Active Adversary Report von Sophos: Cyberkriminelle setzten 2022 mehr als 500 unterschiedliche Tools und Taktiken ein

- *Die häufigste Ursache für Angriffe sind ungepatchte Sicherheitslücken und kompromittierte Zugangsdaten*
- *Ransomware ist weiterhin die am stärksten verbreitete Bedrohung für Unternehmen*
- *Die Zeit vom Beginn eines Angriffs bis zu seiner Entdeckung hat sich von 15 auf 10 Tage verkürzt*

Wiesbaden, 26. April 2023 – Sophos hat heute sein „Active Adversary Playbook for Business Leaders“ veröffentlicht. Der Report bietet einen detaillierten Blick auf die veränderten Verhaltensweisen und Angriffstechniken, die Angreifer im Jahr 2022 einsetzten. Für diesen Report wurden Daten aus mehr als 150 Sophos Incident-Response-Fällen analysiert. Die Sophos-Forscher identifizierten mehr als 500 einzigartige Tools und Techniken, darunter 118 „Living off the Land“-Binaries (LOLBins). Im Gegensatz zu Malware handelt es sich bei LOLBins um ausführbare Dateien, die legal auf Betriebssystemen zu finden sind. Dadurch ist es für Verteidiger wesentlich schwieriger, sie zu blockieren, wenn Angreifer sie für schädliche Aktivitäten nutzen.

Darüber hinaus hat Sophos festgestellt, dass ungepatchte Schwachstellen die häufigste Ursache dafür sind, dass Angreifer einen Erstzugang zu den Zielsystemen erhalten. In der Hälfte der Untersuchungen nutzten Angreifer ProxyShell- und Log4Shell-Schwachstellen (erstmals aufgetreten in 2021) aus, um Unternehmen zu infiltrieren. Die zweithäufigste Ursache für Angriffe waren kompromittierte Anmeldedaten.

„Wenn Angreifer nicht einbrechen können, loggen sie sich ein. Die Bedrohungslage ist mittlerweile so umfangreich und komplex geworden, dass es keine klar definierbaren Einfallstore mehr gibt. Die meisten Unternehmen haben heute keine Chance mehr, die Angriffe alleine abzuwehren. Es gibt jedoch Tools und Dienste, die Unternehmen einen Teil der Verteidigungslast abnehmen können, so dass sie sich auf ihre Kernkompetenzen konzentrieren können“, sagt John Shier, Field CTO Commercial bei Sophos.

Ransomware dominiert, Verweildauer der Angreifenden in Unternehmenssystemen sinkt

Mehr als zwei Drittel der vom Sophos Incident Response Team untersuchten Angriffe (68 Prozent) bestanden aus Ransomware. Dies bestätigt, dass Ransomware nach wie vor eine der am weitesten verbreiteten Bedrohungen für Unternehmen darstellt. Ransomware war auch für fast drei Viertel der Incident-Response-Untersuchungen von Sophos in den letzten drei Jahren verantwortlich.

Ransomware dominiert zwar nach wie vor die Bedrohungslandschaft, doch die Verweildauer der Angreifer sank im Jahr 2022 für alle Angriffsarten von 15 auf 10 Tage. Bei Ransomware-Fällen sank die Verweildauer von 11 auf 9 Tage, während der Rückgang bei Nicht-Ransomware-

Angriffen noch stärker ausfiel. Bei Letzteren ging die Verweildauer von 34 Tagen im Jahr 2021 auf nur 11 Tage im Jahr 2022 zurück. Anders als in den vergangenen Jahren gibt es jedoch keine signifikanten Unterschiede in der Verweildauer zwischen Unternehmen unterschiedlicher Größe oder Branchen.

„Unternehmen, die erfolgreich mehrschichtige Verteidigungsmaßnahmen mit ständiger Überwachung implementiert haben, verzeichnen bessere Ergebnisse in Bezug auf die Schwere der Angriffe“, so Shier. „Der Nebeneffekt einer verbesserten Abwehr bedeutet, dass die Angreifer schneller werden müssen, um ihre Angriffe durchzuführen. Schnellere Angriffe erfordern daher eine frühere Erkennung. Der Wettlauf zwischen Angreifern und Verteidigern wird weiter eskalieren, und diejenigen, die keine proaktive Überwachung durchführen, werden die größten Konsequenzen tragen.“

Über den Report

Der Sophos Active Adversary Report for Business Leaders basiert auf 152 Incident Response (IR)-Untersuchungen, die weltweit durchgeführt wurden und sich über 22 Branchen erstrecken. Die untersuchten Unternehmen befinden sich in 31 verschiedenen Ländern, darunter die USA und Kanada, Großbritannien, Deutschland, die Schweiz, Italien, Österreich, Finnland, Belgien, Schweden, Rumänien, Spanien, Australien, Neuseeland, Singapur, Japan, Hongkong, Indien, Thailand, die Philippinen, Katar, Bahrain, Saudi-Arabien, die Vereinigten Arabischen Emirate, Kenia, Somalia, Nigeria, Südafrika, Mexiko, Brasilien und Kolumbien. Die am stärksten vertretenen Branchen sind mit 20 Prozent das verarbeitende Gewerbe, gefolgt vom Gesundheitswesen (12 Prozente)), dem Bildungswesen (9 Prozent) und dem Einzelhandel (8 Prozent).

Der Sophos Active Adversary Report for Business Leaders liefert Unternehmen umsetzbare Bedrohungsdaten und Erkenntnisse, die sie zur Optimierung ihrer Sicherheitsstrategien und Abwehrmaßnahmen benötigen

Der Sophos Active Adversary Report for Business Leader steht unter sophos.com als download zur Verfügung.

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/
Twitter: @sophos_info

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