

Wie Cyber Crucible im Vergleich abschneidet

Klare Antworten auf die Vergleichs- und Bewertungsfragen von Käufern – im Vergleich zu EDR, XDR, MDR, Antivirus, DLP und Backup-basierter Wiederherstellung.

- [Ist Cyber Crucible ein EDR, XDR, MDR? Oder etwas anderes wie Agentic AI?](#)
- [Handelt es sich hierbei um ein Überwachungstool wie meine anderen Sicherheits-Dashboards?](#)
- [Kann Cyber Crucible mit anderen Sicherheitsprodukten koexistieren?](#)
- [Was passiert, wenn eines meiner Sicherheitsprodukte einen Konflikt mit Cyber Crucible hat?](#)
- [Wie unterscheidet sich Cyber Crucible von EDR, XDR und MDR?](#)
- [Ersetzt Cyber Crucible meine EDR-Lösung, oder arbeitet es parallel dazu?](#)
- [Ist Cyber Crucible ein Antivirenprogramm?](#)
- [Warum reichen Backup und Wiederherstellung nicht aus, um mit Ransomware umzugehen?](#)
- [Warum ist das Abfangen von Ransomware-Verschlüsselungsschlüsseln keine gültige Verteidigung mehr?](#)
- [Warum haben Sicherheitstools mit „Cloud-Collector“ Schwierigkeiten bei modernen Angriffen?](#)
- [Verlangsamt Cyber Crucible meine Systeme?](#)

Ist Cyber Crucible ein EDR, XDR, MDR? Oder etwas anderes wie Agentic AI?

Kurze Antwort: Es weist Elemente sowohl von EDR als auch von XDR auf, aber die Frage nach der Kategorie ist die falsche. Entscheidend ist, *wo die Entscheidung getroffen wird*. Die Reaktionslogik von Cyber Crucible läuft vollständig auf dem Endpunkt und nutzt ausschließlich die dort im Moment des Angriffs verfügbaren Informationen — denn entfernte Analyseserver bringen zwei fatale Schwächen mit sich: Latenz und Anfälligkeit.

Die ehrliche Antwort auf die Frage nach der Bezeichnung

- **Als EDR:** Wenn ein EDR Endpunkt-Telemetrie nutzt, um Entscheidungen zu treffen, dann ist die automatisierte Reaktion von Cyber Crucible ein EDR. Es unterbindet Erpressungsverhalten in Millisekunden, allein anhand lokaler Informationen.
- **Als XDR:** Telemetriedaten werden auch an eine Datenbank (Kunden-Appliance oder zentral) gesendet, für Korrelation, Threat Hunting, Insider-Threat-Arbeit und IT-Audits. Nach der Marketingdefinition von XDR erfüllt dies die Kriterien.

Das Team ist mit der Bezeichnung „EDR zur Erpressungsabwehr“ einverstanden, auch wenn Edge Computing in manchen Kreisen als Technologie der vorletzten Generation angesehen wird. Die folgende Argumentation zeigt, warum diese Sichtweise rückständig ist.

Warum entfernte Analytik zu einem Risiko wurde — Latenz

Das „X“ in XDR steht dafür, Analyserechenleistung auf entfernte Server zu verlagern. Das bringt Rechenleistung, kostet aber Zeit — und Angreifer haben ihr Vorgehen genau auf diese Lücke ausgerichtet:

- **Geschwindigkeit:** Angriffe wurden beschleunigt, sodass irreversible Aktionen abgeschlossen sind, bevor ein Analyseserver reagieren kann. Dies zeigt sich besonders deutlich bei kleinen, hochwertigen Objekten wie Passwörtern.

