Informe

Mensual (Enero)

Inteligencia de amenaza cibernéticas

COLCERT IN-20260206-027

TIC

TLP:CLEAR

Resumen Ejecutivo

Durante el mes de enero, el panorama de ciberseguridad para Colombia y la región evidenció una exposición alta y sostenida de amenazas orientadas al acceso inicial, persistencia y extorsión digital. La actividad de múltiples grupos criminales en América Latina, sumada a la similitud tecnológica y sectorial con el entorno nacional, incrementa la probabilidad de materialización de este tipo de incidentes en organizaciones públicas y privadas del país.

Se presentaron detecciones masivas de kits de *phishing* y evasión de autenticación multifactor, particularmente **Tycoon 2FA** y **EvilProxy**, así como la presencia recurrente de troyanos de acceso remoto como **AsyncRAT** y **XWorm**, confirmando que los adversarios están priorizando el compromiso de credenciales válidas, la instalación de mecanismos de persistencia y el movimiento lateral dentro de las redes antes de ejecutar acciones disruptivas. Este comportamiento refleja un modelo de ataque escalonado donde el *phishing* y los RATs actúan como habilitadores directos de incidentes de mayor impacto, incluyendo exfiltración de información y despliegue posterior de *ransomware*.

En este escenario, resulta prioritario fortalecer la protección de identidades, la segmentación de redes, el monitoreo continuo, la gestión de vulnerabilidades y la resiliencia operativa mediante respaldos y planes de continuidad probados, así como consolidar capacidades de detección temprana e inteligencia de amenazas. La adopción de estas medidas permitirá reducir la superficie de exposición, contener oportunamente los incidentes y mitigar los efectos de campañas cada vez más coordinadas y persistentes contra sectores estratégicos del país.

Panorama nacional de incidentes

El panorama nacional de incidentes estuvo marcado principalmente por campañas de *ransomware* dirigidas contra organizaciones del sector privado en industrias agro-industriales, de financiación de bienes y de manufactura. Los casos reportados evidencian tácticas de doble extorsión, incluyendo la publicación de muestras de información comprometida y el cifrado de activos críticos, así como la posible exfiltración de datos financieros y directorios internos. Entre los actores asociados se identifican grupos como **Lynx**, **Thegentlemen** y **Tengu**, lo que sugiere una actividad sostenida de amenazas organizadas con capacidad de impacto operativo y reputacional. Este comportamiento resalta la necesidad de reforzar controles de respaldo, segmentación de red, monitoreo de accesos y planes de respuesta a incidentes para reducir la exposición frente a intrusiones que derivan en cifrado y filtración de información sensible.

Tipo de incidente	Fecha	Descripción	Posible actor
Ransomware	05/01/2026	Una compañía agro-industrial recibió un presunto ataque de ransomware en el que el actor de amenazas publicó una muestra de los datos y el cifrado que realizaron.	Lynx
Ransomware	17/01/2026	Una compañía tecnológica de gestión del aprendizaje soportado sufrió un presunto ataque de ransomware donde filtraron datos en el calnal del actor de amenaza.	Qilin
Ransomware	20/01/2026	Una empresa especializada en programas de financiación de bienes y servicios fue víctima de un ataque de ransomware. No se divulgó la naturaleza de la información exfiltrada y cifrada.	Thegentlemen
Ransomware	26/01/2026	Una empresa especializada en la fabricación de elementos para calzado fue víctima de un ataque de ransomware en el que se comprometió información financiera y directorios de la red interna de la compañía.	Tengu

Tabla 1. *Incidentes identificados en enero*

COLCERT

En el mes de enero, el comportamiento de las detecciones en Colombia mostró una clara concentración en amenazas orientadas al robo de credenciales, la toma de control remoto y la evasión de mecanismos de autenticación, consolidando el acceso inicial como el principal objetivo de los adversarios. Sobresale el volumen significativamente superior de **Tycoon 2FA** y **EvilProxy**, que acumularon la mayor cantidad de eventos, evidenciando el uso extensivo de plataformas de phishing como servicio para eludir controles de autenticación multi factor (MFA). Seguidos de la actividad de **Sneaky 2FA**, **XWorm** y **AsyncRAT**, y familias como **Mamba 2FA**, **Remcos**, **Agent Tesla** y **Stealc**, las cuales mantienen campañas orientadas al espionaje, exfiltración de datos y persistencia en los sistemas comprometidos. En conjunto, este patrón confirma una tendencia sostenida hacia operaciones que priorizan la suplantación de identidad y el establecimiento de accesos duraderos dentro de las redes corporativas, incrementando el riesgo operativo y la probabilidad de intrusiones más complejas en etapas posteriores.

