

Bereitstellung in einer bereits infizierten Umgebung

- [Hintergrund](#)
- [Was unmittelbar nach der Installation passiert](#)
- [Was geschieht mit ruhender Malware, die auf zukünftige Aufgaben wartet?](#)
- [Zusätzliche Details – Neustarts können wertvoll sein](#)

Hintergrund

Bei Cyber Crucible-Kundenbereitstellungen werden regelmäßig zuvor unbekannte Infektionen entdeckt. Netzwerke sind normalerweise nicht infektiösfrei, selbst wenn bestehende Cybersicherheits-Tools „alles klar“ gemeldet haben.

Ein Ransomware-Angriff bietet einen deutlich sichtbaren Abgrenzungspunkt bzw. einen entscheidenden Wendepunkt, an dem ein Unternehmen messen kann, wie oft Hacker erfolgreich erneut angreifen und wie erfolgreich sie dabei sind.

- Open-Source-Berichte und Bedrohungsanalysen zeigen eine Wiederangriffsrate von etwa 80 % bei Unternehmen, die keine Cyber Crucible-Kunden sind.
- Cyber Crucible beobachtete, dass bei etwa 10 % der Endpunkte pro 90-Tage-Zeitraum mindestens ein Versuch von Identitätsdiebstahl stattfand, etwa von Passwörtern, Schlüsseln oder Tokens.
- Cyber Crucible beobachtet, dass Angreifer ungefähr monatlich versuchen, wieder Fuß in einer Umgebung zu fassen.

Aus Sicht der Vorfallreaktion (Incident Response) bzw. Forensik ist Cyber Crucible ein hervorragendes Werkzeug, um die Kontrolle über das Netzwerk zurückzugewinnen. Insbesondere bei Opfern von Angriffen gehen wir davon aus, dass die Angreifer den Wiederherstellungs- und finanziellen Status der Opfer weiterhin im Blick behalten, um den richtigen Zeitpunkt für einen erneuten Angriff besser abschätzen zu können.

Was unmittelbar nach der Installation passiert

Cyber Crucible beginnt automatisch damit, laufende Programme zu suspendieren, die sich beobachtbar böse verhalten.

Der Rollout des Cyber Crucible-Produkts kann dazu führen, dass mehrere Programme auf mehreren Rechnern suspendiert werden, während die Umgebung bereinigt wird.

Mitunter kann ein teilweiser Rollout von Cyber Crucible dazu führen, dass der Hacker versucht, über die Rechner ohne Cyber Crucible-Schutz wieder Kontrolle zu erlangen.

So wurde Cyber Crucible beispielsweise bei einem kürzlichen Opfer einer Datenpanne nur auf einem Teil der Desktop-Rechner installiert. Die Hacker versuchten, Cyber Crucible zu deinstallieren, indem sie sich von den ungeschützten Rechnern aus verbanden, und begannen schließlich, die geschützten Rechner abzuschalten.

Was geschieht mit ruhender Malware, die auf zukünftige Aufgaben wartet?

Malware, die nicht im Auftrag von Angreifern aktiv wird, wird ausgelöst, sobald sie beginnt, auf Daten zuzugreifen.

Gehen wir ein Szenario durch:

Zwei Rechner sind mit Malware infiziert. Nennen wir sie Rechner A und Rechner B.

Beide Malware-Proben sind derzeit von Ihren bevorzugten Sicherheitstools nicht erkennbar.

Die Malware auf Rechner A tut nichts, sondern wartet auf Anweisungen. Cyber Crucible erkennt die Malware nicht. Die Malware ist auch von anderen Sicherheitstools noch nicht erkennbar.

Die Malware auf Rechner B versucht, auf Daten oder Identitätsdaten zuzugreifen. Unmittelbar nach einem erfolgreichen Angriff besteht das häufigste Verhalten, das wir beobachten, wenn Angreifer ihre Malware beauftragen, darin, sicherzustellen, dass sie über aktuelle Identitätsdaten wie Passwörter oder Tokens verfügen, sowie neue Daten zu erfassen. Also teils „die neuen Passwörter beschaffen, nachdem die Administratoren die Passwörter zurückgesetzt haben“ und teils „im Blick

behalten, ob es neue Daten gibt“.

Auf Rechner B suspendiert Cyber Crucible die Anwendung sofort.

Nach einem Zeitraum von einem Monat bis zu einem Jahr wird die Malware auf Rechner A entdeckt, nachdem genügend Opfer die Malware an Sicherheitsanbieter-Datenbanken gemeldet haben. Je disziplinierter die Angreifer bei der Verbreitung dieser Probe vorgehen, desto länger bleibt diese bestimmte Malware unentdeckt.

Die Malware auf Rechner B wurde neutralisiert und ist eingefroren.

Die Malware auf Rechner A sitzt in der Falle. In dem Moment (genauer: nach 100 Millisekunden), in dem sie versucht, auf Daten oder Identitätsinformationen zuzugreifen, wird die Malware auf Rechner A suspendiert. Der Kunde ist geschützt, selbst wenn die Malware Tage bis Jahre existiert, ohne von anderen Tools erkannt zu werden.

Zusätzliche Details – Neustarts können wertvoll sein

Einige unserer Analysen sind am genauesten, wenn der Lebenszyklus eines Prozesses vom Start der Anwendung bis zum aktuellen Zustand nachverfolgt werden kann.

Ein Neustart des Rechners nach der Installation kann von Vorteil sein.

Programme, die bereits vor der Installation liefen, werden von Cyber Crucible nicht vollständig analytisch überprüft. Ein Neustart erzwingt, dass diese Programme neu starten, wodurch eine vollständige Überprüfung aller Programme ermöglicht wird.

Revision #1

Created 2026-07-24 04:13:47 UTC by Dennis Underwood

Updated 2026-07-24 04:13:48 UTC by Dennis Underwood