SOPHOS
Security made simple.

Exploits unter der Lupe:

Welche Security-Produkte wehren Exploits zuverlässig ab?

Exploits nutzen Schwachstellen in legitimen Software-Produkten wie Adobe Flash und Microsoft Office aus, um Computer für kriminelle Zwecke zu infizieren. Häufig werden sie von Cyberkriminellen genutzt, um die Abwehrmaßnahmen von Unternehmen zu überlisten. Die Beweggründe dieser Kriminellen sind vielfältig: Manche wollen Daten stehlen oder Lösegeld für die Herausgabe von Daten erpressen, andere Informationen über ihr Ziel sammeln oder einfach nur mehr gewöhnliche Malware in Umlauf bringen.

Exploits werden häufig im Rahmen von Cyberangriffen verwendet: Bei über 90 % aller gemeldeten Datenpannen kann der Einsatz eines Exploits an einem oder mehreren Punkten der Angriffskette nachgewiesen werden. Eine Exploit Prevention darf also in keiner umfassenden Sicherheitslösung fehlen.

Exploits gibt es schon seit mehr als 30 Jahren. Kein Wunder also, dass die meisten IT-Security-Anbieter die eine oder andere Form der Exploit Prevention im Angebot haben. Die Qualität dieser Exploit Prevention kann jedoch stark variieren. Für einige Anbieter ist Exploit Prevention eine reine Pflichtübung, für andere wiederum ein wichtiger strategischer Schwerpunkt. In diesem Whitepaper erfahren Sie mehr über Exploits und welche Exploit-Prevention-Funktionen die führenden Security-Produkte zu bieten haben.

Die Exploit-Branche: Crimeware as a Service

Dank Exploit-Kits müssen sich Malware-Autoren keine Gedanken darüber machen, wie sie in Java, Silverlight oder Flash Bugs finden, wie sie aus diesen Bugs Exploits machen, wie sie unsichere Web-Server zum Hosten von Exploits finden oder wie sie potenzielle Opfer auf schädliche Webseiten locken.

Gleichzeitig müssen die Exploit-Kit-Autoren selbst keine Malware schreiben. Sie müssen keine Server betreiben, um infizierte Computer im Auge zu behalten, oder Geld von einzelnen Opfern eintreiben. Und sie müssen sich nicht mit der Exfiltration oder dem Verkauf von Daten befassen.

Cyberkriminalität hat sich zu einer milliardenschweren Branche entwickelt, die Prognosen zufolge bis 2019 Schäden in Höhe von fast 2 Trillionen USD anrichten wird. Kriminelle befinden sich in der „glücklichen" Lage, sich auf einen oder mehrere Teile der Bedrohungslandschaft spezialisieren zu können – in einem System, das mittlerweile scherzhaft auch als Crimeware-as-a-Service oder kurz CaaS bezeichnet wird.

In dieser mittlerweile sehr lukrativen Branche treten immer häufiger sogenannte Exploit-Broker in Erscheinung: Diese Broker kaufen Exploits von Personen, die diese entdecken, und verkaufen sie anschließend an Interessierte weiter, z. B. an staatliche Stellen oder Hacker.

Die Käufer behalten ihre Motive gerne für sich. Kevin Mitnick, der Gründer von Mitnick's Absolute Zero Day Exploit Exchange, erklärt Wired: „Wenn einer unserer Kunden eine Zero-Day-Schwachstelle kaufen möchte, stellen wir keine Fragen und würden, selbst wenn wir das täten, keine Antwort erhalten." Forscher finden die Schwachstellen, verkaufen sie für X an uns, wir verkaufen Sie für Y an unsere Kunden und streichen die Gewinnmarge durch den Weiterverkauf ein."

> „Wenn einer unserer Kunden eine Zero-Day-Schwachstelle kaufen möchte, stellen wir keine Fragen und würden, selbst wenn wir das täten, keine Antwort erhalten. Forscher finden die Schwachstellen, verkaufen sie für X an uns, wir verkaufen Sie für Y an unsere Kunden und streichen die Gewinnmarge durch den Weiterverkauf ein."
>
> KEVIN MITNICK

Techniken zur Exploit-Abwehr

Da mittlerweile täglich mehr als 400.000 einzigartige Malware-Samples erstellt und jedes Jahr Tausende neuer Schwachstellen aufgedeckt werden, wird es immer schwieriger, Angriffe zu verhindern. Das explosive Wachstum von Malware-Varianten erfordert neue und innovative Abwehrkonzepte zum Schutz vor Cyberkriminellen.

Bei näherer Betrachtung der modernen Cybercrime-Branche wird deutlich, dass gute Voraussetzungen für eine asymmetrische Abwehr vorhanden sind. Denn trotz der endlos erscheinenden Flut neuer Angriffe gibt es insgesamt nur etwa 20 Techniken zur Ausnutzung von Software. Ein Konzept, das sich auf die Bekämpfung dieser zahlenmäßig relativ beschränkten Exploit-Techniken konzentriert, ist anderen Ansätzen klar überlegen, da nicht jeder einzelne Exploit bekämpft werden muss.

Je nach Schwachstelle müssen Angreifer oft eine Reihe von Exploit-Techniken kombinieren, bis sie in der Lage sind, ihre Malware erfolgreich zu übertragen. Diese Techniken verändern sich von Jahr zu Jahr nicht sonderlich: Unter Umständen kommen ein paar neue Tricks zur Liste der existierenden Techniken hinzu.

Wenn man jedoch die führenden Security-Produkte unter die Lupe nimmt, fällt schnell auf, dass erstaunlich wenige leistungsstarke Verfahren zur Bekämpfung von Exploit-Techniken anbieten. Manche der neuen selbst ernannten „Next-Gen-Technologie"-Anbieter räumen der Exploit-Abwehr zwar mehr Bedeutung ein, vernachlässigen jedoch wichtige Aspekte.

