Ransomware-Gruppen erhöhen Druck auf Zahlungsunwillige

Sophos X-Ops beschreibt in einem neuen Report, wie die Cyberkriminellen die Informationen aus gestohlenen Daten nutzen, um die Opfer zur Zahlung zu zwingen.

Wiesbaden, 06. August 2024 – Sophos veröffentlicht heute den neuen Dark-Web-Report "Turning the Screws: The Pressure Tactics of Ransomware Gangs". Im Report beschreiben die Security-Spezialisten detailliert, wie Cyberkriminelle gestohlene Daten als Mittel einsetzen, um den Druck auf zahlungsunwillige Zielpersonen zu erhöhen. Zu den Druckmitteln gehören die Weitergabe von Kontaktdaten, das Veröffentlichen von Informationen über Familienmitglieder von CEOs und Geschäftsinhabern oder die Drohung, Informationen über illegale Geschäftsaktivitäten, die in gestohlenen Daten aufgedeckt wurden, an die Behörden zu melden. Der Sophos X-Ops Bericht zeigt zudem, dass Ransomware-Banden ihre Zielpersonen als „unverantwortlich und fahrlässig" bezeichnen und einzelne Opfer, deren persönliche Informationen gestohlen wurden, dazu auffordern, einen Rechtsstreit gegen ihren Arbeitgeber zu führen.

„Im Dezember 2023, im Zuge des MGM Casino Breach, stellte Sophos die Tendenz bei Ransomware-Gruppen fest, dass sie die Medien als eines ihrer Werkzeuge versuchen zu instrumentalisieren. Auf diese Art und Weise können die Cyberkriminellen nicht nur den Druck auf ihre Opfer erhöhen, sondern die Kontrolle über die Story übernehmen und die Schuld abschieben. Zudem beobachten die Sicherheitsspezialisten, dass die Banden die Führungskräfte der Unternehmen, die sie für die Ransomware-Attacke verantwortlich machen, ins Visier nehmen. In einem Post veröffentlichten die Angreifer ein Foto eines Geschäftsinhabers mit Teufelshörnern zusammen mit dessen Sozialversicherungsnummer. In einem anderen Posting forderten die Angreifer die Mitarbeiter auf, von ihrem Unternehmen eine „Entschädigung" zu verlangen, und in anderen Fällen drohten die Angreifer damit, Kunden, Partner und Konkurrenten über Datenverletzungen zu informieren. Dieses Vorgehen schafft eine Art Blitzableiter für Schuldzuweisungen, erhöht den Druck auf Unternehmen für das Zahlen von Lösegeldern und verschlimmert möglicherweise den Imageschaden aufgrund eines Angriffs für das Unternehmen", sagt Christopher Budd, Director, Threat Research bei Sophos.

Sophos X-Ops hat außerdem mehrere Posts von Ransomware-Angreifern gefunden, in denen sie ihre Pläne beschreiben, wie sie nach Informationen in gestohlenen Daten suchen, um diese als Druckmittel zu verwenden, wenn Unternehmen nicht zahlen. In einem Posting weist der Ransomware-Akteur WereWolves beispielsweise darauf hin, dass alle gestohlenen Daten „einer strafrechtlichen, einer kommerziellen und einer Bewertung im Hinblick auf Insider-Informationen für Wettbewerber" unterzogen werden. In einem anderen Beispiel stellte die Ransomware-Gruppe Monti fest, dass ein Angestellter eines Zielunternehmens nach Material über sexuellen Kindesmissbrauch suchte und drohte, mit den Informationen zur Polizei zu gehen, wenn das Unternehmen das Lösegeld nicht zahle.

Diese Nachrichten spiegeln den allgemeinen Trend wider, bei dem Kriminelle zunehmend versuchen, Unternehmen mit sensiblen Daten über Mitarbeiter, Kunden oder Patienten zu erpressen – beispielsweise psychiatrische Daten, medizinische Daten von Kindern, Informationen über sexuelle Probleme von Patienten oder Bilder von nackten Patienten. In einem Ransomware-Fall postete die Qiulong-Ransomware-Gruppe die persönlichen Daten der Tochter eines CEO sowie einen Link zu ihrem Instagram-Profil.

„Ransomware-Banden werden immer invasiver und dreister darin, wie und was sie als Waffe einsetzen. Um den Druck auf Unternehmen zu erhöhen, stehlen sie nicht nur Daten und drohen mit deren Weitergabe. Sie analysieren zudem intensiv die Daten und Informationen, um den Schaden zu maximieren und neue Möglichkeiten für Erpressungen zu schaffen. Das bedeutet, dass sich Unternehmen nicht nur um Unternehmensspionage, den Verlust von Geschäftsgeheimnissen oder illegale Aktivitäten von Mitarbeitern sorgen müssen, sondern auch um derartige Probleme im Zusammenhang mit Cyberattacken“, so Budd.

Lesen Sie den vollständigen Bericht "Turning the Screws: The Pressure Tactics of Ransomware Gangs" auf Sophos.com.

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

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter fortschrittlicher Lösungen zur Abwehr von Cyberangriffen, darunter Managed Detection and Response (MDR) sowie Incident Response Services. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 600.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr. Die Dienste und Produkte von Sophos sind über die cloudbasierte Management-Konsole Sophos Central verbunden und werden vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen.
Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung. Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.
Weitere Informationen unter: www.sophos.de

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