BlackByte kapert mit "Bring Your Own Driver"-Prinzip EDR-Lösungen

Mit dieser Masche umgeht BlackByte mehr als 1.000 Treiber, die branchenweit in vielen Endpoint Detection and Response (EDR)-Produkten verwendet werden.

Die Security-Spezialisten von Sophos enttarnten eine neue Masche der relativ jungen Ransomware-Gang BlackByte. Diese setzen das "Bring Your Own Driver"-Prinzip ein, um mehr als 1.000 Treiber zu umgehen, die branchenweit in Endpoint Detection and Response (EDR)-Lösungen zum Einsatz kommen. Sophos beschreibt die Angriffstaktiken, -techniken und -verfahren (TTPs) im neuen Report "Remove all the Callbacks - BlackByte Ransomware Disables EDR via RTCore64.sys Abuse".

BlackByte, das Anfang des Jahres in einem Sonderbericht des Secret Service und des FBI als Bedrohung für kritische Infrastrukturen genannt wurde, tauchte im Mai nach einer kurzen Pause mit einer neuen Leak-Site und neuen Erpressungstaktiken wieder auf. Jetzt hat die Gruppe offenbar auch neue Angriffsmethoden entwickelt. Konkret nutzen sie eine Schwachstelle in RTCorec6.sys aus, einem Grafiktreiber für Windows-Systeme. Diese besondere Schwachstelle ermöglicht es ihnen, direkt mit dem Kernel des Zielsystems zu kommunizieren und ihm zu befehlen, die von EDR-Anbietern verwendeten Callback-Routinen sowie den ETW-Provider (Event Tracing for Windows) namens Microsoft-Windows-Threat-Intelligence zu deaktivieren. EDR-Anbieter verwenden diese Funktion, um die Verwendung von häufig böswillig missbrauchten API-Aufrufen zu überwachen. Sobald diese Funktion deaktiviert wird, wird EDR, das auf dieser Funktion aufbaut, ebenfalls unwirksam gemacht. Sophos Produkte bieten Schutzmaßnahmen gegen die beschriebenen Angriffstaktiken.

"Wenn man sich Computer als eine Festung vorstellt, ist ETW für viele EDR-Anbieter die Wache am Eingangstor. Wenn der Wächter ausfällt, ist der Rest des Systems extrem verwundbar. Und da ETW von vielen Anbietern verwendet wird, ist der Pool an potenziellen Zielen für BlackByte enorm groß", kommentiert Chester Wisniewski, Prinicpal Research Scientist, Sophos.

BlackByte ist nicht die einzige Ransomware-Gruppe, die sich den "Bring Your Own Driver" zunutze macht, um Sicherheitslösungen zu umgehen. AvosLocker hat im Mai eine Schwachstelle in einem anderen Treiber ausgenutzt, um Antiviren-Lösungen zu deaktivieren.

"Rückwirkend betrachtet, scheint es, dass die Umgehung von EDR eine immer beliebtere Technik für Ransomware-Gruppen wird, was nicht überraschend ist. Bedrohungsakteure nutzen häufig Tools und Techniken, die von der "offensiven Security" entwickelt wurden, um Angriffe schneller und mit minimalem Aufwand durchzuführen. Tatsächlich scheint BlackByte zumindest einen Teil seiner EDR-Bypass-Implementierung aus dem Open-Source-Tool EDRSandblast übernommen zu haben", kommentiert Wisniewski. "Angesichts der Tatsache, dass Cyberkriminelle die Technologien der Security-Industrie adaptieren, ist es für Verteidiger entscheidend, neue Umgehungs- und Ausnutzungstechniken zu beobachten und Maßnahmen zu implementieren, bevor diese Techniken in der Cybercrime-Szene weit verbreitet sind.

Um mehr über die neuesten TTPs von BlackByte zu erfahren und wie Sie Ihre Systeme schützen können, laden Sie den vollständigen Report von Sophos.com herunter.

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