HORNETSECURITY

INFO SHEET

RANSOMWARE

CÓMO PUEDEN PROTEGERSE EFICAZMENTE LAS EMPRESAS

El ransomware se considera la ciberamenaza más importante para las organizaciones de todo el mundo (fuente: World Economic Forum, 2025). Los delincuentes están adoptando, cada vez más, cadenas de ataque automatizadas y muy desarrolladas que se vuelven más sofisticadas gracias al uso de tecnologías de IA generativa. Lo más peligroso es que muchos ataques comienzan con correos electrónicos que parecen inofensivos y terminan con el cifrado de sistemas completos. Según un estudio reciente de Hornetsecurity revela que una de cada tres empresas sufrió pérdidas de datos debido al ransomware en 2024.

¿QUÉ ES EL RANSOMWARE?

El ransomware es un tipo de software malicioso que cifra ordenadores o archivos y bloquea el acceso a ellos hasta que se paga un rescate. Por lo general, se instala sin que se note y luego se pone en contacto directo con la víctima. El ransomware es especialmente peligroso porque puede propagarse por las redes y paralizar organizaciones enteras.

LOS VECTORES DE ATAQUE MÁS COMUNES:



Ataques de phishing: a menudo, basta con hacer clic en un enlace malicioso o responder a un correo electrónico manipulado para desencadenar un ataque.



Correos electrónicos y archivos adjuntos: el ransomware se propaga con frecuencia a través de documentos de Office, archivos ZIP o PDF infectados. Los correos electrónicos con contenido personalizado son especialmente difíciles de detectar y pueden eludir los filtros convencionales.



Contraseñas débiles: las contraseñas fáciles de adivinar o la ausencia de autenticación multifactor (MFA) facilitan a los atacantes el acceso al sistema.

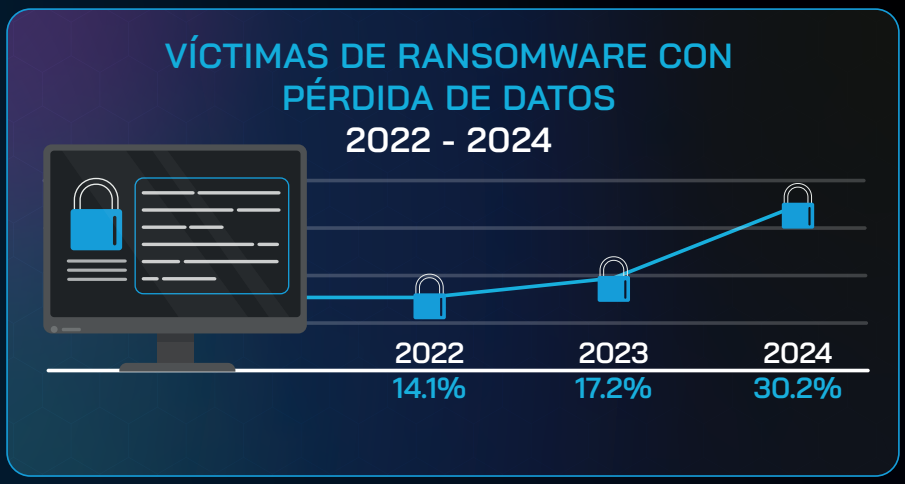


Sistemas sin parches: los atacantes aprovechan las vulnerabilidades conocidas del software y los sistemas. Por lo tanto, los parches incompletos son un objetivo principal para el ransomware.



Tácticas de ingeniería social: se manipula deliberadamente a los empleados, por ejemplo, mediante llamadas telefónicas o solicitudes de asistencia específicas. Los atacantes suelen recurrir al estrés, la autoridad o la urgencia para provocar acciones impulsivas.

HORNETSECURITY



LAS ESTRATEGIAS DE PROTECCIÓN CONTRA EL RANSOMWARE:

BLOQUEA DE FORMA FIABLE LOS CORREOS ELECTRÓNICOS MALICIOSOS	SPAM & MALWARE PROTECTION	El phishing sigue siendo una de las vías de entrada más comunes para el ransomware. Las soluciones de seguridad, como Spam and Malware Protection, bloquean los archivos adjuntos dañinos o los enlaces infectados antes de que puedan causar daños.
DETECTA LAS AMENAZAS MODERNAS DESDE EL PRINCIPIO	ADVANCED THREAT PROTECTION	El ransomware es cada vez más sofisticado. La protección basada en IA con autoaprendizaje puede identificar y detener amenazas ocultas o nuevas. Utiliza soluciones como Advanced Threat Protection.
VIGILA LAS VULNERABILIDADES CRÍTICAS		Los atacantes suelen aprovechar las vulnerabilidades conocidas del software o los sistemas obsoletos para desplegar el ransomware. Mantén tus sistemas actualizados de forma continua, preferiblemente mediante una gestión centralizada de parches, y utiliza la autenticación multifactor siempre que sea posible.
INVOLUCRA ACTIVAMENTE A LOS EMPLEADOS	SECURITY AWARENESS	Incluso la mejor tecnología es inútil si el comportamiento humano se convierte en el punto débil. Sensibiliza a tus equipos con formación periódica y campañas de phishing simuladas con el servicio Security Awareness Service, y fomenta una cultura de seguridad sostenible en tu organización.
RESTAURA LOS DATOS RÁPIDAMENTE EN CASO DE EMERGENCIA	VM BACKUP 365 TOTAL BACKUP	A pesar de todos los esfuerzos de prevención, la protección nunca puede garantizarse al 100 %. Por eso es fundamental proteger tus datos. Con VM Backup V9 y 365 Total Backup, puedes almacenar tus copias de seguridad de forma segura en la infraestructura de Hornetsecurity y proteger tus datos de los ataques de ransomware.