Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20251025 – 012

TLP:CLEAR

Resumen Ejecutivo

Durante la última semana se observó una actividad moderada en el panorama de amenazas cibernéticas regional, con un único incidente identificado y una baja general en la cantidad de campañas activas; No obstante,, se recomienda mantener una vigilancia constante ante la persistencia de actores como Crimson Collective, Blind Eagle y Radar ransomware, quienes continúan desarrollando operaciones de espionaje y extorsión en sectores críticos.

En materia de vulnerabilidades, se destacaron las CVE-2025-53072 y CVE-2025-62481 (Oracle Marketing) y la CVE-2025-7850 (TP-Link Omada), todas con impacto crítico sobre la confidencialidad, integridad y disponibilidad de los sistemas. Asimismo, la caída global de AWS evidenció la necesidad de fortalecer los planes de resiliencia y continuidad operativa en entornos corporativos dependientes de servicios en la nube. En conjunto, los eventos de la semana refuerzan la importancia de mantener controles de actualización, segmentación de red, monitoreo de comportamiento y preparación ante incidentes de gran escala.

Tendencias observadas

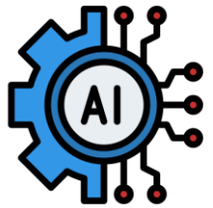
Caída de plataformas por AWS, aprendizajes para el sector digital

Aunque la caída global de Amazon Web Services (AWS) no fue un incidente de seguridad, su impacto en Colombia fue significativo. Provocó interrupciones masivas en servicios digitales críticos, especialmente en el sector financiero, evidenciando la alta dependencia en esta infraestructura *cloud*. Este evento resalta la importancia de contar con planes de contingencia, redundancia y diversificación de proveedores para fortalecer la resiliencia y evitar efectos en cascada similares en el futuro.

Reducción en el fraude digital, pero evolución de tácticas

Colombia ha registrado una reducción en los intentos de fraude digital, sin embargo, esta mejora se acompaña de la evolución de las tácticas criminales, que ahora incluyen bots sofisticados para simular usuarios reales, IP que se disfrazan para evadir controles, y modalidades como *smishing* (mensajes de texto fraudulentos) y *vishing* (llamadas engañosas). Estas amenazas más complejas exigen a las organizaciones actualizar y fortalecer sus estrategias de prevención sin afectar la experiencia del usuario.

Uso de inteligencia artificial en la sofisticación de amenazas



La incorporación de la inteligencia artificial (IA) en las actividades cibernéticas maliciosas está aumentando la sofisticación de los ataques. Las capacidades de IA generativa permiten a los cibercriminales crear amenazas más dinámicas y adaptativas, dificultando la detección y mitigación. Esta tendencia implica un desafío creciente para las defensas digitales en Colombia, que deben adaptarse para contrarrestar ataques impulsados por tecnologías emergentes.

Panorama nacional

En el siguiente gráfico se presenta un análisis de los malware detectados en Colombia durante la última semana, comparando su comportamiento con la semana anterior. En la visualización se destacan principalmente amenazas enfocadas en la captura de credenciales y eludir mecanismos de autenticación multifactor, como **Tycoon 2FA** y **EvilProxy**, que mantienen los mayores volúmenes de detección. Se observa un ligero aumento en **Sally 2FA** y **Lumma *stealer***. En contraste, familias como **Remcos**, **Rhadamanthys** y **DcRat** registran una leve disminución frente a la semana anterior. Estos datos reflejan una persistente actividad asociada a campañas orientadas la **captura de credenciales**, **control remoto** y **bypass de autenticación**, consolidando una tendencia continua de amenazas enfocadas en comprometer accesos a cuentas corporativas y personales.

