

Warum kann herkömmliche Antivirensoftware Zero-Day- und dateilose Ransomware-Angriffe nicht stoppen?

Kurze Antwort: Signaturbasierte Sicherheitstools verlassen sich auf das Erkennen bekannter Angriffsmuster, aber moderne Angreifer testen ihre Werkzeuge gezielt gegen genau diese Abwehrmechanismen, bevor sie sie einsetzen, und vermeiden zunehmend, überhaupt erkennbare Dateien abzulegen. Diese Kombination aus mutierten, nicht erkannten Bedrohungen und rein speicherbasierten Techniken hat traditionelle Erkennungsmethoden deutlich unzuverlässiger gemacht.

Das Problem beim Vertrauen auf bekannte Signaturen

Zero-Day-Angriffe sind per Definition so neu oder verändert, dass sie außerhalb dessen liegen, was bestehende Sicherheitstools bereits erkennen. Hersteller versprechen seit Langem Verbesserungen bei der Erkennung solcher Bedrohungen, doch Angreifer haben einen inhärenten Vorteil: Sie haben Zugang zu denselben kommerziellen Sicherheitsprodukten, die auch von Verteidigern eingesetzt werden. Vor dem Start einer Kampagne testen Angreifer ihre Malware routinemäßig gegen gängige Erkennungstools und verfeinern sie so lange, bis sie unbemerkt bleibt. Dadurch wird Erkennung zu einem sich ständig verändernden Ziel statt zu einer festen Verteidigungslinie.

Dateilose Techniken untergraben das Whitelisting

Angreifer verzichten zunehmend darauf, offensichtlich bösartige ausführbare Dateien auf einem System abzulegen. Stattdessen kapern sie legitime, vertrauenswürdige Anwendungen, die bereits von Whitelisting-Tools für Anwendungen genehmigt wurden, und führen bösartige Aktivitäten über Prozesse aus, die von der Sicherheitssoftware als sicher eingestuft werden. Wird dieser dateilose Ansatz mit sich schnell veränderndem Code kombiniert, können Angriffe in einem sehr kurzen

Zeitfenster abgeschlossen sein – manchmal innerhalb von nur einer halben Stunde –, lange bevor ein menschliches Incident-Response-Team realistisch eine Untersuchung durchführen könnte.

Angreifer verwischen ihre eigenen Spuren

In vielen Fällen löschen Angreifer, da der Angriff im Arbeitsspeicher und nicht auf der Festplatte stattfindet, Protokolle, Beweise und sogar Sicherheitssensoren, bevor sie ihre Operation abschließen. Dies ähnelt einem Einbrecher, der Überwachungskameras und Alarmanlagen deaktiviert, bevor er eine Straftat begeht: Wenn jemand nach Beweisen sucht, ist die nützlichste Sichtbarkeit bereits zerstört. Diese Mischung aus unvorhersehbaren Angriffsmethoden und selbstlöschenden Beweisen ist der Grund, warum Cyber Crucible erhebliche Anstrengungen in die Entwicklung eines automatisierten, skalierbaren Ansatzes investiert hat – einen Ansatz, der darauf ausgelegt ist, die entscheidenden Daten zu erfassen, die für präzise Entscheidungen notwendig sind, bevor Angreifer die Spur verwischen können, statt sich auf die nachträgliche Erkennung von Bedrohungen zu verlassen.

<https://player.vimeo.com/video/1164197533?texttrack=de>

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

Revision #2

Created 2026-07-24 05:07:54 UTC by Dennis Underwood

Updated 2026-08-06 18:37:17 UTC by Dennis Underwood