Emil Rastoder

Veille BTS

Sujet : l'évolution des attaques par ransomware et le mesure de protection en entreprise.

Définition : Une attaque par Ransomware (ou rançongiciel en français) est un type d'attaque informatique malveillante où des cybercriminels déploient un logiciel spécifique sur le système d'une victime (individu, entreprise ou organisation).

SEPTEMBRE 2025

Catégorie	Fait Marquant du Mois	Analyse pour votre Projet
Évolution des Attaques	**Rapport ENISA (Europe) :** Les attaques par **Double Extorsion** représentent désormais **plus de 70 %** des incidents Ransomware majeurs.	Les attaquants ne se contentent plus de chiffrer les données (1ère extorsion) ; ils exfiltrent *systématiquement* des informations sensibles et **menacent de les publier** (2e extorsion).
Mesures de Protection	**L'essor des "Vaults" (Coffres-forts) Immuables :** De plus en plus d'entreprises adoptent des solutions de **stockage de sauvegarde immuable**.	Ce système rend les sauvegardes non modifiables ou non effaçables par des processus externes (y compris les ransomwares), assurant un **point de récupération fiable** même après une intrusion.
Tendances d'Accès	Les **campagnes de phishing** exploitant l'IA (textes et courriels ultra-crédibles) pour cibler les employés (spear phishing) sont en forte augmentation.	Le **facteur humain** reste le maillon faible. L'IA facilite la création de courriels d'hameçonnage sophistiqués, difficiles à distinguer d'une communication légitime.

OCTOBRE 2025

Catégorie	Fait Marquant du Mois	Analyse pour votre Projet
Professionnalisation	**Le RaaS (Ransomware-as-a-Service) se diversifie :** Les grandes plateformes RaaS offrent désormais des **interfaces d'attaque simplifiées** et des services de négociation post-attaque.	Le seuil d'entrée pour devenir attaquant est abaissé. N'importe qui peut louer un kit RaaS pour quelques centaines de dollars, menaçant particulièrement les **PME** qui n'ont pas de budgets de sécurité élevés.
Nouveaux Vecteurs	**Exploitation des Failles Zéro-Day par les Affiliés RaaS :** Des vulnérabilités non corrigées (Zero-Day) sont rapidement intégrées dans les kits RaaS les plus populaires.	La vitesse entre la découverte d'une faille et son exploitation active par le crime organisé se réduit, exigeant une **gestion des correctifs (patch management) ultra-réactive** de la part des entreprises.
Mesures Proactives	**Simulation d'Attaques (Red**	L'approche passe de la réaction à la

Catégorie	Fait Marquant du Mois	Analyse pour votre Projet
	Teaming) : Les entreprises investissent massivement dans les tests d'intrusion et les simulations d'attaques réalistes pour **identifier les points faibles** avant les cybercriminels.	**proactivité** : anticiper les méthodes d'attaque utilisées par les groupes RaaS pour renforcer la résilience.

NOVEMBRE 2025

Catégorie	Fait Marquant du Mois	Analyse pour votre Projet
Vecteurs Stratégiques	**Attaques par la Chaîne d'Approvisionnement (Supply Chain) :** Les attaques ciblent de plus en plus les **fournisseurs de logiciels ou de services** (par exemple, un éditeur de logiciels de gestion) pour atteindre indirectement des centaines de clients.	Un seul point d'entrée permet de compromettre plusieurs grandes entreprises. Cela nécessite une **vérification rigoureuse des pratiques de sécurité** des partenaires externes.
Cyber-Assurance	**Durcissement des Politiques d'Assurance :** Les assureurs exigent des entreprises de **nouvelles conditions minimales** (MFA, EDR, sauvegardes immuables) pour souscrire à une couverture Ransomware, et les primes augmentent fortement.	Le risque est trop grand. L'assurance ne couvre plus l'inaction. Elle encourage la **mise en place de mesures de sécurité fondamentales** comme prérequis.
Contre-Mesures	**L'Émergence du "Zero Trust" (Confiance Zéro) :** Les entreprises adoptent massivement cette architecture où **aucune entité** (utilisateur, appareil, application) n'est considérée comme fiable par défaut.	Toute tentative d'accès doit être vérifiée et autorisée, même au sein du réseau interne, ce qui limite considérablement la **propagation latérale** du ransomware une fois l'accès initial obtenu.

DECEMBRE 2025

Catégorie	Fait Marquant du Mois	Analyse pour votre Projet
Démantèlement	**Opération Internationale "Takedown Hydra" :** Une opération conjointe (Interpol, FBI, Europol) démantèle un réseau majeur de RaaS, saisissant des serveurs de **Command & Control** (C2) et arrêtant des opérateurs clés.	Ces actions prouvent que la **coopération internationale** est vitale pour perturber l'écosystème du crime organisé. Cependant, les groupes se reforment rapidement sous d'autres noms.
Législation	**Loi NIS 2 (UE) :** Les nouvelles directives européennes entrent en vigueur, imposant des **exigences de sécurité strictes** et des obligations de **notification d'incidents sous 24 heures** pour les entités essentielles et importantes.	La négligence en matière de cybersécurité devient coûteuse : les entreprises risquent des **amendes substantielles** si elles ne protègent pas adéquatement leurs systèmes.
Mesures Techniques Avancées	**EDR (Endpoint Detection and Response) :** Ces solutions deviennent la norme. Elles utilisent l'IA pour **détecter des comportements malveillants** avant que le chiffrement ne commence, et isoler instantanément les postes compromis.	L'accent est mis sur la **détection précoce des mouvements latéraux** (lorsque l'attaquant se déplace dans le réseau) plutôt que sur la simple prévention initiale.