„Gängige Bedrohungen wie Loader, Dropper und Initial Access Broker, die es schon lange vor der großen Ransomware-Welle gab, werden in das scheinbar alles verschlingende `schwarze Loch' der Ransomware hineingesogen."
(Chester Wisniewski, Principal Research Scientist bei Sophos)

Sophos Threat Report 2022:
Im Sog der Ransomware

Die SophosLabs identifizieren neue Trends bei Ransomware, Standard-Malware, Angriffs-Tools, Cryptominern und mehr.
Ransomware vereinnahmt andere Cyberbedrohungen, um eine massive, vernetzte Bereitstellungsinfrastruktur für seine Erpressungsaktivitäten zu schaffen.
Fortschreitende Deepfake-Video- und Sprachsynthese-Technologien eröffnen Cyberkriminellen neue Möglichkeiten.

Wiesbaden 9. November 2021 Sophos hat heute seinen alljährlichen IT-Security-Bedrohungsbericht veröffentlicht. Der Sophos 2022 Threat Report sammelt die Forschungsergebnisse und Bedrohungsdaten von den Sophos Labs, den Experten aus den Abteilungen Managed Threat Response und Rapid Response sowie dem Sophos AI-Team und bietet eine mehrdimensionale Perspektive auf Sicherheitsbedrohungen, mit denen Unternehmen im Jahr 2022 konfrontiert sein werden. Der Report beschreibt Entwicklungen und Trends von Ransomware, Angriffs-Tools, Commodity-Malware, Cryptomining und mehr. Sophos geht davon aus, dass die im Report behandelten Erkenntnisse die Bedrohungslandschaft und die IT-Sicherheit bis 2022 und darüber hinaus maßgeblich beeinflussen.

Der Sophos 2022 Threat Report skizziert die folgenden Haupttrends:

1. **Das Geschäftsmodell Ransomware entwickelt sich weiter**, hin zu mehr Modularität und Einheitlichkeit – und der Einfluss auf die Bedrohungslandschaft nimmt zu. Ransomware ist für Cyberkriminelle so effektiv und lukrativ, dass sie andere Cyberbedrohungen wie Initial Access Broker, Loader und Dropper einbeziehen, um ein massives, vernetztes Ransomware-Verbreitungssystem zu schaffen.
   Die Cyberkriminellen bieten zudem verschiedene Elemente für einen Angriff "as-a-Service" an und stellen Playbooks mit Tools und Techniken zur Verfügung, mit denen weitere Gruppen ihre Attacken durchführen können.
   Laut den Sophos-Forscher:innen machten die Angriffe einzelner Ransomware-Gruppen im Jahr 2021 bereits mehr und mehr Ransomware-as-a-Service (RaaS)-Angeboten Platz, bei denen sich spezialisierte Ransomware-Kriminelle darauf konzentrieren, Schadcode und Infrastruktur an andere Cyberkriminelle zu vermieten. Sobald sie über die benötigte Malware verfügen, können sich RaaS-Nutzer und andere Ransomware-Betreiber an Initial Access Broker und Plattformen zur Verbreitung von Malware wenden, um potenzielle Opfer zu finden und anzugreifen.

2. **Etablierte Cyber-Bedrohungen werden sich weiter anpassen**, um Ransomware zu verbreiten und bereitzustellen. Dazu gehören Loader, Dropper und andere Standard-Malware sowie zunehmend fortschrittliche, von Menschen betriebene Initial Access Broker, Spam und Adware. Im Jahr 2021 berichtete Sophos z.B. über die Schadsoftware Gootloader, die neuartige hybride Angriffe durchführt, bei denen Massenkampagnen mit

sorgfältiger Filterung kombiniert werden, um Ziele für bestimmte Malware-Pakete zu finden.

3. **Erpresserische Bedrohungen** wie die Herausgabe von Daten und andere Druckmittel werden zunehmend Teil der Ransomware-Bedrohung sein. Im Jahr 2021 katalogisierte das Sophos-Incident-Response-Team zehn verschiedene Arten von Erpressungstaktiken – von Datendiebstahl und Offenlegung über Drohanrufe bis hin zu Distributed Denial of Service (DDoS)-Attacken und mehr.

4. **Kryptowährungen** werden weiterhin Cyberkriminalität wie Ransomware und bösartiges Kryptomining anheizen. Sophos geht davon aus, dass sich dieser Trend fortsetzt, bis die globalen Kryptowährungen besser reguliert sind. Im Jahr 2021 entdeckten Sophos-Forscher:innen Kryptominer wie Lemon Duck und den weniger verbreiteten MrbMiner, die den Zugang zu neu gemeldeten Schwachstellen und zu Zielen, die bereits von Ransomware-Betreibern angegriffen wurden, ausnutzen, um Kryptominer auf Computern und Servern zu installieren.