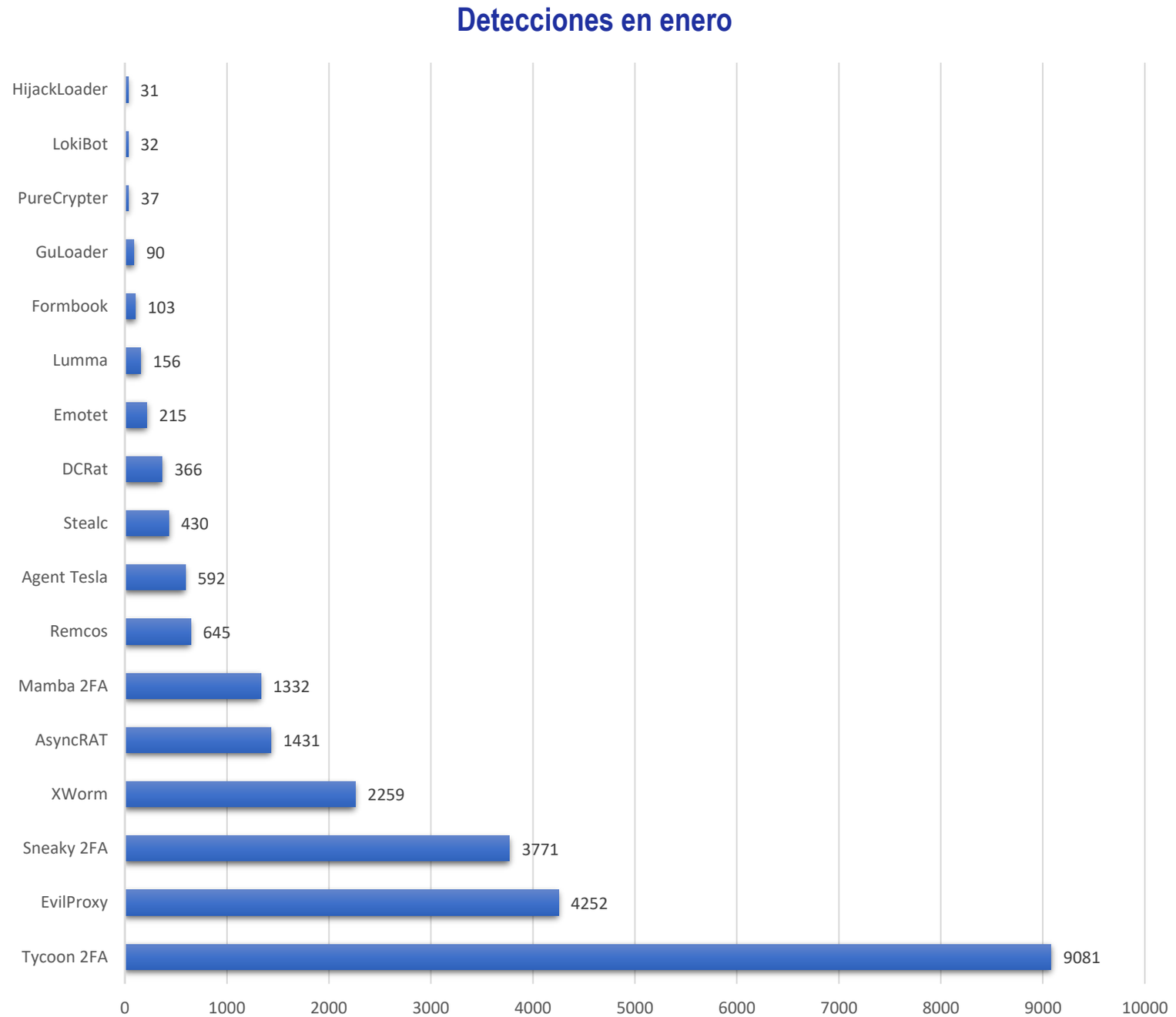

Gráfico 1. *Detecciones visualizadas en el mes de enero.*

Análisis de actores y campañas activas a nivel nacional

En enero de 2026, el análisis de actores y campañas activas a nivel nacional evidencia múltiples operaciones de ransomware con fines netamente económicos, dirigidas contra organizaciones de diversos sectores. Los incidentes observados se concentraron en industrias como alimentación y agricultura, servicios financieros e infraestructura industrial, donde la dependencia operativa de los sistemas tecnológicos incrementa la probabilidad de pago ante escenarios de interrupción. Las tácticas empleadas incluyen cifrado de información crítica, exfiltración previa de datos y presión reputacional mediante la publicación de muestras, lo que confirma la consolidación de esquemas de doble extorsión como mecanismo principal de monetización.

El grupo **Lynx** dirigió su actividad hacia una compañía del sector de alimentos y agricultura, combinando la sustracción de información con el bloqueo de sistemas, generando impactos financieros directos y riesgos reputacionales derivados de la posible exposición de datos. Este enfoque sugiere una selección de víctimas con alta sensibilidad operativa, donde la interrupción de la cadena productiva puede acelerar negociaciones de rescate.

Por su parte, **Thegentlemen** centró su campaña en una compañía de financiación de bienes y servicios, un segmento atractivo por el valor de la información gestionada y su criticidad para clientes y terceros. Los eventos asociados reflejan afectaciones tanto económicas como de confidencialidad, reforzando la tendencia de los actores a priorizar la captura de datos antes del cifrado para maximizar la presión extorsiva.

Finalmente, **Tengu** mostró actividad contra organizaciones industriales, comprometiendo información corporativa y directorios internos de red, lo que podría facilitar movimientos laterales y un mayor alcance del ataque dentro de los entornos comprometidos. Este patrón denota un interés por lograr persistencia y ampliar el impacto más allá del cifrado inicial.

Actor	Tipo de amenaza	Sectores principalmente afectados	Motivación principal	Impacto observado