Comparativa entre semanas

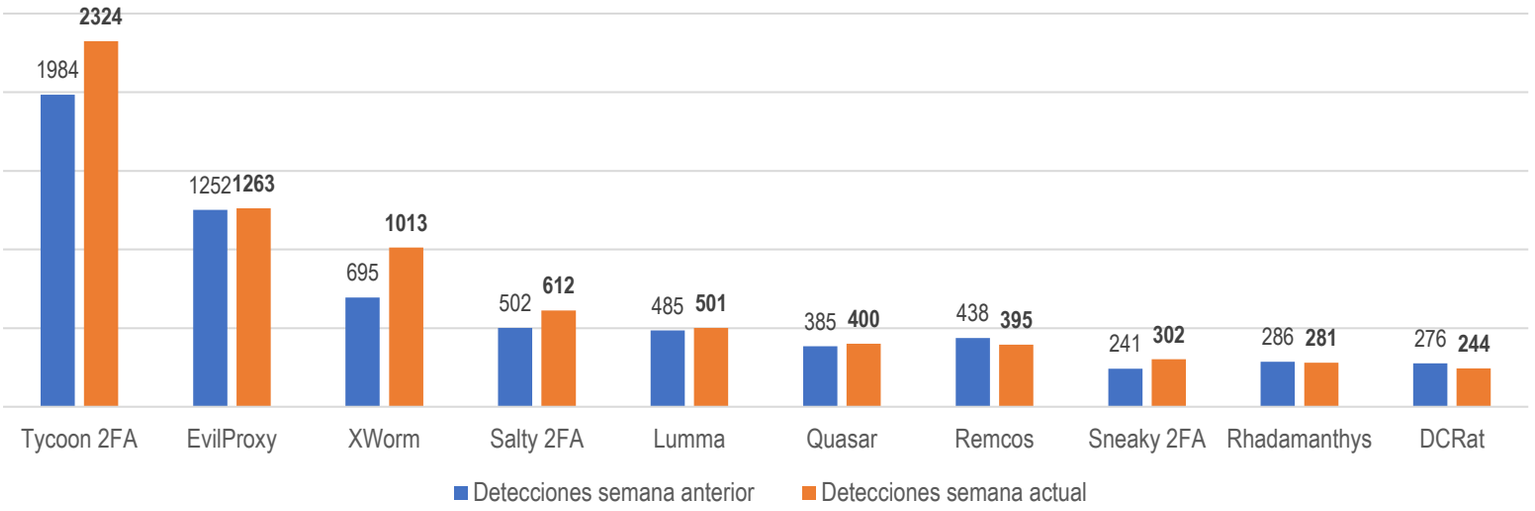


Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

Durante la última semana, a nivel regional, se identificó un único incidente relevante de seguridad digital en Latinoamérica, correspondiente a un ataque de *ransomware* dirigido a una empresa del sector comercio en Perú. De acuerdo con los indicadores recopilados, el posible actor involucrado sería el grupo Radar, conocido por sus campañas de extorsión y cifrado de información en entornos corporativos. Aunque esta semana no se observó una alta actividad en la región, es fundamental mantener la vigilancia y fortalecer las medidas de prevención, ya que los grupos delictivos suelen aprovechar periodos de aparente calma para preparar nuevas campañas dirigidas.

Sector	Amenaza	Locación	Posible actor involucrado
Comercio	Ransomware	Perú	**Radar**

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

Vulnerabilidades relevantes de la semana

Durante la última semana se destacaron tres vulnerabilidades críticas que requieren atención prioritaria. Estas fallas representan un alto riesgo para entornos corporativos al afectar directamente la confidencialidad, integridad y disponibilidad de los sistemas, por lo que se recomienda su inmediata mitigación y aplicación de parches.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Oracle Marketing	**CVE-2025-53072**	Permite a un atacante no autenticado, con acceso de red vía HTTP, comprometer completamente el sistema.	**9.8**
Oracle Marketing	**CVE-2025-62481**	Requiere acceso de red vía HTTP sin autenticación y permite la toma total del módulo.	**9.8**
TP-Link Omada Gateway	**CVE-2025-7850**	Se trata de una inyección de comandos en el sistema operativo que podría ser explotada (con credenciales de administrador) para ejecutar comandos arbitrarios en el dispositivo.	**9.3**

Tabla 2. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de actores y campañas activas

❑ Crimson Collective

Es un grupo de amenazas cibernéticas emergente, identificado por primera vez en 2025, con un enfoque en brechas de datos masivas y extorsión, particularmente en entornos cloud y repositorios de código. Se les asocia con motivaciones financieras, utilizando tácticas de exfiltración de datos sensibles para luego venderlos o extorsionar a las víctimas. Entre sus actividades más recientes se destaca el compromiso de repositorios privados de Red Hat y el uso de herramientas de búsqueda de secretos, como TruffleHog, para identificar credenciales de AWS expuestas y obtener acceso inicial a los entornos comprometidos.

