

O que é um ataque em memória a DLLs do System32?

Resposta curta: Trata-se de um ataque que infecta as bibliotecas de código essenciais do Windows (DLLs do System32) enquanto estas estão em execução na memória. Como praticamente todas as aplicações e ferramentas de segurança dependem dessas bibliotecas para funcionar, comprometê-las confere a um atacante controlo quase total do endpoint, deixando muito pouco rasto.

Por que razão isto é o expoente máximo da tradecraft de endpoint

As DLLs do System32 fornecem as operações fundamentais das quais o Windows e as suas aplicações dependem — alocação de memória, criptografia, redes. Foram concebidas para velocidade e fiabilidade, nunca para serem corrigidas ou interceptadas ("hooked") em tempo real em ambiente de produção.

Um atacante que consiga alterá-las em memória obtém o poder de inspecionar, criar, alterar ou destruir dados e programas no sistema, com um nível de furtividade quase impossível de rastrear.

Por que razão a maioria das ferramentas não consegue detetá-lo

Os produtos de segurança que dependem de dados de sensores fornecidos pela Microsoft estão, por definição, a confiar precisamente nas bibliotecas que estão a ser atacadas. Os sensores necessários para detetar esta classe de ataque simplesmente não existem nos conjuntos de ferramentas padrão — pelo que a ferramenta fica silenciosa enquanto reporta que está tudo em ordem.

O Cyber Crucible foi deliberadamente concebido para ser independente das bibliotecas do Windows, de modo a que um sistema operativo comprometido não o possa cegar ou desativar.