Les rançongiciels peuvent-ils toujours atteindre les données stockées dans des services cloud comme OneDrive ou Google Drive ?

Réponse courte : Oui. Si le stockage cloud était autrefois hors de portée des rançongiciels, les attaquants ont adapté leurs méthodes et peuvent désormais cibler les données stockées dans le cloud grâce à des techniques telles que le mappage de lecteurs et, plus couramment aujourd'hui, le vol de clés API et de jetons de session.

Comment l'approche des rançongiciels vis-à-vis des données cloud a évolué

Lorsque le travail à distance a entraîné une transition rapide vers le stockage cloud, les entreprises comme les cybercriminels se sont adaptés simultanément à ce nouvel environnement. Aux premiers stades de cette transition, les rançongiciels ne pouvaient généralement pas atteindre les fichiers stockés sur des plateformes cloud — si les données se trouvaient dans le cloud plutôt que sur un serveur local, les attaquants les laissaient généralement de côté car ils ne disposaient d'aucun accès direct à celles-ci.

Cette situation a changé lorsque les attaquants ont appris à connecter manuellement un stockage cloud, tel qu'un compte Amazon, OneDrive ou Google Drive, à un système infecté. Ils procédaient en montant le stockage cloud sous forme de lettre de lecteur local, de manière similaire à un périphérique USB apparaissant comme un lecteur distinct sur un ordinateur. Une fois monté de cette façon, les fichiers hébergés dans le cloud devenaient tout aussi exposés au chiffrement que les fichiers présents sur un disque dur local.

La menace la plus importante aujourd'hui : le vol de clés et de jetons

À mesure que l'utilisation du cloud a mûri, les tactiques des attaquants ont de nouveau évolué. Plutôt que de monter manuellement des lecteurs, beaucoup s'attaquent désormais aux clés API et aux jetons de session — des identifiants qui accordent un accès direct, au niveau applicatif, aux comptes et aux données du cloud. Obtenir l'un de ces éléments équivaut à voler un mot de passe, si ce n'est que cela offre souvent un accès plus large et plus rapide aux ressources cloud qu'un simple mot de passe volé.

Cette évolution est importante car la même rapidité et la même évolutivité qui rendent l'informatique en nuage précieuse pour les équipes informatiques légitimes sont désormais également à la disposition des attaquants. Parmi les clients de Cyber Crucible l'année dernière, plus de la moitié ont subi une tentative de vol de jeton de session cloud visant à détourner la session active d'un utilisateur, tandis que moins de 9 % ont constaté une compromission réelle de données. Cela suggère que les attaquants privilégient le vol d'identifiants et de jetons comme point d'entrée principal, le vol de données étant un objectif secondaire.

Les données stockées dans le cloud sont-elles automatiquement en sécurité ?

Le stockage cloud ne garantit pas une protection contre les rançongiciels ou le vol de données. Il modifie simplement la méthode que les attaquants doivent employer pour atteindre ces données — déplaçant le risque principal vers la compromission des identifiants et des jetons de session plutôt que vers le chiffrement direct des fichiers.

https://player.vimeo.com/video/1047006345

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

Revision #1
Created 2026-07-24 07:22:36 UTC by Dennis Underwood
Updated 2026-07-24 07:22:36 UTC by Dennis Underwood