayor cantidad de detecciones, consolidándose como una de las principales amenazas en circulación. También se identificaron campañas significativas de **EvilProxy** y **AgentTesla**, que continuaron apuntando a usuarios y organizaciones a través de técnicas de captura de credenciales y exfiltración de información.

Asimismo, los troyanos de acceso remoto como **AsyncRAT**, **Remcos** y **DCRat** tuvieron presencia relevante, evidenciando la persistencia de herramientas utilizadas para control remoto y espionaje en los sistemas comprometidos. Aunque en menor medida, se registraron detecciones de **HijackLoader** y la aparición puntual de **DarkCloud** y **Qilin ransomware**, lo que refleja la diversidad de familias activas y la constante adaptación de los actores maliciosos en el panorama local.

Comparativa entre semanas

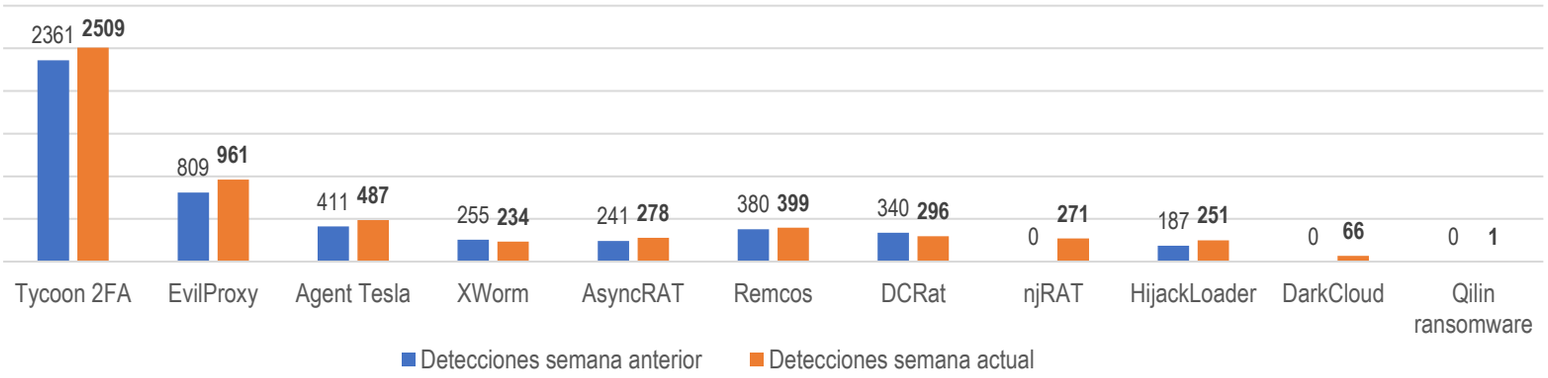

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la semana anterior, en la región de Latinoamérica se evidenció una superioridad del *ransomware* como principal técnica utilizada por los actores maliciosos, afectando diversos sectores estratégicos. En Brasil, el sector industrial fue impactado por el grupo **Ciphbit**, mientras que en Chile y la República Dominicana se observaron incidentes en los sectores de comercio y agricultura atribuidos al grupo **Qilin**, que ha mantenido una fuerte actividad en la región. Por su parte, en México se reportaron ataques contra el sector transporte, presuntamente vinculados al grupo **The Gentlemen**, lo que refleja una tendencia preocupante hacia la diversificación de objetivos y una intensificación de campañas contra infraestructuras críticas y productivas.

Sector	Técnica / Vector predominante	Locación	Posible actor involucrado	Nivel alerta
Industria	Ransomware	Brasil	Ciphbit	**Alto**
Comercio	Ransomware	Chile	Qilin	**Alto**
Agricultura	Ransomware	República Dominicana	Qilin	**Alto**
Transporte	Ransomware	México	The gentlemen	**Alto**

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

Vulnerabilidades críticas

Durante la semana **se identificaron vulnerabilidades críticas** que afectan plataformas ampliamente utilizadas a nivel empresarial y de usuario final. La de mayor severidad corresponde a Cisco Secure Firewall ASA/FTD (CVE-2025-20333) con un puntaje CVSS de 9.9. También destaca una falla en SolarWinds Web Help Desk (CVE-2025-26399) con 9.8. En el caso de los usuarios finales, Google Chrome (CVE-2025-10890) presentó una vulnerabilidad de tipo side-channel con puntaje 9.1, la cual expone datos privados entre sitios web, aumentando el riesgo de fuga de información sensible. Finalmente, se observó una falla en Cisco IOS/IOS XE (CVE-2025-20352) con 7.7, relacionada con el servicio SNMP, que puede causar reinicios del sistema y, en casos de explotación avanzada, permitir control total del dispositivo. Estos hallazgos evidencian la necesidad de **aplicar parches de seguridad de manera inmediata**, ya que afectan tanto infraestructuras críticas como aplicaciones de uso masivo.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Cisco Secure Firewall — ASA / FTD (VPN web server)	CVE-2025-20333	Permite a un atacante que obtenga credenciales válidas de la VPN para enviar solicitudes maliciosas y ejecutar código en el firewall	9.9
SolarWinds — Web Help Desk (WHD)	CVE-2025-26399	Una vulnerabilidad que permite a un atacante ejecutar comandos en el servidor que ejecuta la herramienta (contexto SYSTEM), con posibilidad de borrar/alterar datos o crear cuentas.	9.8
Google Chrome (V8 engine) - navegador (versiones < 140.0.7339.207)	CVE-2025-10890	Una falla de side-channel que permite a una página web maliciosa filtrar/exponer información de otra página (cross-origin), es decir, riesgo que datos privados se revelen entre sitios.	9.1
Cisco IOS / IOS XE — subsistema SNMP (gestión de red)	CVE-2025-20352	Un fallo en SNMP que puede provocar reinicios (DoS) con credenciales limitadas. Si el atacante obtiene credenciales privilegiadas, podría ejecutar código como root (control total del equipo).	7.7

