Pourquoi le vol d'identifiants et d'identité est-il plus dangereux que le chiffrement par ransomware ?

Réponse courte : Le chiffrement par ransomware est l'étape visible et finale d'une attaque, mais les dégâts réels surviennent souvent plus tôt, de manière inaperçue, lorsque les attaquants récupèrent automatiquement les mots de passe, les jetons de session, les clés et les portefeuilles de cryptomonnaies. Cyber Crucible se concentre sur la détection et l'arrêt de cette étape précoce et cachée, plutôt que d'attendre le moment où les données sont verrouillées.

Pourquoi les outils de sécurité passent souvent à côté de la menace la plus importante

De nombreux produits de sécurité sont conçus pour réagir au chiffrement, car c'est la partie de l'attaque qu'une entreprise remarque réellement : les systèmes tombent en panne, les fichiers deviennent illisibles et les opérations s'arrêtent. Cette perturbation visible attire naturellement le plus d'attention et d'investissements. Cependant, le chiffrement est généralement la dernière action entreprise par un attaquant, et non la première. Au moment où une entreprise constate les effets d'un ransomware, l'attaquant a généralement déjà achevé la partie la plus lourde de conséquences de l'intrusion : la collecte discrète de données liées à l'identité, telles que les identifiants, les jetons d'authentification, les clés de chiffrement et l'accès aux portefeuilles numériques. Cette phase précoce ne provoque aucune perturbation visible, ce qui explique qu'elle soit souvent sous-estimée, alors même qu'elle offre aux attaquants un accès durable et répétable au réseau.

La première étape silencieuse d'une attaque

Les attaques modernes sont largement automatisées, et la phase de vol d'identité peut être menée à bien en quelques secondes seulement à l'échelle de toute une organisation. Comme il n'y a pas d'interruption immédiate de l'activité, cette étape ne bénéficie pas de l'urgence et de la visibilité que crée le chiffrement par ransomware, ce qui la rend facile à négliger. Pourtant, c'est bien cette étape qui donne aux attaquants la possibilité de revenir quand ils le souhaitent et de causer des dommages supplémentaires, y compris de déployer un ransomware par la suite.

Comment Cyber Crucible répond à cette lacune

Cyber Crucible est conçu pour détecter les accès non autorisés aux données d'identité au moment même où ils se produisent, plutôt que d'attendre le début du chiffrement. Étant donné que cette activité se déroule si rapidement et si discrètement, des efforts d'ingénierie considérables ont été consacrés à rendre la détection à la fois rapide et précise, afin d'identifier qui accède aux données d'identité sensibles sans ralentir les opérations commerciales quotidiennes ni l'activité des utilisateurs.

https://player.vimeo.com/video/1141670023

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

Revision #1
Created 2026-07-24 07:27:44 UTC by Dennis Underwood
Updated 2026-07-24 07:27:44 UTC by Dennis Underwood