„Pacific Rim“-Report: Sophos deckt riesiges, gegnerisches Angriffs-Ökosystem auf

Umfangreicher Forschungsbericht gibt Einblicke in ein über mehrere Jahre andauerndes Katz-und-Maus-Spiel zwischen Sophos und mehreren, miteinander verbundenen nationalstaatlichen Gegnern mit Sitz in China

Wiesbaden, 31. Oktober 2024 – Sophos hat heute den Report „Pacific Rim“ veröffentlicht, der detailliert ein jahrelanges Katz-und-Maus-Spiel aus Angriffs- und Verteidigungsoperationen mit mehreren staatlich unterstützten Cybercrime-Gruppierungen aus China beschreibt. Im Fokus der Attacken standen dabei Cybersicherheits-Perimetergeräte, darunter Sophos Firewalls. Die Angreifer nutzten eine Reihe von Kampagnen mit neuartigen Exploits und maßgeschneiderter Malware, um Tools zur Durchführung von Überwachung, Sabotage und Cyberspionage einzubetten, die sich zudem mit Taktiken, Tools und Verfahren (TTPs) bekannter chinesischer Nationalstaatsgruppen wie Volt Typhoon, APT31 und APT41 überschnitten. Die Gegner nahmen vor allem in Süd- und Südostasien sowohl kleine als auch große kritische Infrastrukturen und Regierungsziele ins Visier, darunter Kernenergielieferanten, den Flughafen einer Landeshauptstadt, ein Militärkrankenhaus, den Staatssicherheitsapparat und zentrale Ministerien.

Im gesamten pazifischen Raum arbeitete Sophos X-Ops, die Cybersicherheits- und Threat-Intelligence-Abteilung des Unternehmens, daran, die Bewegungen der Gegner zu neutralisieren sowie Verteidigungs- und Gegenoffensiven kontinuierlich weiterzuentwickeln. Nachdem Sophos erfolgreich auf die ersten Angriffe reagiert hatte, verstärkten die Gegner ihre Bemühungen und holten erfahrenere Operatoren hinzu. Im Lauf der anschließenden Auseinandersetzung entdeckte Sophos ein riesiges, gegnerisches Cybercrime-Ökosystem.

Während Sophos seit 2020 immer wieder Details zu einzelnen Kampagnen aus den Angriffswellen veröffentlichte, darunter Cloud Snooper und Asnarök, teilt das Unternehmen nun die Gesamtanalyse der letzten fünf Jahre, um das Bewusstsein für die Hartnäckigkeit chinesischer Nationalstaatgegner und deren absoluten Fokus auf die Kompromittierung von ungepatchten oder End-of-Life-Geräten im Netzwerkperimeter; häufig über Zero-Day-Exploits, die speziell für diese Geräte entwickelt wurden. Sophos fordert alle Organisationen auf, mit absoluter Priorität Patches für Schwachstellen einzuspielen, die in ihren mit dem Internet verbundenen Geräten entdeckt wurden, sowie alle älteren, nicht mehr durch Updates unterstützte Geräte auf aktuelle Modelle zu migrieren. Sophos aktualisiert regelmäßig alle unterstützten Produkte auf der Grundlage neuer Bedrohungen und Kompromittierungsindikatoren (IoCs), um Kunden zu schützen. Sophos Firewall-Kunden werden durch schnelle Hotfixes geschützt, die standardmäßig aktiviert sind.

„Die heutige Realität ist, dass Geräte am Netzwerkperimeter zu äußerst attraktiven Zielen für chinesische Nationalstaatsgruppen wie Volt Typhoon und andere geworden sind“, so Ross McKerchar, CISO bei Sophos. „Die Gruppen verschleiern und unterstützten ihre Attacken durch sogenannte Operational Relay Boxes (ORB), die zum Beispiel über kompromittierte IoT-Geräte zum Einsatz kommen. Im Mittelpunkt der Aktivitäten steht die direkte Spionage oder die indirekte Ausnutzung von Schwachstellen für zukünftige Angriffe mit entsprechenden Kollateralschäden, da auch Organisationen getroffen werden, die ursprünglich keine Zielscheibe waren. Für Unternehmen entwickelte Netzwerkgeräte sind besonders attraktive Ziele für diese Zwecke – sie sind leistungsstark, immer aktiv und verfügen über ständige Konnektivität. Als eine Gruppe, die ein globales ORB-Netzwerk aufbauen wollte, einige

unserer Geräte ins Visier nahm, reagierten wir mit der Anwendung derselben Erkennungs- und Reaktionstechniken, die wir zum Schutz unserer Unternehmensendpunkte und Netzwerkgeräte verwenden. Dies ermöglichte es uns, die Vorgänge zu stoppen und auf wertvolle Bedrohungsinformationen zuzugreifen, die wir nutzten, um unsere Kunden zu schützen."

