Neue Ransomware-Attacke nutzt bekanntes Remote-Access-Programm aus

Die Ransomware-Gruppe „Mad Liberator“ nutzt Anydesk als Brücke, um in Unternehmensnetzwerke zu gelangen. Sophos X-Ops deckt Details zum Angriff auf und gibt Hinweise für mehr Schutz vor diesen Attacken.

Das Sophos X-Ops Incident-Response-Team hat die Taktiken der Ransomware-Gruppe „Mad Liberator“ untersucht. Bei dieser Gruppe handelt es sich um einen neuen Bedrohungsakteur, der erstmals Mitte Juli 2024 auf der Bildfläche erschien. Im neuen Report „Don’t get Mad, get wise“ befasst sich Sophos X-Ops mit den Angriffstechniken dieser Gruppe im Zusammenhang mit der beliebten Remote-Access-Anwendung Anydesk. Zudem geben die Security-Spezialisten Tipps, wie Unternehmen das Risiko, Opfer dieser Art von Attacken zu werden, minimieren können.

Angriffsmuster
Im aktuellen Fall haben die Angreifer die legitime Software Anydesk missbraucht, im Prinzip könnte aber jedes andere Remote-Access-Programm ebenso für die kriminellen Zwecke von „Mad Liberator“ in die Schusslinie gelangen.
Die Fernwartungssoftware weist jedem Gerät, auf dem die Anwendung installiert wird, eine eindeutige ID zu, in diesem Fall eine zehnstellige Adresse. Sobald die Anwendung auf einem Gerät installiert ist, kann ein Benutzer den Zugriff auf ein entferntes Gerät anfordern, um die Kontrolle mit Hilfe der ID zu übernehmen. Wahlweise kann ein Benutzer einen anderen Benutzer einladen, die Kontrolle über sein Gerät zu übernehmen.

Sobald der Angreifer eine Anydesk-Verbindungsanfrage sendet, findet folgender Ablauf statt:
• Das Opfer erhält ein Popup-Fenster, in dem es aufgefordert wird, die Verbindung zu autorisieren. Für Benutzer, deren Organisationen Anydesk nutzen, erscheint dies möglicherweise nicht ungewöhnlich
• Nachdem eine Verbindung hergestellt wurde, überträgt der Angreifer eine Binärdatei auf das Gerät des Opfers. Diese Datei zeigt einen Bildschirm an, der ein Windows Update nachahmt; in der Zwischenzeit deaktiviert der Angreifer die Eingabe über Tastatur und Maus des Benutzers, sodass dieser die Aktivitäten, die der Angreifer im Hintergrund ausführt, nicht wahrnimmt (und nicht stoppen kann).
• Der Angreifer greift dann auf das OneDrive-Konto des Opfers zu und nutzt die Anydesk-FileTransfer-Funktion, um Unternehmensdateien zu exfiltrieren, bevor er nach anderen Geräten im selben Subnetz sucht, die ausgenutzt werden können
• Während das Opfer von dieser Hintergrundoperation nichts mitbekommt, aktiviert der Angreifer im Anschluss mehrere Lösegeldforderungen auf dem befallenen Rechner, in denen er ankündigt, dass die Daten gestohlen wurden, und wie das Lösegeld gezahlt weren muss, um die Offenlegung der gestohlenen Dateien zu verhindern.

Zum jetzigen Zeitpunkt ist nicht eindeutig geklärt, ob oder wie Angreifer eine bestimmte Anydesk-ID abgreifen. Theoretisch wäre es möglich, die Adressen so lange durchzuspielen, bis ein Rechner eine Verbindungsanfrage annimmt – bei potenziell 10 Milliarden 10-stelligen Nummern erscheint dies jedoch ineffizient. Im Fall, den das Sophos Incident-Response Team untersuchte, wurden keine Hinweise auf einen Kontakt zwischen den Mad-Liberator-Angreifern und dem Opfer identifiziert, bevor das Opfer eine unaufgeforderte Anydesk-Verbindungsanfrage erhielt. Soweit die Ermittler feststellen konnten, war der Angriff nicht mit zusätzlichen Social-Engineering-Maßnahmen der Angreifer verbunden – es wurden keine E-

Mail-Kontakte, Phishing-Versuche oder Ähnliches festgestellt. Bei dem Benutzer handelte es sich um keinen prominenten oder öffentlich sichtbaren Mitarbeiter und es gab keinen nachvollziehbaren Grund, warum er gezielt angegriffen werden sollte.

Maßnahmen, um diese Angriffe zu vermeiden
Beim analysierten „Mad Liberator"-Angriff im Zusammenhang mit Anydesk handelte es sich um eine unkomplizierte Attacke. Das Opfer glaubte, dass die Anydesk-Anfrage zu den alltäglichen Aktivitäten gehört. „Dieser Vorfall unterstreicht einmal mehr die Relevanz und Tragweite von kontinuierlichen Schulungen zu aktuellen Angriffsmustern", so Michael Veit, Cybersecurity-Experte bei Sophos. „Unternehmen sollten klare Richtlinien festlegen, wie IT-Abteilungen Remote-Sitzungen organisieren und auf jeden Fall
die Anydesk-Zugangskontrolllisten nutzen. Damit ist gewährleistet, dass nur Verbindungen von definierten Geräten zugelassen sind. Unabhängig davon, wie die Angreifer an die Verbindungs-ID kommen oder ob menschliche Fehler passieren, indem eine Verbindung arglos bestätigt wird, kann mit den Zugangskontrolllisten das Risiko stark minimiert werden." Zudem bietet Anydesk Anleitungen und Hinweise für weitere Sicherheitsmaßnahmen.

Veit weiter: „Es kann eine schwierige Aufgabe sein, bei der Implementierung von Tools die Sicherheit und Benutzerfreundlichkeit abzuwägen – vor allem wenn diese Tools den Fernzugriff für genau die Personen erleichtern sollen, die mit der Betreuung geschäftskritischer Systeme betraut sind. Es empfiehlt sich daher, dass bei der Implementierung von Fernzugriffsapplikationen die Sicherheitsempfehlungen des Herstellers sorgfältig geprüft werden. Können diese Empfehlungen nicht befolgt werden, sollte diese Entscheidung im Rahmen des Risikomanagementprozesses im Unternehmen dokumentiert sein. Damit können Administratoren kontinuierlich die Verbindungen prüfen oder andere Abhilfemaßnahmen treffen, damit die Risikobereitschaft des Unternehmens innerhalb des gesteckten Rahmens bleibt."

Den kompletten Bericht mi„Don't get Mad, get wise" mit verschiedenen Screenshots zur Veranschaulichung kann hier nachgelesen werden: https://news.sophos.com/en-us/2024/08/13/dont-get-mad-get-wise/

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

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