HORNETSECURITY

FICHE
D'INFORMATION

RANÇONGICIEL

COMMENT LES ENTREPRISES PEUVENT SE PROTÉGER

Les rançongiciels sont considérés comme la menace informatique la plus importante pour les organisations à l'échelle mondiale (source : World Economic Forum, 2025). Les cybercriminels adoptent de plus en plus des chaines d'attaque hautement perfectionnées et automatisées, qui deviennent toujours plus sophistiquées grâce à l'utilisation de technologies d'IA générative. Particulièrement insidieuses, de nombreuses attaques commencent par des courriels apparemment inoffensifs, et se terminent par le chiffrement de système entier. Un récent sondage mené par Hornetsecurity révèle qu'une entreprise sur trois a subi une perte de données due aux rançongiciels en 2024.

QU'EST-CE QU'UN RANÇONGICIEL ?

Un rançongiciel est un type de programme malveillant qui chiffre les ordinateurs ou les fichiers et bloque l'accès jusqu'à ce qu'une rançon soit versée. Il est habituellement installé à l'insu de la victime, puis entre en contact direct avec elle. Les rançongiciels sont particulièrement dangereux, car ils peuvent se propager à l'ensemble d'un réseau et paralyser des organisations entières.

VECTEURS D'ATTAQUE COURANTS :

Hameçonnage : Souvent, un simple clic sur un lien malveillant ou la réponse à un courriel manipulé suffit à déclencher une attaque.

Courriels et pièces jointes : Les rançongiciels se propagent fréquemment par des documents Microsoft Office infectés, des fichiers ZIP ou des PDF. Les courriels personnalisés sont particulièrement difficiles à détecter et peuvent contourner les filtres classiques.

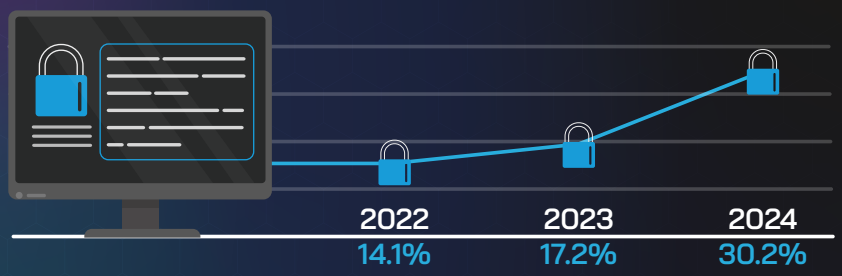
Identifiants de connexion faibles : Des mots de passe faciles à deviner ou l'absence d'authentification multifactorielle (AMF) facilitent l'accès des attaquants aux systèmes.

Systèmes non corrigés : Les attaquants exploitent les vulnérabilités connues des logiciels et des systèmes. L'absence ou l'incomplétude des mises à jour constitue une cible de choix pour les rançongiciels.

Techniques d'ingénierie sociale : Les employés sont volontairement manipulés, par exemple par des appels téléphoniques ou des demandes d'assistance ciblées. Les attaquants misent souvent sur le stress, l'autorité ou l'urgence pour provoquer des actions impulsives.

HORNETSECURITY

PERTE DE DONNÉES DUE AUX RANÇONGICIELS 2022 - 2024



STRATÉGIES DE PROTECTION CONTRE LES RANÇONGICIELS :

BLOQUER DE FAÇON FIABLE LES COURRIELS MALVEILLANTS	SPAM & MALWARE PROTECTION	Les courriels d'hameçonnage demeurent l'un des principaux points d'entrée des rançongiciels. Les solutions de sécurité telles que Spam and Malware Protection bloquent les pièces jointes dangereuses ou les liens infectés avant que des dommages ne surviennent.
DÉTECTER RAPIDEMENT LES MENACES MODERNES	ADVANCED THREAT PROTECTION	Les rançongiciels deviennent de plus en plus sophistiqués. Une protection fondée sur l'IA autoapprenante peut repérer et neutraliser les menaces nouvelles ou dissimulées-utilisez des solutions comme Advanced Threat Protection.
SURVEILLER DE PRÈS LES VULNÉRABILITÉS CRITIQUES		Les attaquants exploitent souvent des failles connues dans les logiciels ou des systèmes désuets pour déployer un rançongiciel. Maintenez vos systèmes continuellement à jour, idéalement avec une gestion centralisée des correctifs, et utilisez l'authentification multifactorielle partout où c'est possible.
IMPLIQUER ACTIVEMENT LES EMPLOYÉS	SECURITY AWARENESS	Même la meilleure technologie est inefficace si le comportement humain devient le maillon faible. Sensibilisez vos équipes grâce à des formations régulières et à des campagnes simulées d'hameçonnage, comme avec le Security Awareness Service, et instaurez une culture de sécurité durable au sein de votre organisation.
RESTAUREZ RAPIDEMENT LES DONNÉES EN CAS D'URGENCE	VM BACKUP 365 TOTAL BACKUP	Malgré toutes les mesures de prévention, la protection ne peut jamais être garantie à 100 %. C'est pourquoi la protection de vos données est essentielle. Avec VM Backup V9 et 365 Total Backup, vous pouvez stocker vos copies de sauvegarde de façon sécuritaire dans l'infrastructure de Hornetsecurity – protégeant ainsi vos données contre les attaques par rançongiciel.