

# Testando se o Software Cyber Crucible Está "Funcionando"

## Introdução

O Cyber Crucible foi projetado para funcionar sem interromper os usuários finais ou funcionários, ao mesmo tempo em que notifica discretamente os usuários do Dashboard escolhidos (normalmente membros selecionados das equipes de TI e Segurança) sobre as respostas automatizadas.

Muitos dos simuladores de ransomware ou malware não capturam com precisão o comportamento de um hacker. Embora isso cause problemas para ferramentas como o Cyber Crucible que (corretamente) identificam a simulação como um falso positivo, isso não é necessariamente algo ruim.

Alguns fornecedores chegam a construir seus mecanismos de detecção em torno desses simuladores para parte de sua funcionalidade de detecção, para garantir que quaisquer testes de clientes sejam aprovados com louvor.

Ações reais de malware, como a criptografia de ransomware, correm o risco de criptografar ou corromper dados de forma irrecuperável. Na Cyber Crucible, já vimos até ransomware ativar secretamente outros malwares na rede, ou realizar outras ações que poderiam prejudicar a empresa que está tentando testar o Cyber Crucible.

Portanto, você não quer usar malware, e também não quer usar um simulador tão preciso a ponto de correr o risco de corromper acidentalmente seus dados.

## Testando o Cyber Crucible

Existe uma maneira fácil de testar o Cyber Crucible sem usar malware ou uma simulação tão realista que coloque em risco os dados sua empresa ou os seus.

O Cyber Crucible avalia os acessos à identidade digital a cada milissegundo do dia. Muitas dessas identidades digitais são armazenadas nos navegadores - é por isso que os atacantes colocam os navegadores web no topo da lista para seus ataques automatizados.

A análise comportamental de acesso à identidade do Cyber Crucible resultará em uma das três respostas:

1. Não fazer nada
2. Ocultar os dados
  1. aplicativo legítimo conhecido que passa em todas as verificações de memória e kernel, mas não precisa de acesso àquele dado de identidade específico - exemplo: Windows Explorer não explorado
3. Suspender o processo
  1. aplicativo legítimo conhecido que deveria ter acesso ao dado de identidade, mas foi hackeado, ou
  2. um aplicativo estranho

Aqui estão dois locais comuns para usuários do Windows:

Neste caso, o nome de usuário do Windows é "denni", e estes são os locais onde os dados de sessão são armazenados. Você pode descobrir que a variável %LOCALAPPDATA% funciona para você, caso não queira descobrir o nome de usuário.

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
  - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
  - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

## A Visualização Sem o Cyber Crucible Instalado

Vamos primeiro ver como uma dessas pastas se apresenta com o Explorer.exe, sem o Cyber Crucible instalado.

Screenshot 2025-05-14 103339.png

Aqui, vemos múltiplas Sessões do Chrome sob o perfil "default" do Google Chrome.

Essas informações normalmente contêm dados sensíveis que um atacante desejaria usar para sequestrar sessões com programas importantes, como portais de administração de TI, bancos, e-mail, ou ferramentas de armazenamento como Google Drive ou Dropbox.

## A Visualização Com o Cyber Crucible Instalado

Após instalar o Cyber Crucible, um teste rápido pode ser realizado, sem usar malware ou qualquer tipo de técnica criminosa ou uso indevido de equipamentos de TI.

Neste caso, o mesmo local de armazenamento de sessão do navegador é usado:

- C:\Users\denni\AppData\Local\Google\Chrome\User Data\Default\Sessions
  - %LOCALAPPDATA%\Google\Chrome\User Data\Default\Sessions
- C:\Users\denni\AppData\Local\Microsoft\Edge\User Data\Default\Sessions
  - %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Sessions

Screenshot 2025-05-14 103620.png

O Cyber Crucible, imediatamente após a instalação, já está bloqueando o acesso aos dados naquela pasta.

Observe que este é exatamente o mesmo processo do Explorer que já estava em execução no momento da instalação, portanto o programa em execução teve seu acesso subitamente revogado na camada do "disco rígido" ou kernel. Mesmo programas benignos, explorados ou malwares que já estejam em execução são avaliados corretamente pelo Cyber Crucible.

## Visualizando seu Teste no Dashboard do Cyber Crucible

Existe um grande número de acessos a dados de identidade em um sistema em execução, o tempo todo.

O Software as a Service e os programas baseados em nuvem resultaram em muitos sites e aplicativos que têm conteúdo limitado no próprio site, enquanto o navegador (ou navegador incorporado para aplicativos) se comunica constantemente com servidores de dados para preencher planilhas, tabelas, gráficos e conteúdo de mídia social.

## Página de Acesso à Identidade

Os acessos à identidade considerados apropriados para o Cyber Crucible suspender o aplicativo infrator são listados na página de Acesso à Identidade.

Estas são situações em que o programa que acessa os dados de identidade deve ser interrompido, e não apenas ter os dados ocultados.

Neste caso, o Explorer não foi interrompido após a infinidade de verificações que o Cyber Crucible realizou. Em vez disso, os dados foram apenas ocultados.

Screenshot 2025-05-14 103741.png

Portanto, não há violações de acesso à identidade listadas aqui.

## Página de Ocultação de Acesso à Identidade

O Cyber Crucible tem, opcionalmente, a capacidade de mostrar aos clientes do Dashboard situações em que dados de identidade foram ocultados, mas nas quais o programa que acessava os dados não foi interrompido.

O Explorer não foi explorado nem malicioso neste teste; ele estava apenas acessando dados de identidade altamente privilegiados dos navegadores Chrome e Edge.

A maioria dos usuários não tem acesso a essas informações, dada a carga adicional nas máquinas e redes dos clientes ao transmitir esses dados para os servidores do Cyber Crucible.

Por favor, solicite se desejar acesso, mas saiba que a atividade que você está vendo não é uma atividade maliciosa, mas sim comportamentos de privacidade de dados de identidade que o Cyber Crucible realiza sob uma perspectiva de GRC, ou aplicação de políticas.

[Identity Hide Explorer.mp4](#)

Aqui, vemos neste pequeno vídeo que o Explorer foi impedido de visualizar os dados de sessão do navegador, mesmo que o próprio Explorer não tenha sido interrompido.

---

Revision #1

Created 2026-07-24 05:30:06 UTC by Dennis Underwood

Updated 2026-07-24 05:30:06 UTC by Dennis Underwood