Neue Spielart bei Ransomware-Attacken:
Sophos findet Schadcode in Treibern mit gültigen Zertifikaten

- Sophos vereitelt Ransomware-Angriff durch seltenen, bösartigen Treiber, der mit einem gültigen digitalen Zertifikat signiert ist
- Treiber zielt auf Endpoint Detection and Response (EDR)-Software ab
- Angriffe stehen in Verbindung mit der Cuba Ransomware Group

Sophos hat Schadcode in mehreren Treibern gefunden, die mit legitimen digitalen Zertifikaten signiert sind. Der neue Report „Signed Driver Malware Moves up the Software Trust Chain“ beschreibt die Untersuchung, die mit einem versuchten Ransomware-Angriff begann. Die Angreifer verwendeten einen bösartigen Treiber, der mit einem legitimen digitalen Windows Hardware Compatibility Publisher-Zertifikat von Microsoft signiert war.

Der maliziöse Treiber zielt speziell auf Prozesse ab, die von wichtigen Endpoint Detection and Response (EDR)-Softwarepaketen verwendet werden. Er wurde von einer Malware installiert, die mit Bedrohungsakteuren im Umfeld der Cuba Ransomware Goup in Verbindung gebracht wird – einer äußerst produktiven Gruppe, die im vergangenen Jahr weltweit mehr als 100 Unternehmen erfolgreich angegriffen hat. Sophos Rapid Response konnte den Angriff erfolgreich vereiteln. Diese Untersuchung löste eine umfassende Zusammenarbeit zwischen Sophos und Microsoft aus, um Maßnahmen zu ergreifen und die Bedrohung zu beseitigen.

Schadhafte Treiber mit gestohlenen Zertifikaten signiert
Treiber können hoch privilegierte Operationen auf Systemen durchführen. So können Kernel-Mode-Treiber unter anderem viele Arten von Software, einschließlich Sicherheitssoftware, beenden. Die Kontrolle darüber, welche Treiber geladen werden können, ist eine Möglichkeit, Computer vor dieser Art von Angriffen zu schützen. Windows verlangt, dass Treiber eine kryptografische Signatur - einen "Genehmigungsstempel" - tragen, bevor der Treiber geladen werden kann.

Allerdings sind nicht alle digitalen Zertifikate, die zum Signieren von Treibern verwendet werden, gleichermaßen vertrauenswürdig. Einige gestohlene und ins Internet gelangte digitale Signierzertifikate wurden später zum Signieren von Malware missbraucht; andere Zertifikate wurden von skrupellosen PUA-Softwareherstellern gekauft und verwendet. Sophos' Untersuchung eines schädlichen Treibers, der zur Sabotage von Endpoint Security-Tools während eines Ransomware-Angriffs verwendet wurde, ergab, dass die Angreifer konzertiert vorgingen, um sich von weniger vertrauenswürdigen zu immer vertrauenswürdigeren digitalen Zertifikaten zu bewegen.

Cuba höchstwahrscheinlich involviert
„Diese Angreifer, höchstwahrscheinlich Mitglieder der Ransomware-Gruppe Cuba, wissen, was sie tun - und sie sind hartnäckig“, sagt Christopher Budd, Senior Manager, Threat Research bei Sophos. „Wir haben insgesamt zehn bösartige Treiber gefunden, die alle Varianten der ursprünglichen Entdeckung sind. Diese Treiber zeigen ein konzertiertes Bestreben, in der Vertrauenswürdigkeit aufzusteigen, wobei der älteste Treiber mindestens bis Juli zurückreicht. Die ältesten Treiber, die wir bisher gefunden haben, waren mit Zertifikaten unbekannter chinesischer Unternehmen signiert. Danach haben sie es geschafft, den Treiber mit einem gültigen, durchgesickerten und widerrufenen NVIDIA-Zertifikat zu signieren. Jetzt verwenden sie ein legitimes Windows Hardware Compatibility Publisher Digital Zertifikat von Microsoft, einer der vertrauenswürdigsten Instanzen im Windows-Ökosystem. Wenn man aus der Sicherheitsperspektive eines Unternehmens betrachtet, haben die Angreifer gültige

Unternehmensausweise erhalten, um das Gebäude ohne Fragen zu betreten und zu tun, was sie wollen", so Christopher Budd weiter.

Eine genauere Untersuchung der ausführbaren Dateien, die bei dem versuchten Ransomware-Angriff verwendet wurden, ergab, dass der bösartige, signierte Treiber mit einer Variante des Loaders BURNTCIGAR auf das Zielsystem heruntergeladen wurde, einer bekannten Malware, die der Ransomware-Gruppe Cuba angehört. Sobald der Loader den Treiber auf das System heruntergeladen hat, wartet er darauf, dass einer von 186 verschiedenen Programmdateinamen, die üblicherweise von wichtigen Endpunktsicherheits- und EDR-Softwarepaketen verwendet werden, gestartet wird, und versucht dann, diese Prozesse zu beenden. Wenn dies gelingt, können die Angreifer die Ransomware einsetzen.

Aktueller Trend: Versuch alle gängigen DER-Produkte zu umgehen
„Im Jahr 2022 haben wir beobachtet, dass Ransomware-Angreifer zunehmend versuchen, die EDR-Produkte vieler, wenn nicht sogar der meisten großen Hersteller zu umgehen“, so Christopher Budd weiter. „Die gebräuchlichste Technik ist als 'Bring your own driver' bekannt, die BlackByte vor kurzem verwendet hat. Dabei nutzen die Angreifer eine bestehende Schwachstelle in einem legitimen Treiber aus. Es ist weitaus schwieriger, einen bösartigen Treiber von Grund auf neu zu erstellen und ihn von einer legitimen Behörde signieren zu lassen. Sollte dies jedoch gelingen, ist es unglaublich effektiv, da der Treiber beliebige Prozesse ausführen kann, ohne dass dies in Frage gestellt wird.“

Im Fall dieses speziellen Treibers ist praktisch jede EDR-Software anfällig. Glücklicherweise konnten die zusätzlichen Manipulationsschutzmaßnahmen von Sophos den Ransomware-Angriff stoppen. Die Sicherheits-Community muss sich dieser Bedrohung bewusst sein, damit sie zusätzliche Sicherheitsmaßnahmen implementieren kann. Es ist davon auszugehen, dass weitere Angreifer dieses Modell nachahmen werden.“

Sophos hat nach Entdeckung des Treibers umgehend mit Microsoft zusammengearbeitet, um das Problem zu beheben. Microsoft hat in seinem Sicherheitshinweis weitere Informationen veröffentlicht und im Rahmen des Patch Tuesday veröffentlicht.

Weitere Informationen zu diesem Thema finden Sie in dem Artikel „Signed Driver Malware Moves up the Software Trust Chain“ auf Sophos.com.

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