"Die Schöpfer von Gootkit haben den bekannten Banking-Trojaner zu einer komplexen Plattform für alle Arten von Argriffen einschließlich der Banking Malware Kronos und der Ransomware REvil weiterentwickelt. Dies zeigt deutlich, dass Cyberkriminelle dazu neigen, bewährte Angriffs-Tools wiederzuverwenden, anstatt aufwändig neue zu designen."
Gabor Szappanos, Threat Research Director bei Sophos

Aus „Gootkit" wird „Gootloader": Banking Trojaner mutiert zu komplexer Malware-Plattform mit multiplen Angriffsvektoren

Die Gootkit-Malware-Familie ist ein bekannter Scherge – ein Trojaner, der sich initial auf den Diebstahl von Bankgeschäftsdaten fokussiert und sich heute unter anderem des Analysetools Cobalt-Strike, der Banking Malware Kronos sowie der REvil-Ransomware bedient. IT-Security-Experten haben sich bereits 2020 intensiv mit der Schadsoftware und insbesondere ihrer geschickten Übermittlungsmechanismen beschäftigt. Neu ist nun, dass die Angreifer die Malware zu einer Multi-Payload-Plattform ausgebaut haben. Mit variablen Angriffsmechanismen – inklusive Social Engineering – ist sie heute am stärksten in Deutschland sowie in den USA und Südkorea aktiv. Aufgrund der Aktualität und des Plattform-Charakters haben die Security-Experten der SophosLabs der Multi-Payload-Malware einen eigenen Namen gegeben: Gootloader.

Die Gootloader-Angreifer hacken sich in legitime Webseiten, verändern diese subtil und manipulieren auch die SEO, um die gefälschten Webseiten den Nutzern als Top-Ergebnisse in ihren Suchmaschinenabfragen, wie zum Beispiel Google Search, anzuzeigen. Der gezielte Fokus auf bestimmte Länder geht neben den lokalisierten Fake-Webseiten sogar so weit, dass Nutzer von „Nicht-Ziel-Ländern", die auf solch einer Webseite landen, lediglich zufälligen Fake-Inhalte angezeigt bekommen und sonst nichts weiter passiert.

"Die Schöpfer von Gootloader verwenden eine Reihe von Social-Engineering-Tricks, die selbst technisch versierte IT-Anwender täuschen können. Allerdings existieren Warnzeichen, auf die man achten sollte", so Gabor Szappanos, Threat Research Director bei Sophos. „Dazu gehören Google-Suchergebnisse mit dem Verweis auf Webseiten, die in keinerlei logischem Zusammenhang mit den scheinbar angebotenen Ratschlägen stehen. Auffällig sind auch Tipps, die genau mit den Suchbegriffen übereinstimmen, die in der anfänglichen Frage verwendet wurden, sowie Seiten im Stil eines Forums."

Wer sich außerdem aktiv gegen Payloadsysteme wie Gootloader schützen will, kann die Funktion ‚Erweiterungen bei bekannten Dateitypen ausblenden' in den Ordneroptionen des Windows Explorers deaktivieren. Dadurch können Nutzer erkennen, dass das von den Angreifern gelieferte ZIP-Paket eine Datei mit .js-Endung enthält. Javascript.-Dateien werden immer wieder für Hackerangriffe verwendet und das Ausführen einer solchen heruntergeladenen Datei sollte immer die Alarmglocken klingeln lassen. Zusätzlich können Script-Blocker wie beispielsweise NoScript für Firefox für Sicherheit vor solchen Attacken sorgen, da sie den Fake-Inhalt einer gehackten Internetseite blocken."

Der komplette technische Report kann hier eingesehen werden: „Gootloader" expands its payload delivery options.

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