Por que a proteção de dados de identidade requer acesso em nível de kernel?

Resposta curta: Porque o roubo acontece no espaço entre um programa que solicita dados de credenciais e o sistema operacional que os entrega. Apenas uma defesa que opera no kernel — abaixo dos aplicativos e bibliotecas que um invasor pode manipular — consegue ver essa solicitação, avaliar sua intenção e impedi-la a tempo.

Os três requisitos

1. Ver o acesso no momento em que ocorre. O roubo de identidade não é um arquivo que aparece no disco; é uma leitura. Ferramentas que buscam arquivos maliciosos não veem nada, porque em um infostealer moderno nada é gravado. O evento a ser detectado é a própria tentativa de acesso.

2. Decidir com rapidez suficiente. Ferramentas automatizadas podem se infiltrar, coletar dados e se autodestruir em segundos. Qualquer arquitetura que envie telemetria para um serviço em nuvem e aguarde um veredito já perdeu a corrida. A decisão precisa acontecer localmente, em milissegundos.

3. Não depender do que o invasor controla. Ferramentas de segurança que dependem de bibliotecas do sistema operacional podem ser cegadas quando um invasor compromete essas bibliotecas em memória — o agente continua em execução, mas não relata nada. O Cyber Crucible foi deliberadamente desacoplado das bibliotecas do Windows, de modo que um sistema operacional comprometido não consegue silenciá-lo.

A consequência

A operação em nível de kernel é o que permite as três coisas simultaneamente: visibilidade sobre a tentativa de acesso, uma decisão local em menos de 200 milissegundos e independência de um sistema operacional potencialmente comprometido.

É também por isso que a proteção funciona sem qualquer conectividade — em ambientes isolados (air-gapped), offline ou no mar — já que nada precisa sair do dispositivo para que uma decisão seja tomada.

Revision #1
Created 2026-07-24 05:42:58 UTC by Dennis Underwood
Updated 2026-07-24 05:42:58 UTC by Dennis Underwood