



Aufgedeckte Schleichfahrt: Analyse einer modernen „Musterattacke“



Bereits im April dieses Jahres wurde eine neue Ransomware-Gruppe namens „Money Message“ aktiv. Während die Cyberkriminellen bislang unter dem Radar flogen, konnte Sophos X-Ops die Aktivitäten der Cyberkriminellen nun bei der mit der Untersuchung eines Angriffs auf eine australische Organisation näher unter die Lupe nehmen. Die Gruppierung liefert ein Musterbeispiel für eine mittlerweile sehr weit verbreitete Angriffsvariante: die Schleichfahrt durch gekaperte Firmennetzwerke auf verschiedenste Weise, um der Erkennung und Eliminierung zu entgehen. So wurden zum Beispiel bei 78 Prozent der im ersten Halbjahr 2023 analysierten Fälle des Sophos Incident Response Teams interne RDP-Dienste von Cyberkriminellen für ihre Zwecke missbraucht.

In diesem speziellen Fall nutzte Money Message eine anfällige VPN-Verbindung, um Zugriff auf das Netzwerk zu erhalten. Anschließend bewegten sie sich lateral im Netzwerk, indem sie das vom Unternehmen verwendete Remote Desktop Protocol (RDP) nutzten. Zudem war es den Angreifern möglich, Windows Defender zu deaktivieren und sich Zugriff auf verschiedene Anmeldeinformationen der Organisation zu verschaffen, ehe sie begannen, sensible Daten abzuschöpfen.

Alle Details zur Attacke und Tipps zu Verhinderung solcher Verschleierungsangriffe gibt der englische Untersuchungsbericht [„Step by step through the money message ransomware“](#).

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, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lucht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de