Wen greifen Ransomware-Angreifer heute tatsächlich an?

Kurze Antwort: Ransomware-Betreiber konzentrieren sich nicht mehr nur auf große, prominente Organisationen. Automatisierung und KI-gestützte Tools haben es rentabel gemacht, Unternehmen nahezu jeder Größe anzugreifen. Das bedeutet, dass die meisten Organisationen davon ausgehen sollten, ein potenzielles Ziel zu sein.

Wie sich die Zielauswahl seit 2020 verändert hat

In den Anfängen moderner Ransomware erforderte die Durchführung eines Angriffs vom initialen Zugriff bis zur Erpressung erfahrene, versierte Hacker, die größtenteils manuell arbeiteten. Das begrenzte den Kreis der fähigen Angreifer und lenkte den Fokus auf große, hochwertige Ziele, bei denen der Ertrag den Aufwand rechtfertigte.

Mit wachsender Nachfrage begannen etablierte Hackergruppen, zunehmend wie skalierende Unternehmen zu agieren. Statt sich ausschließlich auf eine kleine Zahl von Elite-Operatoren zu verlassen, entwickelten sie Ransomware-as-a-Service-Programme, die bewährte Angriffsmethoden in wiederholbare, automatisierte Playbooks verpacken. Dies ermöglichte es weniger erfahrenen Akteuren, effektive Kampagnen durchzuführen – vergleichbar damit, wie ein Junior-Vertriebsmitarbeiter mithilfe eines aus den Methoden eines Top-Performers erstellten Skripts erfolgreich sein kann.

Warum kleinere Organisationen nun gefährdet sind

Automatisierung, maschinelles Lernen und robotergestützte Prozessautomatisierung ermöglichen es diesen Akteuren, viele Angriffe gleichzeitig durchzuführen, Lösegeldverhandlungen zu führen und Zahlungs- oder Wiederherstellungsunterstützung in großem Maßstab zu verwalten. Sobald diese Funktionen weitgehend automatisiert waren, wurde auch das Vorgehen gegen kleinere Unternehmen rentabel, da Maschinen – nicht Menschen – den Großteil der Kontaktaufnahme und Nachverfolgung übernehmen.

Dieser Wandel bedeutet, dass Angreifer weniger selektiv vorgehen. Große „Big Game“-Ziele ziehen aufgrund der Höhe des potenziellen Gewinns weiterhin Aufmerksamkeit auf sich, doch der alltägliche Betrieb dieser kriminellen Operationen ähnelt zunehmend routinemäßiger Vertriebsakquise: Automatisierte Systeme suchen kontinuierlich nach jeder Organisation, die zahlen könnte. Die Systeme, die die Zielauswahl durchführen, haben in der Regel kein Bewusstsein dafür, wer oder was das Ziel tatsächlich ist – ob es sich um ein großes Unternehmen oder eine kleine gemeinnützige Organisation handelt.

Was das für Organisationen bedeutet

Da die Zielauswahl weitgehend automatisiert und unspezifisch erfolgt, ist für die meisten Organisationen nicht die Frage relevant, ob sie gezielt ausgewählt werden könnten, sondern wie gut sie auf einen eventuellen Angriffsversuch vorbereitet sind. Lösungen wie Cyber Crucible, die auf FortressAI basieren, sind darauf ausgelegt, Organisationen dabei zu unterstützen, Ransomware und verwandte Bedrohungen zu erkennen und zu stoppen – unabhängig von Größe oder Profil des Ziels.

https://player.vimeo.com/video/1047715793

Auf Vimeo ansehen · Untertitel: Englisch, Französisch, Spanisch, Arabisch

---

Revision #1
Created 2026-07-24 05:05:21 UTC by Dennis Underwood
Updated 2026-07-24 05:05:21 UTC by Dennis Underwood