Reporte

Semanal

Inteligencia Amenaza Cibernéticas

COLCERT RS – 20251003 - 009

TLP:CLEAR

Resumen Ejecutivo:

Durante la última semana se registraron alertas relevantes en el ámbito cibernético que afectan tanto a entidades públicas como privadas, incluyendo campañas de correo con archivos maliciosos, **sitios fraudulentos** que suplantan entidades oficiales para distribuir aplicaciones no autorizadas, ataques de ***defacement*** y **páginas falsas** que buscan capturar credenciales corporativas. También se identificaron **vulnerabilidades** críticas en plataformas ampliamente utilizadas como Cisco y VMware.

Estas tendencias evidencian un incremento en la sofisticación y alcance de los ataques, con potencial impacto en la continuidad operativa, la reputación institucional y la seguridad de la información. A futuro, las organizaciones deben fortalecer sus programas de gestión de vulnerabilidades, realizar modelado de amenazas, establecer procedimientos de inteligencia de amenazas, implementar controles avanzados de detección y respuesta, y reforzar la cultura de ciberseguridad en usuarios y empleados como líneas críticas de defensa.

Incidentes de la semana

Durante la presente semana se identificó un único incidente de seguridad informática, correspondiente a un defacement que afectó a un sitio web asociado al dominio legítimo del consejo de un municipio colombiano. Este tipo de actividad consiste en la alteración no autorizada del contenido publicado en la página, lo que puede impactar la confianza de los usuarios en el servicio y afectar la reputación de la entidad.

Tipo de incidente	Fecha del evento	Descripción	Posible actor
Defacement	29/09/2025	Se ha detectado un ataque de Defacement en un sitio web asociado al dominio legítimo del consejo de un municipio colombiano.	Mr Kodek

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

Tendencias nacionales observadas

- Se ha observado un aumento en sitios web fraudulentos que se hacen pasar por entidades gubernamentales, con el objetivo de que usuarios descarguen archivos APK maliciosos bajo la apariencia de aplicaciones oficiales.
- Campañas de correo electrónico con archivos adjuntos maliciosos siguen siendo comunes, utilizando asuntos provocativos o urgentes como “Demandas”, “Proceso penal por abuso sexual”, “Citación judicial”, “Embargo”, u “Orden de captura” para inducir al engaño y lograr que los destinatarios abran los archivos.
- Se reportan sitios web falsos que suplantan a Microsoft, para capturar credenciales corporativas de correo electrónico, mediante páginas que imitan nombres y diseño oficiales, buscando engañar a empleados a nivel institucional.

Panorama nacional

Durante la última semana en Colombia se observó una variación significativa en las detecciones de diferentes familias de malware en comparación con la semana anterior. Los kit de *phishing* **Tycoon 2FA** y **EvilProxy** continúan siendo los más detectados, aunque presentaron una disminución respecto al periodo. En contraste, se evidenció un incremento en campañas asociadas a **Lumma** y **AgentTesla**. Asimismo, **XWorm** y **AsyncRAT** mantuvieron niveles similares, mientras que **Remcos** y **DcRAT** mostraron una reducción en la actividad reportada. Otras amenazas como **njRAT** y **DarkCloud** no registraron actividad en la semana actual, aunque sí habían estado presentes anteriormente. Este comportamiento refleja un dinamismo en las tácticas de los actores de amenaza, con cambios en las familias empleadas para afectar a usuarios y organizaciones en el país.

