Testet Cyber Crucible erschöpfend jede mögliche Ransomware?

Cyber Crucible arbeitet auf Basis kernelseitiger Verhaltensmodellierung, um Datendiebstahl, Zugangsdatendiebstahl und Ransomware-Verschlüsselungsverhalten sehr schnell zu erkennen. Die Verhaltensentscheidungen basieren auf Informationen aus Prozessverhalten, speicherbasierten Verhaltensweisen und bestimmten dateibasierten Verhaltensweisen, um eine Entscheidung genau in dem Moment zu treffen, in dem die Erpressung unmittelbar bevorsteht.

Trotz der sehr großen Anzahl an Ransomware- und Erpressungssoftware-Beispielen lassen sich diese verhaltensbasiert in eine relativ kleine Anzahl von Kategorien einteilen.

Oberflächlich betrachtet müssen jedoch die „oberflächlichen“ Abwehrmechanismen, die von einer Vielzahl von Sicherheitstools verwendet werden, einer sehr großen Anzahl von Erpressungswerkzeugen entgegenwirken. Es ist wichtig zu verstehen, dass unsere Verhaltensanalytik viel tiefer in die Werkzeuge und Vorgehensweisen der Angreifer eindringt und dadurch die Notwendigkeit einer (unmöglichen) erschöpfenden Testung sämtlicher potenzieller Schadsoftware zu jedem Zeitpunkt drastisch reduziert.

Die Entwickler von Cyber Crucible kategorisieren die kernelseitigen Speicher-, Prozess- und Dateiverhaltensweisen eines Erpressungswerkzeugs und stellen anschließend sicher, dass es in eine der bekannten Abwehrfähigkeiten passt. Gelegentlich kann die Formel, ähnlich wie bei einem Impfstoff, leicht angepasst werden, um eine präzisere Reaktion zu erzielen.

Nur sehr selten tritt etwas völlig Neues auf.

Das Cyber-Crucible-Team arbeitet unermüdlich daran, neuartige Techniken vorbeugend aufzudecken, die in unserem Kundenstamm oder in Threat-Intelligence-Daten noch nicht beobachtet wurden.

Der Effekt?

1. Die Abwehr von Erpressungswerkzeugen durch Cyber Crucible ist gegenüber allen bekannten Ransomware-Varianten vollständig.

2. Neue Ransomware-Varianten werden blockiert, noch bevor sie die ersten Kunden erreichen. Bei den meisten Programmen, gegen die wir schützen, wissen wir etwa 120 Tage lang nicht einmal, wie sie heißen sollen, bis die Forscher „aufgeholt“ haben.

3. Entwickler von Ransomware- und Erpressungswerkzeugen rufen uns manchmal an, um herauszufinden, womit wir uns beschäftigen, in der Hoffnung, einen Ansatzpunkt zu finden. Leider scheint die Frustration über unsere Präsenz manchmal ihre Weiterentwicklung anzuspornen, wodurch andere Werkzeuge noch weniger wirksam werden.

4. Wir begrüßen die Prüfung unserer Software. Wenn Penetrationstester, Malware-Analysten oder Fachleute für Adversary Emulation in den Verkaufsprozess einsteigen, freuen wir uns sehr!

Revision #1
Created 2026-07-24 04:40:38 UTC by Dennis Underwood
Updated 2026-07-24 04:40:38 UTC by Dennis Underwood