KMUs im Fokus – Sophos veröffentlicht neuen Report zu LockBit-Ransomware

Sophos präsentiert seine neueste Studie zur LockBit-Ransomware. Zwei Techniken fallen dabei auf: Erstens, der Einsatz von automatisierten Tools, um bestimmte Steuer- und Buchhaltungssoftware in gehackten Netzwerken mit Ransomware zu infizieren und zweitens, das Umbenennen von PowerShell-Dateien zur eigenen Tarnung.

"LockBit-Angreifer nutzen automatisierte Angriffstools, um vielversprechende Ziele zu identifizieren", fasst Sean Gallagher, Senior Threat Researcher bei Sophos, zusammen. Die Analyse zeigt auf, wie die Kriminellen mit PowerShell-Tools nach bestimmten Geschäftsanwendungen in gehackten Netzwerken suchen, darunter Steuer- und Buchhaltungssoftware. Wenn ein durch diese Suche erzeugter Fingerabdruck den Schlüsselwort-Kriterien entspricht, führen die Tools automatisch eine Reihe von Aufgaben aus, darunter das Starten der LockBit-Attacke.

Die Forscher konnten auch eine Reihe neuer Angriffsmethoden identifizieren, mit denen LockBit der Entdeckung entgeht. Dazu gehören das Umbenennen von PowerShell-Dateien und die Verwendung eines Remote-Google-Dokuments für die Befehls- und Kontrollkommunikation. Aufgrund des hochgradig automatisierten Charakters der Angriffe kann sich die Ransomware, sobald sie einmal gestartet ist, innerhalb von fünf Minuten über das Netzwerk verbreiten und dabei gleichzeitig ihre Aktivitätsprotokolle löschen.

Neu: LockBit-Angreifer suchen gezielt nach kleineren Unternehmen als Opfer
"Das Interesse von LockBit an bestimmten Geschäftsanwendungen und Schlüsselwörtern deutet darauf hin, dass die Angreifer eindeutig Systeme identifizieren wollten, die für kleinere Unternehmen wertvoll sind – Systeme, die Finanzdaten speichern und das Tagesgeschäft abwickeln – um die Opfer massiv unter Druck zu setzen, zu zahlen ", so Gallagher. "Wir haben schon gesehen, wie Ransomware Geschäftsanwendungen bei der Ausführung stillgelegt hat, aber dies ist das erste Mal, dass Angreifer nach bestimmten Arten von Anwendungen mit einem automatisierten Ansatz suchen, um potenziell erfolgsversprechende Ziele zu identifizieren.“

LockBit-Gruppe folgt Ransomware-Fraktionen wie Ryuk
"Die LockBit-Bande scheint anderen Cybergangstergruppen zu folgen, darunter Ryuk. Über diese Gruppe hatte Sophos erst kürzlich herausgefunden, dass sie Cobalt Strike verwendet. Dabei handelt es sich um adaptierte Tools, die für Penetrationtests entwickelt wurden, um Angriffe zu automatisieren und zu beschleunigen. In diesem Fall helfen die PowerShell-Skripte den Angreifern dabei, Systeme zu identifizieren, auf denen Anwendungen mit besonders wertvollen Daten vorhanden sind. Sie wollen auf diese Weise ihre Zeit nicht mit Opfern verschwenden, die mit geringerer Wahrscheinlichkeit zahlen werden.“

Missbrauch legitimer Tools und Modifikation des Anti-Malware-Schutzes
Die LockBit-Angreifer versuchen, ihre Aktivitäten zu verbergen, indem sie sie wie normale, automatisierte Verwaltungsaufgaben aussehen lassen und legitime Tools nutzen: Die Kriminellen erstellen z.B. getarnte Kopien von Windows-Scripting-Komponenten und benutzen dann den Taskplaner von Windows, um sie zu starten. Zusätzlich modifizieren sie den eingebauten Anti-Malware-Schutz, so dass er nicht mehr funktionieren kann.

"Die einzige Möglichkeit, sich gegen diese Art von Ransomware-Angriffen zu verteidigen, ist eine mehrschichtige Verteidigung mit einer konsequenten Umsetzung des Malware-Schutzes über alle Systeme hinweg. Wenn Dienste ungeschützt bleiben oder falsch konfiguriert werden, können Angreifer sie leicht ausnutzen", resümiert Gallagher.

Der aktuelle Bericht setzt die intensive Beobachtung von LockBit fort, die Sophos im April 2020 veröffentlicht hat. Die Studie enthüllt das Innenleben der LockBit-Aktivitäten und zeigt, wie die Gruppierung neben Maze und REvil in das gezielte Erpressungsgeschäft expandiert. Die Studie enthüllt das Innenleben der LockBit-Aktivitäten und zeigt, wie die Gruppierung neben Maze und REvil in das gezielte Erpressungsgeschäft expandiert.

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, +49-1608449656
Ariane Wendt +49-172-4536839
sophos@tc-communications.de