„Initial Access Broker (IAB) haben eine eigene Cybercrime-Industrie entwickelt, indem sie in ein Ziel eindringen, es auskundschaften oder eine Backdoor installieren und dann den schlüsselfertigen Zugang an Ransomware-Banden für deren eigene Angriffe verkaufen."

„Mit den Möglichkeiten, die sich durch ungepatchte ProxyLogon- und ProxyShell-Schwachstellen ergeben, und dem Aufkommen von IABs sehen wir verstärkt, dass sich mehrere Angreifer in ein und demselben Ziel-Netzwerk befinden. Wenn es dort eng wird, wollen sie schnell handeln, um ihren Konkurrenten zuvor zu kommen."

„Zu den Warnsignalen, auf die Unternehmen achten sollten, gehört die Entdeckung eines legitimen Tools oder einer Kombination von Tools und Aktivitäten an einem unerwarteten Ort oder zu einer ungewöhnlichen Zeit."

John Shier, Senior Security Advisor bei Sophos

Sophos Active Adversary Playbook 2022 – Neue Analyse aus weltweiten Angriffen zeigt:

Cyberkriminelle bleiben immer länger unbemerkt im Unternehmensnetzwerk

Unbemerkte, angriffslose Schleichfahrt von Cyberkriminellen im Netzwerk steigt auf durchschnittlich 34 Tage. Kleinere Unternehmen und Bildungssektor besonders betroffen.

Vor Ransomware-Attacken dauert das Versteckspiel im Netz durchschnittlich 15 Tage

Verwendung des Remote-Desktop-Protokolls für den externen Zugriff gesunken, für Bewegungen innerhalb des Netzwerks gestiegen

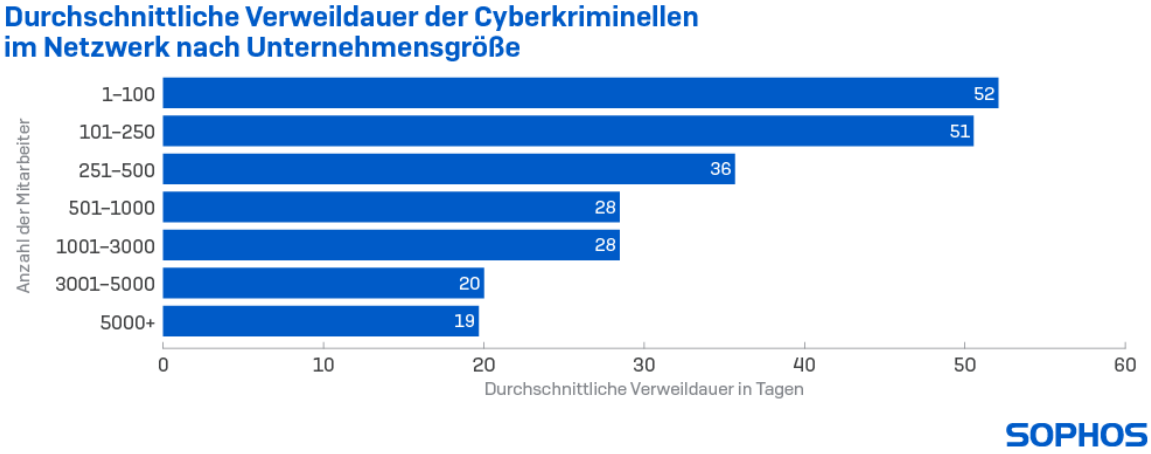
Florierender Handel mit „schlüsselfertigen" Zugängen unter den Kriminellen

Teilweise mehrere Angreifer gleichzeitig im Netzwerk

Wiesbaden, 7. Juni 2022 – Sophos veröffentlicht heute sein „Active Adversary Playbook 2022". Es beschreibt detailliert das Verhalten von Cyberkriminellen, die das Rapid Response Team von Sophos im Jahr 2021 beobachtet hat. Die Untersuchungen zeigen einen Anstieg der Verweildauer der Cyberkriminillen in Unternehmensnetzwerken um 36 Prozent. Der durchschnittliche, unentdeckte Aufenthalt im Netzwerk ohne größere Attacke wie etwa Ransomware liegt bei 34 Tagen. Der Report zeigt auch die Auswirkungen der ProxyShell-Schwachstellen in Microsoft Exchange auf, die Sophos zufolge von einigen Initial Access Brokern (IABs) ausgenutzt wurden, um in Netzwerke einzudringen und den Zugang dann an andere Cybergangster zu verkaufen.
„Die Welt der Cyberkriminalität ist unglaublich vielfältig und spezialisiert geworden", sagt John Shier, Senior Security Advisor bei Sophos. „Initial Access Broker (IAB) haben eine eigene Cybercrime-Industrie entwickelt, indem sie in ein Ziel eindringen, es auskundschaften oder eine Backdoor installieren und dann den schlüsselfertigen Zugang an Ransomware-Banden für deren eigene Angriffe verkaufen. In dieser zunehmend dynamischen und spezialisierten Cyber-Bedrohungslandschaft kann es für Unternehmen schwierig sein, mit den sich ständig

