O que é um ataque sem arquivo (em memória)?

Resposta curta: Um ataque sem arquivo é aquele que nunca grava um programa em disco. O atacante injeta código malicioso diretamente na memória de um processo legítimo e confiável e constrói sua carga maliciosa (payload) ali. Como nenhum arquivo chega a ser criado, as ferramentas de segurança que analisam arquivos — incluindo a maioria dos EDR — não têm nada a encontrar.

Por que derrota as ferramentas baseadas em arquivos

A proteção tradicional de endpoint é construída sobre uma suposição simples: malware é um arquivo, portanto inspecione arquivos. As técnicas sem arquivo eliminam completamente o arquivo.

Em uma implantação real, uma empresa de serviços financeiros utilizava três produtos EDR líderes do setor (Microsoft, CrowdStrike e Sophos) juntamente com um SOC gerenciado Top-50. Os atacantes comprometeram uma ferramenta confiável de monitoramento remoto, injetaram código nos processos de gerenciamento do Microsoft SQL Server e compilaram seu ransomware e malware de roubo de dados diretamente na memória do servidor. Como nada tocou o disco rígido, os três EDRs, o MDR e o SOC ficaram completamente cegos. O Cyber Crucible interceptou de forma autônoma quase 10.000 processos maliciosos — 98% deles na farm de servidores SQL — sem um único alerta da pilha de ferramentas legadas.

Como o Cyber Crucible enxerga isso

O Cyber Crucible observa comportamento e intenção no nível do kernel, em vez de analisar arquivos. Um processo que age de forma maliciosa é interrompido em menos de 200 milissegundos, tenha um arquivo sido gravado ou não.

Revision #1
Created 2026-07-24 05:39:38 UTC by Dennis Underwood
Updated 2026-07-24 05:39:38 UTC by Dennis Underwood