Ene, mene, muh?
Wie Ransomware-Gruppen ihre Opfer auswählen

Sophos X-Ops Untersuchung zeigt: Ransomware-Kriminelle treffen zumeist keine strategische Auswahl ihrer Opfer

Die Sophos X-Ops Counter Threat Unit (CTU) untersucht in einer neuen Studie, wie Ransomware-Akteure ihre Ziele auswählen. Das Ergebnis macht einmal mehr klar, dass die Cyberkriminelle gerne den Weg des geringsten Widerstands gehen: die überwiegende Mehrheit der untersuchten Ransomware-Angriffe erfolgte opportunistisch und nicht gezielt. Die Analyse der CTU-Telemetriedaten belegt, dass Angreifer in den meisten Fällen ihre vorhandenen Zugriffsrechte ausnutzen, anstatt Opfer nach Branche, Standort oder strategischer Bedeutung auszuwählen.

Obwohl einige Gruppen gezielt versuchen, über den Zugang zu umsatzstarken Unternehmen höhere Lösegeldforderungen durchzusetzen, zeigen die Untersuchungsergebnisse, dass die Mehrheit der Ransomware-Angriffe kleine Unternehmen trifft. Die Gründe hierfür liegen auf der Hand: Begrenzte Budgets und fehlende eigene Ressourcen für Cybersicherheit erhöhen die Verwundbarkeit dieser Betriebe. Sie werden von Angreifern als besonders leicht erreichbare Ziele wahrgenommen.

Opportunismus anstelle von gezielter Auswahl
Ausgangspunkt der Untersuchung war die wiederkehrende Frage an die Sophos-Forscher, ob bestimmte Ransomware-Gruppen gezielt einzelne Branchen oder Regionen ins Visier nehmen. Auch wenn diese Sorge nachvollziehbar ist, greift eine rein gruppen- oder täterbezogene Abwehr zu kurz. Entscheidend ist vielmehr zu verstehen, dass die meisten Ransomware-Angriffe opportunistisch erfolgen.

Organisationen sollten ihren Fokus daher weniger auf einzelne Akteure richten, sondern darauf, wie sie sich grundsätzlich und wirksam gegen Ransomware- und Datendiebstahlangriffe wappnen können, und zwar unabhängig davon, wer dahintersteht. Zuverlässige Sicherheitsupdates, phishing-resistente Multi-Faktor-Authentifizierung (MFA), Endpoint Detection and Response (EDR) sowie unveränderliche Backups machen Ransomware-Angriffe weiterhin gut vermeidbar. In der Praxis zeigt sich jedoch, dass viele betroffene Unternehmen diese Maßnahmen nicht konsequent umsetzen.

Regulierte Branchen sind schwierigere Ziele
Ein anschauliches Beispiel für den opportunistischen Charakter von Ransomware-Angriffen ist der Bankensektor. Banken sind umsatzstarke Unternehmen, und eine durch Ransomware verursachte Betriebsstörung könnte grundsätzlich einen starken Anreiz zur Lösegeldzahlung darstellen. Dennoch beobachten die CTU-Forscher nur sehr wenige Finanzinstitute, die tatsächlich Opfer solcher Angriffe werden.

Grund hierfür ist vermutlich vor allem der hohe Regulierungsgrad der Branche. Verbindliche Cybersicherheitsstandards sorgen dafür, dass Investitionen in Sicherheitsmaßnahmen wettbewerbsneutral erfolgen. Entsprechend sind Kontrollrahmen etabliert, Perimeter gut geschützt und Netzwerke so gestaltet, dass Angriffsflächen minimiert werden.

Organisationen in unregulierten Sektoren sind anfälliger für opportunistische Angriffe, da der Einsatz robuster Cybersicherheitspraktiken nicht in gleicher Weise gefördert wird. So erhöht

die Verbesserung der Sicherheitsmaßnahmen im Fertigungssektor etwa die Kostenbasis eines Unternehmens und macht die Produkte der Konkurrenz damit vergleichsweise günstiger.

Gezielte Angriffe auf bestimmte Branchen sind eher die Ausnahme
Werden Organisationen eines bestimmten Sektors Opfer einer spezifischen Gruppe, liegt dies wahrscheinlich daran, dass diese Gruppe eine Schwachstelle in einem in diesem Sektor weit verbreiteten Dienst ausnutzt. Organisationen desselben Sektors weisen tendenziell ähnliche Sicherheitskonzepte auf. Es gibt jedoch Ausnahmen. Manche Gruppen greifen Organisationen in Sektoren an, von denen sie annehmen, dass diese eher bereit sind, Lösegeld zu zahlen.

