REPORTE TRIMESTRAL // Q3 2026

ESTADO DEL RANSOMWARE EN MÉXICO

Panorama de amenazas, familias activas y vectores observados contra empresas mexicanas.

PUBLICADO POR

Equipo Black Husk Security

FECHA DE PUBLICACIÓN

Julio 2026

RESUMEN EJECUTIVO

Q3 2026: México en el mapa del ransomware

México se ha consolidado como uno de los mercados más atacados por operaciones de ransomware en América Latina. Reportes de firmas internacionales de threat intelligence lo posicionan como el **segundo país con mayor volumen de ataques** en la región durante 2026, superado únicamente por Brasil. Este reporte resume el panorama observado por nuestro equipo de DFIR en incidentes reales atendidos y en monitoreo activo de la actividad de los grupos que operan contra la región.

Cinco familias concentran la mayoría de la actividad observable en México: **Phobos, Akira, LockBit, Medusa y Qilin**. Cada una tiene un perfil operativo distinto — vector inicial, tiempo dentro de la red, extensiones características y sector preferido — que este reporte detalla para que los equipos de seguridad puedan orientar defensas de manera específica.

Hallazgos clave del trimestre

- El vector inicial más común en incidentes atendidos sigue siendo **acceso remoto sin MFA** — RDP expuesto o VPN sin segundo factor.
- Se observa un incremento en **ataques dirigidos a proveedores de manufactura**, especialmente aquellos integrados a cadenas de exportación con clientes en EE.UU. y Europa.
- Las **credenciales corporativas mexicanas continúan filtrándose** en foros underground en español, muchas veces meses antes del ataque final.
- La **exfiltración de datos antes del cifrado** es hoy práctica estándar en 4 de las 5 familias activas — el incidente casi siempre se convierte también en brecha de datos personales.

PANORAMA REGIONAL

México en el mapa del ransomware LATAM

La actividad de ransomware contra América Latina se ha profesionalizado. Los grupos que operan hoy contra empresas mexicanas no son atacantes oportunistas — son **operaciones organizadas**, muchas con presencia sostenida en foros en español, alianzas con *initial access brokers* que venden accesos a empresas específicas, y modelo de "ransomware as a service" (RaaS) que permite a afiliados operar con infraestructura compartida.

Esto tiene tres consecuencias directas para el ecosistema empresarial en México:

1. El acceso inicial es un mercado. Credenciales VPN, RDP y accesos cloud se venden en foros por precios que van de decenas a miles de dólares, dependiendo del tamaño de la empresa.

2. Los grupos conocen el ecosistema local. Las notas de rescate se personalizan al idioma y país. Los operadores investigan la capacidad financiera de la víctima antes de fijar el monto del rescate.

3. La exfiltración es tan importante como el cifrado. Aunque una empresa tenga backups impecables, el chantaje continúa sobre los datos filtrados — muchos incluyen información sujeta a la LFPDPPP.

Sectores con mayor incidencia observable

Sector	Perfil de riesgo observado
Manufactura y proveeduría industrial	Cadenas justo-a-tiempo, ERPs expuestos, presión de OEMs por controles.
Servicios financieros y fintech	Datos altamente monetizables + presión regulatoria de CNBV.
Retail y comercio	Superficie de ataque amplia, POS y e-commerce como vectores frecuentes.
Salud privada	Datos sensibles, presión operativa que empuja a pagar rescates.
Servicios profesionales	Cadena de proveeduría a corporativos que sí tienen madurez alta.

FAMILIAS ACTIVAS EN Q3 2026

Perfil operativo por grupo

Los perfiles a continuación resumen lo que hemos observado en incidentes reales atendidos por nuestro equipo y en monitoreo activo de la actividad pública de cada grupo. Cada familia tiene un patrón distinto que puede orientar defensas específicas.

PHOBOS / 8BASE	
Extensiones observadas	.eight, .eking, .faust, .devos, .8base, .phobos, patrones [ID].[correo].[ext]
Vector inicial más común	RDP expuesto directamente a Internet con credenciales débiles.
Tiempo típico dentro de la red	De horas a pocos días — grupo relativamente rápido tras acceso inicial.
Sector con mayor incidencia	PyMEs de servicios, retail regional y sector salud.
Notas de campo	Grupo antiguo aún prolífico contra PyMEs. El 8base es la variante más activa en 2026 en el sitio de filtración público.

AKIRA	
Extensiones observadas	.akira, .powerranges
Vector inicial más común	VPNs y firewalls sin MFA (Cisco ASA, SonicWall) con credenciales comprometidas.
Tiempo típico dentro de la red	Días o semanas — reconocimiento extenso antes del cifrado.
Sector con mayor incidencia	Manufactura, servicios profesionales y corporativos medianos.
Notas de campo	Sitio público con estética terminal característica. Instala AnyDesk / RustDesk como mecanismo de persistencia.

LOCKBIT

Extensiones observadas	Cadenas aleatorias (ej. .HLJkNskOq). Nota: [ext].README.txt
Vector inicial más común	Servicios de perímetro sin parchar (Fortinet, Citrix, Ivanti) o credenciales VPN.
Tiempo típico dentro de la red	Variable — depende del afiliado. Puede ser horas o semanas.
Sector con mayor incidencia	Sectores con alto valor de rescate: manufactura, servicios financieros, energético.
Notas de campo	Operación con historial de rebranding tras acciones policiales. Sigue siendo relevante por su modelo RaaS.

MEDUSA

Extensiones observadas	.medusa, .mylock. Nota: !!!READ_ME_MEDUSA!!!.txt
Vector inicial más común	Servicios expuestos (RDP, ScreenConnect) y phishing con accesos vendidos por brokers.
Tiempo típico dentro de la red	De horas a varios días — velocidad media.
Sector con mayor incidencia	Sector salud, educación privada y servicios públicos concesionados.
Notas de campo	Sitio de filtración muy activo publicando víctimas sistemáticamente. Alta presión mediática sobre el rescate.

QILIN	
Extensiones observadas	Cadena única por víctima. Nota: README-RECOVER-.txt
Vector inicial más común	VPNs sin MFA, phishing dirigido y accesos comprados a initial access brokers.
Tiempo típico dentro de la red	Típicamente varios días de reconocimiento antes del cifrado.
Sector con mayor incidencia	Empresas medianas y grandes con capacidad de pago identificable.
Notas de campo	Operación cuidadosa que investiga antes de atacar. Ha atendido incidentes de perfil alto en la región.

VECTORES INICIALES

Cómo entran los atacantes

En incidentes reales atendidos por nuestro equipo durante los últimos meses, la vasta mayoría del acceso inicial se concentra en tres vectores. Todos son **prevenibles con controles conocidos**. La brecha entre lo conocido y lo aplicado es donde ocurren los incidentes.

Vector	Familias que lo usan	Control que lo bloquea
RDP expuesto a Internet	Phobos (dominante), LockBit	Cerrar puerto 3389 al exterior. Acceso remoto solo por VPN con MFA.
VPN / firewall sin MFA	Akira (dominante), Qilin, LockBit	MFA obligatorio en todo acceso remoto. Parchar CVEs de perímetro con prioridad crítica.
Credenciales corporativas filtradas	Todas las familias	Monitoreo continuo de dark web. Rotación forzada tras cualquier detección.
Phishing con credenciales robadas	Medusa, Qilin, LockBit	MFA + entrenamiento + email protection avanzada + monitoreo de logins anómalos.
CVEs sin parchar en servicios expuestos	LockBit, Qilin	Ventana de parcheo <7 días para CVEs KEV. Escaneo externo continuo.

RECOMENDACIONES

Prioridades defensivas para Q4 2026

Con base en lo observado, estas son las prioridades que recomendamos evaluar en los siguientes 90 días. No sustituyen un plan de seguridad integral — pero atacan directamente los vectores observados con mayor incidencia.

01 **Cerrar todo acceso RDP expuesto directamente a Internet.**
No hay caso legítimo de negocio. Todo acceso remoto debe ir por VPN con MFA. Este único cambio bloquea la mayoría de los ataques de Phobos.

02 **MFA obligatorio en toda VPN, firewall y consola administrativa.**
El vector inicial más común de Akira, Qilin y LockBit vía credenciales comprometidas. MFA lo neutraliza casi por completo.

03 **Monitoreo continuo de dark web para credenciales de tu dominio.**
Las credenciales aparecen en foros meses antes del ataque. Detectarlas y rotar es el mejor uso de threat intelligence.

04 **Ventana de parcheo <7 días para CVEs KEV en dispositivos de perímetro.**
Firewalls, VPNs, gateways expuestos. Prioriza por el catálogo KEV de CISA, no solo por CVSS.

05 **Copias de respaldo verdaderamente inmutables o aisladas.**
Un backup en el mismo dominio con credenciales del admin es un backup que el ransomware va a cifrar. Aislar es la única defensa real.

06 **Simulacro de respuesta a incidentes al menos anual.**
La primera decisión ante un ransomware activo es la que más impacta la recuperación. Si nunca se ha practicado, se practicará mal.

07 **Plan de comunicación bajo LFPDPPP preparado antes del incidente.**
Casi todos los incidentes hoy incluyen exfiltración. Notificación tardía a titulares es un agravante en cualquier auditoría.

SOBRE ESTE REPORTE

Black Husk Security

Black Husk Security es una empresa de ciberseguridad con sede en la Ciudad de México, especializada en **SOC-as-a-Service, pentesting, DFIR y threat intelligence**. Atendemos clientes en México, LATAM y otros mercados internacionales, con enfoque específico en amenazas activas contra la región y capacidad de servicio global.

Este reporte se elabora trimestralmente con base en la actividad observada por nuestro equipo en incidentes reales atendidos, monitoreo activo de la infraestructura pública de los grupos y seguimiento de foros underground en español. La próxima edición se publicará al cierre del Q4 2026.

Contacto para prensa y consultas

Sitio web	black-husk.com
Emergencias 24/7	WhatsApp — respuesta DFIR en menos de 1 hora
Consultas de prensa	Solicitar contacto vía sitio web
Diagnóstico gratuito	Reporte de exposición externa sin costo (5–7 días)

Nota metodológica: *Este reporte describe patrones observados y no representa un análisis estadístico exhaustivo. Los perfiles de familias se basan en incidentes atendidos por el equipo de Black Husk Security y en monitoreo abierto de la actividad pública de cada grupo. Los datos de sectores y vectores reflejan tendencias cualitativas, no un censo estadístico. Para consultas específicas sobre metodología, contactar al equipo por el sitio.*

¿QUIERES CONOCER TU EXPOSICIÓN AHORA?

Ofrecemos un diagnóstico sin costo del perímetro de tu empresa. Contáctanos en black-husk.com.