Neues Sophos X-Ops Active Adversary Whitepaper: Mehrfachangriffe machen Schule – *Hive, LockBit und BlackCat Ransomware-Banden greifen nacheinander dasselbe Netzwerk an*

Die angegriffene Organisation erhielt drei verschiedene Ransomware-Meldungen für dreifach verschlüsselte Dateien.
Mehrfachangriffe scheinen insgesamt zu einem Trend zu werden.

Wiesbaden, 09. August 2022 – Im aktuellen Sophos X-Ops Active Adversary Whitepaper "Multiple Attackers: A Clear and Present Danger" berichtet Sophos, dass die drei bekannten Ransomware-Gruppen Hive, LockBit und BlackCat, nacheinander dasselbe Netzwerk angegriffen haben. Die ersten beiden Angriffe erfolgten innerhalb von zwei Stunden, der dritte Angriff fand zwei Wochen später statt. Jede Ransomware-Gruppe hinterließ ihre eigene Lösegeldforderung und einige der Dateien waren dreifach verschlüsselt.

„Es ist schon schlimm genug, eine einzige Ransomware-Meldung von einer Cyberkriminellen-Gruppe zu erhalten, ganz zu schweigen von gleich dreien", sagt John Shier, Senior Security Advisor bei Sophos. „Mehrere Angreifer schaffen eine ganz neue Ebene der Komplexität für die Wiederherstellung, insbesondere wenn Dateien dreifach verschlüsselt sind. Cybersicherheit mit Prävention, Erkennung und Reaktion ist für Unternehmen jeder Größe und Art von entscheidender Bedeutung – kein Unternehmen ist vor Angriffen gefeit."

In dem Whitepaper werden weitere Fälle von sich überschneidenden Cyberangriffen beschrieben, darunter Kryptominers, Remote-Access-Trojaner (RATs) und Bots. Wenn in der Vergangenheit mehrere Angreifer auf ein und dasselbe System abzielten, erstreckten sich die Angriffe in der Regel über viele Monate oder mehrere Jahre hinweg. Die im aktuellen Sophos Whitepaper beschriebenen Attacken fanden innerhalb weniger Tage und Wochen statt – in einem Fall sogar gleichzeitig. Oft werden die Organisationen von den Angreifenden über denselben verwundbaren Einstiegspunkt in das Netzwerk attackiert.

Von Konkurrenz zu vorsichtiger Kooperation zwischen den Cybergangstern
Normalerweise konkurrieren Cyberkriminelle, was es für mehrere Angreifer schwieriger macht, gleichzeitig zu operieren. Meist eliminieren sie ihre Konkurrenten auf demselben System. Die heutigen RATs weisen in kriminellen Foren häufig auf die Möglichkeit des Bot-Killings hin. Bei dem Angriff, an dem die drei Ransomware-Gruppen beteiligt waren, löschte BlackCat als letzte Ransomware-Gruppe auf dem System nicht nur Spuren ihrer eigenen Aktivitäten, sondern auch die von LockBit und Hive. In einem anderen Fall wurde ein System von LockBit-Ransomware infiziert. Etwa drei Monate später gelang es Mitgliedern von Karakurt Team, einer Gruppe mit Verbindungen zu Conti, die von LockBit geschaffene Hintertür zu nutzen, um Daten zu stehlen und Lösegeld zu verlangen.

„Im Großen und Ganzen scheinen sich Ransomware-Gruppen nicht offen feindlich gegenüberzustehen. Tatsächlich verbietet LockBit seinen Mitgliedern nicht ausdrücklich, mit Konkurrenten zusammenzuarbeiten", sagt Shier. „Wir haben keine Beweise für eine Zusammenarbeit. Aber es ist möglich, dass Angreifer erkennen, dass es in einem zunehmend umkämpften Markt nur eine begrenzte Anzahl von Angriffszielen gibt. Oder sie glauben, je mehr Druck auf ein Ziel ausgeübt wird, beispielsweise durch mehrere Angriffe, desto wahrscheinlicher ist es, dass die Opfer zahlen. Vielleicht führen sie Gespräche auf hoher Ebene und treffen Vereinbarungen, die für beide Seiten vorteilhaft sind, etwa dass eine Gruppe

die Daten verschlüsselt und die andere exfiltriert. Irgendwann müssen diese Gruppen entscheiden, ob sie zusammenarbeiten und dieses Vorgehen weiter ausbauen, oder ob sie mehr auf Wettbewerb setzen. Im Moment aber ist das Spielfeld für mehrere Angriffe durch verschiedene Gruppen offen."

Das alte Leid: Nicht gepatchte Sicherheitslücken als Einfallstore
Bei den im Whitepaper beschriebenen Angriffen erfolgten die meisten Erstinfektionen über nicht gepatchte Sicherheitslücken. Dazu gehören Lücken in Log4Shell, ProxyLogon und ProxyShell oder schlecht konfigurierte beziehungsweise ungesicherte RDP-Server (Remote Desktop Protocol). In den meisten Fällen, in denen mehrere Angreifer beteiligt waren, gelang es den Opfern nicht, den ursprünglichen Angriff wirksam zu beheben, so dass die Tür für künftige cyberkriminelle Aktivitäten offenstand. Damit wurden die gleichen RDP-Fehlkonfigurationen sowie Anwendungen wie RDWeb oder AnyDesk zu einem leicht ausnutzbaren Weg für Folgeangriffe. Ungeschützte oder manipulierte RDP- und VPN-Server gehören zu den beliebtesten „Angeboten“, die im Dark Web verkauft werden.

„Im aktuellen Active Adversary Playbook stellt Sophos für das Jahr 2021 fest, dass Unternehmen gleichzeitig mehrfach angegriffen werden und dass dies ein wachsender Trend sein könnte", sagt Shier. „Die Tatsache, dass die Zunahme von Mehrfachangriffen aktuell noch auf Basis einzelner Fälle nachvollzogen werden muss, gibt Cyberkriminellen reichlich Gelegenheit, sich über die ausnutzbaren Systeme noch weiter in diese Richtung zu bewegen."

Um mehr über multiple Cyberangriffe zu erfahren, einschließlich Details über den kriminellen Untergrund sowie praktischer Ratschläge zum Schutz von Systemen vor solchen Angriffen, steht das vollständige Whitepaper „Multiple Attackers: A Clear and Present Danger" auf Sophos.com zum Download bereit.

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