„RobbinHood“ hat aufgerüstet und macht sich im Windows-Kernel breit

Ransomware nutzt Hardwaretreiber mit Schwachstellen und entfernt Sicherheitssoftware

Sophos hat zwei Ransomware-Angriffe näher untersucht, bei denen die Gegner legitime, digital signierte Hardwaretreiber nutzen, um vor dem Start der Dateiverschlüsselung Sicherheitsprodukte vom angegriffenen Rechner zu löschen. Das perfide daran: Selbst vollständig gepatchte Computer, die keinerlei bekannte Schwachstellen haben, können von der neuen Attacke betroffen sein, da die Kriminellen ihr eigene Schwachstelle einfach mitbringen.

Der signierte Treiber als Ausgangspunkt der Attacke ist Teil eines inzwischen veralteten Softwarepakets, das vom taiwanesischen Motherboard Hersteller Gigabyte veröffentlicht wurde, und hat eine bekannte Schwachstelle (CVE-2018-19320).

Die im Jahr 2018 veröffentliche Verwundbarkeit wurde auf zahlreichen Plattformen publik gemacht, allerdings gleichzeitig vom Hersteller als irrelevant bezeichnet, da dessen Produkte angeblich nicht von den gemeldeten Sicherheitsanfälligkeiten betroffen seien. Das Unternehmen widerrief diese Aussage später und hat die Verwendung des anfälligen Treibers eingestellt. Allerdings ist die Software weiterhin über inoffizielle Kanäle im Umlauf und scheinbar eine reale Bedrohung. Umso mehr, da weder Microsoft noch Verisign, deren Codesignierungsmechanismen zum digitalen Signieren des Treibers verwendet wurde, die Zertifikate widerrufen haben, sodass diese weiterhin gültig sind. So können die Kriminellen im aktuellen Angriffsszenario den Gigabyte-Treiber als Türöffner verwenden, um einen weiteren, nicht signierten Treiber ins Windows-System einzuspeisen. Diese schadhafte Komponente beendet auf Kernel-Ebene unter Umgehung des Manipulationsschutzes Prozessen und Dateien, die zu Endpoint-Sicherheitsprodukten gehören, um die Basis für den dann folgenden Ransomware-Angriff zu liefern. Bislang war noch keine vollständig böswillige Verwendung des Treibers bekannt, allerdings wurde dessen Schwachstelle in den letzten Jahren u.a. dazu genutzt, um Antibetrugsmechanismen in Online-Spielen auszuhebeln.

„Dies ist das erste Mal, dass wir Ransomware beobachten, die einen von Microsoft mitsignierten und dennoch anfälligen Treiber nutzt, um den Windows Kernel direkt im Speicher zu überschreiben, einen eigenen, nicht signierten Treiber zu laden und dann Sicherheitsanwendungen aus dem Kernel zu entfernen“, so Michael Veit, IT-Security-Experte bei Sophos. „Die von den SophosLabs in beiden Fällen aufgedeckte Ransomware nennt sich selbst RobbinHood und hat bereits Ende letzten Jahres für Schlagzeilen gesorgt. Bei Sophos haben wir zum Schutz vor der Attacke den ungewöhnlichen Schritt unternommen, die anfällige Gigabyte-Treiberdatei gdrv.sys als bösartig zu klassifizieren, wenn sie im Kontext dieses Angriffs installiert wird. Dazu gehört die Verwendung mit den Pfaden desktop\robin\gdrv.sys oder \windows\temp\gdrv.sys.“

Detaillierte Informationen zu der neuen Hacking-Technik gibt es im englischsprachigen Blogartikel der SophosLabs:
https://news.sophos.com/en-us/2020/02/06/living-off-another-land-ransomware-borrows-vulnerable-driver-to-remove-security-software/

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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