Wer trägt das größte Risiko eines Ransomware-Angriffs, und warum werden diese Ziele ausgewählt?

Kurze Antwort: Das Ransomware-Risiko hängt oft davon ab, wen kriminelle „Access Broker“ am leichtesten kompromittieren können oder gezielt dafür bezahlt werden, zu kompromittieren. Das bedeutet, dass Schulen, Krankenhäuser und Infrastrukturanbieter mit schwächeren Verteidigungsmaßnahmen oder wertvollen Daten häufig ganz oben auf der Liste stehen.

Wie Ziele überhaupt ausgewählt werden

Hinter den meisten Ransomware-Vorfällen steht ein Marktplatz, den die meisten Menschen nie zu Gesicht bekommen. Eine Gruppe, oft als Initial Access Broker bezeichnet, verbringt ihre Zeit damit, in Netzwerke einzudringen, ohne einen konkreten Plan dafür zu haben, was danach geschieht. Sobald sie sich Zugang verschafft haben, bieten sie diesen Zugang zum Verkauf an und beschreiben genau, was sie kontrollieren – etwa administrative Rechte für Sicherheitstools, die Fähigkeit, Virenschutzmaßnahmen zu deaktivieren, oder Zugriff auf einen großen Teil der Geräte einer Organisation. Sie könnten beispielsweise beschreiben, dass sie die Geräteflotte eines Schulbezirks oder die Remote-Access-Tools eines IT-Anbieters kompromittiert haben. Käufer – von Gruppen für Datendiebstahl über Ransomware-Betreiber bis hin zu staatlich unterstützten Akteuren – bieten dann auf diesen Zugang, je nachdem, wie wertvoll und vollständig er erscheint.

Wenn Angriffe in Auftrag gegeben werden, nicht nur opportunistisch erfolgen

Es gibt außerdem ein zweites, gezielteres Muster. Hierbei stellt ein Käufer, etwa eine Ransomware-Gruppe oder ein staatlich unterstützter Akteur, eine konkrete Anfrage: Man soll eine bestimmte

Anzahl von Organisationen finden und kompromittieren, die bestimmten Kriterien entsprechen – zum Beispiel Krankenhäuser einer bestimmten Größe in einer bestimmten Region oder Versorgungsunternehmen wie Wasseraufbereitungsanlagen. Access Broker behandeln dies dann wie einen Verkaufsauftrag und suchen aktiv nach Organisationen, die dem Profil entsprechen. Sobald sie erfolgreich sind, verkaufen sie diesen Zugang an den ursprünglichen Auftraggeber weiter, auch wenn beide Seiten in der Regel nie direkt miteinander in Kontakt treten oder die Identität der jeweils anderen kennen. Aus diesem Grund spiegeln plötzliche Häufungen von Angriffen auf ähnliche Organisationen, etwa mehrere Krankenhäuser in einer Region, oft eine koordinierte Kaufanfrage wider und keinen Zufall.

Warum das für die Verteidigung wichtig ist

Da die Zielauswahl sowohl opportunistisch als auch gezielt in Auftrag gegeben erfolgen kann, kann jede Organisation mit schwachen Sicherheitskontrollen, sensiblen Daten oder kritischen Diensten zum Ziel werden, unabhängig von Größe oder Branche. Das Verständnis dieser Dynamik zwischen Käufern und Verkäufern unterstreicht, warum proaktive, durchgehend aktive Verteidigungsmaßnahmen wichtiger sind als eine Reaktion, nachdem ein Zugang bereits an den Höchstbietenden verkauft wurde.

https://player.vimeo.com/video/1047715835

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

Revision #1
Created 2026-07-24 05:05:42 UTC by Dennis Underwood
Updated 2026-07-24 05:05:42 UTC by Dennis Underwood