Egregor-Ransomware unter der Lupe – der heimliche Erbe von Maze?

Seit September 2020 macht die Egregor-Ransomware ihre unheilvolle Runde durch die Netzwerke von Unternehmen und dabei mit ungewöhnlichen Methoden auf sich aufmerksam. Sophos Forscher haben sich angeschaut und zusammengefasst, wie die Angreifer dabei vorgehen.

Der Bericht "Egregor ransomware: Maze's heir apparent," stützt sich auf mehrere Vorfälle, an denen Egregor seit September beteiligt war. Sophos-Forscher fanden dabei unter anderem:

- Unterschiedliche Taktiken, Techniken und Prozeduren (TTPs) bei Angriffen verschiedener Urheber, die zeigen, wie sehr kriminelle RaaS-Kunden ihre Angriffsansätze variieren können und damit einen Abwehrschutz schwieriger machen
- Ähnlichkeiten mit Maze Ransomware, wie z. B. die Verwendung der ChaCha- und RSA-Verschlüsselungsalgorithmen
- Verbindungen zwischen Egregor und Sekhmet (Egregor ist eine Ableitung von Sekhmet)
- Ähnlichkeiten mit Ryuk-Ransomware-Angriffen. In einem vom Sophos Rapid Response-Team untersuchten Vorfall stimmen die Verwendung von Cobalt Strike, das Kopieren von Dateien in das Verzeichnis C: \ perflogs sowie die Verwendung von SystemBC - einem böswilligen Tor-Netzwerk-Proxy - mit dem beobachteten Verhalten während einer Ryuk-Attacke im September 2020 überein

Sean Gallagher, leitender Sicherheitsforscher bei Sophos erläutert:

„Die Ergebnisse zeigen, wie schwierig es für IT-Sicherheitsteams sein kann, sich gegen Ransomware-as-a-Service-Angriffe zu verteidigen, da Ransomware-Betreiber häufig auf mehrere Vertriebskanäle für Malware setzen, um ihre Opfer zu erreichen. Hierdurch entsteht ein vielfältigeres Angriffsprofil, das schwerer vorherzusagen ist."

Die Anzahl der Taktiken, Techniken und Prozeduren (TTPs), die von jedem Ransomware-Typ verwendet werden sind den Forschern zufolge deutlich gestiegen. Eine durchdachte Verteidigungsstrategie ist daher unerlässlich. „Angesichts der Tatsache, dass die Gruppe hinter Egregor behauptet, gestohlene Daten zu verkaufen, wenn Lösegeld nicht gezahlt wird, reicht es nicht aus, nur eine gute Sicherung der Organisationsdaten zu haben, um Ransomware zu entschärfen," so Gallagher weiter. „Das Blockieren gängiger Exfiltrationsrouten für Daten - beispielsweise das Verhindern von Tor-Verbindungen - kann das Stehlen von Daten erschweren." Die beste Verteidigung bestehe jedoch darin, zu verhindern, dass Angreifer überhaupt im Netzwerk Fuß fassen: „Eine gute Aufklärung der Mitarbeiter ist dafür ebenso wichtig wie der Einsatz eines Threat-Hunting-Expertenteams."

Den gesamten Bericht finden Sie in englischer Sprache hier:
Egregor ransomware: Maze's heir apparent

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