"Admins sollten den Exchange Server auf Web-Shells scannen und Server auf ungewöhnliche Prozesse überwachen, die scheinbar aus dem Nichts auftauchen. Eine hohe Prozessorauslastung durch ein unbekanntes Programm könnte ein Zeichen für Krypto-Mining-Aktivitäten oder Ransomware sein."
Andrew Brandt, Principal Threat Researcher, Sophos

SophosLabs warnt: Angreifer nutzen Exchange-Schwachstelle für Kryptominer – Unternehmen sollten wachsam sein

Die bekannten, jüngsten Probleme rund um die Microsoft Exchange Server-Schwachstellen sind wohl noch lange nicht endgültig vom Tisch:
Auch nach den Sicherheits-Patches vom 2. und 9. März nutzen immer neue Angreifer den Exploit für ihre Attacken aus.

SophosLabs hat nun einen unbekannten Angreifer ausfindig gemacht, der die „ProxyLogon"-Schwachstelle nutzt, um einen Kryptominer zu installieren, der die noch nicht gepatchten Server angreift. Der „Schürfer" gehört zur Familie des legitimen Open-Source-Monero-Miners xmr-stak.

Andrew Brandt, Principal Threat Researcher bei Sophos, verrät weitere Details der Kryptominer-Attacke:

„Unsere Analyse dieser Kampagne zeigt, dass am 9. März Mining-Werte in die Monero-Wallets der Angreifer flossen und die Attacke danach schnell an Umfang verlor. Dies deutet darauf hin, dass wir es hier mit einem weiteren schnell zusammengestellten, opportunistischen und möglicherweise experimentellen Angriff zu tun haben, der versucht, etwas leichtes Geld abzugreifen, bevor ein weitverbreitetes Patching stattfindet. Unternehmen sollten nicht nur ihre Server umgehend patchen, sondern diese auch weiterhin aufmerksam überwachen. Für die meisten Opfer ist das erste Anzeichen einer Kompromittierung wahrscheinlich ein signifikanter Abfall der Verarbeitungsleistung. Server, die nicht gepatcht sind, können bereits seit einiger Zeit kompromittiert sein, bevor dies deutlich wird. Admins sollten den Exchange Server auf Web-Shells scannen und Server auf ungewöhnliche Prozesse überwachen, die scheinbar aus dem Nichts auftauchen. Eine hohe Prozessorauslastung durch ein unbekanntes Programm könnte ein Zeichen für Krypto-Mining-Aktivitäten oder Ransomware sein."

Weitere Informationen zum Vorgehen der Angreifer gibt es im ausführlichen Artikel „Compromised exchange server hosting cryptojacker targeting other exchange servers".

https://news.sophos.com/en-us/2021/04/13/compromised-exchange-server-hosting-cryptojacker-targeting-other-exchange-servers/

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