Reporte

Semanal

Inteligencia de amenaza cibernéticas

COLCERT RS -20260313- 027

TLP:CLEAR

Resumen Ejecutivo

Durante el periodo analizado, el panorama de amenazas en Colombia y la región mostró una dinámica intensa, marcada por una ofensiva contra la infraestructura estatal. A nivel técnico, se evidenció una evolución en las herramientas de acceso remoto y exfiltración; mientras que vectores de evasión de **MFA** como **Tycoon 2FA** mostraron fluctuaciones, familias de malware como **Agent Tesla**, **Remcos** y **AsyncRAT** mantuvieron una tendencia al alza.

La evolución del ecosistema de ransomware evidencia un creciente nivel de profesionalización entre los actores de amenaza. Grupos como **Qilin** y **TheGentleman** han incorporado lenguajes modernos como **Rust** y **Go** para desarrollar herramientas capaces de comprometer entornos **multiplataforma y virtualizados**, integrando además técnicas avanzadas de evasión como **BYOVD (Bring Your Own Vulnerable Driver)** para desactivar controles de seguridad a nivel del kernel y evadir soluciones EDR.

En el ámbito regional, **América Latina** experimentó una actividad sostenida de ransomware dirigida principalmente a sectores críticos como **logística, comercio e industria**. **Brasil** se consolidó como el principal foco de incidentes, con operaciones atribuidas a grupos como **Qilin** y **CoinbaseCartel**, mientras que **Colombia** y **Perú** registraron campañas significativas vinculadas a **TheGentleman**.

De forma paralela, la actividad del grupo **Akira** en **México** refuerza la tendencia regional hacia modelos de **triple extorsión**, donde los atacantes combinan cifrado de sistemas, filtración de datos y presión directa sobre clientes o socios comerciales. Este enfoque se complementa con la **explotación de identidades digitales comprometidas**, priorizando organizaciones que forman parte de **cadenas de suministro esenciales**, con el objetivo de maximizar el impacto operativo y la capacidad de presión sobre las víctimas.

Finalmente, la publicación del Patch Tuesday de marzo de 2026 por parte de Microsoft reveló vulnerabilidades críticas de ejecución remota de código en servicios de alta sensibilidad como SQL Server (**CVE-2026-21536**) y Office, además de fallos en el Spooler de impresión. Estos hallazgos, junto con las tácticas de los grupos de ransomware analizados, subrayan la urgencia de aplicar parches de seguridad de forma inmediata, fortalecer las políticas de detección en soluciones EDR y robustecer la gestión de identidades con MFA para mitigar los vectores de intrusión y movimiento lateral detectados.

Tendencias observadas

Vulnerabilidad en la apertura de datos y riesgos de la IA: en el marco del Día de los Datos Abiertos (celebrado el 11 de marzo), expertos han alertado sobre el reto de equilibrar la transparencia gubernamental con la protección de la privacidad, tras detectarse un volumen cercano a los 13.000 eventos que intentan explotar bases de datos públicas. La tendencia actual muestra que los atacantes están utilizando inteligencia artificial para automatizar el descubrimiento de vulnerabilidades en infraestructuras para sofisticar las estafas en redes sociales y aplicaciones de mensajería como WhatsApp. Esta situación está impulsando a las empresas y al sector público en Colombia a priorizar la "identidad como el nuevo perímetro", buscando soluciones de autenticación multifactor más robustas para frenar el robo de identidades digitales.

