Pourquoi les antivirus traditionnels ne peuvent-ils pas arrêter les attaques de ransomware zero-day et sans fichier ?

Réponse courte : Les outils de sécurité basés sur des signatures s'appuient sur la reconnaissance de schémas d'attaque connus, mais les attaquants modernes testent délibérément leurs outils contre ces mêmes défenses avant de les déployer, et évitent de plus en plus de déposer des fichiers détectables. Cette combinaison de menaces mutées et non reconnues, associée à des techniques opérant uniquement en mémoire, a rendu les méthodes de détection traditionnelles beaucoup moins fiables.

Le problème de la dépendance aux signatures connues

Les attaques zero-day sont, par définition, suffisamment nouvelles ou modifiées pour échapper à ce que les outils de sécurité existants reconnaissent déjà. Les fournisseurs promettent depuis longtemps des améliorations pour détecter ces menaces, mais les attaquants disposent d'un avantage inhérent : ils ont accès aux mêmes produits de sécurité commerciaux que ceux utilisés par les défenseurs. Avant de lancer une campagne, les attaquants testent régulièrement leurs logiciels malveillants contre les outils de détection populaires, les affinant jusqu'à ce qu'ils passent inaperçus. Cela transforme la détection en une cible mouvante constante plutôt qu'en une défense fixe.

Les techniques sans fichier compromettent la liste blanche d'applications

Les attaquants ont également cessé de déposer des exécutables malveillants évidents sur un système. Ils détournent à la place des applications légitimes et fiables, déjà approuvées par les outils de liste blanche d'applications, en exécutant des activités malveillantes via des processus que le logiciel de sécurité considère comme sûrs. Lorsque cette approche sans fichier est combinée à un code qui mute rapidement, les attaques peuvent se conclure dans une fenêtre de temps très courte — parfois en une demi-heure — bien avant qu'une équipe humaine de réponse aux incidents ne puisse réalistement mener une investigation.

Les attaquants effacent eux-mêmes leurs traces

Dans de nombreux cas, comme l'attaque réside en mémoire plutôt que sur le disque, les attaquants effacent les journaux, les preuves, voire les capteurs de sécurité avant de terminer leur opération. Cela ressemble à un cambrioleur désactivant les caméras de sécurité et les alarmes avant de commettre un délit : lorsque quelqu'un cherche des preuves, la visibilité la plus utile a déjà été détruite. Cette combinaison de méthodes d'attaque imprévisibles et de preuves autodestructrices explique pourquoi Cyber Crucible a investi des efforts considérables dans la construction d'une approche automatisée et évolutive — conçue pour capturer les données critiques nécessaires à la prise de décisions précises avant que les attaquants ne puissent effacer leurs traces, plutôt que de dépendre de la reconnaissance des menaces après coup.

https://player.vimeo.com/video/1164197533

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

Revision #1
Created 2026-07-24 07:28:13 UTC by Dennis Underwood
Updated 2026-07-24 07:28:13 UTC by Dennis Underwood