- **Parallelität:** Viele Endpunkt-Tools prüfen ein Programm, warten, und gehen dann zum nächsten über. Angreifer führen mehrere Erpressungsprogramme gleichzeitig aus — 5.000 Dateien werden parallel statt 500 nacheinander angegriffen.
- **Verteilung:** Erpressungsangriffe laufen gleichzeitig auf vielen Maschinen ab. Cyber Crucible hat bereits rund 75 Maschinen gleichzeitig beobachtet. Ein Tool steht dann vor 50 Programmen auf 75 Maschinen — 3.750 zu prüfenden Programmen.
- **Steuerungsprozesse:** Manche Angreifer betreiben einen lokalen Controller, der jedes beendete Erpressungstool sofort neu startet.

Detection-and-Response-Strategien warten naturgemäß, bis der Angriff bereits im Gange ist. Der treffendere Vergleich ist, Bankräuber an der Tür zu stoppen, statt erst zu reagieren, wenn bereits eine bestimmte Menge Bargeld aus dem Tresor verschwunden ist.

Warum entfernte Analytik zu einem Risiko wurde — Anfälligkeit

Rund 80 % der EDR- und XDR-Lösungen benötigen Zugriff auf entfernte Analyseserver, um optimal zu funktionieren, und sind ohne dieses Cloud-„Gehirn“ kaum funktionsfähig.

Angreifer nutzen dies gezielt aus: Verschaffen sie sich ausreichend Zugriff, um Firewall-Regeln zu ändern und das Endpunkt-Tool daran zu hindern, seine Analyseserver zu erreichen, verliert das Tool seine Fähigkeit zur Analyse und Reaktion. Es bleibt unangetastet, installiert, aktiv — und nahezu vollständig wirkungslos.

Was Cyber Crucible stattdessen tut

Da Latenz und Anfälligkeit eine Cloud-Abhängigkeit für die Erpressungsabwehr untragbar machen, hat Cyber Crucible eine Erkennungs- und Reaktionsfunktion entwickelt, deren Verhaltensanalytik **ausschließlich Informationen nutzt, die zum Zeitpunkt des Angriffs auf dem Endpunkt verfügbar sind**. Die Unterbindung erfolgt lokal, typischerweise in unter 200 Millisekunden, ohne Cloud-Kommunikation im kritischen Ablaufpfad.

Die Telemetriedaten, die dennoch an die Datenbank übermittelt werden, dienen der Untersuchung und nicht dem Schutz — Threat Hunting, Insider-Threat-Erkennung, IT-Audits — und eine offene API ermöglicht die Einspeisung in offene XDR-Plattformen, SOAR- oder RPA-Tools. Diese Arbeit ist wertvoll, steht aber niemals zwischen Ihnen und einem laufenden Angriff.

Handelt es sich hierbei um ein Überwachungstool wie meine anderen Sicherheits-Dashboards?

Die Antwort lautet: Es kommt darauf an, wie Sie und Ihr Unternehmen das Tool nutzen möchten, aber wahrscheinlich „nein“.

Es ist wichtig, die Produktdesign-Strategien von Cyber Crucible zu beachten:

1. Der Schutz sollte hochgradig automatisiert sein und weder ständige Pflege und Zuwendung (Alarmbeachtung) noch Feinjustierung (Konfiguration) durch die Benutzer erfordern.
2. Für ressourcenstärkere Sicherheitsteams sollte die wertvolle Telemetrie für fortgeschrittene Bedrohungsjagd-Aktivitäten oder zur Unterstützung von Forensik- und Incident-Response-Aktivitäten verfügbar sein.
3. Maßnahme Nr. 2 oben sollte den bestehenden Schutz gemäß Maßnahme Nr. 1 in keiner Weise beeinträchtigen.

Die häufigste Rückmeldung, die wir von der IT-Leitung erhalten, ist, dass ihre Mitarbeiter nicht wussten, dass Cyber Crucible sie bereits seit Wochen schützt.

