Neuer Sophos Incident-Response-Almanach: Cybergangster verweilen durchschnittlich 11 Tage lang unentdeckt in Netzwerken

*Sophos veröffentlicht neues „Active Adversary Playbook 2021“ mit Telemetriedaten seines MTR- und Rapid-Response-Teams: Hacker verwendeten mehr als 400 unterschiedliche Tools und Techniken, i*n 81 Prozent der Vorfälle war Ransomware im Spiel und in 69 Prozent der Angriffe wurde das Remote-Desktop-Protokoll (RDP) für Schleichfahrten verwendet.

Sophos hat heute sein “Active Adversary Playbook 2021“ veröffentlicht. Hierin werden das Verhalten sowie Tools, Techniken und Verfahren (TTPs) der Angreifer beschrieben, wie die Sophos-Bedrohungsjäger und -analysten sie im Jahr 2020 bis einschließlich Frühjahr 2021 beobachten konnten. Das Playbook basiert dabei auf Telemetriedaten sowie 81 Untersuchungen konkreter Vorfälle durch das Sophos Managed Threat Response (MTR)-Team sowie das Sophos Rapid-Response-Team. Ziel des neuen Almanachs ist es, Sicherheitsteams dabei zu unterstützen, Angriffstaktiken besser zu verstehen sowie schädliche Aktivitäten in Netzwerken effektiver zu erkennen und abzuwehren.

Die Ergebnisse zeigen unter anderem, dass die Angreifer vor der Entdeckung durchschnittlich elf Tage im Netzwerk verweilten, der längste unentdeckte Einbruch dauerte sogar 15 Monate. In 81 Prozent der Vorfälle war Ransomware im Spiel und in 69 Prozent der Angriffe wurde das Remote-Desktop-Protokoll (RDP) für die laterale Infiltrierung des Netzwerks genutzt.

Zu den wichtigsten Erkenntnissen des Reports gehören:

Die durchschnittliche Verweildauer der Angreifer vor der Entdeckung betrug 11 Tage.
Um dies in einen Kontext zu setzen: elf Tage bieten Angreifern potenziell 264 Stunden für kriminelle Aktivitäten wie Zugangsdatendiebstahl oder Datenexfiltration. In Anbetracht dessen, dass einige dieser Aktivitäten nur wenige Minuten oder Stunden in Anspruch nehmen, sind 11 Tage unendlich viel Zeit, um im Netzwerk eines Unternehmens Schaden anzurichten. Ausnahme: Angriffe mit traditioneller Ransomware zeigten in der Regel eine kürzere Verweildauer, da es hierbei nur um Zerstörung geht.

Bei 90% der untersuchten Angriffe spielte das Remote Desktop Protocol (RDP) eine Rolle.
Zusätzlich nutzten die Angreifer in 69 Prozent aller Fälle RDP für das unerkannte Bewegen im Netzwerk. Sicherheitsmaßnahmen für RDP wie VPNs oder Multifaktor-Authentifizierung konzentrieren sich in der Regel auf den Schutz des externen Zugriffs. Sie funktionieren jedoch nicht, wenn sich der Angreifer bereits innerhalb des Netzwerks befindet. In der Folge setzen Angreifer bei aktiven, tastaturgesteuerten Angriffen, z.B. mit Ransomware, RDP zur Infiltrierung eines Systems immer häufiger ein..

Unter den fünf am häufigsten genutzten Tools zeigen sich interessante Zusammenhänge.
Wenn zum Beispiel PowerShell in einem Angriff verwendet wird, ist auch Cobalt Strike in 58 Prozent der Fälle, PsExec in 49 Prozent, Mimikatz in 33 Prozent und GMER in 19 Prozent mit von der Partie. Cobalt Strike und PsExec werden in 27 Prozent der Angriffe zusammen verwendet, während Mimikatz und PsExec in 31 Prozent der Angriffe gemeinsam auftreten. Schließlich tritt die Kombination aus Cobalt Strike, PowerShell und PsExec in 12 Prozent aller Angriffe auf. Solche Korrelationen sind wichtig, da ihre Erkennung als Frühwarnung eines

bevorstehenden Angriffs dienen oder das Vorhandensein eines aktiven Angriffs bestätigen kann.

Ransomware war in 81 Prozent der von Sophos untersuchten Angriffe involviert.
Erst die tatsächliche Ransomware-Aktivierung ist oft der Moment, an dem ein Angriff für ein IT-Sicherheitsteam erstmals sichtbar wird. Wenig überraschend ist also, dass die überwiegende Mehrheit der durch Sophos dokumentierten Vorfälle Ransomware betraf. Zu den anderen Angriffstypen gehörten u.a. reine Datenexfiltration, Cryptominer, Banking-Trojaner sowie Pen-Test-Attacken.

Gut und Böse sind nicht immer leicht zu unterscheiden
„Die Bedrohungslandschaft wird immer unübersichtlicher und komplexer. Die Cyberkriminellen starten ihre Angriffe mit den unterschiedlichsten Fähigkeiten und Ressourcen, von Skript-Kiddies bis hin zu staatlich unterstützten Hackergruppen. Das macht die Arbeit für Verteidiger schwierig“, sagt John Shier, Senior Security Advisor bei Sophos. „Im letzten Jahr hat unser Incident-Response-Team geholfen, Angriffe zu neutralisieren, die von verschiedensten Angriffsgruppen mit mehr als 400 verschiedenen Tools durchgeführt wurden.“

Viele dieser Tools werden auch von IT-Administratoren und Sicherheitsexperten für ihre täglichen Aufgaben verwendet und es ist eine Herausforderung, rechtzeitig den Unterschied zwischen gutartigen und bösartigen Aktivitäten auszumachen. Besonders vor dem Hintergrund, dass Angreifer ihre Aktivitäten im Durchschnitt elf Tage im Netzwerk durchführen, während sie sich in die routinemäßigen IT-Aktivitäten einmischen, ist es laut Shier wichtig, dass Verteidiger die Warnzeichen kennen, auf die sie achten und denen sie nachgehen müssen. So sollte beispielsweise Alarmstufe Rot herrschen, wenn ein legitimes Tool oder eine bekannte Aktivität an einem unerwarteten Ort oder zu einer außergewöhnlichen Zeit entdeckt wird. Shier weiter: „Technologie kann heutzutage viel bewirken, aber in der aktuellen Bedrohungslandschaft sind menschliche Erfahrung und die Fähigkeit, individuell zu reagieren, ein wichtiger Teil jeder Sicherheitslösung.“

Weitere Themen im „Active Advisory Playbook 2021“ sind die am häufigsten verwendeten Angriffstechniken und -taktiken, die frühesten Anzeichen eines Angriffs, die am meisten beobachteten Bedrohungstypen sowie die am häufigsten identifizierten Hackergruppen..

Das komplette „Active Adversary Playbook 2021“ gibt es hier zum Nachlesen: https://bit.ly/3hu0uOb

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

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