Lynx	Ransomware	**Alimentación y Agricultura**	Económica	Reputacional, financiero y exfiltración
Qilin	Ransomware	**Tecnológico**	Económica	Reputacional, financiero y exfiltración
Thegentlemen	Ransomware	**Financiero**	Económica	Reputacional, financiero y exfiltración
Tengu	Ransomware	**Industria**	Económica	Reputacional, financiero y exfiltración

Tabla 2. Actores de amenaza observados. Fuente: ColCERT.

En conjunto, la actividad registrada confirma que el ecosistema local continúa siendo atractivo para grupos de ransomware organizados que operan bajo modelos de negocio estructurados. La recurrencia de impactos financieros, operativos y reputacionales resalta la necesidad de fortalecer estrategias de segmentación de red, copias de seguridad resilientes, monitoreo continuo y planes de respuesta que permitan reducir el tiempo de detección y contención frente a este tipo de campañas.

Tendencias globales y regionales con riesgo local

El análisis de los incidentes observados durante el periodo analizado muestra una predominancia sostenida de incidentes dirigidos a sectores estratégicos de América Latina, particularmente Salud y Protección Social, Gobierno/Estado, Comercio, Industria y Turismo, Recursos Minero-Energéticos, Educación, Tecnologías de la Información y Transporte. Esta distribución sectorial evidencia una preferencia de los adversarios por organizaciones con alta dependencia operativa de sus sistemas y baja tolerancia a la interrupción del servicio, lo que incrementa la probabilidad de pago ante esquemas de extorsión basados en cifrado y filtración de datos.

A nivel geográfico, México y Brasil concentran la mayor recurrencia de casos, seguidos por Paraguay, Chile, Perú, Ecuador, Venezuela y Argentina, lo que sugiere una actividad distribuida pero constante en múltiples jurisdicciones. En estos territorios se observó la participación reiterada de grupos como **Qilin**, **Tengu**, **Lynx**, **Devman**, **Anubis**, **Thegentlemen**, **LockBit**, **Morpheus**, **Incransom**, **Nova**, **Sinobi** y **Safepay**, lo que apunta a un ecosistema criminal diverso con múltiples operadores activos y campañas simultáneas.