Wir haben viele Benutzer, die das Tool auf drei Arten nutzen:

Einrichten und Vergessen (Wie Ihre Rauchmelder)

Vielen Organisationen fehlen die Ressourcen, um Threat Hunter die Telemetriedaten von Cyber Crucible (oder anderen Tools) durchforsten zu lassen, aber sie möchten das Risiko von Datenerpressung „von ihrem Teller haben“. Das ist völlig in Ordnung, und genau dafür ist Cyber Crucibles Data Extortion Prevention konzipiert.

Diesen Benutzern fehlen die Ressourcen, um Zeit mit der Betrachtung der Datenfeeds zu Process Injection, Credential Protection und Process Creation zu verbringen.

Daher stellen wir fest, dass sie sich, sofern sie nicht auf eine seltene automatisierte Reaktion von Cyber Crucible reagieren oder eine Bestandsverwaltung durchführen, etwa wenn auf einem neuen Rechner Cyber Crucible bereitgestellt werden muss...

...einfach nicht im Cyber Crucible Webportal anmelden und die Automatisierung ihre Arbeit machen lassen.

Das ist völlig in Ordnung!

Fortgeschrittene Bedrohungsjagd + automatisierter Schutz

Die Funktionen [Process Injection](#), Überwachung der Anmeldedatennutzung und [Process Creation](#) liefern einen umfangreichen Datensatz, der über verhaltensbasierte Analysen auf Kernel-Ebene erfasst wird, um Bedrohungsjagd durchzuführen.

Der automatisierte Schutz greift, sobald Datendiebstahl, Diebstahl von Anmeldedaten (Token, Passwort) oder Ransomware-Verschlüsselung beginnt. Für alles andere ist dies eine hervorragende Ressource.

Der häufigste Befund bisher sind nicht verwaltete (zumindest von den aktuellen IT-Administratoren) Remote-Management-Tools, die von Benutzern installiert wurden. Ja, dies führt manchmal zu einem automatisierten Erpressungsschutz (d. h., das nicht verwaltete RMM wird von einem böswilligen Akteur genutzt), aber es ist immer besser, im Voraus mehr über Ihre Umgebung zu wissen, unabhängig davon!

Hier ist ein kurzes Video zu einer Angriffsart, die wir bei Angreifern in mehreren Kundenumgebungen beobachtet haben und die erfolgreich zur Umgehung der EDR-Lösungen der Kunden eingesetzt wurde (wir nennen ungern Namen ... es waren 3 Produkte in vier Unternehmen).

[rr-com-dll.mp4](#)

Forensische Analyse und Behebung nach einem Vorfall

Es gibt mehrere Anwendungsfälle für Cyber Crucible-Daten.

Der erste besteht darin, dass eine Sicherheits- oder IT-Fachkraft im Unternehmen die Grundursache für die Beendigung eines Programms untersuchen kann. Bei einigen Kunden, die unsere Software typischerweise installieren und sich dann erst wieder anmelden, wenn neue Mitarbeiter eingearbeitet werden müssen, wurde noch nie eine Cyber-Crucible-Funktion außer der Seite „Manage Agents“ genutzt. Wir helfen ihnen gerne dabei, die [Ursachenanalyse \(Root Cause Analysis\)](#) kennenzulernen – die für technisch versierte und halbtechnische Benutzer schmerzlos und einfach ist.

Die zweite Art von Kunden für die forensische Analyse nach einem Vorfall sind DFIR-Firmen, die zur Untersuchung eines Problems bei einem Kunden hinzugezogen werden, manchmal auf Anfrage der Cyber-Versicherung, und bei denen Cyber Crucible erst nach einem Vorfall installiert wird. (Nun, wir können nicht immer vor dem Angreifer da sein, so sehr wir das auch wollen ... sonst hätte jedes Unternehmen der Welt uns bereits, und Erpressung wäre Geschichte!)