Panorama nacional

El monitoreo de esta semana revela una dinámica de amenazas en constante transformación. Aunque **Tycoon 2FA** se mantiene como el vector con mayor volumen de registros pese a una ligera contracción, el panorama general muestra un repunte significativo en la mayoría de las herramientas analizadas. Destaca especialmente el crecimiento de **EvilProxy**, que junto con **Sneaky 2FA**, refuerza la persistencia de tácticas diseñadas para comprometer entornos con autenticación de doble factor. Por otro lado, se hace evidente una tendencia al alza en el uso de troyanos y recolectores de información. El incremento en las detecciones de **AsyncRAT**, **XWorm**, **Agent Tesla** y **Stealc** sugiere que los atacantes están intensificando sus esfuerzos en campañas de acceso remoto y exfiltración de datos sensibles. En conclusión, mientras que herramientas específicas como **DCRat** mostraron un leve retroceso, el fortalecimiento de las familias de malware **infostealer** y **RATs** mantiene el nivel de riesgo en una zona crítica, obligando a una vigilancia constante sobre estos vectores de intrusión.

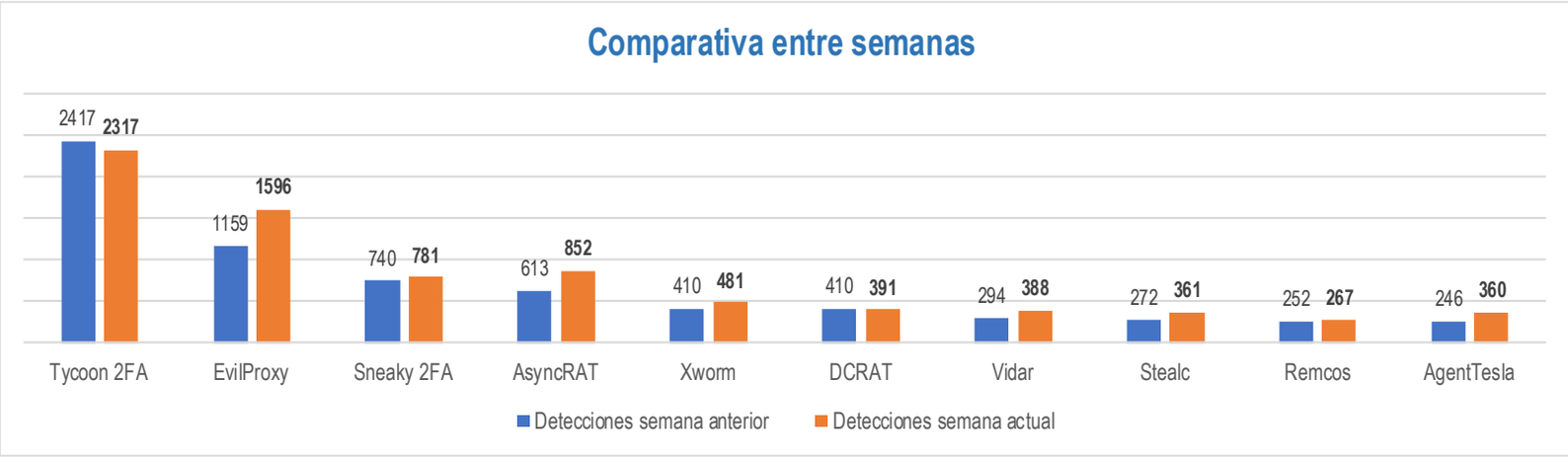

Gráfico 1. *Detecciones visualizadas. Fuente AnyRun.*

Panorama regional

Durante el periodo evaluado, el ecosistema de ciberamenazas en América Latina se caracterizó por una actividad focalizada de ransomware contra sectores clave de la economía regional. **Brasil** destacó como un foco crítico, registrando incidentes dirigidos a los rubros de comercio, importación y alimentos, atribuidos a los actores **Qilin** y **Coinbasecartel**. Simultáneamente, se identificó la expansión del actor **Thegentlemen**, quien impactó operaciones de logística en **Colombia** y sectores industriales y comerciales en **Perú**. Finalmente, en México se reportó la incursión de **Akira** afectando al segmento de servicios profesionales. Estos eventos subrayan la persistencia de campañas de extorsión digital que priorizan organizaciones con roles estratégicos en la cadena de suministro y la gestión de servicios especializados en la región.