La repetición de los mismos actores en diferentes sectores y países sugiere la reutilización de accesos iniciales, el intercambio de infraestructura y la aplicación de tácticas estandarizadas de intrusión, tales como explotación de servicios expuestos, credenciales comprometidas y movimiento lateral previo al despliegue del cifrado. Este comportamiento favorece ataques oportunistas y escalables, capaces de impactar cadenas de suministro y proveedores compartidos entre organizaciones de distintos mercados.

Desde la perspectiva de riesgo para Colombia, estas dinámicas regionales resultan especialmente relevantes debido a la similitud de los sectores afectados y a la interconexión tecnológica y comercial con los países vecinos. La presencia activa de múltiples bandas de ransomware en el entorno latinoamericano incrementa la probabilidad de campañas transfronterizas y de efectos colaterales sobre filiales, socios o infraestructuras tercerizadas, reforzando la necesidad de fortalecer controles preventivos, monitoreo continuo y capacidades de respuesta temprana frente a incidentes de extorsión digital.

Gráfico 2. *Incidentes por país. Fuente: ColCERT.*

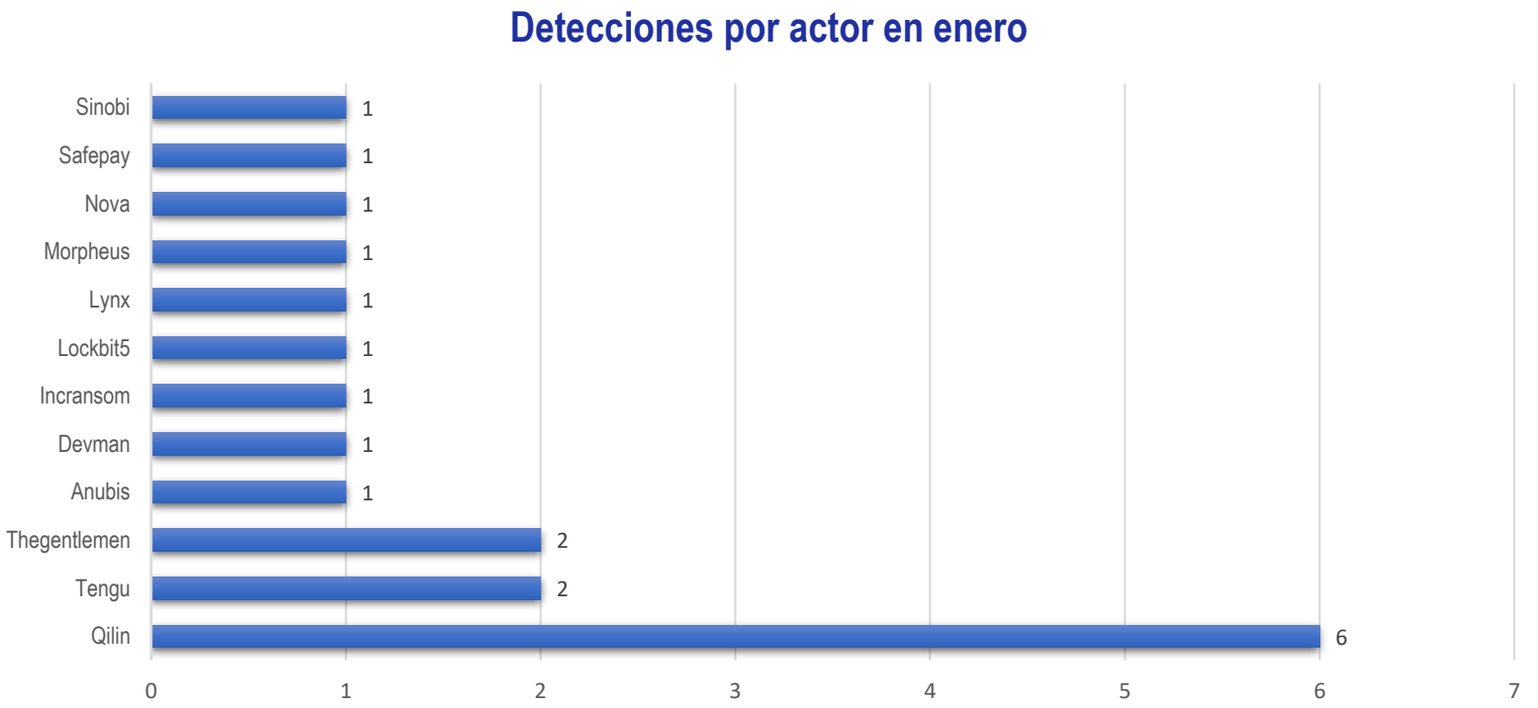

***Gráfico 3**. Detecciones por actor. Fuente: ColCERT.*

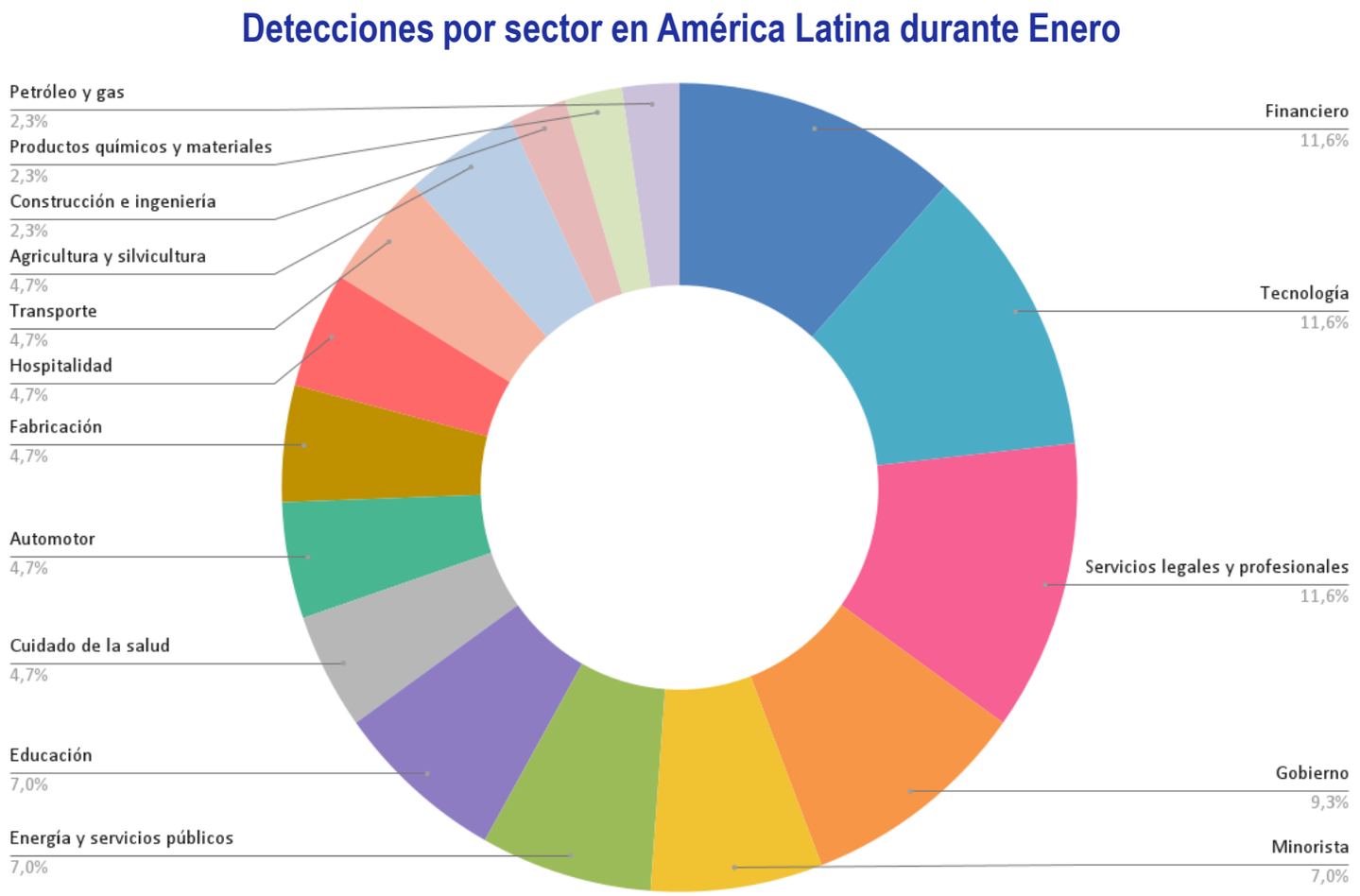

***Gráfico 4**. Detecciones por sector. Fuente: ColCERT.*

Análisis de riesgo estratégico

El ransomware continúa representando el escenario más severo en términos de impacto, debido a la afectación directa sobre la disponibilidad, integridad y confidencialidad de la información en sectores críticos. La recurrencia de intrusiones basadas en explotación de accesos expuestos, credenciales comprometidas y movimiento lateral dentro de las redes posiciona esta amenaza en un nivel crítico, especialmente por sus consecuencias financieras, legales y reputacionales, así como por la interrupción de servicios esenciales.

