Resumen Ejecutivo:

En la última semana, el panorama de ciberseguridad en Colombia y la región mostró un incremento en la explotación de vulnerabilidades críticas, la distribución de troyanos de acceso remoto (RAT) a través de campañas de *phishing*, y ataques visibles como *ransomware* contra empresas y *defacement* en portales institucionales.

A nivel regional, también se observaron campañas de actores como Thegentlemen, AlphaLocker, LunaLock y Spacebears, lo que refleja la diversificación de amenazas. Este panorama evidencia una tendencia hacia ataques más sofisticados, potenciados incluso por el uso de inteligencia artificial, lo que obliga a reforzar controles técnicos en correo, servidores web y endpoints, así como fortalecer la concienciación del personal para anticipar impactos operativos y reputacionales en las organizaciones.

Incidentes de la semana

En la siguiente tabla se presentan los incidentes de ciberseguridad identificados en el país durante la última semana. Esta recopilación reúne los casos confirmados a través de fuentes abiertas, con el fin de ofrecer una visión consolidada de las tendencias recientes y apoyar el análisis de riesgos tanto en el sector público como en el privado.

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Ransomware	17 - SEP - 2025	Una compañía colombiana del sector de salud, con sede en Santa Marta, fue víctima de un ataque de *ransomware*	Thegentlemen
Defacement	13 - SEP - 2025	El sitio web oficial de una alcaldía municipal en Colombia fue comprometido mediante un ataque de *defacement*	fitwilliamx1337

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

Tendencias nacionales observadas

- La exposición a **vulnerabilidades críticas** en entornos corporativos continúa siendo un foco de atención. Estas tendencias refuerzan la necesidad de aplicar parches y actualizaciones en los plazos más cortos posibles para reducir riesgos de explotación en entornos críticos.

- Otra tendencia relevante está marcada por el **uso de inteligencia artificial** (IA), tanto como motor de innovación en soluciones de seguridad como en la **sofisticación de ataques**. Se han identificado campañas que aprovechan algoritmos de IA para personalizar correos de *phishing* y evadir controles de detección. El equilibrio entre aprovechar la IA para defender y enfrentar su uso ofensivo es uno de los principales desafíos del panorama actual.

- En materia de archivos maliciosos en circulación, los **Remote Access Trojans** (**RAT**) continúan destacándose en el país, **distribuidos principalmente a través de correos electrónicos** con adjuntos maliciosos y descargas desde páginas web comprometidas. Estos troyanos permiten a los ciberdelincuentes tener control remoto de los equipos afectados, exfiltrar información sensible y desplegar cargas adicionales. La tendencia sugiere que el correo electrónico sigue siendo el vector más explotado para comprometer a usuarios y organizaciones en Colombia.

Panorama nacional

En la comparativa de detecciones de malware observadas en Colombia durante la última semana se evidencia un incremento significativo del kit de *phishing* **Tycoon 2FA**, posicionándose de nuevo como la amenaza con mayor crecimiento. Por el contrario, **EvilProxy** muestra una disminución notoria, lo que refleja una caída en su actividad. Otras familias como **Quasar**, **AgentTesla** y **Remcos** mantienen volúmenes relevantes con variaciones menores frente a la semana anterior, mientras que **XWorm** presenta una reducción. En general, la tendencia refleja un panorama dinámico, con picos de aumento en amenazas relacionadas con la captura de credenciales y persistencia remota, al tiempo que otras herramientas de acceso y exfiltración muestran una reducción en su propagación.