Im Sog der Ransomware
„Ransomware floriert, da sie sich ständig anpasst und erneuert", sagt Chester Wisniewski, Principal Research Scientist bei Sophos. "RaaS-Angebote sind zwar nicht neu, aber in den vergangenen Jahren haben sie vor allem dazu beigetragen, Ransomware in die Reichweite von weniger qualifizierten oder weniger finanzstarken Angreifer:innen zu bringen. Dies hat sich geändert: Im Jahr 2021 investieren RaaS-Entwickler ihre Zeit und Energie in die Erstellung von ausgefeiltem Code und in die Frage, wie sie am besten die höchsten Zahlungen von Opfern, Versicherungsgesellschaften und Unterhändlern erbeuten können. Die Suche nach Opfern, die Installation und Ausführung der Malware sowie das Waschen der erpressten Kryptowährungen geben sie nun an andere weiter. Das führt zu einer Verzerrung der Cyberbedrohungslandschaft und gängige Bedrohungen wie Loader, Dropper und Initial Access Broker, die es schon lange vor der großen Ransomware-Welle gab, werden in das scheinbar alles verschlingende `schwarze Loch‘ der Ransomware hineingesogen.“

Weitere von Sophos analysierte Trends sind:

- **Missbrauch von Admin-Tools und Internet-Diensten**. Nachdem die ProxyLogon- und ProxyShell-Schwachstellen im Jahr 2021 entdeckt (und gepatcht) wurden, wurden sie von Angreifern so schnell ausgenutzt, dass Sophos davon ausgeht, dass es weiterhin Versuche geben wird, IT-Administrations-Tools und ausnutzbare Internet-Dienste massenhaft zu missbrauchen – sowohl von erfahrenen Angreifern als auch von gewöhnlichen Cyberkriminellen.

- **Täuschungsmanöver.** Sophos erwartet außerdem, dass Cyberkriminelle verstärkt Tools zur Simulation von Angriffen mit Cobalt Strike Beacons, Mimikatz und PowerSploit missbrauchen werden. IT-Sicherheitsteams sollten jeden Alarm, der sich auf missbräuchlich genutzte legitime Tools oder Tool-Kombinationen bezieht, genauso überprüfen wie eine Schadcode-Erkennung, da diese auf die Anwesenheit eines Eindringlings im Netzwerk hinweisen könnte.

- **Bedrohungen von Linux-Systemen**. Im Jahr 2021 haben die Forscher von Sophos eine Reihe neuer Bedrohungen beschrieben, die auf Linux-Systeme abzielen. Die Spezialist:innen erwarten für 2022 ein wachsendes Interesse an Linux-basierten Systemen, sowohl in der Cloud als auch auf Web- und virtuellen Servern.

- **Mobile Bedrohungen und Social-Engineering-Betrug.** Tools wie Flubot und Joker werden sich weiter ausbreiten, um sowohl Einzelpersonen als auch Unternehmen anzugreifen.

- **Fake-Apps in den Schlupflöchern der iOS-Plattform.** Mehr betrügerische Apps werden versuchen, Schlupflöcher in der iOS-Plattform auszunutzen, da die Techniken von kriminellen Gruppen besser bekannt und verstanden werden. Im Jahr 2021 berichtete Sophos beispielsweise über "CryptoRom", einen gefälschten iOS-Kryptowährungsbetrug, der es auf Nutzer beliebter Dating-Websites in aller Welt abgesehen hatte. Die gefälschten Apps wurden über iOS-"Test"-Plattformen für Entwickler verbreitet.

- **KI boomt auf beiden Seiten.** Der Einsatz künstlicher Intelligenz in der Cybersicherheit wird sich fortsetzen und beschleunigen, da leistungsstarke maschinelle Lernmodelle ihren Wert bei der Erkennung von Bedrohungen und der Priorisierung von Warnungen unter Beweis stellen. Auf der anderen Seite ist zu erwarten, dass auch Cyberkriminelle zunehmend KI einsetzen. In den nächsten Jahren sind Angriffe zu erwarten, die von KI-gestützten Desinformationskampagnen und gefälschten Social-Media-Profilen bis hin zu Watering-Hole-Angriffen auf Webinhalte, Phishing-E-Mails und mehr reichen, da fortschrittliche Deepfake-Video- und Sprachsynthese-Technologien verfügbar werden.

"Es reicht nicht mehr aus, wenn Unternehmen davon ausgehen, dass sie sicher sind, indem sie einfach Sicherheitstools überwachen und vermeintlich sicherstellen, dass hierdurch bösartiger Code erkannt wird. Bestimmte Kombinationen von Erkennungen oder sogar Warnungen sind das moderne Äquivalent eines Einbrechers, der eine Blumenvase zerbricht, während er durch das Hinterfenster einsteigt. IT-Sicherheitsteams müssen alle Alarme untersuchen, selbst solche, die in der Vergangenheit unbedeutend gewesen sein mögen. Eindringlinge von heute haben gelernt , mit ihren Schleichfarten ganze Netzwerke zu übernehmen und sind deshalb gefährlich wie nie“, so Wisniewski.

Um mehr über die Bedrohungslandschaft im Jahr 2021 zu erfahren und was dies für die IT-Sicherheit im Jahr 2022 bedeutet, lesen Sie den vollständigen Sophos 2022 Threat Report (Englisch): www.sophos.com/threatreport

Neu: 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 Anbieter von Next Generation Cybersecurity und schützt mehr als 500.000 Unternehmen und Millionen von Verbrauchern in mehr als 150 Ländern vor den modernsten Cyberbedrohungen. Basierend auf Threat Intelligence, KI und maschinellem Lernen aus den SophosLabs und von SophosAI bietet Sophos ein breites Portfolio an fortschrittlichen Produkten und Services, um Anwender, Netzwerke und Endpoints vor Ransomware, Malware, Exploits, Phishing und einer Vielzahl anderer Cyberattacken zu schützen. Sophos bietet mit Sophos Central eine einzige, integrierte und cloudbasierte Management-Konsole. Sie ist das Herzstück eines anpassungsfähigen Cybersecurity-Ökosystems mit einem zentralen Data Lake, der eine Vielzahl offener API-Schnittstellen bedient, die Kunden, Partnern, Entwicklern und anderen Cybersecurity-Anbietern zur Verfügung stehen. Sophos vertreibt seine Produkte und Services über Partner und Managed Service Provider (MSPs) weltweit. Der Sophos-Hauptsitz ist 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