Die beste Beschreibung für eine Einführung nach einem Erpressungsangriff ist „chaotisch“. Nicht weil wir schwer zu installieren sind oder schwer mit dem Schutz beginnen können. Ganz im Gegenteil! In diesem Fall haben sich die Angreifer normalerweise bereits im System bewegt und sind in Betriebssysteme, Netzwerkgeräte, Active Directory eingebettet und arbeiten im Speicher. Bei mehreren Rechnern werden Prozesse beendet, und manchmal versuchen die Angreifer sogar, die Kontrolle zurückzugewinnen. Es ist ein wenig so, als würde man ein Medikament einnehmen, das einen zu Beginn krank macht, das man aber braucht, um wieder gesund zu werden.

Kunden, die bereits gestresst sind, reagieren manchmal emotional auf „mehr“ Lärm, wenn die Angreifer endlich aufgespürt und besiegt werden. Es ist viel Aufklärungsarbeit nötig, warum oder wie ihre bestehenden Sicherheitslösungen die Angreifer nicht gefunden haben. Am Ende gewinnt das Unternehmen jedoch wieder die Kontrolle über seine IT-Infrastruktur zurück. Sie werden nicht zu den 80–90 % der Unternehmen gehören, die ein oder zwei Jahre später erneut erpresst werden – in dem, was wir „die Erpressungs-Abo-Wirtschaft“ nennen.

Die dritte Art von Kunden, die wir haben, ist ein MSSP, der oft ein Partner von Cyber Crucible ist und auf einen automatisierten Schutz von Cyber Crucible reagiert. Sie müssen herausfinden, wie der Angreifer einen vorübergehenden Zugang erlangt hat, und alle Sicherheitslücken schließen. Die gute Nachricht ist, dass HIPAA- oder andere Compliance-Berichte aufgrund der Geschwindigkeit der automatisierten Reaktion typischerweise nur wenig oder gar keine Vertraulichkeitsverletzung ausweisen. Oft berichtet der MSSP „nichts zu melden“, was alle Beteiligten freut. Nun, außer den Kriminellen.

Kann Cyber Crucible mit anderen Sicherheitsprodukten koexistieren?

Ja!

Cyber Crucible ist derzeit im Einsatz und koexistiert mit jedem Sicherheitsanbieter im Gartner Magic Quadrant.

Unsere Software erkennt automatisch die Aktivitäten anderer Sicherheitstools und konfiguriert sich entsprechend, um diese zu berücksichtigen.

Im seltenen Fall eines potenziellen Konflikts finden Sie weitere Informationen in [diesem Knowledgebase-Artikel](#).

Was passiert, wenn eines meiner Sicherheitsprodukte einen Konflikt mit Cyber Crucible hat?

Cyber Crucible koexistiert derzeit mit jedem bedeutenden Sicherheitsanbieter, wenn wir Gartner's Magic-Quadrant-Berichte als Maßstab für die etablierten Anbieter der Branche heranziehen.

Die Endpoint-Software von Cyber Crucible ist nachweislich widerstandsfähiger als andere Software, einschließlich anderer Endpoint-Sicherheitstools. Zudem verfügt die andere Sicherheitssoftware in der Regel nicht einmal über vollständige Einsicht in die Software von Cyber Crucible.

Ein anderes Sicherheitstool versucht, Cyber Crucible abzuschalten

Zusammenfassung:

Das andere Tool versucht, einen Teil von Cyber Crucible abzuschalten. Das gelingt ihm nicht. Das Tool des anderen Anbieters wurde nicht darauf getestet, was passiert, wenn ein anderes Tool (also Cyber Crucible) sagt: „Nein, ich schalte mich nicht ab.“ Das andere Tool stürzt ab oder gerät in einen Fehlerzustand.

Die Reaktion von Cyber Crucible:

Die Reaktion kann zweigeteilt sein. Zunächst wird die Cyber Crucible-Software beim anderen Anbieter auf die Whitelist gesetzt. Dies führt dazu, dass das andere Tool die Cyber Crucible-Software ignoriert, was (hoffentlich) verhindert, dass das andere Tool in einen Fehlerzustand gerät.

