Sophos entdeckt 100 schädliche Treiber, die vom Microsoft Windows Hardware Compatibility Publisher (WHCP) signiert wurden

Sophos X-Ops hat 133 bösartige Treiber entdeckt, die mit legitimen digitalen Zertifikaten signiert sind; 100 davon wurden vom Microsoft Windows Hardware Compatibility Publisher (WHCP) signiert. Den von WHCP signierten Treibern vertraut jedes Windows-System grundsätzlich, sodass Angreifer sie installieren können, ohne Alarm auszulösen und anschließend praktisch ungehindert böswillige Aktivitäten ausführen können.

Bei vielen der gefundenen Treiber (81) handelte es sich um sogenannte „EDR-Killer“, die speziell dafür entwickelt wurden, verschiedene EDR/AV-Software auf den Systemen der Opfer anzugreifen und zu beenden. Diese Treiber ähneln den bereits im Dezember 2022 von Sophos X-Ops entdeckten Treibern. Die restlichen Treiber – 32 davon wurden von WHCP signiert – waren Rootkits. Viele dieser Programme wurden entwickelt, um vertrauliche Daten, die über das Internet gesendet werden, heimlich zu überwachen. X-Ops hat die bösartigen Treiber nach der Entdeckung umgehend an Microsoft gemeldet und die Probleme wurden mit dem letzten Patch Tuesday behoben.

Alle Details zu der Untersuchung gibt es im englischsprachigen X—Ops-Blog-Artikel. Dieser Beitrag ist eine Fortsetzung eines Beitrags vom Dezember 2022, in dem Sophos, Mandiant und SentinelOne über die Signierung mehrerer Treiber durch Microsoft berichteten. Diese Treiber zielten speziell auf eine breite Palette von AV/EDR-Software ab.

Christopher Budd, Director Threat Research bei Sophos X-Ops, über die aktuelle Entwicklung: „Seit Oktober letzten Jahres beobachten wir einen besorgniserregenden Anstieg von Aktivitäten durch Kriminelle, die böswillig signierte Treiber ausnutzen, um verschiedene Cyberangriffe, einschließlich Ransomware, durchzuführen. Wir gingen damals davon aus, dass Angreifer diesen Angriffsvektor weiterhin ausnutzen würden, was sich nun bewahrheitet hat. Da Treiber häufig mit dem ‚Kern‘ des Betriebssystems kommunizieren und damit vor der Sicherheitssoftware geladen werden, können sie bei Missbrauch besonders wirksam bei der Deaktivierung von Sicherheitsmaßnahmen sein – insbesondere, wenn sie von einer vertrauenswürdigen Autorität signiert sind. Viele der von uns entdeckten bösartigen Treiber wurden speziell dafür entwickelt, EDR-Produkte anzugreifen und ‚auszuschalten‘, wodurch die betroffenen Systeme für eine Reihe bösartiger Aktivitäten anfällig werden. Es ist schwierig, eine Signatur für einen bösartigen Treiber zu erhalten, daher wird diese Technik vor allem von fortgeschrittenen Bedrohungsakteuren bei gezielten Angriffen eingesetzt. Darüber hinaus sind diese speziellen Treiber nicht herstellerspezifisch, sie zielen auf eine breite Palette von EDR-Software ab. Aus diesem Grund müssen sich alle IT-Security-Teams mit dem Thema auseinandersetzen und bei Bedarf zusätzliche Schutzmaßnahmen implementieren. Es ist wichtig, dass Unternehmen, die am Patch Tuesday von Microsoft bereitgestellten Patches implementieren.“

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/
Twitter: @sophos_info

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