ändernden Tools und Methoden der Angreifenden Schritt zu halten. Es ist wichtig, dass sie wissen, worauf sie in jeder Phase der Angriffskette achten müssen, damit sie Angriffe so schnell wie möglich erkennen und neutralisieren können."

Verweildauer in kleineren Unternehmen und im Bildungssektor länger
Die Untersuchungen von Sophos zeigen auch, dass die Verweildauer von Angreifenden in kleineren Unternehmen länger war als in größeren Unternehmen. Die Cyberkriminellen hielten sich in Unternehmen mit bis zu 250 Mitarbeitern etwa 51 Tage auf. Im Vergleich dazu verbrachten sie in Unternehmen mit 3.000 bis 5.000 Mitarbeitern in der Regel „nur" 20 Tage. Einen Sonderfall stellen Ransomware-Attacken dar. Hier agieren die Kriminellen insgesamt „schneller", jedoch stieg auch hier der unbemerkte Aufenthalt im Netzwerk von 11 Tagen in 2020 auf 15 Tage in 2021.



Größere Firmen für Cyberkriminelle „wertvoller", Drängelei im Netzwerk
„Angreifer halten größere Organisationen für wertvoller und sind daher stärker motiviert, schnell einzudringen und auch schnell wieder zu verschwinden. Kleinere Unternehmen haben einen geringeren `Wert´, so dass es sich die Eindringlinge leisten können, sich länger im Hintergrund im Netzwerk aufzuhalten. Es ist allerdings auch möglich, dass diese Angreifenden über weniger Erfahrung verfügen und deshalb mehr Zeit im Netzwerk mit Auskundschaften verbringen. Auch haben kleinere Unternehmen in der Regel weniger Einblick in die Angriffskette, um Attacken zu erkennen und zu vertreiben. Dies verlängert ebenfalls die Präsenz der Angreifenden", so Shier. „Mit den Möglichkeiten, die sich durch ungepatchte ProxyLogon- und ProxyShell-Schwachstellen ergeben, und dem Aufkommen von IABs sehen wir verstärkt, dass sich mehrere Angreifer in ein und demselben Ziel-Netzwerk befinden. Wenn es dort eng wird, wollen sie schnell handeln, um ihren Konkurrenten hervorzukommen."

Weitere Ergebnisse des Active Adversary Playbook 2022

- **Die durchschnittliche Verweildauer bis zur Entdeckung war länger bei "heimlichen" Angriffen**, die sich nicht zu einem größeren Angriff wie Ransomware entwickelt hatten, sowie bei kleineren Organisationen mit weniger IT-Sicherheitsressourcen. Die durchschnittliche Verweildauer der Angreifer in Unternehmen, die von Ransomware betroffen waren, betrug 15 Tage. Bei Organisationen, die zwar verletzt wurden, aber noch nicht von einem größeren Angriff wie Ransomware betroffen waren (23 Prozent aller untersuchten Fälle), lag die durchschnittliche Verweildauer bei 34 Tagen. Bei Organisationen im Bildungssektor oder mit weniger als 500 Mitarbeitern war die Verweildauer ebenfalls länger.

- **Längere Verweilzeiten und offene Einstiegspunkte machen Unternehmen anfällig für mehrere Angreifer**. Sophos-Forensiker deckten Fälle auf, in denen mehrere Angreifer, darunter IABs, Ransomware-Banden, Cryptominer und gelegentlich sogar mehrere Ransomware-Gruppen, gleichzeitig auf dieselbe Organisation zielten

- **Trotz eines Rückgangs bei der Verwendung des Remote Desktop Protocol (RDP) für externe Zugriffe nutzten Angreifende das Tool verstärkt für Schleichfahrten im Netzwerk.** Im Jahr 2020 nutzten Angreifer RDP in 32 Prozent der analysierten Fälle für externe Aktivitäten. Dieser Anteil sank auf 13 Prozent im Jahr 2021. Diese Veränderung ist zwar zu begrüßen und deutet darauf hin, dass Unternehmen ihr Management externer Angriffsflächen verbessert haben, doch Angreifende missbrauchen RDP immer noch für interne Seitwärtsbewegungen. Sophos fand heraus, dass Angreifer RDP im Jahr 2021 in 82 Prozent der Fälle für interne Netzwerkerkundungen nutzten, im Jahr 2020 waren es noch 69 Prozent.