„Jüngste Hinweise der CISA (Cybersecurity and Infrastructure Security Agency) haben deutlich gemacht, dass chinesische Nationalstaatgruppen zu einer ständigen Bedrohung für die kritische Infrastruktur vieler Nationen geworden sind", fährt McKerchar fort. „Was wir oft vergessen, ist, dass kleine und mittlere Unternehmen – also diejenigen, die den Großteil der Lieferkette für kritische Infrastrukturen ausmachen – Ziele sind, da sie oft die schwächsten Glieder in diesem Geschäftssystem sind. Leider verfügen diese Organisationen oft über weniger Ressourcen, um sich gegen solch komplexe Bedrohungen zu verteidigen. Erschwerend kommt hinzu, dass die aktuellen Gegner dazu neigen, sich heimlich in Systemen einzunisten und auf Schleichfahrt im Netzwerk zu gehen. Das macht es sehr schwierig, sie zu entdecken und zu vertreiben – und sie werden nicht aufhören, bis sie gestört werden."

Eine Einschätzung, die auch Jeff Greene, CISA Executive Assistant Director for Cybersecurity teilt: „Durch das JCDC (Joint Cyber Defense Collaborative) erhält und teilt CISA wichtige Informationen über die Cybersicherheitsherausforderungen, mit denen wir konfrontiert sind, einschließlich der fortschrittlichen Taktiken und Techniken, die von staatlich geförderten Cyberakteuren eingesetzt werden. Das Fachwissen von Partnern wie Sophos und Berichte wie Pacific Rim bieten der globalen Cyber-Community mehr Einblicke in die sich entwickelnden Verhaltensweisen in der Volksrepublik China. Indem wir Seite an Seite arbeiten, helfen wir Cyber-Verteidigern, das Ausmaß und die weit verbreitete Ausnutzung von Edge-Netzwerkgeräten zu verstehen und Abhilfemaßnahmen umzusetzen. CISA weist weiterhin darauf hin, dass bestimmte Schwachstellengruppen, einschließlich SQL-Injections und Sicherheitslücken im Speicher, weiterhin massenhaft ausgenutzt werden. Wir fordern Softwarehersteller dringend auf, unsere Secure-by-Design-Ressourcen zu nutzen und, wie Sophos es in diesem Fall getan hat, diese Prinzipien konsequent umzusetzen."

Ratschläge für Verteidiger

Unternehmen sollten damit rechnen, dass alle mit dem Internet verbundenen Geräte Hauptziele nationalstaatlicher Gegner sind, insbesondere Geräte in kritischen Infrastrukturen. Sophos empfiehlt Unternehmen, die folgenden Maßnahmen zu ergreifen, um ihre Sicherheitslage zu stärken.

- Minimieren Sie nach Möglichkeit internetbasierte Dienste und Geräte.
- Priorisieren Sie Patches mit Dringlichkeit für mit dem Internet verbundene Geräte und überwachen Sie diese.
- Ermöglichen Sie, dass Hotfixes für Edge-Geräte zugelassen und automatisch angewendet werden.
- Erstellen Sie einen Plan für den Umgang Ihrer Organisation mit End-of-Life-Geräten.
- Arbeiten Sie mit Strafverfolgungsbehörden, öffentlichen und privaten Partnern sowie der Regierung zusammen, um relevante IoCs (Kompromittierungsindikatoren) auszutauschen und darauf zu reagieren.

Ross McKerchar weiter: „Wir müssen mit dem öffentlichen und privaten Sektor, den Strafverfolgungsbehörden und Regierungen sowie der Sicherheitsbranche zusammenarbeiten, um unser Wissen über diese feindlichen Operationen auszutauschen. Es ist eine clevere Taktik der Angreifer, genau jene Perimetergeräte ins Visier zu nehmen, die zum Schutz von Netzwerken eingesetzt werden. Organisationen, Vertriebspartner und Managed Service Provider müssen sich darüber im Klaren sein, dass diese Geräte die Hauptziele für Angreifer sind und sollten sicherstellen, dass sie entsprechend abgesichert sind sowie kritische Patches sofort nach ihrer Veröffentlichung angewendet werden. Tatsächlich wissen wir, dass Angreifer aktiv nach EOL-Geräten suchen. Auch hier spielen Anbieter eine große Rolle. Sie müssen Kunden helfen, indem sie zuverlässige und gut getestete Hotfixes

unterstützen, ein einfaches Upgrade von EOL-Plattformen ermöglichen, Legacy-Code, der noch bestehende Schwachstellen bergen kann, systematisch umgestalten oder entfernen, und standardmäßig sichere Designs kontinuierlich verbessern, um die Integrität der eingesetzten Geräte zu gewährleisten."

Den gesamten Report mit zahlreichen Details sowie den wichtigsten Meilensteinen der Pacific-Rim-Historie gibt es unter www.Sophos.com/pacificrim

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