HORNETSECURITY

FICHE
D'INFORMATION

RANÇONGICIEL

COMMENT LES ENTREPRISES PEUVENT SE PROTÉGER EFFICACEMENT

Les ransomwares sont considérés comme la menace informatique la plus importante pour les entreprises à l'échelle mondiale (source : World Economic Forum, 2025). Les cybercriminels utilisent de plus en plus des chaînes d'attaque automatisées et complexes, renforcées par l'usage de technologies d'IA générative. Particulièrement insidieux : de nombreuses attaques commencent par des emails apparemment inoffensifs – et se terminent par le chiffrement de systèmes entiers. Un sondage récent mené par Hornetsecurity révèle qu'une entreprise sur trois a subi une perte de données due aux ransomwares en 2024.

QU'EST-CE QU'UN RANSOMWARE ?

Un ransomware est un type de malware qui chiffre des ordinateurs ou des fichiers et bloque l'accès tant qu'une rançon n'a pas été payée.
Il s'installe généralement de manière invisible, puis prend directement contact avec la victime.
Les ransomwares sont particulièrement dangereux, car ils peuvent se propager dans les réseaux et paralyser des entreprises entières.

VECTEURS D'ATTAQUE COURANTS

Phishing : souvent, un simple clic sur un lien malveillant ou une réponse à un email manipulé suffit à déclencher une attaque.

Emails et pièces jointes : les ransomwares se propagent fréquemment via des documents Office infectés, des fichiers ZIP ou des PDF. Les emails personnalisés sont particulièrement difficiles à détecter et peuvent contourner les filtres classiques.

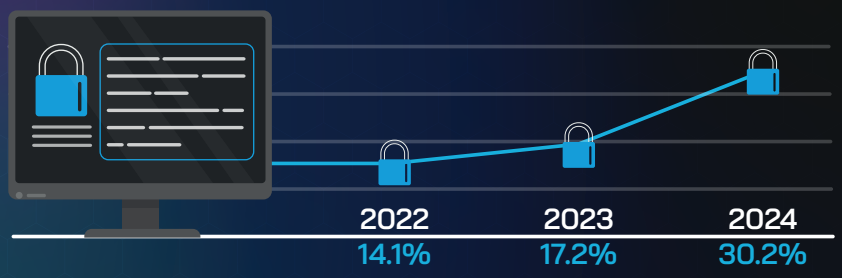
Identifiants de connexion faibles : des mots de passe faciles à deviner ou l'absence d'authentification multifacteur (MFA) facilitent l'accès des attaquants.

Systèmes non corrigés : les attaquants exploitent des failles connues dans les logiciels et systèmes non mis à jour. Un patching incomplet reste une cible privilégiée pour les ransomwares.

Techniques d'ingénierie sociale : les employés sont manipulés intentionnellement, par exemple par téléphone ou via de fausses demandes de support. Les attaquants exploitent souvent le stress, l'autorité ou l'urgence pour provoquer des actions impulsives.

HORNETSECURITY

PERTE DE DONNÉES DUE AUX RANSOMWARES 2022 - 2024



STRATÉGIES DE PROTECTION CONTRE LES RANSOMWARES

BLOQUER EFFICACEMENT LES EMAILS MALVEILLANTS	SPAM & MALWARE PROTECTION	Les emails de phishing demeurent l'un des principaux points d'entrée des ransomwares. Des solutions de sécurité comme Spam and Malware Protection bloquent les pièces jointes dangereuses ou les liens infectés avant tout dommage.
DÉTECTER LES MENACES MODERNES RAPIDEMENT	ADVANCED THREAT PROTECTION	Les ransomwares deviennent de plus en plus complexes. Une protection basée sur l'IA auto-apprenante peut identifier et stopper les menaces nouvelles ou cachées, par exemple avec Advanced Threat Protection.
SURVEILLER LES VULNÉRABILITÉS CRITIQUES		Les attaquants exploitent souvent des failles connues dans des logiciels ou systèmes obsolètes. Gardez vos systèmes à jour en continu, idéalement avec une gestion centralisée des correctifs, et utilisez l'authentification multifacteur partout où c'est possible.
IMPLIQUER ACTIVEMENT LES EMPLOYÉS	SECURITY AWARENESS	Même la meilleure technologie est inutile si le facteur humain devient la faille. Sensibilisez vos équipes par des formations régulières et des campagnes de phishing simulées grâce à Security Awareness Service, afin d'instaurer une culture de sécurité durable dans votre entreprise.
RESTAURER RAPIDEMENT LES DONNÉES EN CAS D'INCIDENT	VM BACKUP 365 TOTAL BACKUP	Malgré toutes les mesures préventives, aucune protection n'est garantie à 100 %. Il est donc essentiel de protéger vos données. Avec VM Backup V9 et 365 Total Backup, vous pouvez stocker vos sauvegardes de manière sécurisée dans l'infrastructure de Hornetsecurity protégeant ainsi vos données contre les attaques par ransomwares.