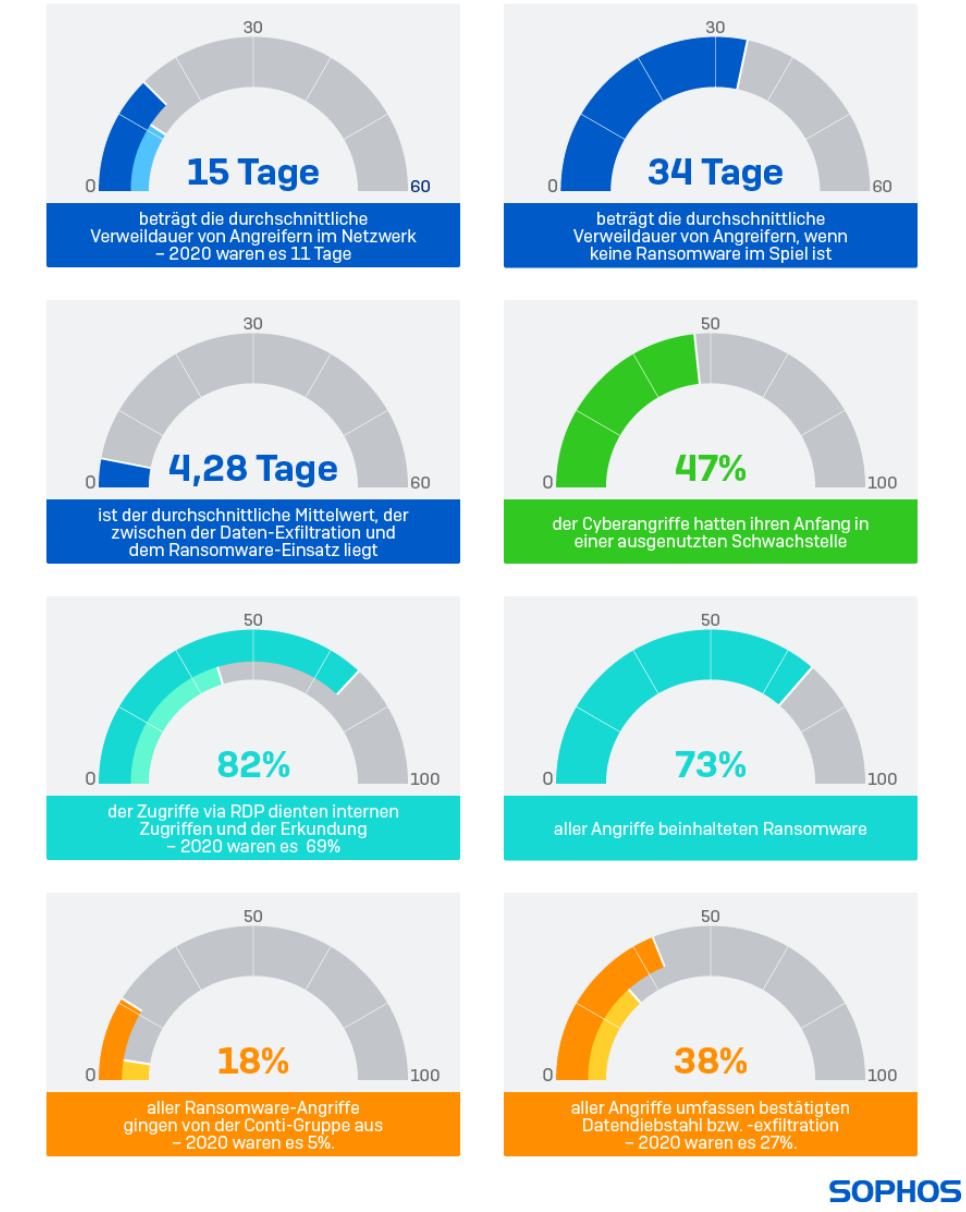
- **Häufige bei Angriffen verwendete Tool-Kombinationen sind ein deutliches Warnsignal für Cyber-Angriffe.** Die Untersuchungen der Vorfälle ergaben beispielsweise, dass im Jahr 2021 in 64 Prozent der Fälle PowerShell und bösartige Nicht-PowerShell-Skripte zusammen verwendet wurden. PowerShell und Cobalt Strike wurden in 56 Prozent der Fälle kombiniert und PowerShell und PsExec fanden die Sophos-Forscher in 51 Prozent der Fälle in Kombination. Die Erkennung solcher Korrelationen kann als Frühwarnung vor einem bevorstehenden Angriff dienen oder das Vorhandensein eines aktiven Angriffs bestätigen.

