Qu'est-ce qu'une attaque en mémoire visant une DLL System32 ?

Réponse brève : Il s'agit d'une attaque qui infecte les bibliothèques de code fondamentales de Windows (les DLL System32) pendant qu'elles sont en cours d'exécution en mémoire. Comme presque toutes les applications et tous les outils de sécurité dépendent de ces bibliothèques pour fonctionner, leur compromission confère à l'attaquant un contrôle quasi total du poste de travail, avec très peu de traces.

Pourquoi il s'agit du summum de l'art offensif sur les postes de travail

Les DLL System32 fournissent les opérations fondamentales sur lesquelles s'appuient Windows et ses applications — allocation mémoire, cryptographie, réseau. Elles ont été conçues pour la rapidité et la fiabilité, jamais pour être corrigées ou instrumentées ("hookées") à la volée en production.

Un attaquant capable de les modifier en mémoire acquiert le pouvoir d'inspecter, de créer, de modifier ou de détruire des données et des programmes sur le système, avec une discrétion quasiment indétectable.

Pourquoi la plupart des outils ne peuvent pas la détecter

Les produits de sécurité qui dépendent des données de capteurs fournies par Microsoft s'appuient, par définition, sur les bibliothèques mêmes qui sont attaquées. Les capteurs nécessaires pour détecter cette catégorie d'attaque n'existent tout simplement pas dans les outils standards — l'outil devient alors muet tout en signalant que tout va bien.

Cyber Crucible a été délibérément conçu pour être indépendant des bibliothèques Windows, de sorte qu'un système d'exploitation compromis ne puisse ni l'aveugler ni le désactiver.

Revision #1
Created 2026-07-24 06:50:22 UTC by Dennis Underwood

Updated 2026-07-24 06:50:22 UTC by Dennis Underwood