Angreifer missbrauchen Forensik-Tool für Ransomware-Versuch

Sophos-Analysten stoppten Angriff über das Open-Source-Programm Velociraptor, das als Deckmantel für die Cyberkriminellen dienen sollte

Das Counter Threat Unit™ (CTU) Team von Sophos hat einen Cyberangriff vereitelt, bei dem Kriminelle ein eigentlich seriöses Open-Source-Programm für digitale Forensik, Velociraptor, missbrauchten. Statt es wie vorgesehen für Sicherheitsanalysen einzusetzen, nutzten die Täter das Tool, um sich verdeckt Zugang zu einem Unternehmensnetzwerk zu verschaffen und weitere Schadsoftware nachzuladen. Ziel war offenbar ein Ransomware-Angriff.

So gingen die Angreifer vor
Die Kriminellen installierten das Tool über eine präparierte Cloud-Domain und luden zusätzlich eine manipulierte Version einer Entwickler-Software herunter. Diese sollte einen versteckten Fernzugang schaffen und weitere Programme nachziehen. Durch diese Tarnung wollten die Angreifer typische Sicherheitsmechanismen umgehen.

Taegis-Alarm verhinderte Schlimmeres
Eine ungewöhnliche Netzwerkaktivität löste einen Alarm im Sophos-Sicherheitssystem Taegis™ aus. Dadurch konnten Analysten das betroffene Gerät sofort isolieren und den Angriff stoppen, bevor er sich ausbreiten konnte.

Missbrauch legitimer IT-Programme nimmt zu
Die Sophos-CTU-Experten warnen, dass Angreifer zunehmend auf bereits vorhandene oder legitime Administrator- oder Sicherheitstools setzen, um unentdeckt zu bleiben. Im aktuellen Fall zeigt sich, dass selbst Incident-Response-Werkzeuge wie Velociraptor missbraucht werden können.

Empfehlungen für Unternehmen
Unternehmen sollten genau im Blick behalten, welche Tools in ihrem Netzwerk eingesetzt werden, und Auffälligkeiten sofort prüfen. Moderne Sicherheitslösungen wie Endpoint Detection & Response (EDR), konsequente Systempflege und regelmäßige Backups sind entscheidend, um Schäden zu verhindern oder im Ernstfall schnell reagieren zu können.

„Dass Angreifer sogar ein Sicherheits- und Forensik-Tool für ihre Zwecke missbrauchen, zeigt, wie raffiniert Cyberattacken inzwischen sind. Unternehmen müssen damit rechnen, dass selbst vermeintlich harmlose Anwendungen zu einem Einfallstor werden können. Entscheidend ist deshalb, ungewöhnliche Aktivitäten schnell zu erkennen und sofort zu handeln," erklärt Michael Veit, Security Experte bei Sophos.

Weitere technische Details zum Fall beschreibt das CTU-Team in seinem Blog-Artikel (in englischer Sprache).

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