Sollte das nicht funktionieren, liegt es an unserem Team, eine Lösung zu finden. Wir haben festgestellt, dass andere Anbieter deutlich langsamer (mehrere Monate oder gar nicht) reagieren, um einen Fehler auf ihrer Seite zu beheben.

In den wenigen Fällen, in denen dies historisch aufgetreten ist, haben wir im Wesentlichen eine Umgebung geschaffen, in der das andere Tool glaubt, erfolgreich gewesen zu sein. Eine nicht-technische Analogie wäre, ein jüngeres Familienmitglied oder Kind beim Dame-Spiel gewinnen zu lassen.

Ein anderes Sicherheitstool versucht, Code als Cyber Crucible auszuführen

Zusammenfassung:

Dies kommt sehr selten vor, aber es gab Fälle, in denen ein Sicherheitstool versucht hat, seinen Code in das laufende Programm von Cyber Crucible einzuschleusen und Code auszuführen, der sich als wir ausgibt.

Dies unterscheidet sich nicht davon, dass sich ein Hacker als Sicherheitstool ausgibt, und es gibt keine Möglichkeit zu unterscheiden, ob ein Hacker die Kontrolle über das „vertrauenswürdige“ Sicherheitsprogramm (oder ein anderes Programm) übernommen hat.

Die Reaktion von Cyber Crucible:

Es gibt kein Szenario, in dem Cyber Crucible zulässt, dass ein anderes Unternehmen (oder ein Hacker) Code ausführt, der sich als unser Produkt ausgibt. Die einzige Lösung wäre in diesem Fall, die Cyber Crucible-Software beim Tool des anderen Anbieters auf die Whitelist zu setzen. Cyber Crucible kann keine Abhilfemaßnahme bereitstellen, um zu verhindern, dass das andere Tool dieses Verhalten versucht.

Glücklicherweise handelt es sich hierbei um ein sehr seltenes Ereignis.

Cyber Crucible wird von einem anderen Tool deaktiviert

Es gab verschiedene Fälle, in denen Sicherheitstools mit weitreichenden Zugriffsrechten wiederholt versuchten, die Cyber Crucible-Software zu deaktivieren. Dies umfasste wiederholte Versuche, unseren Treiber zu entfernen oder unseren Dienst immer wieder zu beenden.

Auch wenn diese Probleme nie die Abwehr von Erpressung beeinträchtigt haben, wirkten sie sich negativ auf die Benutzererfahrung und die Systemleistung aus.

All dies gehört der Vergangenheit an.

Wenn ein anderes Tool - berechtigt oder nicht - in der Lage ist, Cyber Crucible zu stören, dann könnte dies auch ein Hacker.

Wenn Sie vermuten oder beobachten, dass die Cyber Crucible-Software in irgendeiner Weise beeinträchtigt ist, unabhängig davon, welche Software dies verursacht hat, kontaktieren Sie uns bitte umgehend.

Wir sind in der Regel das letzte verbleibende Tool zwischen einem Erpresser und Ihren kritischen Daten. In dieser Situation ist kein Raum für Schwäche.

Wie unterscheidet sich Cyber Crucible von EDR, XDR und MDR?

Kurze Antwort: EDR, XDR und MDR sind Erkennungs- und Reaktionswerkzeuge: Sie beobachten einen Angriff, erzeugen eine Warnung und verlassen sich auf einen Menschen oder einen Cloud-Dienst, um zu entscheiden, was zu tun ist. Cyber Crucible ist ein Präventionswerkzeug: Es entscheidet autonom auf dem Endpunkt und stoppt den bösartigen Prozess in unter 200 Millisekunden, bevor Schaden entsteht.

