Por que vocês respondem suspendendo programas?

Os criminosos aprenderam que operar apenas em memória, utilizando técnicas como a injeção de processos, oferece uma variedade de vantagens:

1. Assumir o controle da identidade de um usuário para esse programa.
2. Evasão de verificações de gerenciamento de identidade.
3. Evasão de regras de firewall baseadas em aplicativos e listas de permissões.
4. Evasão de ferramentas de prevenção de perda de dados em servidores.
5. Eliminação de quase todas as evidências em memória quando o processo é encerrado.
6. Eliminação de quase todas as evidências em memória quando o computador é reiniciado.

Ao suspender os programas sob controle do invasor, as evidências ficam congeladas no tempo.

O invasor também fica congelado.

As evidências ficam disponíveis para ferramentas forenses como parte de um processo de investigação.

Se a organização não estiver equipada para realizar a perícia forense no momento, uma simples reinicialização por parte do invasor fará com que o sistema retorne a um estado saudável. Forçar o encerramento do programa suspenso e reiniciá-lo geralmente também produz o efeito desejado.

Revision #1
Created 2026-07-24 05:45:30 UTC by Dennis Underwood
Updated 2026-07-24 05:45:30 UTC by Dennis Underwood