Comparativa entre semanas

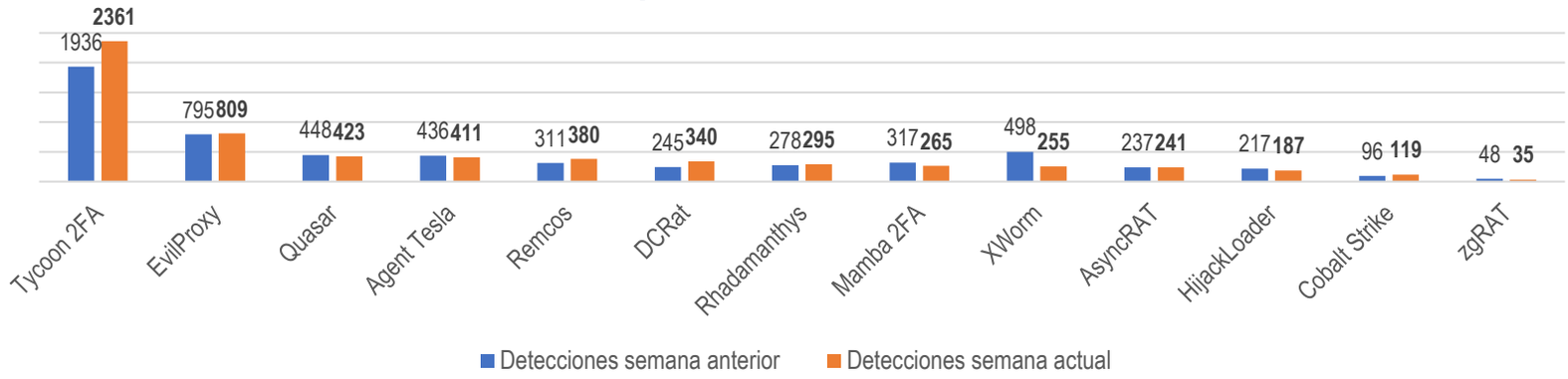

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la última semana, en la región se identificaron múltiples incidentes de ciberseguridad que afectaron principalmente a los sectores de comercio, energético, tecnológico y gubernamental. En República Dominicana y México se reportaron ataques de ***ransomware*** con un nivel de alerta alto, vinculados a los grupos **Spacebears**, **Alphalocker** y **Lunalock**, lo que evidencia una actividad constante de los ciberdelincuentes dirigidos a infraestructuras críticas y empresas privadas. En paralelo, en Brasil se registraron casos de ***defacement*** contra entidades gubernamentales.

Sector	Técnica / Vector predominante	Locación	Posible actor involucrado	Nivel alerta
Comercio	Ransomware	República Dominicana	Spacebears	**Alto**
Energético	Ransomware	Mexico	Alphalocker	**Alto**
Tecnologías de la Información y Comunicaciones	Ransomware	Mexico	Lunalock	**Alto**
Gubernamental	Defacement	Brasil	Rici144	**Medio**
Gubernamental	Defacement	Brasil	ExoticX86	**Medio**

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

Vulnerabilidades críticas

En la siguiente tabla se presentan las vulnerabilidades críticas más relevantes identificadas durante la última semana. Estos hallazgos evidencian riesgos significativos que requieren atención en las organizaciones para evitar posibles incidentes de seguridad.

Plataforma afectada	CVE	Impacto principal	Score CVSS	Vector de Ataque	Exploit activo
Google Chrome afectando todas las versiones anteriores 140.0.7339.185 / 140.0.7339.186.	CVE-2025-10585	Puede permitir que un ciberdelincuente ejecute malware en el equipo de la víctima, afecte el funcionamiento del navegador o incluso tome control del sistema.	8.8 (alto)	Remoto (navegador)	No confirmado
XenSource Xen 4.13	CVE-2025-58143	Un ciberdelincuente local podría aprovechar esta vulnerabilidad para obtener información confidencial o bloquear el host.	9.8 (crítico)	Local (Privilegios)	Si

Tabla 3. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de Actores y Campañas Activas

- **The Gentlemen:** grupo de ransomware emergente, detectado en agosto de 2025. Opera como Ransomware-as-a-Service (RaaS), con tácticas avanzadas como Bring-Your-Own-Vulnerable-Driver (BYOVD) usando drivers legítimos para evadir EDR/AV, abuso de GPO para compromiso de dominio y doble extorsión. Motivación financiera. Según MITRE ATT&CK, se han observado los siguientes comportamientos: T1215 (Kernel Modules and Extensions), T1484.001 (Domain Policy Modification: Group Policy) y T1486 (Data Encrypted for Impact).

- **Fitwilliamx1337**: nuevamente este actor está activo con ataques de *defacement*. Sus actividades solo se limitan a manipular la apariencia de los sitios web, no a captura de datos masivos o persistencia avanzada. De acuerdo con MITRE ATT&CK, esta actividad corresponde a T1505.003 (Server Software Component: Web Shell).

- **SpaceBears**: grupo de ransomware afiliado a Phobos (RaaS), emergido en abril 2024. Opera como data broker con doble extorsión (captura y cifrado de datos), usando sitios de fugas temáticos corporativos y "muro de la vergüenza" para presión reputacional. Según MITRE ATT&CK, se han identificado las técnicas T1041 (Exfiltration Over C2 Channel) y T1071.001 (Application Layer Protocol: Web Protocols).

