Le ransomware sans chiffrement : pourquoi le pire est devant nous

6 mai 2026 • Mis à jour le 17 mai 2026 • 9 min de lecture • 1319 mots • 98 vues •

En 2026, les groupes d'extorsion abandonnent le chiffrement pour l'exfiltration pure. Pourquoi nos défenses sont calibrées pour la mauvaise menace, et comment pivoter.

En 2026, les groupes les plus dangereux ne chiffrent plus rien. Ils volent, menacent, publient. Et c'est précisément ce qui les rend redoutables : on ne peut pas restaurer ce qu'on n'a pas perdu, et on ne peut pas négocier ce qui est déjà publié.

La fin du modèle "pay or restore"

Pendant cinq ans, le ransomware a suivi un schéma stable. L'attaquant pénétrait, se déplaçait latéralement, désactivait les sauvegardes, chiffrait les données, et présentait sa note. La victime avait alors un choix binaire : payer pour la clé, ou restaurer depuis des backups. Tout le débat sécurité s'est construit autour de cette équation : sauvegardes immutables, segmentation, détection précoce, plan de continuité. Et globalement, ça a marché. Les organisations matures ont appris à ne plus payer, à restaurer en quelques jours, à absorber le coup.

En 2026, ce modèle est en train de mourir. Pas parce que les attaquants ont perdu, mais parce qu'ils ont changé de jeu. Quand on regarde les leaks récents — ShinyHunters sur Instructure (275 millions d'utilisateurs), Cushman & Wakefield (500 000 enregistrements Salesforce), Match Group, Adelante en Colombie — un pattern frappe : aucun chiffrement. Juste de l'exfiltration, et la menace de publication.

Ce n'est pas un détail technique. C'est une mutation stratégique qui rend l'ensemble de notre arsenal défensif partiellement obsolète.