# Sophos deckt chinesische Spionagekampagne in Südostasien auf

*Sophos X-Ops findet Verbindungen zwischen fünf bekannten chinesischen Bedrohungsgruppen, darunter APT41 und BackdoorDiplomacy; Angreifer nutzen zwei bisher unbekannte Malware-Varianten für Spionage und Persistenz.*

**Wiesbaden, 5. Juni 2024** Sophos, ein weltweit führender Anbieter innovativer Sicherheitslösungen zur Abwehr von Cyberangriffen, veröffentlichte heute seinen Bericht „Operation Crimson Palace: Sophos Threat Hunting Unveils Multiple Clusters of Chinese State-Sponsored Activity Targeting Southeast Asia“, in dem eine hochentwickelte, fast zweijährige Spionagekampagne gegen ein hochrangiges Regierungsziel detailliert unter die Lupe genommen wird. Im Rahmen der 2023 gestarteten Untersuchung von Sophos X-Ops fand das Managed-Detection-and Response-Team (MDR) drei verschiedene Aktivitätscluster, die auf dieselbe Organisation abzielten. Zwei davon umfassten Taktiken, Techniken und Verfahren (TTP), die sich mit bekannten chinesischen, nationalstaatlichen Gruppen überschneiden: BackdoorDiplomacy, APT15 und die APT41-Untergruppe Earth Longzhi.

Die Angreifer konzipierten ihre Operation mit dem Ziel, bestimmte Nutzer auszuspähen sowie sensible politische, wirtschaftliche und militärische Informationen zu sammeln. Dabei verwendeten sie während der Kampagne, die Sophos „Crimson Palace“ nennt, eine Vielzahl unterschiedlicher Malware und Tools. Dazu gehören zwei bisher unbekannte Malware-Stämme: ein Backdoor- und ein Persistenz-Tool, die Sophos „CCoreDoor“ bzw. „PocoProxy“ nannte.

**Unterschiedliche chinesische Angreifer nutzen gemeinsame Infrastruktur**
„Die verschiedenen Cluster scheinen im Sinne chinesischer Staatsinteressen gearbeitet zu haben, indem sie militärische und wirtschaftliche Informationen zur Unterstützung der Strategien des Landes im Südchinesischen Meer gesammelt haben“, so Paul Jaramillo, Director Threat Hunting & Threat Intelligence bei Sophos. „In dieser speziellen Kampagne glauben wir, dass die drei Cluster unter der Leitung einer zentralen staatlichen Behörde parallel gegen dasselbe Ziel vorgegangen sind. Innerhalb eines der drei von uns identifizierten Cluster – Cluster Alpha – sahen wir Überschneidungen zwischen Malware und TTPs mit vier separat gemeldeten chinesischen Bedrohungsgruppen. Es ist bekannt, dass chinesische Angreifer Infrastruktur und Tools gemeinsam nutzen, und diese jüngste Kampagne ist ein mahnendes Beispiel dafür, wie umfassend diese Gruppen ihre Tools und Techniken teilen.“

Jaramillo weiter: „Während westliche Regierungen das Bewusstsein für Cyberbedrohungen aus China schärfen https://www.reuters.com/world/uk/china-poses-genuine-increasing-cyber-risk-uk-spy-agency-head-says-2024-05-14/, ist die von Sophos aufgedeckte Überschneidung eine wichtige Erinnerung daran, dass eine zu starke Konzentration auf einen einzelnen chinesischen Akteur dazu führen kann, dass Unternehmen Gefahr laufen, Trends bei der Art und Weise zu übersehen, wie diese Gruppen ihre Operationen koordinieren. Durch den Blick über den Tellerrand hinaus können Unternehmen ihre Abwehrmaßnahmen intelligenter gestalten.“

**So deckte Sophos X-Ops das Bewegungsmuster der Cluster auf:**
Die Experten von Sophos X-Ops erfuhren erstmals im Dezember 2022 von böswilligen Aktivitäten im Netzwerk der Zielorganisation, als sie ein Datenexfiltrationstool fanden, das zuvor der chinesischen Bedrohungsgruppe Mustang Panda zugeschrieben wurde. Von da an

begann das MDR-Team mit einer umfassenderen Suche nach böswilligen Aktivitäten. Im Mai 2023 entdeckte das Sophos X-Ops Threat Hunting Team eine anfällige, ausführbare VMWare-Datei und nach der Analyse drei verschiedene Aktivitätscluster im Netzwerk des Ziels, im Folgenden Cluster Alpha Cluster Bravo und Cluster Charlie benannt.

