Pourquoi le rançongiciel attaque-t-il les fichiers partagés avant d'atteindre mon poste de travail ?

Réponse courte : Lorsqu'un rançongiciel infecte un poste de travail individuel, cette machine est rarement la cible réelle. Les attaquants utilisent l'infection initiale comme point de lancement pour atteindre les ressources réseau partagées, et ils ne chiffrent ou n'endommagent le poste de travail local qu'après s'être déjà attaqués à des données de plus grande valeur ailleurs.

Pourquoi le poste de travail est le dernier arrêt, pas le premier

Une idée reçue courante est que si un rançongiciel atteint l'ordinateur d'un employé donné, ce sont les fichiers de cet employé que les attaquants recherchent. En réalité, le logiciel malveillant est programmé pour dépasser la machine locale presque immédiatement. Une fois qu'il obtient un point d'ancrage, il commence à analyser le réseau à la recherche de ressources accessibles de plus grande valeur, telles que des serveurs de fichiers, des wikis internes ou des bases de données contenant des informations sur les clients. Le chiffrement ou l'exfiltration de ces données centralisées constitue le véritable objectif, car cela affecte une bien plus grande partie de l'organisation que le dossier d'un seul utilisateur.

La note de rançon arrive en dernier, pas en premier

Étant donné que les attaquants privilégient les données à l'échelle du réseau avant de toucher l'appareil d'origine, l'employé infecté est généralement la dernière personne à remarquer un problème. Au moment où une note de rançon apparaît sur son écran, les attaquants ont généralement déjà terminé de chiffrer ou de voler des données à travers une grande partie de l'infrastructure de l'entreprise. Cet ordonnancement est intentionnel. Il permet aux attaquants d'infliger un dommage opérationnel maximal avant que quiconque au sein de l'organisation n'ait la

possibilité de détecter l'intrusion ou d'y répondre. La note de rançon visible n'est essentiellement qu'un signal indiquant que les dommages les plus graves se sont déjà produits en coulisses.

Ce que cela signifie pour la défense

Les photos ou documents personnels stockés localement sur un poste de travail constituent généralement la cible la moins importante lors d'une attaque par rançongiciel, même s'ils peuvent en être le signe le plus visible. Une défense efficace doit tenir compte de ce schéma en se concentrant sur la détection et l'arrêt de l'activité malveillante le plus tôt possible, avant qu'elle ne puisse atteindre les systèmes partagés. FortressAI de Cyber Crucible a été conçu en tenant compte de cette séquence d'attaque, visant à intervenir dès les premières étapes d'une intrusion plutôt que de réagir uniquement une fois que le chiffrement devient visible sur les machines individuelles.

https://player.vimeo.com/video/1043466243

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

Revision #1
Created 2026-07-24 07:25:08 UTC by Dennis Underwood
Updated 2026-07-24 07:25:08 UTC by Dennis Underwood