No obstante, las detecciones elevadas de kits de *phishing* y *bypass* de autenticación multifactor, como **Tycoon 2FA**, **EvilProxy** y **Sneaky 2FA**, evidencian una presión constante sobre la identidad digital de usuarios corporativos y gubernamentales. Estas herramientas facilitan la captura de credenciales válidas y tokens de sesión, reduciendo la necesidad de explotar vulnerabilidades técnicas y aumentando la efectividad de accesos no autorizados. Por su alta frecuencia y capacidad de evadir controles tradicionales, este vector presenta una probabilidad alta y un impacto medio–alto, consolidándose como un habilitador directo de incidentes mayores.

De manera complementaria, la presencia sostenida de troyanos de acceso remoto (RAT) y stealers como **AsyncRAT**, **XWorm**, **Remcos**, **Agent Tesla** y **Stealc** confirma la continuidad de campañas orientadas al espionaje, exfiltración de información y establecimiento de persistencia en los equipos comprometidos. Estas infecciones, aunque menos disruptivas en el corto plazo, amplían la superficie de ataque y pueden actuar como precursores de fraudes, movimientos laterales o despliegues posteriores de ransomware, configurando un riesgo alto a nivel estratégico.

Criterios de evaluación utilizados

- **Probabilidad**: estimada con base en recurrencia regional, presencia de actores activos, similitud sectorial y madurez de controles comúnmente observados.
- **Impacto**: evaluado considerando afectación a la continuidad del negocio, integridad de la información, cumplimiento normativo, reputación institucional y posibles sanciones.
- **Nivel de riesgo**: resultado cualitativo de la combinación probabilidad e impacto (Bajo, medio, alto y crítico).

