Sophos Active Adversary Report 2024

Der Wolf im Schafspelz – Cyberkriminelle setzten vermehrt auf vertrauenswürdige Anwendungen für ihre Angriffe

Die kriminelle Verwendung von Anwendungen und Tools auf Windows-Systemen, gemeinhin als „Living Off the Land"-Binärdateien bezeichnet, steigt um 51%. Lockbit ist trotz staatlicher Intervention die Ransomware Nummer 1.

Wiesbaden, 12. Dezember 2024 – Sophos hat heute seinen neuesten Active Adversary Report unter dem Titel „The Bite from Inside" veröffentlicht, der einen detaillierten Blick auf die veränderten Verhaltensweisen und Techniken der Angreifer im ersten Halbjahr 2024 wirft. Die Analysedaten stammen aus fast 200 Incident-Response-Fällen, die das Sophos X-Ops IR-Team und Sophos X-Ops Managed Detection and Response Team in den ersten sechs Monaten 2024 bearbeitet haben.

Die wichtigste Erkenntnis der aktuellen Untersuchungen: Für ihre Aktivitäten nutzen Angreifer zunehmend vertrauenswürdige Anwendungen und Tools auf Windows-Systemen – auch als „Living Off the Land"-Binärdateien (LOLbins) bezeichnet. Dadurch wollen Cyberkriminelle einer schnellen Erkennung entgehen und sich möglichst lange auf Schleichfahrt in einer kompromittierten IT-Infrastruktur umsehen. Im Vergleich zu 2023 verzeichnete Sophos hier einen Anstieg um 51 Prozent, und sogar um 83 Prozent seit 2021.

Unter den 187 verschiedenen Microsoft LOLbins, die im ersten Halbjahr 2024 illegal zweckentfremdet wurden, war das Remote Desktop Protocol (RDP) die am häufigsten missbrauchte, vertrauenswürdige Anwendung. Von den fast 200 analysierten Incident-Response-Fällen nutzten Angreifer in 89 Prozent RDP aus. Diese Dominanz setzt einen Trend fort, der erstmals im Active Adversary-Bericht 2023 beobachtet wurde. Hier lag der Anteil des RDP-Missbrauchs bei 90 Prozent aller untersuchten IR-Fälle.

„LOLbins bieten nicht nur die Möglichkeit, die Aktivitäten eines Angreifers zu verbergen, sondern bringen leider oftmals auch eine stillschweigende Billigung seiner Aktivitäten mit sich", sagt John Shier, Field CTO bei Sophos. „Während der Missbrauch anderer legitimer Tools bei Verteidigern mittlerweile häufig die Alarmglocken läuten lässt, hat der Missbrauch einer Microsoft-Binärdatei oft den gegenteiligen Effekt, da sie ein integraler Bestandteil von Windows ist und legitime Verwendungszwecke hat. Für die schnelle Identifizierung eines Missbrauchs ist es extrem wichtig, dass Systemadministratoren genau wissen, wie diese Dateien in ihren Umgebungen verwendet werden. Denn ohne ein differenziertes und kontextbezogenes Bewusstsein für die IT-Umgebung, einschließlich kontinuierlicher Wachsamkeit gegenüber neuen und sich entwickelnden Ereignissen im Netzwerk, laufen die oftmals überlasteten IT-Teams Gefahr, wichtige Bedrohungsaktivitäten zu übersehen. Für Abhilfe kann hier zum Beispiel ein moderner Managed Detection and Response Service sorgen, der externe Experten an Bord holt und IT-Teams entlastet."

Weitere wichtige Erkenntnisse aus dem aktuellen Active Adversary Report:

- **Lockbit ist immer noch die Nummer 1**. LockBit war trotz staatlicher Interventionen gegen die wichtigste Leak-Website sowie dessen Infrastruktur im Februar die am häufigsten anzutreffende Ransomware-Gruppe und machte etwa 21 Prozent der Infektionen im ersten Halbjahr 2024 aus.
- **Haupteinfallstor sind weiterhin kompromittierte Zugangsdaten**. Damit setzt sich ein Trend fort, der erstmals im „Active Adversary Report for Tech Leaders" festgestellt wurde.

Kompromittierte Zugangsdaten sind in 39 Prozent der Fälle immer noch die Hauptursache für Angriffe. Dies ist jedoch ein Rückgang gegenüber den 56 Prozent im Jahr 2023.

- **Ältere Active-Directory-Server werden schwerpunktmäßig kompromittiert**. Angreifer haben zu 87 Prozent die Serverversionen von Active Directory aus den Jahren 2019, 2016 und 2012 kompromittiert. Für alle drei dieser Versionen gibt es keinen Mainstream-Support mehr von Microsoft – sie sind also einen Schritt vor End-of-Life (EOL) bei dem ohne kostenpflichtigen Support von Microsoft kein Patch mehr möglich ist.

Alle Details zu den Untersuchungen gibt es im umfangreichen, englischen Blogartikel „The Bite from Inside: The Sophos Active Adversary Report“

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