Hasta La Vista, Baby.
Das Terminator-Tool und seine Varianten haben noch lange nicht ausgedient

Report der Sophos Security-Spezialisten Andreas Klopsch und Matt Wixey beschreibt, wie Cyberkriminelle mithilfe des altbekannten Terminator-Tools anfällige Treiber einschleusen.

BYOVD (Bring Your Own Vulnerable Driver) stehen als EDR-Killer bei Bedrohungsakteuren nach wie vor hoch im Kurs. Ein Grund ist, dass hiermit ein Angriff auf Kernel-Ebene in Aussicht steht, was den Cyberkriminellen ein breites Spektrum an Handlungsmöglichkeiten einräumt – vom Verstecken von Malware über das Ausspähen von Anmeldedaten bis hin zum Versuch, die EDR-Lösungen zu deaktivieren. Die Sophos Security-Spezialisten Andreas Klopsch und Matt Wixey haben das Geschehen mit den Terminator-Tools während der letzten sechs Monate genau unter die Lupe genommen und im ausführlichen Report „It'll be back: Attackers still abusing Terminator tool and variants„ zusammengefasst.

Treiber-Schleusereien sind keine Frage des cyberkriminellen Könnens mehr
BYOVD ist eine Angriffsklasse, bei der Bedrohungsakteure bekannte und zugleich anfällige Treiber auf einen kompromittierten Computer einschleusen, um Rechte auf Kernel-Ebene zu erlangen. Bei der Wahl von anfälligen Treibern haben die Cyberkriminellen leichtes Spiel: Beispielsweise auf dem Open-Source-Repository loldrivers.io sind 364 Einträge für anfällige Treiber inklusive entsprechender Signaturen und Hashes aufgeführt. Dieses bequeme Identifizieren von geeigneten Treibern ist einer der Gründe, weshalb BYOVD-Angriffe heute nicht nur hoch professionellen Bedrohungsakteuren vorbehalten sind, sondern auch von weniger versierten Ransomware- Angreifern durchgeführt werden können.

Ein weiterer möglicher Grund für die anhaltende Beliebtheit von BYOVD bei technisch weniger kompetenten Cyberkriminellen ist die Tatsache, dass sie die benötigten Kits und Tools quasi von der Stange in kriminellen Foren erwerben können. Eines dieser Tools erregte im Mai 2023 besondere Aufmerksamkeit, als der bekannte Bedrohungsakteur "spyboy" im russischsprachigen Ransomware-Forum RAMP ein Tool namens Terminator anbot. Das Tool sollte zwischen 300 USD und 3.000 USD kosten und vierundzwanzig Sicherheitsprodukte deaktivieren können.

So können sich Unternehmen schützen
Viele der Security-Anbieter auf der Liste von spyboy, darunter auch Sophos, haben umgehend gehandelt, um Varianten von Treibern zu untersuchen und Schutzmaßnahmen zu entwickeln. Sophos empfiehlt vier wichtige Schritte, um sich vor BYOVD-Attacken zu schützen:

1. Prüfen, ob das Endpoint Security-Produkt einen Manipulationsschutz implementiert hat.
2. Umsetzung einer strengen Hygiene bei den Windows-Sicherheitsrollen, da BYOVD-Angriffe in der Regel durch Privilegienerweiterung und der Umgehung der UAC ermöglicht wird.
3. Alle Betriebssysteme und Anwendungen stets auf dem neuesten Stand halten sowie das Entfernen von älterer Software.
4. Aufnahme anfälliger Treiber in das Programm zum Schwachstellenmanagement. Bedrohungsakteure könnten versuchen, anfällige legitime Treiber auszunutzen, die bereits auf einem angegriffenen System vorhanden sind.

Zum kompletten Report von Sophos geht es hier:
https://news.sophos.com/en-us/2024/03/04/itll-be-back-attackers-still-abusing-terminator-tool-and-variants/

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/
X/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