Amenaza	Probabilidad	Impacto	Nivel de Riesgo	Observaciones
Ransomware con impacto nacional	Alta	Alto	Crítico	Campañas activas dirigidas a sectores críticos. Incluye cifrado, exfiltración y doble extorsión con interrupción operativa significativa.
Captura de credenciales (phishing y bypass MFA)	Alta	Alto	Crítico	Volumen elevado de detecciones asociadas a kits como Tycoon 2FA y EvilProxy. Facilita accesos iniciales válidos y evasión de autenticación multifactor. Principal vector de intrusión.
Troyanos de acceso remoto (RAT/Stealers)	Alta	Alto	Crítico	Presencia sostenida de AsyncRAT, XWorm, Remcos, Agent Tesla y Stealc. Permiten persistencia, espionaje y preparación de fases posteriores del ataque.
Infraestructura crítica y servicios esenciales	Media	Alto	Alto	Potencial afectación a energía, transporte, agua y salud. Consecuencias operativas amplificadas por dependencia tecnológica y baja tolerancia a la indisponibilidad.
Ransomware emergente en la región (LATAM)	Media	Alto	Alto	Nuevos grupos y campañas activas en países vecinos incrementan la probabilidad de ataques transfronterizos y reutilización de infraestructura criminal.

Tabla 3. *Riesgos a nivel nacional. Fuente: ColCERT.*

Perspectivas para febrero

De acuerdo con la actividad registrada a nivel nacional y regional, se prevé la continuidad de campañas orientadas al acceso inicial mediante phishing, captura de credenciales y herramientas de acceso remoto, seguidas de incidentes de ransomware con fines extorsivos. El volumen sostenido de detecciones asociadas a kits de suplantación de autenticación como **Tycoon 2FA** y **EvilProxy**, junto con la presencia recurrente de RATs como **AsyncRAT** y **XWorm**, sugiere que los adversarios continuarán priorizando el compromiso silencioso de cuentas válidas y la persistencia en los entornos antes de ejecutar acciones disruptivas.

