Pourquoi les attaques par rançongiciel deviennent-elles plus fréquentes chaque année ?

Réponse courte : Les attaques par rançongiciel augmentent parce que les groupes cybercriminels sont passés d'acteurs désorganisés et opportunistes à des opérations disciplinées qui utilisent l'automatisation pour attaquer efficacement de nombreuses victimes et obtenir rapidement un paiement.

De startups chaotiques à des opérations organisées

Lorsque le rançongiciel est devenu une menace répandue, de nombreux attaquants manquaient d'expérience. Une vague de personnes nouvellement au chômage pendant la période pandémique a tenté sa chance dans la cybercriminalité, souvent avec des résultats inégaux. Comme dans toute industrie émergente, seuls les opérateurs les plus organisés et les plus compétents ont survécu à cette première période de tri. Avec le temps, ces groupes ont commencé à fonctionner moins comme des opportunistes dispersés et davantage comme des entreprises structurées axées sur des revenus constants.

D'ici 2024, cette maturité s'est traduite par une forte dépendance à l'automatisation. Les opérations de rançongiciel établies utilisent désormais des outils automatisés pour intégrer des participants moins expérimentés dans leurs attaques tout en maintenant des processus efficaces et reproductibles. Cela leur a permis d'étendre leurs activités bien au-delà de ce qu'une petite équipe de pirates informatiques qualifiés pourrait accomplir manuellement.

Calibrer l'attaque pour un gain maximal

Un élément clé de cette évolution consiste à apprendre à dimensionner correctement une attaque. Si une intrusion est trop mineure, une équipe informatique bien préparée peut simplement restaurer les systèmes et éviter de payer quoi que ce soit. Si une attaque est trop étendue, anéantissant toute l'infrastructure de l'entreprise, il se peut qu'il ne reste aucune activité viable pour effectuer un paiement de rançon. Les groupes de rançongiciel modernes visent un juste milieu : suffisamment de perturbation pour pousser une entreprise à payer rapidement, sans

causer des dommages tels que la reprise ou la négociation deviennent sans objet.

Pourquoi l'automatisation entraîne cette augmentation

Une fois qu'un processus d'attaque peut être automatisé, les cybercriminels ne se contentent plus de viser une seule victime à la fois. À l'aide d'outils qui s'apparentent à l'intelligence artificielle, à l'apprentissage automatique et à l'automatisation robotisée des processus, ils peuvent cibler simultanément des dizaines, voire des centaines d'organisations. De nombreuses victimes choisissent de ne pas divulguer publiquement les incidents, ce qui permet aux attaquants d'achever un cycle d'extorsion et de passer à de nouvelles cibles. Ce modèle économique évolutif et reproductible — plutôt qu'une quelconque nouvelle technologie isolée — est la principale raison pour laquelle les attaques par rançongiciel continuent d'augmenter.

https://player.vimeo.com/video/1043463561

Regarder sur Vimeo · Sous-titres : English, Français, Español, العربية

Revision #1
Created 2026-07-24 07:26:55 UTC by Dennis Underwood
Updated 2026-07-24 07:26:55 UTC by Dennis Underwood