# ¿Cuál fue el tipo de ransomware que más afectó México en lo corrido de 2023?

El panorama de ciberseguridad en México, al igual que en todo el mundo, ha experimentado una creciente amenaza de ransomware en 2023. Según varias fuentes de seguridad cibernética, el tipo de ransomware que más afectó a México en lo que va de 2023 es el conocido como “BlackCat”. Este ransomware ha ganado notoriedad debido a sus tácticas de doble extorsión y su capacidad para infligir daño significativo a empresas de diversos sectores.

**BlackCat: Ransomware de Doble Extorsión**

BlackCat es un ransomware que cifra los archivos de las víctimas y luego exige un rescate en criptomonedas, generalmente Bitcoin, a cambio de la clave de descifrado. Sin embargo, lo que distingue a BlackCat es su enfoque en la “doble extorsión”. Además de cifrar los archivos, este ransomware roba datos sensibles de las víctimas, que pueden incluir información de tarjetas de crédito, contraseñas, registros médicos y otros datos confidenciales. La amenaza de publicar estos datos robados agrega una capa adicional de presión para que las víctimas paguen el rescate.

**Casos notables de ataques con BlackCat en México**

BlackCat se ha utilizado para atacar a empresas en México de varios sectores, lo que incluye al gobierno, la educación y la salud. Un caso especialmente destacado fue el ataque al Instituto Mexicano del Seguro Social (IMSS), el principal sistema de salud pública de México. Este ataque resultó en la interrupción de los servicios del IMSS durante varios días, afectando a miles de pacientes y provocando una gran preocupación en todo el país.

**Otros ransomware que afectaron a México en 2023**

Además de BlackCat, México también ha enfrentado otros tipos de ransomware en 2023. Algunos de los más prominentes incluyen LockBit, Conti y REvil. Estos ransomware también operan bajo la modalidad de doble extorsión y se han utilizado para atacar a empresas en todo el mundo.

**Cómo protegerse de ransomware**

 © 2026 www.seguridadendpoint.co

La amenaza del ransomware es real y constante, por lo que es crucial tomar medidas para protegerse. Aquí hay algunas recomendaciones clave:

1. **Mantenga copias de seguridad regulares de sus datos y sistemas.**
2. **Eduque a los empleados sobre la ciberseguridad y la prevención de ataques de phishing.**
3. **Mantenga su software y sistemas actualizados con parches de seguridad.
4. **Utilice soluciones de seguridad cibernética confiables que incluyan protección contra ransomware.
5. Considere la implementación de soluciones de doble autenticación para mejorar la seguridad de las cuentas.
6. Tenga un plan de respuesta a incidentes en caso de un ataque de ransomware, incluyendo la posibilidad de no pagar el rescate.

La amenaza del ransomware, incluido BlackCat, es una realidad seria en México y en todo el mundo. La prevención y la preparación son clave para protegerse contra estos ataques cibernéticos. Mantenerse al tanto de las últimas amenazas y seguir las mejores prácticas de seguridad es esencial para mantener la seguridad de los datos y sistemas empresariales.

 © 2026 www.seguridadendpoint.co