Qu'est-ce qu'une attaque sans fichier (en mémoire) ?

Réponse courte : Une attaque sans fichier est une attaque qui n'écrit jamais de programme sur le disque. L'attaquant injecte du code malveillant directement dans la mémoire d'un processus légitime et fiable, et y construit sa charge utile. Comme aucun fichier n'est jamais créé, les outils de sécurité qui analysent les fichiers — y compris la plupart des EDR — n'ont rien à détecter.

Pourquoi cela déjoue les outils basés sur les fichiers

La protection traditionnelle des terminaux repose sur une hypothèse simple : un logiciel malveillant est un fichier, il faut donc inspecter les fichiers. Les techniques sans fichier suppriment entièrement le fichier de l'équation.

Dans un déploiement réel, une entreprise de services financiers utilisait trois produits EDR leaders du secteur (Microsoft, CrowdStrike et Sophos) aux côtés d'un SOC géré du Top 50. Les attaquants ont compromis un outil de surveillance à distance fiable, injecté du code dans les processus de gestion de Microsoft SQL Server, et compilé leur ransomware ainsi que leur logiciel malveillant de vol de données directement dans la mémoire du serveur. Comme rien n'a touché le disque dur, les trois EDR, le MDR et le SOC ont été entièrement aveugles. Cyber Crucible a intercepté de manière autonome près de 10 000 processus malveillants — dont 98 % sur la ferme de serveurs SQL — sans la moindre alerte de la part de la suite d'outils historique.

Comment Cyber Crucible perçoit cela

Cyber Crucible surveille le comportement et l'intention au niveau du noyau plutôt que d'analyser les fichiers. Un processus agissant de manière malveillante est arrêté en moins de 200 millisecondes, qu'un fichier ait été écrit ou non.

Revision #1
Created 2026-07-24 06:49:40 UTC by Dennis Underwood
Updated 2026-07-24 06:49:40 UTC by Dennis Underwood