Tabla 2. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de Actores y campañas Activas

- **Qilin ransomware:** operación de ransomware-as-a-service (RaaS) que existe desde 2022 y que se ha vuelto muy activa en 2025. Opera mediante afiliados, el "core" del grupo proporciona la herramienta y la infraestructura, y los afiliados ejecutan intrusiones.
- **The Gentlemen**: grupo de ransomware detectado públicamente en agosto de 2025, se han documentado campañas y actividad en septiembre 2025 con víctimas en múltiples sectores (manufactura, salud, construcción, seguros) y en varios países. Los reportes describen ataques dirigidos y técnicas de evasión avanzadas.
- **CiphBit**: es un ransomware identificado en 2023 que combina cifrado de archivos con amenazas de filtrar información capturada en la dark web si no se paga el rescate. Ha afectado a sectores como banca, salud, manufactura, logística y servicios profesionales.

Recomendaciones

- **Implementar actualizaciones de seguridad de forma inmediata** en plataformas críticas como Cisco Secure Firewall, Cisco IOS/IOS XE, SolarWinds y Google Chrome, priorizando aquellas con puntajes CVSS altos. Esto reduce la superficie de ataque frente a vulnerabilidades que permiten ejecución remota de código, filtración de datos o pérdida de disponibilidad.
- Fortalecer la protección contra *ransomware* mediante **políticas de respaldo cifrado**, **pruebas periódicas de restauración** y **segmentación de redes**. Esto limita el impacto de un ataque y asegura la continuidad del negocio en sectores críticos como industria, comercio y transporte.
- Adoptar medidas contra *phishing*, incluyendo **filtros de correo avanzados**, **autenticación multifactor** y **simulaciones de ataques de concienciación**. La capacitación del personal es clave para reducir la efectividad de campañas de ingeniería social, principal vector de ataque en Colombia y la región.
- Monitorear de manera proactiva la red y los endpoints con soluciones EDR/XDR que permitan identificar y contener actividades asociadas a malware como **AgentTesla**, **Remcos** y **AsyncRAT**, que buscan la captura de credenciales y control remoto de sistemas.
- Incorporar controles de seguridad adaptados a PyMEs y usuarios finales, incluyendo **políticas de contraseñas robustas**, **acceso mínimo necesario** y **soluciones de protección en la nube**.
- Explorar el uso de soluciones de detección basadas en IA y automatización defensiva para contrarrestar el aumento de *malware* con estas capacidades.

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

Las fuentes utilizadas combinan repositorios oficiales (NVD, CISA), medios especializados y empresas líderes en ciberseguridad, lo que otorga un nivel de confianza alto en la información. En la información recolectada persisten limitaciones, dado que algunos datos son globales y no siempre reflejan el contexto colombiano, aunque en general respaldan con solidez los hallazgos y tendencias analizadas.

Ransomware.live, 25/09/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 25 de septiembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
The Hacker News, 23/09/2025, 25/09/2025, SAP Patches Critical NetWeaver Vulnerability (CVSS 9+), Medio especializado en ciberseguridad.
https://thehackernews.com/2025/09/sap-patches-critical-netweaver-cvss-up.html
Cybersecurity News, 20/09/2025, 25/09/2025, Cisco IOS 0-day RCE Vulnerability, Medio especializado en ciberseguridad.
https://cybersecuritynews.com/cisco-ios-0-day-rce-vulnerability
NVD – NIST, 23/09/2025, 25/09/2025, CVE-2025-20352 (Cisco IOS/IOS XE SNMP Vulnerability), Fuente oficial de vulnerabilidades (NVD)
https://nvd.nist.gov/vuln/detail/CVE-2025-20352
NVD – NIST, 22/09/2025, 25/09/2025, CVE-2025-10890 (Google Chrome Data Leakage Vulnerability), Fuente oficial de vulnerabilidades (NVD).
https://nvd.nist.gov/vuln/detail/CVE-2025-10890
NVD – NIST, 24/09/2025, 25/09/2025, CVE-2025-26399 (SolarWinds Web Help Desk RCE Vulnerability), Fuente oficial de vulnerabilidades (NVD).
https://nvd.nist.gov/vuln/detail/CVE-2025-26399
CISA, 25/09/2025, 25/09/2025, CISA Directs Federal Agencies to Identify and Mitigate Potential Compromise in Cisco Devices, Agencia gubernamental de ciberseguridad (EE.UU.).
https://www.cisa.gov/news-events/alerts/2025/09/25/cisa-directs-federal-agencies-identify-and-mitigate-potential-compromise-cisco-devices
Check Point, 18/09/2025, 25/09/2025, Qilin Ransomware, Empresa de ciberseguridad.
https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/qilin-ransomware/
Trend Micro, 19/09/2025, 25/09/2025, Unmasking The Gentlemen Ransomware, Empresa de ciberseguridad.
https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html
Nexsys Latinoamérica, 21/09/2025, 25/09/2025, Ciberataques disfrazados de IA aumentan 115% en 2025, Distribuidor tecnológico regional.
https://www.nexsysla.com/co/noticias-nexsys/ciberataques-disfrazados-de-ia-aumentan-115-en-2025/