AYI NEDJIMI Consultants

Ransomware en 24 heures : la fin du luxe de la réponse lente

Catégorie : Cybersécurité Générale Lecture : 7 min Publié le : 12/04/2026 Auteur : Ayi NEDJIMI

Le ransomware se déploie en 24h : Storm-1175 et Medusa changent la donne. Analyse d'expert sur ce que ça implique pour votre défense.

On a longtemps vécu avec l'idée qu'un attaquant mettait des semaines à se déplacer dans un réseau avant de frapper. Cette époque est révolue. Les données de Microsoft sur Storm-1175 le confirment : certains groupes ransomware passent de l'accès initial au chiffrement complet en moins de 24 heures. Ce n'est pas un exploit technique ponctuel — c'est un changement structurel dans la façon dont le ransomware opère. Et ça remet en question tout ce qu'on pensait savoir sur la réponse à incident. En tant que consultant terrain, je vois chaque semaine des organisations construire leur défense autour d'hypothèses de temporalité qui ne tiennent plus. Il est temps d'en parler clairement, sans langue de bois.

Le mythe du « dwell time » confortable

Pendant des années, les rapports de l'industrie nous ont bercé avec des moyennes de « dwell time » (temps de présence de l'attaquant avant détection) de 20 à 200 jours. Ces chiffres ont structuré toute notre approche de la défense : on investit dans la détection, on forme les SOC à analyser les alertes, on construit des playbooks de réponse avec des délais de 24 à 72 heures. Le problème, c'est que ces moyennes masquent une réalité bien plus brutale.

Storm-1175 ne passe pas 200 jours dans votre réseau. Il entre par une faille web connue, désactive votre antivirus via PowerShell en quelques minutes, exfiltre vos données avec Rclone, et déploie Medusa avant que votre équipe ait fini son premier café. Les chiffres de Microsoft sont sans appel : dans certains cas, l'ensemble de la chaîne d'attaque prend moins de 24 heures. Et Storm-1175 n'est pas seul. On observe la même accélération chez les affiliés de BlackCat/ALPHV et chez les opérateurs de Play ransomware.

Pourquoi les attaquants accélèrent

Cette accélération n'est pas aléatoire. Elle répond à une logique économique et tactique. D'abord, la fenêtre de vulnérabilité entre la publication d'un patch et son application en entreprise est prévisible : entre 3 et 30 jours pour la plupart des organisations. Les attaquants le savent et construisent leurs outils d'exploitation en conséquence. Storm-1175 a exploité plus de 16 vulnérabilités différentes, dont des zero-days, avec une industrialisation remarquable.

Ensuite, rester longtemps dans un réseau augmente le risque de détection. Les SOC s'améliorent, les EDR aussi. La stratégie rationnelle pour un attaquant est donc de frapper vite : entrer, exfiltrer, chiffrer, partir. Le modèle RaaS facilite cette approche : l'affilié n'a pas besoin de

développer ses propres outils, tout est fourni par la plateforme. Il se concentre sur l'accès initial et la vitesse d'exécution. On l'a vu avec l'attaque ChipSoft qui a mis des hôpitaux entiers en mode dégradé en quelques heures.

Ce que ça change concrètement pour les défenseurs

Si l'attaquant met 24 heures à compromettre votre SI, votre plan de réponse à incident de 72 heures est obsolète. Point. Ça ne veut pas dire qu'il faut tout jeter, mais ça impose des ajustements structurels dans trois domaines clés.

La prévention redevient reine

Quand la détection arrive trop tard, il faut empêcher l'accès initial. Ça signifie un patch management agressif sur les actifs exposés, une réduction draconienne de la surface d'attaque externe, et une segmentation réseau qui limite la propagation même en cas de compromission. Les fondamentaux, en somme — mais appliqués avec une rigueur que beaucoup d'organisations n'ont pas encore atteinte.

L'automatisation de la réponse n'est plus un luxe

Un SOC qui met 4 heures à qualifier une alerte et 2 heures de plus à décider d'isoler un poste ne tiendra pas face à un attaquant qui boucle sa chaîne en 12 heures. L'isolation automatique des endpoints compromis, le blocage automatique des exfiltrations suspectes, la révocation automatique des sessions après détection d'une compromission de credentials — ces automatisations doivent passer de « nice to have » à « impératif opérationnel ».

Les sauvegardes hors ligne ne suffisent plus

Avec la double extorsion systématique, restaurer depuis une sauvegarde ne règle que la moitié du problème. Les données sont déjà chez l'attaquant. La protection des données sensibles en amont — chiffrement, classification, DLP — devient aussi importante que la capacité de restauration. C'est un changement de paradigme que beaucoup de RSSI n'ont pas encore intégré.

Mon avis d'expert
Je le dis depuis des mois à mes clients : arrêtez de construire votre défense autour du scénario de l'attaquant « patient ». Ce scénario existe encore pour les APT étatiques qui font du renseignement, mais le ransomware — qui représente la menace numéro un pour 90% des organisations — a basculé dans le mode blitz. Si votre plan de réponse à incident ne peut pas être activé en moins de 2 heures, vous n'avez pas un plan de réponse, vous avez un document de conformité. La vraie question n'est plus « est-ce qu'on va détecter l'attaquant ? » mais « est-ce qu'on peut l'empêcher d'entrer ? ». Et ça, ça demande de l'investissement sur le périmètre, pas seulement sur le SOC.

Conclusion

Le ransomware en 24 heures n'est pas une anomalie — c'est la nouvelle norme pour les groupes les plus performants. Storm-1175 et Medusa montrent la voie, et d'autres suivront. Les organisations qui survivront sont celles qui auront compris que la vitesse de l'attaquant impose la vitesse de la défense. Pas demain. Maintenant.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr