

Wer führt Ransomware-Angriffe tatsächlich aus und wie gehen sie vor?

Kurze Antwort: Ransomware-Angriffe werden von einem lose organisierten Netzwerk aus Entwicklern, Wiederverkäufern und Operatoren durchgeführt, das ähnlich wie eine Lieferkette in der Wirtschaft funktioniert. Die effektivsten unter ihnen betreiben Erpressung als professionelles Handwerk und nicht als persönliche Racheaktion.

Ransomware als organisierte Lieferkette

Ransomware ist selten das Werk eines einzelnen, allein handelnden Hackers. Stattdessen funktioniert sie eher wie eine verteilte Branche, bestehend aus Malware-Entwicklern, die die Werkzeuge entwickeln, Wiederverkäufern oder Affiliates, die Zugang zu dieser Malware verteilen, und Operatoren, die die eigentlichen Angriffe auf die Opfer durchführen. Jede Gruppe übernimmt eine eigene Rolle, ähnlich wie sich ein legitimer Softwareanbieter auf Hersteller, Vertriebspartner und Vertriebsteams verlässt. Diese mehrschichtige Struktur trägt maßgeblich zur Widerstandsfähigkeit von Ransomware bei: Die Störung eines einzelnen Glieds in der Kette stoppt nicht zwangsläufig die gesamte Operation.

Die Profis im Vergleich zu den emotionalen Angreifern

Nicht alle Angreifer verhalten sich gleich, sobald ihre Versuche vereitelt werden. Cyber Crucible hat diesen Kontrast unmittelbar erlebt. In einem Fall rief ein Angreifer mit Verbindungen nach Osteuropa an, nachdem er gestoppt worden war, und behandelte die Begegnung als technisches Rätsel, das es zu lösen galt, statt als persönliche Beleidigung. Diese Person verwies sogar auf interne Software-Details, um zu beweisen, dass sie das Produkt zurückentwickelt hatte, und meldete sich danach regelmäßig wieder, wobei sie ihre Operationen fast wie unter Kollegen besprach.

Im Gegensatz dazu reagierte ein anderer Angreifer mit Verbindungen nach Bangladesch nach der Vereitelung mit Wut und Feindseligkeit und griff eher zu Beleidigungen als zu Problemlösungsansätzen. Dieser Kontakt setzte die Kommunikation nicht fort.

Warum das für die Abwehr wichtig ist

Diese Erfahrungen deuten darauf hin, dass die „erfolgreicheren“ und hartnäckigeren Bedrohungsakteure tendenziell diejenigen sind, die Ransomware als geschäftliche Herausforderung angehen – methodisch, geduldig und darauf fokussiert, Umgehungsmöglichkeiten zu finden. Angreifer als geschäftsmäßig handelnde Gegner zu verstehen, statt als rein chaotische Kriminelle, hilft dabei, die Gestaltung von Verteidigungstechnologien wie FortressAI von Cyber Crucible zu informieren: darauf ausgelegt, kalkulierte Versuche zur Umgehung von Schutzmaßnahmen zu antizipieren, nicht nur isolierte oder emotional getriebene Angriffe.

<https://player.vimeo.com/video/1047715866?texttrack=de>

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

Revision #2

Created 2026-07-24 05:05:58 UTC by Dennis Underwood

Updated 2026-08-06 18:37:03 UTC by Dennis Underwood