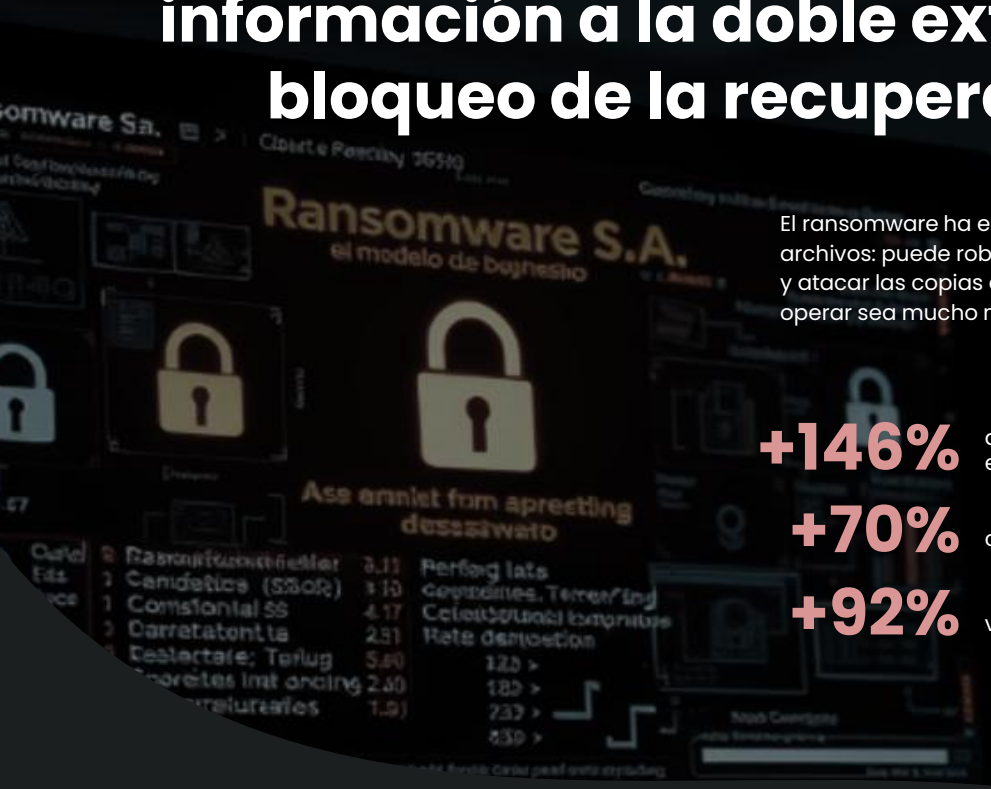
Ransomware: del secuestro de información a la doble extorsión y bloqueo de la recuperación



El ransomware ha evolucionado. Hoy no solo cifra archivos: puede robar datos, amenazar con publicarlos y atacar las copias de seguridad para que volver a operar sea mucho más difícil.

+146% ataques bloqueados a nivel mundial entre 2024 y 2025

+70% casos públicos de extorsión

+92% volumen de datos exfiltrados

Evolución del ransomware

Ransomware como servicio

Herramientas disponibles, afiliados y compra de accesos reducen la barrera de entrada a la cibercriminalidad.

Evolución de la extorsión

De cifrar información a amenazar con publicarla. Presionan con la interrupción del negocio, daños reputacionales y sanciones regulatorias.

Recovery denial

Atacan backups, servicios de identidad o plataformas de virtualización para dificultar la recuperación.

El impacto en tu empresa

Sistemas bloqueados

Interrupción de actividad y servicios críticos.

Datos robados

Amenazan con publicar datos robados como contratos, facturas o datos de clientes.

Impacto reputacional y sanciones

Temor a sanciones regulatorias, daño reputacional y en la relación con terceros.

Recuperación difícil

Backups o sistemas de recuperación también pueden ser objetivo.

Medidas eficaces para protegerse

Protección avanzada de dispositivos (EDR)

Detección y respuesta frente a comportamientos anómalos y malware.

Correo protegido

Frente a phishing, adjuntos maliciosos y credenciales robadas.

Navegación segura

Bloqueo de páginas fraudulentas y descargas peligrosas.

Vigilancia 24x7

Alertas revisadas a tiempo por expertos.

Backups protegidos

Copias aisladas, probadas y preparadas para restaurar.

¿Necesitas ayuda? Contacta con Cyber Guardian

Cyber Guardian