Die praktischen Unterschiede

	EDR / XDR / MDR	Cyber Crucible
Reaktionszeit	Minuten bis Stunden	Unter 200 Millisekunden
Erkennungsmethode	Signaturen und historische Daten	Verhaltensbasierte Absicht, keine Signaturen
Zero-Day-Abdeckung	Teilweise	Für unbekannte Bedrohungen konzipiert
Abhängigkeit von Menschen	Hoch — Analysten und SOCs	Keine — vollständig autonom
Wo Entscheidungen getroffen werden	Cloud-Analysen	Lokal, im Kernel

Warum diese Lücke wichtig ist

Erkennungstools wurden für eine Zeit entwickelt, in der sich Angriffe über Stunden oder Tage erstreckten. Automatisierte Angriffe laufen heute in Sekunden ab. Ein Tool, das eine präzise Warnung erzeugt, nachdem die Daten bereits exfiltriert wurden, hat den Verlust dokumentiert, nicht verhindert.

Das bedeutet nicht, dass Erkennung keinen Wert hat — Forensik und Untersuchungen sind wichtig. Es bedeutet vielmehr, dass Erkennung allein einen Angriff in Maschinengeschwindigkeit nicht stoppen kann.

Ersetzt Cyber Crucible meine EDR-Lösung, oder arbeitet es parallel dazu?

Kurze Antwort: Beides ist möglich. Cyber Crucible wurde so konzipiert, dass es parallel zu bestehenden EDR-, XDR- und MDR-Tools läuft, ohne Konflikte zu verursachen, und viele Kunden setzen es genau so ein. Es funktioniert aber auch als eigenständige Präventionsebene, falls Sie sich entscheiden, Ihren Tool-Stack zu reduzieren.

Paralleler Betrieb mit Ihrem aktuellen Stack

Cyber Crucible erfordert nicht, dass Sie etwas entfernen. Es fügt eine autonome Präventionsebene unterhalb der bereits vorhandenen Erkennungsschicht hinzu und funktioniert sowohl mit als auch ohne vorhandene EDR- und MDR-Lösungen.

Kunden beginnen häufig bewusst auf diese Weise – sie setzen Cyber Crucible ein, um herauszufinden, was ihrem bestehenden Stack entgeht. Bei einer Implementierung im Finanzdienstleistungssektor kam die Antwort innerhalb von 60 Tagen: fast 10.000 bösartige Prozesse wurden abgefangen, auf die drei EDR-Lösungen und ein ausgelagertes SOC nie hingewiesen hatten.

Reduzierung des Stacks

Sobald Teams sehen, wie oft ihre Erkennungstools nicht greifen, entscheiden sich manche für eine Konsolidierung. Es gibt keine Anbieterbindung und keine erzwungenen Integrationen – Sie können Ihre EDR-Lösung vollständig ersetzen oder einfach dort Kosten einsparen, wo sie sich nicht auszahlt.

Ist Cyber Crucible ein Antivirenprogramm?

Kurze Antwort: Nein. Antivirensoftware identifiziert bekannte bösartige Dateien anhand von Signaturen. Cyber Crucible verwendet überhaupt keine Signaturen – es bewertet, was ein laufendes Programm tatsächlich tut, und stoppt bösartiges Verhalten, einschließlich Bedrohungen, die noch niemand zuvor gesehen hat.

Warum Signaturen nicht mehr ausreichen

Eine Signatur kann nur einen Angriff beschreiben, den jemand bereits analysiert hat. Dieses Modell versagt in zwei häufigen Situationen:

- **Zero-Day-Angriffe**, für die noch keine Signatur existiert.
- **Dateilose Angriffe**, bei denen es keine Datei gibt, mit der eine Signatur abgeglichen werden könnte.

Signaturbasierte Erkennung erfordert außerdem eine ständige Aktualisierung durch Threat-Intelligence-Feeds, was bedeutet, dass Ihr Schutz dem Angreifer immer einen Schritt hinterherhinkt.