En paralelo, se estima que los ataques de ransomware mantendrán una probabilidad alta de materialización, especialmente contra sectores con alta dependencia tecnológica y baja tolerancia a la indisponibilidad, replicando el patrón observado en países de la región. La diversificación de operadores y la reutilización de infraestructura criminal incrementan la posibilidad de campañas oportunistas y transfronterizas, así como de esquemas de doble extorsión basados en la exfiltración y publicación de información. Asimismo, es previsible la persistencia de compromisos de aplicaciones web y servicios expuestos, incluyendo explotación de vulnerabilidades conocidas y configuraciones débiles en portales institucionales, con impactos principalmente reputacionales, pero con potencial de escalamiento hacia redes internas. De igual forma, el riesgo asociado a terceros y proveedores tecnológicos continuará siendo un vector relevante para accesos indirectos.

Recomendaciones estratégicas

A partir del análisis consolidado de incidentes regionales, las detecciones de *malware* orientadas a la captura de credenciales y acceso remoto, así como la evaluación de riesgos estratégicos y las perspectivas operativas para el mes de febrero, se identifican un conjunto de medidas prioritarias enfocadas en reducir la probabilidad de acceso inicial no autorizado, limitar la propagación lateral y fortalecer la resiliencia ante eventos de *ransomware* y exfiltración de información. Estas acciones priorizan la protección de identidades, aplicaciones expuestas, infraestructura crítica y cadenas de suministro, integrando controles preventivos y de recuperación. La adopción sistemática de estas recomendaciones permitirá a las organizaciones disminuir su superficie de ataque, mejorar la detección temprana y contener oportunamente incidentes con impacto operativo, reputacional y financiero.

Amenaza prioritaria	Riesgo principal asociado	Recomendación estratégica	Enfoque
Ransomware	Interrupción operativa, cifrado y pérdida de información	Implementar segmentación de red, copias de seguridad, pruebas periódicas de restauración y planes de respuesta a incidentes con escenarios de doble extorsión.	Preventivo – Resiliencia
Captura de credenciales (phishing / bypass MFA)	Acceso inicial no autorizado a cuentas corporativas	Reforzar autenticación multifactor resistente a phishing protección de correo, filtrado de URL maliciosas y campañas continuas de concientización.	Preventivo – Detectivo
Troyanos de acceso remoto (RAT/Stealers)	Persistencia, espionaje y movimiento lateral	Implementar soluciones de detección y monitoreo de comportamiento, bloqueo de ejecución no autorizada y revisión continua de *endpoints* críticos.	Detectivo – Correctivo
Abuso de credenciales y privilegios	Escalamiento de privilegios y accesos indebidos	Aplicar el principio de mínimo privilegio, rotación de contraseñas y monitoreo de accesos anómalos y cuentas privilegiadas.	Preventivo – Detectivo
Compromiso de terceros	Propagación del riesgo por cadena de suministro	Establecer requisitos mínimos de seguridad a proveedores, evaluaciones periódicas y control de accesos remotos y conexiones externas.	Preventivo
Actividad de actores persistentes	Campañas dirigidas y reconocimiento prolongado	Fortalecer inteligencia de amenazas, correlación de eventos y monitoreo continuo para identificar patrones y comportamientos anómalos tempranos.	Estratégico
Phishing y accesos iniciales	Puerta de entrada a ransomware y fraude	Ejecutar simulaciones de phishing, capacitación periódica y mecanismos de reporte rápido por parte de usuarios.	Preventivo

Tabla 4. *Recomendaciones estratégicas. Fuente: ColCERT.*

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

El presente informe se fundamenta en un conjunto de fuentes especializadas de alta credibilidad que permiten sostener con solidez los hallazgos y conclusiones. Con base en la estabilidad y reputación de estas fuentes, el nivel de confianza general de la información analizada se clasifica como alto, aunque se reconocen limitaciones inherentes, como la ausencia de telemetría regional completa y posibles vacíos sobre actividades emergentes que aún no cuentan con documentación abierta suficiente.

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