Sector afectado	Amenaza	Locación	Posible actor involucrado	# de veces visto
Servicios Profesionales	Ransomware	**México**	Akira	1
Logística	Ransomware	**Colombia**	Thegentlemen	1
Alimentos, Comercio, Industria	Ransomware	**Perú**	Thegentlemen	1
Comercio, Importación	Ransomware	**Brasil**	Qilin	1
Comercio, Alimentos	Ransomware	**Brasil**	Coinbasecartel	1
Gobierno	Ransomware	**Paraguay**	Kairos	1
Tecnología	Ransomware	**Paraguay**	Nightspire	1
Industria, Comercio	Ransomware	**Argentina**	Qilin	1

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

Vulnerabilidades relevantes de la semana

Plataforma afectada	CVE	Impacto principal	Score CVSS
Microsoft Devices Pricing Program (Remote Code Execution)	**CVE-2026-21536**	Vulnerabilidad de RCE crítica que permite a atacantes no autenticados ejecutar código arbitrario explotando una debilidad de carga de archivos sin restricción (CWE-434). La explotación no requiere interacción del usuario y puede ser desencadenada enviando archivos maliciosos especialmente diseñados, con el panel de vista previa como vector de ataque.	**9.8 (Crítica)**
Microsoft Office (Remote Code Execution vía Preview Pane)	**CVE-2026-26110 / CVE-2026-26113**	Ambas vulnerabilidades permiten RCE en Microsoft Office disparado simplemente visualizando archivos maliciosos en el Panel de Vista Previa, sin necesidad de abrir el archivo. Involucran fallos en manejo de punteros y confusión de tipos que permiten eludir límites internos de seguridad. Atacantes pueden ejecutar código arbitrario con los privilegios del usuario, abriendo la puerta a despliegue de malware o movimiento lateral.	**8.4 (Crítica)**
Microsoft SQL Server (Escalación de Privilegios)	**CVE-2026-21385**	Vulnerabilidad de control de acceso impropio en SQL Server que permite a un usuario autenticado con bajos privilegios escalar a sysadmin completo sobre la red. Obtener derechos de sysadmin habilita control total sobre bases de datos, servicios vinculados y configuración de SQL Server. Microsoft confirmó que la falla fue divulgada públicamente antes de que el parche estuviera disponible.	**8.8 (Crítica)**

Tabla 2. *Vulnerabilidades relevantes de la semana. Fuente: COLCERT.*

Actores y campañas activas

TheGentleman: Es una operación de Ransomware-as-a-Service (RaaS) de reciente aparición (detectada a mediados de 2025) que ha demostrado una madurez operativa inusual para su corto tiempo de actividad. Su locker principal está desarrollado en el lenguaje **Go (Golang)**, lo que le permite una gran versatilidad para atacar infraestructuras críticas en entornos **Windows**, **Linux** y clústeres de virtualización como **VMware ESXi**, siguiendo un modelo de doble extorsión mediante el robo previo de información sensible.

Este grupo se distingue por el uso de tácticas avanzadas de evasión, destacando la técnica **BYOVD** (Bring Your Own Vulnerable Driver) mediante el uso de controladores firmados pero vulnerables para anular procesos de EDR y antivirus desde el **kernel**. Además, implementan un parámetro de contraseña obligatorio para la ejecución del malware, una medida diseñada específicamente para frustrar el análisis automático en sandboxes y dificultar la labor de los investigadores de seguridad.

Durante los primeros meses de 2026, **TheGentleman** ha intensificado sus operaciones en la región, figurando activamente en plataformas como Ransomware.live con ataques confirmados en países como Brasil, Perú y Colombia. Sus objetivos abarcan sectores diversos, desde instituciones educativas de alto nivel hasta la industria manufacturera y de servicios financieros, aprovechando credenciales comprometidas y paneles administrativos expuestos (como VPNs y Firewalls) para infiltrarse en redes corporativas de gran escala.