Was diesen Ansatz ersetzt

Cyber Crucible modelliert Verhalten – Speicheraktivität, Prozessaktivität und Dateizugriffe – und bewertet Absicht in Echtzeit. Deshalb hat es Zero-Day-Angriffe in Kundennetzwerken bis zu 90 Tage gestoppt, bevor irgendein anderer Anbieter öffentlich darüber berichtet oder darauf reagiert hat.

Warum reichen Backup und Wiederherstellung nicht aus, um mit Ransomware umzugehen?

Kurze Antwort: Backups adressieren nur die letzte Phase eines Ransomware-Angriffs – die Verschlüsselung. Wenn die Verschlüsselung beginnt, haben Angreifer in der Regel bereits Zugangsdaten gestohlen und Ihre Daten exfiltriert. Die Wiederherstellung aus einem Backup stellt Ihre Dateien wieder her; sie ändert jedoch nichts an den Daten, die sich bereits in den Händen des Angreifers befinden.

Ransomware ist der letzte Schritt, nicht der erste

Ein typischer Angriff läuft in drei Phasen ab:

1. **Identitätsdiebstahl** – Zugangsdaten werden kompromittiert, um Zugriff zu erlangen.
2. **Datendiebstahl** – geistiges Eigentum, Kundendaten und andere sensible Informationen werden exfiltriert.
3. **Verschlüsselung** – Dateien werden gesperrt und ein Lösegeld gefordert.

Wiederherstellungsstrategien setzen erst in Phase drei an. Die Vertraulichkeitsverletzung und der Verlust der operativen Kontrolle haben zu diesem Zeitpunkt bereits stattgefunden.

Die tatsächlichen Kosten

Das größte geschäftliche Risiko durch Ransomware ist in der Regel nicht das Lösegeld selbst – es sind die Umsatzeinbußen durch einen längeren Ausfall sowie der daraus resultierende Reputationsschaden. Die Verhinderung der initialen Kompromittierung schützt vor beidem. Deshalb muss Prävention vor der Planung der Wiederherstellung stehen, nicht als Ersatz dafür.

Warum ist das Abfangen von Ransomware-Verschlüsselungsschlüsseln keine gültige Verteidigung mehr?

Kurze Antwort: Das Abfangen von Schlüsseln war ab 2021 technisch nicht mehr zuverlässig. Moderne Ransomware umgeht die Standard-Verschlüsselungsbibliotheken des Betriebssystems, sodass es keine Schlüssel gibt, die ein Verteidigungstool abfangen könnte — und selbst wenn Schlüssel erlangt werden, lassen sie sich oft nicht anwenden.

Wie moderne Ransomware das Abfangen von Schlüsseln umgeht

- **Benutzerdefinierte Bibliotheken:** Der Verschlüsselungscode wird direkt in die Malware kompiliert, anstatt Betriebssystembibliotheken aufzurufen, sodass Schlüssel vollständig innerhalb des Prozesses des Angreifers erzeugt und verwendet werden — unsichtbar für Tools, die Standardaufrufe überwachen.
- **Einzigartige Implementierungen:** Manche Varianten verwenden nicht standardisierte, pro Ausführung unterschiedliche Verschlüsselung. Selbst ein abgefangener Schlüssel lässt sich nicht anwenden, da der Algorithmus selbst maßgeschneidert ist.
- **Streaming-Chiffren:** Diese basieren auf einem grundlegend anderen Konzept als AES und sind gegenüber dem Abfangen von AES-Schlüsseln schlicht immun.

Cyber Crucible hat die Technologie zum Abfangen von Schlüsseln ursprünglich entwickelt und patentiert und anschließend die Kryptoanalyse, die ihre Grenzen aufzeigt, 2021 auf der BSides Pittsburgh vorgestellt. Wir sind weitergezogen, weil die Beweislage dies nahelegte.