❑ Blind Eagle

También conocido como APT-C-36, es un grupo APT (Advanced Persistent Threat) sospechado de origen sudamericano, activo desde al menos 2018. Se especializa en espionaje y cibercrimen, particularmente en Colombia, Ecuador, Panamá y Chile. Se mantienen activos con campañas de espionaje basadas en troyanos de acceso remoto (RAT) dirigidas a sectores críticos, principalmente gubernamental y financiero.

❑ Radar ransomware

Es un grupo de ransomware emergente, identificado en septiembre 2025, operando bajo un modelo de doble extorsión (cifrado de archivos y filtración de datos). Se enfoca en extorsión selectiva a organizaciones medianas, con motivaciones financieras puras. Como grupo nuevo, han realizado ataques selectivos a sectores como salud, finanzas, construcción y minería, con un enfoque en regiones como Norteamérica, Europa y África.

Recomendaciones

- Priorizar la aplicación inmediata de parches en productos de Oracle y TP-Link Omada, siguiendo las actualizaciones oficiales y deshabilitando servicios expuestos temporalmente hasta su corrección. Implementar escaneos de vulnerabilidades continuos para detectar versiones afectadas antes de que sean explotadas.
- Desplegar y afinar reglas en SIEM o EDR para detectar comportamientos asociados a Troyanos de acceso remoto (RAT), como conexiones persistentes a dominios dinámicos, uso inusual de procesos como MSBuild.exe o csc.exe, y tráfico C2 cifrado saliente.
- Restringir el acceso a paneles de administración mediante VPN y MFA. Segmentar las redes y limitar privilegios administrativos, reduciendo el impacto potencial de un acceso inicial. Aislar los servidores críticos con firewalls internos y listas blancas de comunicación saliente.
- Implementar controles de rotación periódica de claves de AWS y API tokens, con escaneos internos de exposición mediante herramientas como TruffleHog o Gitleaks. Aplicar políticas estrictas de Data Loss Prevention (DLP) para evitar la filtración de información confidencial o credenciales en repositorios de código. Utilizar cifrado en tránsito y en reposo en todas las comunicaciones internas y externas.
- Capacitar al personal en la detección temprana de phishing y spearphishing, principal vector usado por Blind Eagle. Realizar ejercicios de simulación de intrusión y ransomware para fortalecer la capacidad de respuesta y validación de respaldos. Asegurar que los planes de contingencia y respaldo se mantengan actualizados y probados ante un escenario de cifrado masivo.
- Distribuir las cargas de trabajo entre múltiples proveedores de nube (AWS, Azure, GCP, etc.) o mantener redundancia local en servidores on-premise. Esto reduce la exposición a fallas globales y mejora la disponibilidad en caso de incidentes masivos del proveedor.

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

Ransomware.live, 23/10/2025, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/
Any Run, 23 de octubre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/
Infobae, 21 Oct 2025, Cae el fraude digital en Colombia: así están cambiando las tácticas de los ciberdelincuentes, Medio de noticias.
https://www.infobae.com/colombia/2025/10/21/cae-el-fraude-digital-en-colombia-asi-estan-cambiando-las-tacticas-de-los-ciberdelincuentes/
Amazon Web Services (AWS), 22 Oct 2025, Update – AWS services operating normally (post-mortem summary), Informe técnico oficial.
https://aws.amazon.com/es/message/101925/
NVD, 21 Oct 2025, CVE-2025-53072 Detail – NVD, Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-53072
NVD, 21 Oct 2025, CVE-2025-62481 Detail – NVD, Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-62481
NVD, 20 Oct 2025, CVE-2025-7850 Detail – NVD, Base de datos de vulnerabilidades.
https://nvd.nist.gov/vuln/detail/CVE-2025-7850
Rapid7, 07 Oct 2025, Crimson Collective: A New Threat Group Observed Operating in the Cloud, Blog de investigación.
https://www.rapid7.com/blog/post/tr-crimson-collective-a-new-threat-group-observed-operating-in-the-cloud
The Hacker News, 27 Aug 2025, Blind Eagle's Five Clusters Target Colombia Using RATs, Phishing Lures, and Dynamic DNS Infra, Medio de noticias.
https://thehackernews.com/2025/08/blind-eagles-five-clusters-target.html
Ransomware.Live, n.d., 23 Oct 2025, Radar (Ransomware-group profile), Base de datos de actores de ransomware.
https://www.ransomware.live/group/radar