Zwei Beispiele: Mitglieder der Conti-Ransomware-Bande attackierten während der COVID-19-Pandemie gezielt Krankenhäuser, in der Annahme, dadurch die Wahrscheinlichkeit einer Lösegeldzahlung zu erhöhen. GOLD VICTOR, der Initiator der Ransomware-Angriffe von Vice Society und Rhysida, hat eine klare Vorliebe für Angriffe auf Organisationen im Gesundheits- und Bildungswesen, vermutlich aus demselben Grund (siehe Abbildung 1). Im zweiten Halbjahr 2025 machte Rhysida jedoch weniger als 1 Prozent aller auf den Leak-Websites aufgeführten Opfer aus. Ransomware-Opfer sind also weiterhin überwiegend zufällig verteilt.

Detaillierte Informationen zu der Untersuchung inklusive der Betrachtung verschiedener Motivationen für Ransomware-Gruppen von Lieferkettenangriffen über staatliche Operationen bis hin „Revierkämpfen“ in der Szene gibt es im englischsprachigen CTU-Blogbeitrag „How Ransomware Operators Choose Victims“

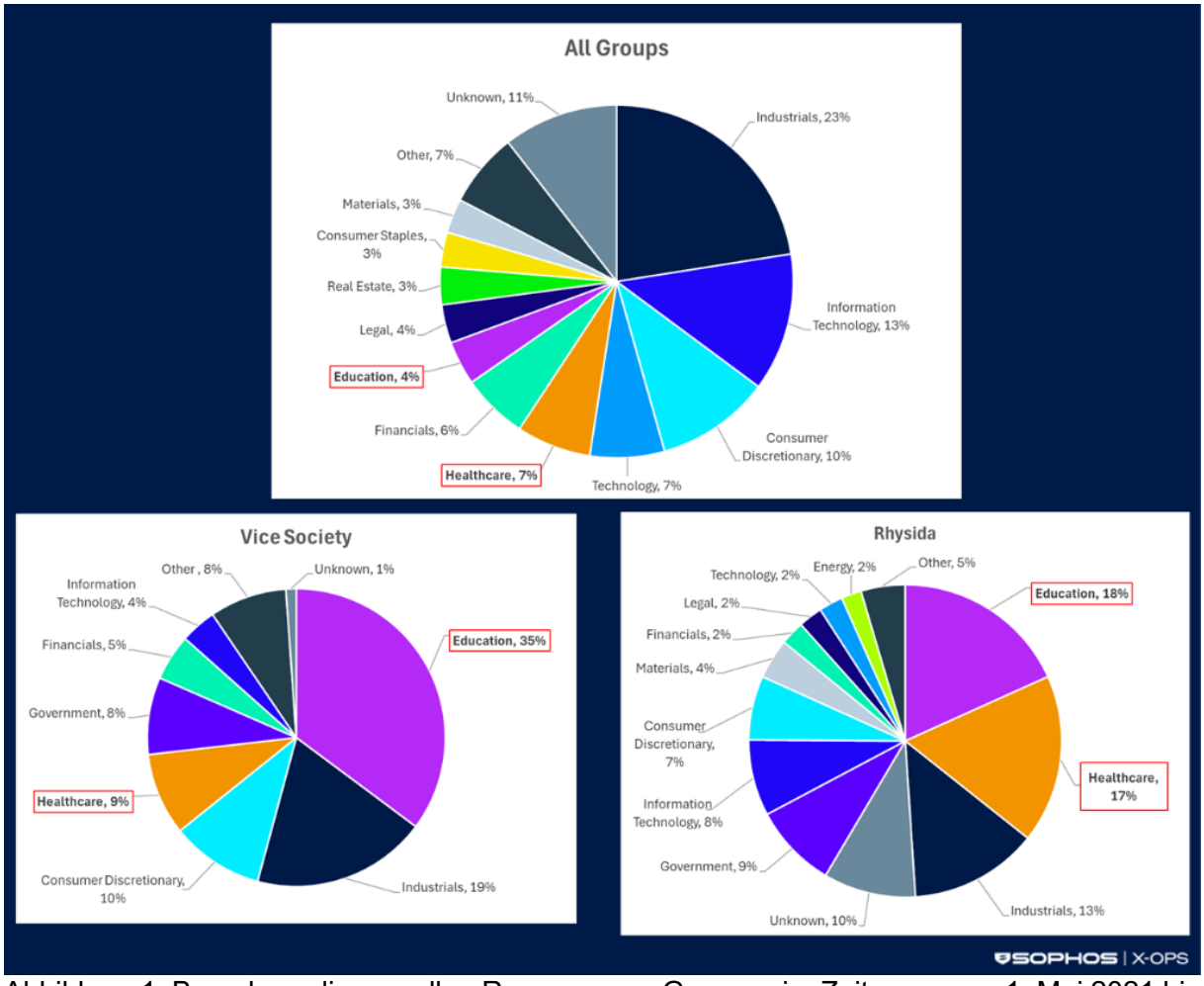

Abbildung 1: Branchen, die von allen Ransomware-Gruppen im Zeitraum vom 1. Mai 2021 bis zum 31. Dezember 2025 betroffen waren, im Vergleich zur Aufschlüsselung für Vice Society und Rhysida.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de