

Por que os ataques automatizados visam os mesmos locais em todos os computadores?

Resposta curta: os atacantes não sabem nada sobre o seu ambiente específico, então a automação deles é escrita para locais que existem em praticamente todas as máquinas — pastas de perfil de usuário, letras de unidade e diretórios de dados de aplicativos. Essa previsibilidade é uma fraqueza que os defensores podem explorar.

Os alvos previsíveis

- **Perfis de usuário e áreas de trabalho:** no Windows, `C:\Users\[Username]` costuma conter dados valiosos de forma confiável. Um script percorre todos os diretórios de usuário sem precisar entender o sistema.
- **Letras de unidade:** ferramentas automatizadas enumeram `C:\`, `D:\` e além para encontrar compartilhamentos de rede, unidades externas e partições montadas para criptografar.
- **Pastas de dados de aplicativos:** todo sistema operacional mantém credenciais, cookies e configurações em caminhos conhecidos — alvos privilegiados para roubo de credenciais.

Transformando a previsibilidade contra o atacante

O padrão de ataque não é ponderado; é uma varredura direta de locais bem conhecidos. A Cyber Crucible monitora exatamente esses pontos de entrada conhecidos para roubo de identidade e roubo de dados. Qualquer programa que tente acessar dados nesses locais — junto com seus processos pai e filho e bibliotecas associadas — tem sua intenção avaliada em uma fração de segundo, e é interceptado caso essa intenção seja maliciosa.