Cluster Alpha war von Anfang März bis mindestens August 2023 aktiv und setzte eine Vielzahl von Malware ein, die sich auf die Deaktivierung des AV-Schutzes, die Ausweitung von Berechtigungen und die Durchführung von Aufklärung konzentrierte. Dazu gehörte eine aktualisierte Version der EAGERBEE-Malware, die mit der chinesischen Bedrohungsgruppe REF5961 in Verbindung gebracht wird. Cluster Alpha nutzte auch TTPs und Malware, die sich mit denen von den chinesischen Bedrohungsgruppen BackdoorDiplomacy, APT15, Worok und TA428 überschneiden.

Cluster Bravo war im März 2023 nur drei Wochen lang im Zielnetzwerk aktiv und bewegte sich auf Schleichfahrt durch das Netzwerk des Opfers, um unentdeckt eine CCore-Hintertür zu laden. Diese Aktion richtete externe Kommunikationswege für die Angreifer ein, führte eine Erkennung durch und exfiltrierte Anmeldeinformationen.

Cluster Charlie war von März 2023 bis mindestens April 2024 aktiv, mit Schwerpunkt auf Spionage und Exfiltration. Dazu gehörte der Einsatz von PocoProxy, einem Persistenztool, das sich als ausführbare Microsoft-Datei ausgibt und die Kommunikation mit der Befehls- und Kontrollinfrastruktur der Angreifer aufbaut. Cluster Charlie arbeitete daran, eine große Menge sensibler Daten für Spionagezwecke zu exfiltrieren, darunter militärische und politische Dokumente sowie Anmeldeinformationen/Tokens für den weiteren Zugriff innerhalb des Netzwerks. Cluster Charlie teilt TTPs mit der chinesischen Bedrohungsgruppe Earth Longzhi, einer gemeldeten Untergruppe von APT41. Im Gegensatz zu Cluster Alpha und Cluster Bravo bleibt Cluster Charlie aktiv.

„Was wir bei dieser Kampagne gesehen haben, ist die aggressive Entwicklung von Cyberspionageoperationen im Südchinesischen Meer. Wir haben mehrere Bedrohungsgruppen, wahrscheinlich mit unbegrenzten Ressourcen, die wochen- oder monatelang dieselbe hochrangige Regierungsorganisation ins Visier nehmen, und sie verwenden fortschrittliche benutzerdefinierte Malware, die mit öffentlich verfügbaren Tools verknüpft ist. Sie waren und sind immer noch in der Lage, sich innerhalb einer Organisation nach Belieben zu bewegen und ihre Werkzeuge häufig zu wechseln. Mindestens einer der Aktivitätscluster ist immer noch sehr aktiv und versucht, weitere Überwachungen durchzuführen. Angesichts der Häufigkeit, mit der sich die Aktivitäten dieser chinesischen Bedrohungsgruppen überschneiden und diese Tools gemeinsam nutzen, ist es möglich, dass die TTPs und neuartige Malware, die wir in dieser Kampagne beobachtet haben, auch in anderen chinesischen Operationen weltweit wieder auftauchen. Wir werden die Geheimdienste über unsere Erkenntnisse auf dem Laufenden halten, während wir unsere Untersuchungen zu diesen drei Clustern fortsetzen“, so Jaramillo.

Alle Infos über die Spionagekampagne gibt es im Blogartikel „Operation Crimson Palace: Sophos Threat Hunting Unveils Multiple Clusters of Chinese State-Sponsored Activity Targeting Southeast Asia“.

Nähere Details zu den Aktivitäten der drei Angriffscluster gibt es im Artikel „Operation Crimson Palace: A Technical Deep Dive“.

**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