

Cyber Crucible collecte-t-elle les clés de chiffrement ?

La réponse la plus courte est : « Non. »

Il fut un temps où le logiciel de Cyber Crucible n'arrêtait pas le chiffrement des rançongiciels avant qu'il ne se produise. Il collectait plutôt des clés de chiffrement ou des paramètres possibles, puis utilisait diverses techniques pour déterminer le bon ensemble de déchiffrement (clés incluses) afin de déchiffrer après une attaque de rançongiciel.

Du point de vue de ce que nous collections, une bonne analogie serait une caméra vidéo qui prendrait des photos de tout ce qui pourrait constituer une clé d'un casier. Ensuite, un serveur effectuerait les divers calculs pour déterminer la clé et les paramètres appropriés pour le bon fichier. Les informaticiens appelleraient cela de l'apprentissage automatique.

Avant de passer à autre chose que l'ancien modèle logiciel « collecter tout ce qui pourrait être une clé », nous organisons automatiquement des milliers de clés et de paramètres de chiffrement par machine lors des attaques.

Le module logiciel d'analyse cryptographique a désormais évolué vers un module analytique comportemental supplémentaire, utilisé comme une source de données parmi d'autres pour déterminer si un logiciel tente d'accéder de manière inappropriée à des données d'identité ou à des « données de données » dans le but de les voler ou de les chiffrer.

Revision #1

Created 2026-07-24 07:00:12 UTC by Dennis Underwood

Updated 2026-07-24 07:00:12 UTC by Dennis Underwood