Plötzlich Gemeinsamkeiten: Sophos entdeckt neue Übereinstimmungen zwischen Hive, Royal und Black Basta Ransomware

Aktuelle Angriffe legen nahe, dass die drei Ransomware-Gruppen Playbooks oder Partner teilen

Wiesbaden, 8. August 2023 Sophos veröffentlicht in seinem Bericht "Clustering Attacker Behavior Reveals Hidden Patterns" neue Erkenntnisse über Verbindungen zwischen den bekanntesten Ransomware-Gruppen des vergangenen Jahres: Hive, Black Basta und Royal.

Ab Januar 2023 hatte Sophos X-Ops über einen Zeitraum von drei Monaten vier verschiedene Ransomware-Angriffe untersucht, bei denen einer auf Hive, zwei auf Royal und einer auf Black Basta zurückging. Dabei wurden deutliche Ähnlichkeiten zwischen den Angriffen festgestellt.

Obwohl Royal als sehr verschlossene Gruppe gilt, die keine Partner aus Untergrundforen sichtbar involviert, deuten feine Ähnlichkeiten in der Forensik der Angriffe darauf hin, dass alle drei Gruppen im Rahmen ihrer Aktivitäten entweder Partner oder hochspezifische technische Details teilen.
Sophos verfolgt und überwacht die Angriffe als "Cluster von Bedrohungsaktivitäten", die Verteidiger nutzen können, um die Erkennungs- und Reaktionszeiten zu verkürzen.

„Da das Ransomware-as-a-Service-Modell externe Partner für die Durchführung der Angriffe erfordert, ist es generell nicht ungewöhnlich, dass es Überschneidungen in den Taktiken, Techniken und Verfahren (TTPs) zwischen verschiedenen Ransomware-Gruppen gibt. In diesen Fällen handelt es sich jedoch um Ähnlichkeiten auf einer sehr feinen Ebene. Diese hochspezifischen Verhaltensweisen legen nahe, dass die Royal-Ransomware-Gruppe viel abhängiger von Partnern ist als bisher angenommen", sagt Andrew Brandt, leitender Forscher bei Sophos.

Die spezifischen Ähnlichkeiten umfassen insbesondere die folgenden drei Aspekte: Hatten erstens die Angreifer die Kontrolle über die Systeme der Ziele übernommen, kamen die gleichen spezifischen Benutzernamen und Passwörter zur Anwendung. Zweitens wurde die endgültige Payload in einem .7z-Archiv, das jeweils nach der Opferorganisation benannt war, bereitgestellt. Drittens wurden Befehle auf den infizierten Systemen mit denselben Batch-Skripten und Dateien ausgeführt.

Sophos X-Ops gelang es, diese Verbindungen im Rahmen einer Untersuchung von vier Ransomware-Angriffen aufzudecken, die im Zeitraum von drei Monaten stattgefunden hatten. Der erste Angriff erfolgte im Januar 2023 mit der Hive-Ransomware. Darauf folgten im Februar und März zwei Angriffe der Royal-Gruppe und sowie schließlich einer von Black Basta im März dieses Jahres.

Eine mögliche Ursache für die Ähnlichkeiten bei den beobachteten Ransomware-Angriffen könnte die Tatsache sein, dass gegen Ende Januar 2023 nach einer geheimen Operation des FBI ein großer Teil der Operationen von Hive aufgelöst wurde. Dies könnte dazu geführt haben, dass Hive-Partner nach einer neuen Beschäftigung suchten – möglicherweise bei Royal und Black Basta – was die auffälligen Übereinstimmungen in den folgenden Ransomware-Angriffen erklären könnte.

Aufgrund dieser Ähnlichkeiten begann Sophos X-Ops, alle vier Ransomware-Vorfälle als Cluster von Bedrohungsaktivitäten zu verfolgen.

„Wenn beim Bedrohungsaktivitäten-Clustering die ersten Schritte darin bestehen, die Zuordnung zu Gruppen vorzunehmen, besteht die Gefahr, dass Forscher sich zu sehr auf das 'Wer' eines Angriffs konzentrieren und dabei wichtige Möglichkeiten zur Stärkung der Verteidigung übersehen. Das Wissen über hochspezifisches Angreifer-Verhalten hilft Managed Detection and Response (MDR)-Teams, schneller auf aktive Angriffe zu reagieren. Es hilft auch Sicherheitsanbietern dabei, stärkere Schutzmaßnahmen für Kunden zu entwickeln. Und wenn Schutzmaßnahmen auf Verhaltensweisen basieren, spielt es keine Rolle, wer angreift. Egal ob Royal, Black Basta oder andere – potenzielle Opfer werden die notwendigen Sicherheitsvorkehrungen getroffen haben, um Angriffe, die einige der charakteristischen Merkmale aufweisen, zu blockieren", sagt Brandt.

Bislang ist die Royal-Ransomware in diesem Jahr die zweithäufigste bei den Sophos Incident Response festgestellte Ransomware-Familie.

Weitere Informationen zu diesen Ransomware-Angriffen finden Sie im Bericht "Clustering Attacker Behavior Reveals Hidden Patterns".

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. 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 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.
Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und 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, PR-Manager Central & Eastern Europe
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