Recomendaciones

- Ejecutar de manera prioritaria la actualización de los parches de Microsoft de marzo de 2026, con especial foco en las vulnerabilidades de ejecución remota de código (RCE) en SQL Server y Office, con el fin de cerrar los vectores de entrada y movimiento lateral.
- Configurar políticas estrictas en soluciones EDR para detectar la carga de controladores vulnerables (táctica BYOVD), monitoreando específicamente el uso de drivers firmados pero obsoletos que actores como Qilin y TheGentleman emplean para anular las defensas del kernel y evadir la detección de seguridad.
- Robustecer la seguridad de las identidades mediante la implementación obligatoria de MFA en todos los accesos remotos y portales administrativos, endureciendo además las políticas de almacenamiento de credenciales en navegadores para mitigar el impacto de los scripts automatizados de robo de datos.
- Implementar reglas de detección basadas en comportamiento para identificar malware de acceso remoto (RATs) y recolectores de información como Agent Tesla o Remcos, centrándose en la creación de persistencia en el sistema y la exfiltración de datos hacia infraestructuras de comando y control (C2).
- Realizar auditorías de seguridad recurrentes a proveedores de servicios gestionados (MSP) y socios de la cadena de suministro en la región, ante el incremento documentado de ataques dirigidos a los sectores de logística, manufactura y comercio en países como Colombia y Brasil.
- Asegurar y segmentar los entornos de virtualización de servidores, como VMware ESXi y Nutanix, limitando estrictamente los privilegios de administración para frenar la efectividad de los nuevos lockers escritos en Rust y Go que permiten a los atacantes cifrar infraestructuras críticas de forma nativa.

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

Ransomware.live, 19 de enero de 2026, "Seguimiento de campañas ransomware", Plataforma OSINT – foros y sitios de filtración.
https://www.ransomware.live/.

Any Run, 6 de marzo de 2026, "Malware Trends", Plataforma de inteligencia de amenazas.
https://any.run/malware-trends/.

El Tiempo, 9 de marzo de 2026, “Balance de ciberseguridad tras la jornada electoral: 100 millones de intentos de ataque bloqueados”, Prensa nacional / Medio de comunicación masivo.
https://www.eltiempo.com/justicia/servicios/ataques-ciberneticos-elecciones-colombia-marzo-2026

El Espectador, 11 de marzo de 2026, “Datos abiertos en Colombia: entre la transparencia y el riesgo de ciberataques por IA”, Prensa nacional / Medio de comunicación masivo.
https://www.elespectador.com/tecnologia/datos-abiertos-colombia-riesgos-ia-2026

SOCRadar, 12 de febrero de 2026, Dark Web Profile: The Gentlemen Ransomware, Blog de ciberseguridad / Inteligencia de amenazas.
https://socradar.io/blog/dark-web-profile-the-gentlemen-ransomware/

Microsoft Security Response Center (MSRC), 10 de marzo de 2026, Security Update Guide - March 2026, Repositorio oficial de seguridad.
https://msrc.microsoft.com/update-guide/release/2026-Mar

Microsoft Security Response Center (MSRC), 10 de marzo de 2026, Microsoft SQL Server Remote Code Execution Vulnerability (CVE-2026-21536), Repositorio oficial de seguridad.
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21536

Microsoft Security Response Center (MSRC), 10 de marzo de 2026, Microsoft Office Remote Code Execution Vulnerability (CVE-2026-26110), Repositorio oficial de seguridad.
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-26110

Microsoft Security Response Center (MSRC), 10 de marzo de 2026, Microsoft Office Remote Code Execution Vulnerability (CVE-2026-26113), Repositorio oficial de seguridad.
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-26113

Microsoft Security Response Center (MSRC), 10 de marzo de 2026, Windows Print Spooler Remote Code Execution Vulnerability (CVE-2026-21385), Repositorio oficial de seguridad.
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-21385