- **Alphalocker**: grupo de ransomware detectado en 2023, opera como RaaS con enfoque en entrenamiento de hackers ("pentesting" falso) vía cursos como Bazooka Code y marketplace ALPentest para servicios de intrusión. Usa TOX para comunicación, paneles seguros y doble extorsión. De acuerdo con MITRE ATT&CK, se han observado las técnicas T1105 (Ingress Tool Transfer) y T1059 (Command and Scripting Interpreter).

- **Lunalock**: grupo de ransomware nuevo (emergido agosto 2025). Usa cifrado y doble extorsión. Utiliza notas de rescate en HTML con temporizador para causar más presión a sus víctimas. Según MITRE ATT&CK, se han observado las técnicas T1056.004 (Credential API Hooking) y T1490 (Inhibit System Recovery).

Recomendaciones

- **Aplicar de inmediato los parches de seguridad** en plataformas como Google Chrome y XenSource Xen. Además establecer un proceso semanal de revisión de los boletines de seguridad de proveedores (Google, Microsoft, Xen, SAP, etc.) para aplicar parches de manera prioritaria en función de su score CVSS y del impacto potencial en la organización.
- **Segmentar y aislar la red interna** de entornos críticos como sistemas de virtualización y servidores de aplicaciones, de manera que un ciberdelincuente con acceso inicial no pueda escalar fácilmente a sistemas sensibles.
- **Implementar soluciones de seguridad en el correo electrónico** con filtros de análisis de adjuntos y enlaces, configurar políticas DMARC, DKIM y SPF para validar la legitimidad de los dominios, bloquear la ejecución de archivos adjuntos sospechosos mediante reglas de seguridad en *endpoints*, y complementar con simulaciones de *phishing* y capacitaciones periódicas al personal para reforzar la identificación temprana de correos maliciosos.
- **Aplicar listas blancas de aplicaciones** (Application Whitelisting) en estaciones de trabajo y servidores críticos, evitando que se ejecute software no autorizado como cargas útiles de ransomware o troyanos RAT.
- Para mitigar los ataques de *defacement* se sugiere **implementar controles de seguridad en el servidor web** mediante parches frecuentes, endurecimiento de configuraciones (deshabilitando servicios innecesarios y permisos de escritura en directorios públicos), uso de un WAF (Web Application Firewall) con reglas activas contra inyecciones SQL, XSS y subida de archivos maliciosos, además de monitoreo continuo de integridad de archivos críticos del sitio web para detectar y revertir cambios no autorizados en tiempo real.
- **Monitorear el tráfico de red en tiempo real** mediante herramientas NDR (Network Detection and Response) o IDS/IPS para identificar comportamientos anómalos, comunicaciones hacia C2, y movimientos laterales. Esta medida permite detectar ataques avanzados en etapas tempranas, especialmente aquellos que logran evadir controles en endpoints o correo electrónico.

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

Las fuentes utilizadas en el reporte semanal combinan plataformas oficiales (Citrix, NVD, Google), proveedores de ciberseguridad (Trend Micro, WatchGuard, SOCRadar) y fuentes de OSINT (Ransomware.live, Any Run), lo que aporta diversidad y contraste con una multiplicidad de fuentes de la información. No obstante, existen algunas limitaciones por sesgos, vacíos técnicos o enfoques narrativos, lo que limita la confianza a un nivel medio-alto.

Ransomware.live, 18/09/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 18 de septiembre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
Citrix, 16/09/2025, 18/09/2025, "CTX695195 – Citrix NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-58143", Boletín de seguridad de proveedor.
https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX695195
NVD (NIST), 16/09/2025, 18/09/2025, "CVE-2025-58143", Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-58143
Trend Micro, 18/09/2025, 18/09/2025, "Unmasking The Gentlemen Ransomware", Reporte de investigación de ciberseguridad.
https://www.trendmicro.com/en_us/research/25/i/unmasking-the-gentlemen-ransomware.html
SOCRadar, 17/09/2025, 18/09/2025, "Dark Web Profile: Spacebears", Reporte de inteligencia de amenazas.
https://socradar.io/dark-web-profile-spacebears/
WatchGuard, 18/09/2025, 18/09/2025, "Ransomware Tracker: Alpha Locker", Plataforma de seguimiento de ransomware.
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/alpha-locker
CyberNews, 17/09/2025, 18/09/2025, "LunaLock ransomware attack against artists' platform", Medio de noticias en ciberseguridad.
https://cybernews.com/ai-news/lunalock-ransomware-attack-against-artists-platform/
Google Chrome Releases, 17/09/2025, 18/09/2025, "Stable Channel Update for Desktop", Blog oficial de actualizaciones de software.
https://chromereleases.googleblog.com/2025/09/stable-channel-update-for-desktop_17.html