

Pourquoi la capture des clés de chiffrement des ransomwares n'est-elle plus une défense valable ?

Réponse courte : La capture de clés a cessé d'être techniquement fiable en 2021. Les ransomwares modernes évitent les bibliothèques de chiffrement standard du système d'exploitation, de sorte qu'il n'existe aucune clé qu'un outil défensif puisse intercepter — et même lorsque des clés sont obtenues, elles ne peuvent souvent pas être appliquées.

Comment les ransomwares modernes contournent la capture de clés

- **Bibliothèques personnalisées :** le code de chiffrement est compilé directement dans le logiciel malveillant au lieu d'appeler les bibliothèques du système d'exploitation, de sorte que les clés sont générées et utilisées entièrement à l'intérieur du propre processus de l'attaquant — invisibles pour les outils qui surveillent les appels standard.
- **Implémentations uniques :** certaines souches utilisent un chiffrement non standard, propre à chaque exécution. Même une clé capturée ne peut pas être appliquée, car l'algorithme lui-même est sur mesure.
- **Chiffrements de flux (streaming ciphers) :** ceux-ci reposent sur un concept fondamentalement différent de l'AES et sont tout simplement immunisés contre la capture de clés AES.

Cyber Crucible a initialement développé et breveté une technologie de capture de clés, puis a présenté la cryptanalyse démontrant ses limites lors de BSides Pittsburgh en 2021. Nous sommes passés à autre chose parce que les preuves l'imposaient.

Le problème de conformité également

La capture de clés nécessite le stockage centralisé des clés de chiffrement — créant un point de défaillance unique et une cible de grande valeur. Un gouvernement pourrait également contraindre l'accès par le biais d'une citation à comparaître classifiée ou d'une lettre de sécurité nationale, à votre insu. Il s'agit d'un risque sérieux en matière de souveraineté des données, qui s'ajoute à une

défense qui ne fonctionne plus.

Revision #1

Created 2026-07-24 06:55:28 UTC by Dennis Underwood

Updated 2026-07-24 06:55:28 UTC by Dennis Underwood