- **50 Prozent der Ransomware-Vorfälle betrafen eine bestätigte Daten-Exfiltration.** Bei den verfügbaren Daten betrug der durchschnittliche Abstand zwischen Datendiebstahl und dem Einsatz von Ransomware 4,28 Tage. 73 Prozent der Vorfälle, auf die Sophos im Jahr 2021 reagierte, betrafen Ransomware. Von diesen Ransomware-Vorfällen waren 50 Prozent auch mit Daten-Exfiltration verbunden. Diese Datenbewegung ist oft die letzte Phase des Angriffs vor der Freisetzung der Ransomware.

- **Conti war im Jahr 2021 mit 18 Prozent aller Vorfälle die am häufigsten auftretende Ransomware-Gruppe.** Auf REvil-Ransomware entfiel einer von zehn Vorfällen. Andere verbreitete Ransomware-Familien sind DarkSide (die RaaS hinter dem berüchtigten Angriff auf Colonial Pipeline in den USA) und Black KingDom, eine der „neuen" Gruppierungen, die im März 2021 im Zuge der ProxyLogon-Schwachstelle auftauchte. Bei den 144 in der Analyse einbezogenen Vorfällen identifizierte Sophos 41 verschiedene Ransomware-Angreifer. Davon waren 28 neue Akteure, die erstmals im Jahr 2021 gesichtet wurden. Achtzehn Ransomware-Gruppen, die bei Vorfällen im Jahr 2020 auftraten, waren 2021 nicht mehr auf der Liste.

Warnsignale

„Zu den Warnsignalen, auf die Unternehmen achten sollten, gehört die Entdeckung eines legitimen Tools oder einer Kombination von Tools und Aktivitäten an einem unerwarteten Ort oder zu einer ungewöhnlichen Zeit", so Shier. „Es ist erwähnenswert, dass es auch Zeiten geben kann, in denen wenig oder gar keine Aktivitäten stattfinden. Das bedeutet aber nicht, dass ein Unternehmen nicht angegriffen wurde. Wahrscheinlich gibt es noch weitere ProxyLogon- oder ProxyShell-Einbrüche, die derzeit noch unbekannt sind. Auch hierbei werden Web-Shells und Backdoors für einen dauerhaften Zugriff implantiert, die bis zum Zeitpunkt der Zugriffsnutzung oder des Verkaufs unbemerkt bleiben. Verteidiger müssen bei verdächtigen Signalen wachsam sein und sofort Nachforschungen anstellen. Sie müssen kritische Fehler – vor allem in weit verbreiteter Software – beheben und vorrangig die Sicherheit von Fernzugriffsdiensten erhöhen. Solange die ungeschützten Zugangspunkte nicht geschlossen und alle Zugangs-Aktivitäten der Angreifer nicht vollständig beseitigt sind, kann so gut wie jeder nach Belieben eindringen und wird es wahrscheinlich auch tun."



Das Sophos Active Adversary Playbook 2022 basiert auf 144 Vorfällen aus dem Jahr 2021, die auf Unternehmen aller Größen und Branchen in den USA, Kanada, Großbritannien, Deutschland, Italien, Spanien, Frankreich, der Schweiz, Belgien, den Niederlanden, Österreich, den Vereinigten Arabischen Emiraten, Saudi-Arabien, den Philippinen, den Bahamas, Angola und Japan abzielten. Die am stärksten vertretenen Sektoren sind das verarbeitende Gewerbe (17 Prozent), gefolgt vom Einzelhandel (14 Prozent), dem Gesundheitswesen (13 Prozent), der IT (9 Prozent), dem Baugewerbe (8 Prozent) und dem Bildungswesen (6 Prozent).
Ziel des Sophos-Reports ist es, dass Sicherheitsteams verstehen, wie Cyber-Kriminelle bei Angriffen vorgehen und wie sie schädliche Aktivitäten im Netzwerk erkennen und abwehren können. Mehr über das Verhalten, die Tools und Techniken von Angreifern sind ausführlich im Sophos Active Adversary Playbook 2022 auf Sophos News zu lesen.

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 Anwendern 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 http://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