Comparativa entre semanas

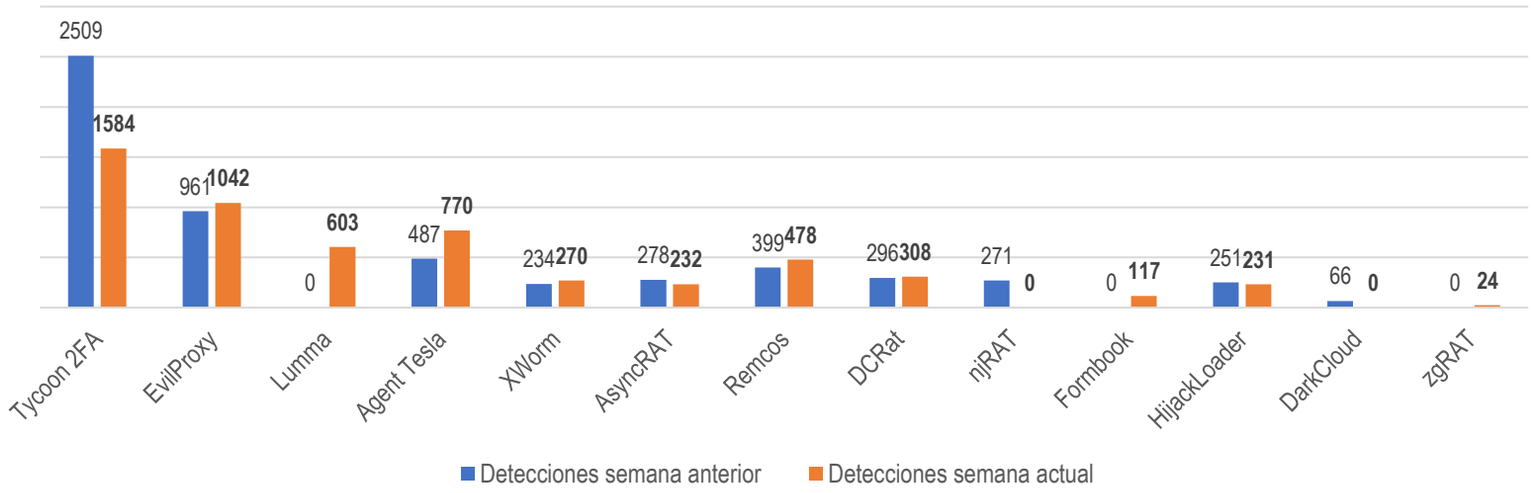

Gráfico 1. Detecciones visualizadas. Fuente AnyRun.

Panorama regional

En la región se han observado recientemente incidentes de *ransomware*. En Brasil, el sector comercio fue impactado por una campaña atribuida al grupo **Alphalocker**, mientras que en Argentina se identificó un ataque dirigido al sector salud, vinculado al grupo **Spacebears**. Ambos incidentes presentan un nivel de alerta alto, lo que evidencia la persistencia de este tipo de amenazas en sectores estratégicos de la región y refuerza la necesidad de fortalecer los controles de ciberseguridad, así como la preparación frente a posibles intentos de extorsión digital.

Sector	Técnica / Vector predominante	Locación	Posible actor involucrado	Nivel alerta
Comercio	Ransomware	Brasil	Alphalocker	**Alto**
Salud	Ransomware	Argentina	Spacebears	**Alto**

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

Vulnerabilidades críticas

Durante la semana se han identificado diversas vulnerabilidades de alta severidad que afectan principalmente a plataformas de **Cisco y VMware.** Estas fallas, consideradas entre las más relevantes del periodo, representan riesgos significativos para la seguridad de la infraestructura tecnológica y requieren especial atención por parte de los equipos responsables de la gestión y mitigación de incidentes.

Plataforma afectada	CVE	Impacto principal	Score CVSS
Cisco	**CVE-2025-20333**	Vulnerabilidad en el servicio WebVPN que permite ejecución remota de código autenticado, logrando comprometer la integridad del dispositivo y mantener acceso persistente.	**9.9 (Crítica)**
Cisco	**CVE-2025-20362**	Falla de autenticación rota que posibilita acceso no autorizado a recursos restringidos en conexiones VPN, lo que permite movimientos iniciales dentro de la red.	**6.7 (Media - Alta)**
Cisco	**CVE-2025-20363**	Vulnerabilidad en los servicios web que permite ejecución remota de código, en algunos casos sin autenticación, lo que expone dispositivos perimetrales y routers a compromiso total.	**9.0 (Crítica)**
Cisco	**CVE-2025-20352**	Vulnerabilidad en la función SNMP de Cisco IOS e IOS XE que permite a un atacante autenticado remoto provocar una denegación de servicio o, con credenciales de alto privilegio, lograr ejecución remota de código (RCE).	**7.7 (Alta)**
VMware	**CVE-2025-41244**	Vulnerabilidad de escalamiento de privilegios locales que permite a un ciberdelincuente sin privilegios ejecutar código con privilegios de *root* en una máquina virtual.	**7.8 (Alta)**
WhatsApp para iOS	**CVE-2025-55177**	Autorización incompleta en mensajes de sincronización de dispositivos vinculados (“linked device sync”) en WhatsApp, que podría permitir que un usuario no autorizado provoque el procesamiento de contenido desde una URL arbitraria en el dispositivo objetivo.	**5.4 (medio)**
Sistemas Apple: iOS	**CVE-2025-43300**	Escritura fuera de límites (out-of-bounds write) en el framework ImageIO al procesar una imagen maliciosa (por ejemplo, un DNG manipulado), lo que puede corromper memoria y permitir ejecución remota de código.	**8.8 (alto)**

Tabla 3. Vulnerabilidades críticas identificadas. Fuente: COLCERT.

Análisis de Actores y Campañas Activas

- **Mr Kodek:** es un actor de amenazas cibernéticas de bajo perfil, principalmente identificado como un "defacer" que opera bajo el alias o equipo "mr kodek". No se asocia con grupos ransomware sofisticados ni con campañas de extorsión a gran escala. Sus actividades se limitan a intrusiones simples para alterar páginas web, posiblemente utilizando vulnerabilidades básicas o credenciales débiles. Ha sido reportado en *defacements* contra sitios gubernamentales y educativos en septiembre de 2025.

