Woher kommen Ransomware-Angriffe eigentlich?

Kurze Antwort: Ransomware-Akteure sind nicht auf eine Handvoll bekannter Länder beschränkt; Automatisierung und günstige kriminelle Tools ermöglichen es Angreifern heute, nahezu von überall auf der Welt aus zu operieren.

Die vereinfachte Medien-Erzählung stimmt nicht mit der Realität überein

Nachrichtenberichte verweisen häufig auf ein einzelnes Land oder eine Region als Ursprung von Ransomware-Angriffen, weil sich damit eine schnelle, leicht verständliche Schlagzeile erzeugen lässt. In der Praxis zeigt die direkte Erfahrung bei der Reaktion auf akute Vorfälle ein weitaus komplizierteres Bild. Als Cyber Crucible begann, aktive Ransomware-Fälle zu bearbeiten, erhielt unser Team eine Vielzahl von Anrufen im Zusammenhang mit den Angriffen – viele davon von Prepaid- oder Wegwerf-„Burner“-Telefonen ohne nachverfolgbare Besitzhistorie. Diese Anrufe kamen aus vielen verschiedenen Regionen, darunter Südasien, dem Nahen Osten, Teilen Europas, Südamerika und sogar Nordamerika. Einige Anrufer waren Akteure auf niedrigerer Ebene, während andere offenbar die eigentlichen Entwickler der Schadsoftware waren und gelegentlich überraschend professionelle Peer-to-Peer-Gespräche über die technischen Details ihrer Angriffe führten.

Automatisierung hat die Einstiegshürde gesenkt

Zwar bringen bestimmte Regionen der Welt möglicherweise weiterhin einen unverhältnismäßig hohen Anteil qualifizierter Ransomware-Entwickler hervor, doch das Aufkommen von Ransomware-as-a-Service-Kits, Automatisierungstools und einfacher KI-gestützter Kontaktaufnahme hat es weniger versierten Akteuren erheblich erleichtert, sich zu beteiligen. Wer über begrenzte technische Fähigkeiten verfügt, kann heute Angriffsinfrastruktur mieten, gestohlenen Netzwerkzugang von sogenannten Initial-Access-Brokern kaufen und mit minimalem Vorabaufwand eine Erpressungskampagne durchführen. Dies hat effektiv die Tür für opportunistische Kriminelle geöffnet, die sich unabhängig von ihrem Standort beteiligen können, anstatt Ransomware-Aktivitäten auf eine kleine Gruppe staatlich verbundener Akteure zu beschränken.

Warum das für die Verteidigung wichtig ist

Regionaler Slang, Sprachmuster und das bei diesen Vorfällen beobachtete Anrufverhalten bestätigen, dass Angreifer geografisch vielfältig sind und nicht auf ein einzelnes „Schurkenstaat“-Land beschränkt sind. Ransomware als global verteiltes, automatisierungsgetriebenes kriminelles Unternehmen zu verstehen – statt als vereinfachte geopolitische Erzählung – führt zu besser fundierten Verteidigungsstrategien und einem klareren Bild des tatsächlichen Risikos, dem Organisationen ausgesetzt sind.

https://player.vimeo.com/video/1047715735?texttrack=de

Auf Vimeo ansehen · Untertitel: Englisch, Français, Español, العربية

Revision #2
Created 2026-07-24 05:05:05 UTC by Dennis Underwood
Updated 2026-08-06 18:36:57 UTC by Dennis Underwood