Comprobación de si el software de Cyber Crucible está "Funcionando"

Introducción

Cyber Crucible está diseñado para funcionar sin interrumpir a los usuarios finales o empleados, mientras notifica discretamente a los usuarios elegidos del Dashboard (normalmente miembros elegidos de los equipos de TI y Seguridad) sobre las respuestas automatizadas.

Muchos de los simuladores de ransomware o malware no capturan con precisión el comportamiento de un hacker. Aunque esto causa problemas para herramientas como Cyber Crucible que (correctamente) identifican la simulación como un falso positivo, eso no es necesariamente algo malo.

Algunos proveedores realmente construyen sus motores de detección en torno a estos simuladores para parte de su funcionalidad de detección, para asegurarse de que las pruebas de cualquier cliente se superen con éxito.

Las acciones de malware reales, como el cifrado por ransomware, corren el riesgo de cifrar o corromper datos de forma irrecuperable. En Cyber Crucible, incluso hemos visto que el ransomware activa en secreto otro malware en la red, o realiza otras acciones que podrían perjudicar a la empresa que intenta probar Cyber Crucible.

Por lo tanto, no querrá usar malware, ni tampoco querrá usar un simulador tan preciso que pueda dañar accidentalmente sus datos.

Probando Cyber Crucible

Existe una forma sencilla de probar Cyber Crucible sin usar malware ni una simulación tan realista que ponga en riesgo sus datos o los de su empresa.

Cyber Crucible evalúa los accesos a identidades digitales en cada milisegundo del día. Muchas de esas identidades digitales se almacenan en los navegadores, razón por la cual los atacantes

colocan los navegadores web en el primer lugar de su lista de objetivos automatizados.

El análisis de comportamiento de acceso a identidades de Cyber Crucible dará lugar a una de tres respuestas:

1. No hacer nada
2. Ocultar los datos
    1. aplicación legítima conocida que supera todas las comprobaciones de memoria y kernel, pero que no necesita acceso a esos datos de identidad en particular - ejemplo: Windows Explorer sin explotar
3. Suspender el proceso
    1. aplicación legítima conocida que debería tener acceso a los datos de identidad pero que ha sido hackeada, o
    2. una aplicación extraña

A continuación se muestran dos ubicaciones comunes para los usuarios de Windows:

En este caso, el nombre de usuario de Windows es "denni", y estas son las ubicaciones donde se almacenan los datos de sesión. Es posible que le funcione la variable %LOCALAPPDATA% si no desea averiguar el nombre de usuario.

- 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

La vista sin Cyber Crucible instalado

Veamos primero cómo se ve una de estas carpetas con Explorer.exe, sin Cyber Crucible instalado.

Screenshot 2025-05-14 103339.png
Aquí vemos múltiples sesiones de Chrome bajo el perfil "predeterminado" de Google Chrome.

Esta información normalmente contiene información sensible que un atacante querría usar para secuestrar sesiones con programas importantes como portales de administración de TI, banca, correo electrónico, o herramientas de almacenamiento como Google Drive o Dropbox.

La vista con Cyber Crucible instalado

Después de instalar Cyber Crucible, se puede realizar una prueba rápida, sin usar malware ni ningún tipo de técnica criminal o uso indebido del equipo de TI.

En este caso, se utiliza la misma ubicación de almacenamiento de sesión del navegador:

- 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
Cyber Crucible, inmediatamente después de la instalación, ya está bloqueando el acceso a los datos en esa carpeta.

Tenga en cuenta que este es exactamente el mismo proceso de Explorer que ya estaba en ejecución al momento de la instalación, por lo que al programa en ejecución de repente se le ha revocado el acceso en la capa del "disco duro" o kernel. Incluso los programas, benignos, explotados o de tipo malware que ya están en ejecución son evaluados correctamente por Cyber Crucible.

Cómo ver su prueba en el Dashboard de Cyber Crucible

Hay una gran cantidad de accesos a datos de identidad en un sistema en ejecución, en todo momento.

El software como servicio y los programas basados en la nube han dado lugar a que muchos sitios web y aplicaciones tengan una funcionalidad limitada en el propio sitio web, mientras que el navegador (o el navegador integrado en el caso de las aplicaciones) se comunica constantemente con servidores de datos para completar hojas de cálculo, tablas, gráficos y contenido de redes sociales.

Página de Acceso a Identidad

Los accesos a identidad que se consideran apropiados para que Cyber Crucible suspenda la aplicación infractora se enumeran en la página de Acceso a Identidad.

Estas son situaciones en las que el programa que accede a los datos de identidad debe detenerse, no simplemente ocultar los datos.

En este caso, Explorer no fue detenido después de la multitud de comprobaciones que realizó Cyber Crucible. En su lugar, los datos simplemente fueron ocultados.

Screenshot 2025-05-14 103741.png
Por lo tanto, no hay violaciones de acceso a identidad enumeradas aquí.

Página de Ocultación de Acceso a Identidad

Cyber Crucible tiene opcionalmente la capacidad de mostrar a los clientes del Dashboard las situaciones en las que se ocultaron datos de identidad, pero en las que el programa que accedía no fue detenido.

Explorer no fue explotado ni fue malicioso de ninguna otra forma en esta prueba, simplemente estaba accediendo a datos de identidad muy privilegiados de los navegadores Chrome y Edge.

La mayoría de los usuarios no tienen acceso a esta información dada la carga adicional en las máquinas y redes de los clientes al transmitir esos datos a los servidores de Cyber Crucible.

Por favor, pregunte si desea acceso, pero tenga en cuenta que la actividad que está viendo no es actividad maliciosa, sino comportamientos de privacidad de datos de identidad que Cyber Crucible realiza desde una perspectiva de GRC, o de cumplimiento de políticas.

Identity Hide Explorer.mp4
Aquí, vemos en este breve video, que Explorer fue bloqueado para ver los datos de sesión del navegador, aunque el propio Explorer no fue interrumpido.

Revision #1
Created 2026-07-24 01:31:56 UTC by Dennis Underwood
Updated 2026-07-24 01:31:56 UTC by Dennis Underwood