- **Alphalocker**: es un grupo de ransomware emergente, detectado por primera vez en enero de 2024. Opera un sitio de filtración de datos (DLS) en la dark web bajo dominios TOR. Se enfoca en la captura y filtración de datos más que en el cifrado, con 23 víctimas confirmadas hasta octubre de 2025. Ataca principalmente a empresas medianas en sectores como energía, tecnología y manufactura, con énfasis en América Latina, EE.UU. y Europa.

- **Spacebears**: es un grupo de extorsión de datos emergente, detectado en abril de 2024, posiblemente basado en Moscú, Rusia. Está alineado con la familia Phobos (ransomware-as-a-service), pero se ha enfocado a la venta y filtración de datos capturados. Mantiene un DLS que lista 8 víctimas, principalmente empresas medianas en manufactura, tecnología y salud, con enfoque en EE.UU. y Europa.

Recomendaciones

- Habilitar políticas estrictas de SPF, DKIM y DMARC y monitorear los reportes de fallo para reducir la suplantación de remitentes y facilitar la detección de campañas de *phishing*.
- Implementar políticas de Mobile Device Management (MDM) y Application Allowlisting para dispositivos corporativos que limiten la instalación de APK solo a tiendas oficiales o repositorios aprobados.
- Realizar campañas de concienciación dirigidas a usuarios móviles sobre señales de suplantación (URL, certificados, errores ortográficos) e indicar procedimientos para verificar fuentes oficiales antes de instalar aplicaciones.
- Configurar y exigir MFA resistente al phishing en todas las cuentas que acceden a recursos corporativos para mitigar el robo de credenciales.
- Implementar un programa de gestión de vulnerabilidades (Vulnerability Management) que incluya inventario completo de activos, priorización basada en riesgo (exposición pública, criticidad) y despliegue rápido de parches.
- Realizar copias de seguridad siguiendo la regla 3-2-1: guardar al menos 3 copias de la información importante, en 2 medios diferentes (por ejemplo, en el computador y en un disco externo) y mantener 1 copia adicional en un lugar separado o en la nube, para poder recuperarla en caso de ataque o pérdida de datos.
- Actualizar los clientes de WhatsApp a versión 2.25.21.73 o superior para iOS y versión 2.25.21.78 o superior para Mac / WhatsApp Business en iOS, así como actualizar los sistemas de Apple a iOS/iPadOS 18.6.2, macOS Sonoma 14.7.8, macOS Ventura 13.7.8, macOS Sequoia 15.6.1.
- Concienciar a los usuarios de alto nivel sobre los riesgos de los ataques zero-click, fortaleciendo la cultura de ciberseguridad frente a este tipo de amenazas. Asimismo, robustecer las políticas de gestión de credenciales y el uso de autenticación multifactor en cuentas corporativas, con el fin de dificultar cualquier explotación secundaria después de un compromiso inicial.

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

Ransomware.live, 02/10/2025, "Seguimiento de campañas ransomware ", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/

Any Run, 02 de octubre de 2025, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/

Cisco, 25 de septiembre de 2025, "Cisco Secure Firewall Adaptive Security Appliance y Threat Defense – vulnerabilidad de ejecución remota en servidor VPN (cisco-sa-asaftd-webvpn-z5xP8EUB)", fuente oficial (Cisco Security Advisory).
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB

Cisco, 25 de septiembre de 2025, "Cisco Secure Firewall ASA / FTD – vulnerabilidad de acceso no autorizado en servidor VPN (cisco-sa-asaftd-webvpn-YROOTUW)", fuente oficial (Cisco Security Advisory).
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW

Cisco, 25 de septiembre de 2025, "Cisco ASA / FTD / IOS / IOS XE / IOS XR – vulnerabilidad de ejecución remota en servicios web (cisco-sa-http-code-exec-WmfP3h3O)", fuente oficial (Cisco Security Advisory).
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O

Cisco, 24 de septiembre de 2025, "Cisco IOS / IOS XE – vulnerabilidad SNMP (cisco-sa-snmp-x4LPhte)", fuente oficial (Cisco Security Advisory).
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte

Broadcom, 29 de septiembre de 2025, sin fecha visible de información, "Broadcom Security Advisories / soporte de seguridad (portal Broadcom)", fuente oficial (Broadcom / soporte).
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149

WatchGuard, "Alpha Locker — seguimiento de ransomware (WatchGuard Ransomware Tracker)", fuente de investigación (WatchGuard Security Hub).
https://www.watchguard.com/wgrd-security-hub/ransomware-tracker/alpha-locker

Tripwire, "Space Bears Ransomware: lo que necesitas saber" (Tripwire – State of Security), fuente técnica / blog.
https://www.tripwire.com/state-of-security/space-bears-ransomware-what-you-need-know