Das Problem ungenutzter und vergessener Tools – Chronologie eines Angriffs mit Midas Ransomware

Das Sophos Rapid-Response-Team beschreibt, wie Cyberkriminelle in einem realen Midas-Angriffsfall vorgegangen sind und wie sie sich von Oktober bis Dezember 2021 im Netzwerk via kommerzieller Tools bewegten, bevor sie schlussendlich die Ransomware-Attacke starteten. Mit einem integrierten Security-Ökosystem und mit Zero Trust wäre es den Angreifern kaum möglich gewesen, das Netzwerk zu infiltrieren und das angegriffene Unternehmen hätte eine größere Kontrolle über unautorisierte Netzwerkzugriffe gehabt.

Nach einer Ransomware-Attacke auf einen Technologieanbieter im Dezember 2021 wurde das Sophos Rapid-Response-Team zur Hilfe gerufen. Die forensischen Erkenntnisse zeigen, dass mindestens zwei verschiedene kommerzielle Remote-Access-Tools und ein Open-Source-Windows-Dienstprogramm für den Angriff mit der eher weniger bekannten Ransomware Midas zum Einsatz kamen. Die Experten entdeckte bei ihrer Analyse zudem Hinweise darauf, dass die Angreifer mindestens zwei Monate vor dem Auftreten der Ransomware auf einem Domain Controller und anderen Computern im Netzwerk aktiv waren. Dies entspricht einer klassischen Ereigniskette, die mit einer durchgängigen Security-Strategie und mit Zero Trust vermutlich hätte verhindert werden können.

Eine typische IT-Struktur birgt Risiken
Das angegriffene Unternehmen betrieb eine IT- und Sicherheits-Infrastruktur, wie sie tausendfach anzutreffen ist. Zum Einsatz kam Citrix zur Virtualisierung der Mitarbeiter-Desktops. Die Netzwerktopologie war flach organisiert, wobei das gesamte Netzwerk über das VPN zugänglich war. Die meisten physischen Geräte bestanden aus Windows-Servern, auf denen virtuelle Maschinen ausgeführt wurden. Es existierte keine Segmentierung des Netzwerks. Alles in allem eine typische Infrastruktur, die einen Cyberangriff vergleichsweise einfach macht.

Verlauf der Attacke
Der Angriff erfolgte mit multiplen Aktionen der Bedrohungsakteure, indem sie Windows-Dienste für die Ausführung mehrerer PowerShell-Skripte auf jeweils einer Maschine erstellten, die wiederum andere Maschinen auf diesem Weg in ihre Attacke einbezogen. Damit gelang es ihnen auf jede andere Maschine, unabhängig ob Server oder VM, über SMB-Protokoll zuzugreifen.
In einer Zero-Trust-Umgebung hätten ordnungsgemäß konfigurierte Zugriffskontrollen die Angreifer daran hindern können, einen kompromittierten Computer gegen einen anderen einzusetzen.

Die Forensik konnte im Nachhinein die vermutlich erste Kompromittierung auf den 13. Oktober datieren. Erst am 7. Dezember begannen die Angreifer mit der Verteilung der Ransomware-Binärdatei auf die Computer im Netzwerk. Die Eindringlinge waren folglich über zwei Monate unbemerkt. Sie führten Befehle aus, starteten interne RDP-Verbindungen, nutzten bereits installierte kommerzielle Fernzugriffssoftware, exfiltrierten Daten in die Cloud und verschoben Dateien auf und von einem der Domänencontroller des Ziels.

Das Problem ungenutzter und vergessener Tools
Midas ist zwar keine der prominenten Bedrohungen wie einige der anderen Ransomware-Familien, aber die Angreifer:innen schienen während des gesamten Vorfalls nach einem bekannten Schema vorzugehen. Sie nutzten herkömmliche Windows-Verwaltungstools und -

Prozesse (z. B. PowerShell und das Deployment Image Servicing and Management Tool) sowie kommerzielle Fernzugriffstools (AnyDesk und TeamViewer), bei denen die Wahrscheinlichkeit, dass sie einen Anti-Malware-Alarm auslösen, geringer ist.
Bei diesem Vorfall hatte das IT-Team des Unternehmens AnyDesk, TeamViewer sowie verschiedene andere Fernzugriffstools getestet. Zwar kamen die Tools schlussendlich nicht zum Einsatz, allerdings bleiben sie auf diverseren Servern ungenutzt installiert, was die Cyberkriminellen zu ihrem Vorteil nutzen. In einigen Fällen setzten sie auch das Open-Source-Tool Process Hacker ein, um die vom angegriffenen Unternehmen eingesetzten Endpoint-Security-Produkte zu identifizieren und zu umgehen.

Ein Security-Ökosystem mit Zero Trust hätte geschützt
"Dies ist ein gutes Beispiel dafür, was sehr vielen Unternehmen passieren kann, weil sie so oder so ähnlich ihre IT betreiben. Unternehmensnetzwerke hauptsächlich nach außen abzuschirmen, ist in Verbindung mit einem integrierten Security-Ökosystem sicherlich eine wirksame Schutzmethode. Allerdings hat auch dieser perimeterbasierte Ansatz zunehmend mehr Lücken. Mitarbeiter:innen arbeiten immer öfter mobil, auch über andere Netzwerke. Hinzu kommen Software-as-a-Service-Anwendungen (SaaS), Cloud-Plattformen und cloudbasierte Services. Es gibt kaum noch das eine Unternehmensnetzwerk, in dem alle darin eingebundenen Systeme sicher sind. Hier kommt das Zero-Trust-Konzept – also nichts und niemandem zu vertrauen und alles zu überprüfen – ins Spiel," sagt Michael Veit, Security-Experte bei Sophos.

Detaillierte und technische Details gibt es in englische Sprache hier:
https://news.sophos.com/en-us/2022/01/25/windows-services-lay-the-groundwork-for-a-midas-ransomware-attack/

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