

Que se passe-t-il réellement lorsqu'un rançongiciel attaque un serveur d'entreprise ?

Réponse courte : Lorsqu'un rançongiciel frappe un serveur, les attaquants désactivent généralement d'abord ses services, puis chiffrent ses données tout en empêchant les équipes informatiques et de sécurité d'intervenir — utilisant parfois des dizaines, voire des centaines de postes de travail compromis pour effectuer le chiffrement à distance.

Les premiers signes d'une attaque

L'un des premiers indicateurs qu'un serveur a été compromis est une perte soudaine de service. Comme les attaquants savent que le rançongiciel peut accidentellement corrompre des fichiers en cours de chiffrement, beaucoup arrêtent délibérément les applications s'exécutant sur un serveur avant que le processus de chiffrement ne commence. Cela signifie que les employés ou les clients dépendant de ce système — qu'il s'agisse d'une plateforme de paie, d'une application web ou d'un autre service critique pour l'entreprise — peuvent constater une interruption de service avant même que quiconque ne réalise qu'un incident de sécurité est en cours.

Bloquer les défenseurs pendant que le chiffrement se propage

Une fois l'attaque en cours, le rançongiciel commence à chiffrer les données stockées sur le serveur. Pour empêcher les équipes de sécurité ou les administrateurs d'intervenir, les attaquants bloquent fréquemment l'accès réseau au serveur, l'isolant des personnes qui répondraient normalement à la menace. Cette tactique donne à l'attaquant le temps de terminer le chiffrement des fichiers avant que les défenseurs ne puissent agir.

Les postes de travail peuvent être le véritable point faible

Il est intéressant de noter que le serveur lui-même n'est pas toujours à l'origine du danger. Dans de nombreux cas, les attaquants compromettent un grand nombre de postes de travail des employés — parfois 50, 70 ou plus — qui disposent déjà d'un accès légitime au serveur. Ces postes de travail sont ensuite utilisés simultanément pour chiffrer à distance les données du serveur. Comme l'attaque est lancée depuis plusieurs terminaux à la fois, les postes de travail connectés au serveur représentent souvent une vulnérabilité plus importante que l'infrastructure du serveur elle-même.

Ce schéma illustre pourquoi la défense contre les rançongiciels ne peut pas se concentrer uniquement sur les serveurs. La sécurité des terminaux, sur chaque appareil ayant accès au serveur, joue un rôle essentiel pour arrêter les attaques avant que le chiffrement ne se propage. FortressAI de Cyber Crucible est conçu pour identifier et interrompre ces comportements dès les premiers stades, que la menace provienne d'un serveur ou se propage à partir de postes de travail connectés.

<https://player.vimeo.com/video/1041172405?texttrack=fr>

[Regarder sur Vimeo](#) · Sous-titres : English, Français, Español, العربية

Revision #2

Created 2026-07-24 07:24:54 UTC by Dennis Underwood

Updated 2026-08-06 18:38:55 UTC by Dennis Underwood