

Warum ist Anmeldedaten- und Identitätsdiebstahl gefährlicher als Ransomware-Verschlüsselung?

Kurze Antwort: Ransomware-Verschlüsselung ist der sichtbare, letzte Schritt eines Angriffs, aber der eigentliche Schaden entsteht oft schon früher und bleibt unbemerkt, wenn Angreifer automatisiert Passwörter, Sitzungstoken, Schlüssel und Krypto-Wallets abgreifen. Cyber Crucible konzentriert sich darauf, diese frühe, verborgene Phase zu erkennen und zu stoppen, statt auf den Moment zu warten, in dem Daten gesperrt werden.

Warum Sicherheitstools die größere Bedrohung oft übersehen

Viele Sicherheitsprodukte sind darauf ausgelegt, auf die Verschlüsselung zu reagieren, da dies der Teil eines Angriffs ist, den ein Unternehmen tatsächlich bemerkt – Systeme fallen aus, Dateien werden unlesbar, der Betrieb steht still. Diese sichtbare Störung zieht naturgemäß die meiste Aufmerksamkeit und die meisten Investitionen auf sich. Die Verschlüsselung ist jedoch in der Regel die letzte Handlung eines Angreifers, nicht die erste. Wenn ein Unternehmen die Auswirkungen von Ransomware bemerkt, hat der Angreifer meist bereits den folgenreicheren Teil des Eindringens abgeschlossen: das unbemerkte Sammeln identitätsbezogener Daten wie Anmeldedaten, Authentifizierungstoken, Verschlüsselungsschlüssel und Zugriffe auf digitale Wallets. Diese frühe Phase verursacht keine sichtbare Störung und wird daher tendenziell unterschätzt, obwohl sie Angreifern langfristigen, wiederholbaren Zugriff auf ein Netzwerk verschafft.

Die stille erste Phase eines Angriffs

Moderne Angriffe sind größtenteils automatisiert, und die Phase des Identitätsdiebstahls kann innerhalb weniger Sekunden für eine gesamte Organisation abgeschlossen werden. Da es keine unmittelbare Betriebsunterbrechung gibt, fehlt dieser Phase die Dringlichkeit und Sichtbarkeit, die eine Ransomware-Verschlüsselung erzeugt, wodurch sie leicht übersehen wird. Dennoch ist es genau diese Phase, die Angreifern die Möglichkeit gibt, jederzeit zurückzukehren und weiteren

Schaden anzurichten, einschließlich der späteren Bereitstellung von Ransomware.

Wie Cyber Crucible diese Lücke schließt

Cyber Crucible ist darauf ausgelegt, unbefugten Zugriff auf Identitätsdaten in dem Moment zu erkennen, in dem er geschieht, statt auf den Beginn der Verschlüsselung zu warten. Da diese Aktivität so schnell und unauffällig erfolgt, wurde erheblicher technischer Aufwand betrieben, um die Erkennung sowohl schnell als auch präzise zu gestalten – um zu identifizieren, wer auf sensible Identitätsdaten zugreift, ohne den alltäglichen Geschäftsbetrieb oder die Benutzeraktivität zu verlangsamen.

<https://player.vimeo.com/video/1141670023?texttrack=de>

[Auf Vimeo ansehen](#) · Untertitel: Englisch, Französisch, Spanisch, Arabisch

Revision #2

Created 2026-07-24 05:07:19 UTC by Dennis Underwood

Updated 2026-08-06 18:37:13 UTC by Dennis Underwood