Auch ein Compliance-Problem

Das Abfangen von Schlüsseln erfordert die zentrale Speicherung von Verschlüsselungsschlüsseln — dies schafft einen Single Point of Failure und ein besonders lohnendes Angriffsziel. Eine Regierung könnte zudem Zugriff durch eine geheime Vorladung oder ein Schreiben zur nationalen Sicherheit erzwingen, ohne dass Sie davon Kenntnis erhalten. Das ist ein erhebliches Risiko für die

Datenhoheit — zusätzlich zu einer Verteidigung, die ohnehin nicht mehr funktioniert.

Warum haben Sicherheitstools mit „Cloud-Collector“ Schwierigkeiten bei modernen Angriffen?

Kurze Antwort: Ein Cloud-Collector ist ein schlanker Endpoint-Agent, der kaum lokale Analysen durchführt und stattdessen rohe Telemetriedaten zur Verarbeitung an eine Cloud-Plattform sendet. Dieser Umweg verursacht eine Verzögerung, die ein automatisierter Angriff nicht zulässt, und der Agent ist zudem von genau den Betriebssystemkomponenten abhängig, die Angreifer heute kompromittieren.

Warum die Branche es so aufgebaut hat

Kernel-Level-Engineering ist schwierig und teuer. Das Versenden von Telemetriedaten in die Cloud erlaubte es Anbietern, günstigere Endpoint-Software zu entwickeln, Cloud-Speicher zu monetarisieren und „Cloud-KI“-Funktionen zu vermarkten. Das Modell wurde auf einfache Entwicklung optimiert, nicht auf Verteidigung.

Die beiden Fehlermodi

1. **Zu langsam.** Automatisierte „Smash-and-Grab“-Angriffe sind innerhalb von Millisekunden abgeschlossen. Cloud-Analysen können in dieser Zeit keine Reaktion auslösen.
2. **Blind, wenn es am wichtigsten ist.** Da diese Agenten zum Funktionieren und zur Datenerfassung auf native Betriebssystembibliotheken angewiesen sind, kann ein Angreifer, der diese Bibliotheken kompromittiert, den Agenten zum Schweigen bringen. Er läuft weiter, meldet aber nichts – ein Dashboard, das signalisiert, alles sei in Ordnung, während Daten abfließen.

Cyber Crucible verarbeitet lokal im Kernel und trifft eigene Entscheidungen, sodass kein Umweg über die Cloud nötig ist und keine Abhängigkeit von einem möglicherweise kompromittierten Betriebssystem besteht.

Verlangsamt Cyber Crucible meine Systeme?

Kurze Antwort: Nein. Die typische CPU-Auslastung liegt bei rund 1 % oder darunter, und die Architektur vermeidet bewusst die Technik, die bei den meisten Endpoint-Agenten für Verlangsamungen sorgt – das Einfügen von Hooks in Windows-Systembibliotheken.

Warum andere Agenten zu Verzögerungen führen

Herkömmliche Sicherheitstools fügen „Hooks“ in hochgradig optimierte Systembibliotheken ein, um schädliches Verhalten zu überwachen. Diese Bibliotheken wurden nie dafür entwickelt, zur Laufzeit verändert zu werden. Wenn ein Sicherheitstool und ein Angreifer gleichzeitig daran manipulieren, führt dies zu einer erheblichen Beeinträchtigung der Systemleistung.

Das darauffolgende Muster ist vorhersehbar: Der Anwender macht das Sicherheitstool für die Verlangsamung verantwortlich und entfernt es. Der Hersteller kann das Problem im Labor nicht reproduzieren, ohne zu wissen, dass ein Angreifer mit Root-Rechten das System manipuliert. Angreifer haben gelernt, dies gezielt auszunutzen – indem sie die Leistung so lange beeinträchtigen, bis Opfer ihre eigenen Schutzmaßnahmen deaktivieren.

Ein anderer Ansatz

Cyber Crucible arbeitet über unabhängige Subsysteme innerhalb des Kernels, anstatt anfällige Windows-Komponenten zu hooken. Dadurch konkurriert es weder mit dem Betriebssystem noch mit einem Angreifer um dieselben störanfälligen Codepfade.