Veille Les Ransomware

En 2025, les **ransomwares** sont clairement de retour et ont évolué : après une période de recul, les attaques repartent à la hausse et deviennent à la fois plus nombreuses et plus sophistiquées. Plusieurs rapports observatoires montrent une montée nette des incidents et des coûts associés : le nombre de groupes d'extorsion a augmenté de façon significative (Check Point a signalé environ 85 groupes actifs au troisième trimestre 2025) et le coût moyen d'un incident a atteint des niveaux qui pèsent lourd sur les bilans des organisations (résultats publiés par Resilience indiquant un coût moyen des incidents supérieur à un million de dollars et une part importante des sinistres cyber liée aux ransomwares). Le modèle RaaS — ransomware-as-a-service — reste un pilier de l'écosystème criminel : il permet à des acteurs peu techniques d'orchestrer des attaques sophistiquées en louant des outils et services, ce qui accélère la prolifération d'acteurs et la fragmentation du paysage (Hornetsecurity, Check Point, Kaspersky).

Sur le plan tactique, plusieurs évolutions inquiètent. D'abord, l'IA est devenue un multiplicateur de force pour les attaquants : les outils d'automatisation accélèrent le tempo des attaques (le « breakout time » — temps entre l'accès initial et la compromission étendue — a été drastiquement réduit dans des études sectorielles), et l'IA est utilisée pour améliorer la capacité de phishing et d'ingénierie sociale, rendant les leurres beaucoup plus crédibles (CrowdStrike, Acronis). Parallèlement, des preuves de concept et des prototypes de ransomwares « IA-native » ou pilotés par des modèles de langage ont été documentés : ces prototypes peuvent générer du code malveillant, s'adapter et orchestrer des phases d'attaque avec peu ou pas d'intervention humaine, ce qui change la nature même de la menace (travaux académiques publiés sur arXiv et médias spécialisés). Une autre tendance marquante est l'augmentation des opérations d'extorsion sans chiffrement massif : au lieu — ou en plus — de chiffrer les systèmes, les attaquants volent des données et menacent de les publier (double extorsion), ce qui accroît la pression sur les victimes et la complexité de la réponse (Resilience, Help Net Security).

Les vecteurs d'entrée restent souvent classiques mais toujours efficaces : exploitation de vulnérabilités non patchées dans des services exposés (VPN, RMM, RDP), compromission d'identifiants via phishing, et abus de chaines d'approvisionnement ou d'outils de gestion à distance. Ces portes d'entrée sont tellement fréquentes que la priorité numéro une pour de nombreuses équipes de sécurité demeure le patch management et la gouvernance des accès. LockBit, groupe historique, a montré des signes de retour avec des variantes plus multi-plateformes (support Windows, Linux, ESXi) et des capacités d'évasion améliorées, illustrant comment des familles établies peuvent se réinventer (Check Point).

Certains secteurs restent particulièrement ciblés : santé, industrie manufacturière, retail et infrastructures critiques enregistrent une forte proportion d'attaques, et leur compromission a des conséquences humaines et économiques lourdes. Les ransomwares s'attaquent également à des cibles moins traditionnelles (IoT, systèmes de sauvegarde, environnements cloud mal configurés) pour élargir la surface d'attaque et neutraliser les options de restauration. Au niveau géographique, des rapports font état d'une pression marquée en Asie-Pacifique, Moyen-Orient et certaines régions d'Afrique, même si la menace demeure globale (Kaspersky, Resilience).

Face à ces évolutions, les réponses ne peuvent plus être uniquement réactives ou basées sur des signatures. Les recommandations récurrentes sont claires et convergentes : appliquer rigoureusement le patch management pour tous les systèmes exposés ; renforcer l'authentification (MFA) et la gestion des accès ; déployer des solutions de détection comportementale et de réponse automatisée capables d'identifier des schémas d'attaque plutôt que des signatures statiques ; et, surtout, revoir la stratégie de sauvegarde. Les sauvegardes doivent être isolées, immuables, testées régulièrement et conçues pour résister à des attaques qui visent explicitement les infrastructures de backup. Les entreprises doivent aussi augmenter la formation et la sensibilisation de leurs employés, en tenant compte du fait que l'IA rend les attaques d'ingénierie sociale beaucoup plus convaincantes. Enfin, l'intégration d'une threat intelligence opérationnelle permet de suivre l'émergence de nouveaux groupes et leurs TTPs (tactiques, techniques et procédures), ce qui est essentiel dans un paysage fragmenté.

Au niveau réglementaire et assurantiel, on observe des changements : le débat public sur l'interdiction ou la régulation du paiement des rançons se renforce (certains gouvernements explorent des exceptions pour les infrastructures critiques), et le marché de l'assurance cyber évolue — mais la couverture n'est pas universelle, beaucoup d'organisations n'ayant pas de police adaptée ou souscrivant des garanties lacunaires. Les attaquants le savent et peuvent calibrer leurs demandes en conséquence ; certains exploitent même des informations sur les polices d'assurance pour ajuster les montants réclamés (analyses de Resilience).

Les perspectives à moyen terme montrent une course entre attaquants et défenseurs autour de l'IA : les cybercriminels intègrent l'IA pour générer, accélérer et adapter leurs attaques, tandis que les défenseurs cherchent à déployer des IA et des approches ML capables de détecter des comportements anormaux, d'automatiser les réponses et de réduire le « dwell time » (temps de présence des attaquants). L'un des risques clefs est que l'IA réduise la barrière technique d'entrée pour des acteurs moins sophistiqués, augmentant ainsi le nombre d'attaques opportunistes et ciblées. En parallèle, l'apparition de ransomwares autonomes et la professionnalisation du RaaS rendent la menace plus scalable et plus imprévisible.

En synthèse, la protection efficace contre les ransomwares en 2025 exige une posture multi-couches : gouvernance des correctifs et des accès, sauvegardes robustes et testées, détection comportementale avancée (idéalement avec capacités d'analyse IA orientée détection d'anomalies), formation continue des équipes humaines, et partage d'informations opérationnelles entre pairs et autorités. Les organisations doivent aussi revoir leurs contrats d'assurance cyber et leurs plans de continuité pour intégrer des scénarios de double extorsion et d'attaques IA-assistées. Sans une approche coordonnée mêlant technologie, processus et formation, le risque financier et opérationnel lié aux ransomwares risque de continuer à augmenter.

Sources principales consultées pour cette veille : rapports et articles de Hornetsecurity (Ransomware Impact Report 2025), Check Point (The State of Ransomware Q3 2025), Resilience (Midyear Cyber Risk / Threatonomics 2025), CrowdStrike, Acronis, Kaspersky, Help Net Security, articles et analyses sur PromptLock et autres ransomwares IA-assisted (Tom's Hardware, Axios), et publications académiques sur arXiv traitant de détection entropique et de prototypes de ransomwares pilotés par LLMs. Si tu veux, je peux te fournir la liste complète des articles exacts et leurs liens — ou bien transformer ce texte en PDF ou en diapos pour ton Oral. Tu veux que je fasse ça maintenant ?