Testen, ob die Cyber Crucible-Software „funktioniert“

Einführung

Cyber Crucible wurde so konzipiert, dass es läuft, ohne Endnutzer oder Mitarbeiter zu stören, während ausgewählte Dashboard-Nutzer (typischerweise ausgewählte Mitglieder der IT- und Sicherheitsteams) im Hintergrund über automatisierte Reaktionen informiert werden.

Viele Simulatoren für Ransomware oder Malware bilden das Verhalten eines Hackers nicht genau ab. Auch wenn dies für Tools wie Cyber Crucible, die die Simulation (korrekt) als Fehlalarm erkennen, Probleme verursacht, ist das nicht unbedingt schlecht.

Manche Anbieter bauen ihre Erkennungs-Engines für einen Teil ihrer Erkennungsfunktionen sogar gezielt auf diese Simulatoren auf, um sicherzustellen, dass alle Kundentests mit Bravour bestanden werden.

Reale Malware-Aktionen wie Ransomware-Verschlüsselung bergen das Risiko, Daten unwiederbringlich zu verschlüsseln oder zu beschädigen. Bei Cyber Crucible haben wir sogar erlebt, dass Ransomware heimlich andere Malware im Netzwerk aktiviert oder andere Aktionen ausführt, die dem Unternehmen schaden könnten, das versucht, Cyber Crucible zu testen.

Sie möchten also weder Malware verwenden, noch einen Simulator, der so realistisch ist, dass Sie versehentlich Ihre Daten beschädigen könnten.

Cyber Crucible testen

Es gibt eine einfache Möglichkeit, Cyber Crucible zu testen, ohne Malware oder eine Simulation zu verwenden, die so realistisch ist, dass Sie Ihre eigenen Daten oder die Ihres Unternehmens gefährden.

Cyber Crucible bewertet jede Millisekunde des Tages Zugriffe auf digitale Identitäten. Viele dieser digitalen Identitäten werden in Browsern gespeichert – deshalb setzen Angreifer Webbrowser bei ihrem automatisierten Targeting ganz oben auf die Liste.

Die Verhaltensanalyse von Cyber Crucible bei Identitätszugriffen führt zu einer von drei Reaktionen:

1. Nichts tun
2. Daten verbergen
    1. bekannte, legitime Anwendung, die alle Speicher- und Kernel-Prüfungen besteht, aber keinen Zugriff auf diese bestimmten Identitätsdaten benötigt – Beispiel: unausgenutzter Windows Explorer
3. Prozess anhalten
    1. bekannte, legitime Anwendung, die eigentlich Zugriff auf die Identitätsdaten haben sollte, aber gehackt wurde, oder
    2. eine ungewöhnliche Anwendung

Hier sind zwei Speicherorte, die bei Windows-Nutzern häufig vorkommen:

In diesem Fall lautet der Windows-Benutzername „denni“, und dies sind die Speicherorte, an denen Sitzungsdaten abgelegt werden. Möglicherweise funktioniert für Sie die Variable %LOCALAPPDATA%, wenn Sie den Benutzernamen nicht ermitteln möchten.

- 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

Die Ansicht ohne installiertes Cyber Crucible

Sehen wir uns zunächst an, wie einer dieser Ordner mit Explorer.exe aussieht, ohne dass Cyber Crucible installiert ist.

Screenshot 2025-05-14 103339.png
Hier sehen wir mehrere Chrome-Sitzungen unter dem „Standard“-Google-Chrome-Profil.

Diese Informationen enthalten typischerweise sensible Daten, mit denen ein Angreifer Sitzungen wichtiger Programme wie IT-Administrationsportale, Banking, E-Mail oder Speicherwerkzeuge wie Google Drive oder Dropbox kapern möchte.

Die Ansicht mit installiertem Cyber Crucible

Nach der Installation von Cyber Crucible kann ein schneller Test durchgeführt werden, ohne Malware oder irgendeine Art von kriminellen Techniken oder Missbrauch der IT-Ausrüstung zu verwenden.

In diesem Fall wird derselbe Speicherort für Browser-Sitzungen verwendet:

- 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 blockiert bereits unmittelbar nach der Installation den Zugriff auf die Daten in diesem Ordner.

Bitte beachten Sie, dass es sich um genau denselben Explorer-Prozess handelt, der bereits vor der Installation lief – dem laufenden Programm wurde also plötzlich der Zugriff auf der „Festplatten“- oder Kernel-Ebene entzogen. Selbst Programme, seien sie harmlos, ausgenutzt oder Malware, die bereits laufen, werden von Cyber Crucible korrekt bewertet.

Ihren Test im Cyber Crucible Dashboard einsehen

Es gibt jederzeit eine große Anzahl von Identitätsdatenzugriffen in einem laufenden System.

Software as a Service und cloudbasierte Programme haben dazu geführt, dass viele Websites und Anwendungen auf der Website selbst nur begrenzt Funktionen bieten, während der Browser (oder der eingebettete Browser bei Anwendungen) ständig mit Datenservern kommuniziert, um Tabellen, Diagramme und Social-Media-Inhalte zu befüllen.

Seite „Identitätszugriff“

Identitätszugriffe, bei denen es als angemessen erachtet wird, dass Cyber Crucible die betreffende Anwendung anhält, werden auf der Seite „Identitätszugriff“ aufgeführt.

Dies sind Situationen, in denen das auf die Identitätsdaten zugreifende Programm gestoppt werden sollte, statt nur die Daten zu verbergen.

In diesem Fall wurde Explorer nach der Vielzahl der von Cyber Crucible durchgeführten Prüfungen nicht gestoppt. Stattdessen wurden lediglich Daten verborgen.

Screenshot 2025-05-14 103741.png

Daher sind hier keine Verstöße gegen den Identitätszugriff aufgeführt.

Seite „Identitätszugriff verborgen“

Cyber Crucible bietet optional die Möglichkeit, Dashboard-Kunden Situationen anzuzeigen, in denen Identitätsdaten verborgen wurden, das zugreifende Programm jedoch nicht gestoppt wurde.

Explorer wurde in diesem Test nicht ausgenutzt oder war anderweitig bösartig, es griff lediglich auf sehr privilegierte Identitätsdaten der Browser Chrome und Edge zu.

Die meisten Nutzer haben aufgrund der zusätzlichen Belastung der Kundenrechner und -netzwerke bei der Übertragung dieser Daten an die Cyber Crucible-Server keinen Zugriff auf diese Informationen.

Bitte fragen Sie nach, wenn Sie Zugriff wünschen. Beachten Sie jedoch, dass die von Ihnen gesehene Aktivität keine bösartige Aktivität ist, sondern ein Verhalten zum Schutz der Privatsphäre von Identitätsdaten, das Cyber Crucible aus GRC- bzw. Richtliniendurchsetzungsperspektive durchführt.

Identity Hide Explorer.mp4
Hier sehen wir in diesem kurzen Video, dass Explorer daran gehindert wurde, die Browser-Sitzungsdaten einzusehen, obwohl Explorer selbst nicht unterbrochen wurde.

Revision #1
Created 2026-07-24 04:15:10 UTC by Dennis Underwood
Updated 2026-07-24 04:15:10 UTC by Dennis Underwood