Im Folgenden finden Sie eine Liste der 23 Exploit-Techniken, die von Cyberkriminellen und Nationalstaaten genutzt werden. Die Abwehrverfahren für jede dieser Techniken variieren je nach Anbieter. Die meisten Anbieter, die behaupten, Exploits abwehren zu können, schützen in Wirklichkeit nur vor einem Bruchteil der weit verbreiteten Exploit-Methoden. Nur Sophos bietet eine wirklich umfassende Exploit Prevention.

Enforce Data Execution Prevention (DEP)

Unter Data Execution Prevention (DEP) verbirgt sich eine Reihe von Hardware- und Software-Technologien, die zusätzliche Speicherüberprüfungen durchführen, um Pufferüberläufe zu verhindern. Ohne DEP kann ein Angreifer versuchen, eine Software-Schwachstelle auszunutzen, indem er zu Schadcode (Shellcode) an einem Speicherort springt, an dem sich vom Angreifer kontrollierte Daten befinden (z. B. Heap oder Stack). Ohne DEP werden diese Bereiche normalerweise als ausführbar markiert, sodass Schadcode ausgeführt werden kann.

DEP ist eine Opt-in-Option für Windows XP und höher, die vom Software-Anbieter beim Kompilieren einer Anwendung aktiviert werden muss. Zudem gibt es Angriffe zum Umgehen vom integriertem DEP-Schutz. Es ist daher nicht anzuraten, sich auf die Betriebssystemimplementierung zu verlassen.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Microsoft EMET, Malware Bytes Anti-Exploit, Palo Alto Network Traps, Crowdstrike Falcon

Mandatory Address Space Layout Randomization (ASLR)

Einige Exploits nehmen gezielt Speicherorte ins Visier, die bekanntermaßen mit bestimmten Prozessen verknüpft sind. In älteren Versionen von Windows (auch Windows XP) wurden Hauptprozesse beim Systemstart in der Regel in vorhersagbare Speicherorte geladen. Address Space Layout Randomization (ASLR) randomisiert die von Systemdateien und anderen Programmen genutzten Speicherorte, sodass Angreifer den Speicherort eines bestimmten Prozesses nicht mehr so leicht vorhersagen können.

ASLR ist ausschließlich unter Windows Vista und höher verfügbar und muss wie DEP vom Software-Anbieter beim Kompilieren der Anwendung aktiviert werden. Und genau wie bei DEP gibt es auch hier Angriffe zum Umgehen von integriertem ASLR-Schutz, weshalb es wiederum nicht anzuraten ist, sich auf die Betriebssystemimplementierung zu verlassen.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Microsoft EMET, Palo Alto Networks Traps, Crowdstrike Falcon

Bottom-up ASLR

Bei Aktivierung verändert die verbindliche ASLR auf einem Windows-Computer die Basisadresse von Anwendungen nur einmal, bis der Computer neu gestartet wird. Angreifer können diesen Umstand ausnutzen, um die Wiederverwendung gefundener Speicherorte für Anwendungen zu ermöglichen, die mehrere Male gestartet werden.

Bottom-up ASLR verbessert die Entropie oder Zufälligkeitsstufe der verbindlichen ASLR. Der Hauptvorteil von Bottom-up ASLR besteht darin, dass es die Basisadresse geschützter Anwendungen bei jedem Anwendungsstart ändert.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Microsoft EMET, Malwarebytes Anti-Exploit

Null Page (Null Dereference Protection)

Seit Windows 8 verweigert Microsoft Programmen, die „NULL Page" (Speicher unter virtuellen Adressen 0x00000000 im Adressraum) zuzuteilen und/oder zuzuordnen. Auf diese Weise verhindert Microsoft die direkte Ausnutzung einer ganzen Kategorie von Schwachstellen, die als „NULL Pointer Dereference"-Schwachstellen bezeichnet werden.

Unter Windows XP, Windows Vista und Windows 7 würde die Ausnutzung einer solchen Schwachstelle den Angreifer in die Lage versetzen, Code im Kontext des Kernels (unter der ring0-CPU-Berechtigungsstufe) auszuführen. Das Ergebnis wäre eine Berechtigungsausweitung bis auf eine der höchsten Ebenen. Über solche Schwachstellen verschaffen sich Angreifer Zugriff auf praktisch alle Bereiche des Betriebssystems.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Microsoft EMET

Heap Spray Allocation

Heap Spray ist eine Technik, die selbst keine Schwachstellen ausnutzt, sondern die Ausnutzung einer Schwachstelle erleichtert. Hierbei kommt eine Technik namens „Heap Feng Shui[1]" zum Einsatz:

Ein Angreifer ist in der Lage, beabsichtigte Datenstrukturen oder Shellcode zuverlässig auf dem Heap zu positionieren und auf diese Weise eine verlässliche Ausnutzung einer Software-Schwachstelle zu erleichtern.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Microsoft EMET, Palo Alto Networks Traps, Crowdstrike Falcon

Dynamic Heap Spray

Die Dynamic Heap Spray Erkennung analysiert die Inhalte von Speicherbelegungen, um Muster zu erkennen, die auf Heap Sprays hindeuten, die NOP Sleds, polymorphe NOP Sleds, JavaScript Arrays, ActionScript Arrays und andere verdächtige Sequenzen enthalten, die platziert werden, um Exploit-Angriffe zu erleichtern.

1 https://cansecwest.com/slides/2014/The%20Art%20of%20Leaks%20-%20read%20version%20-%20Yoyo.pdf

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Palo Alto Networks Traps

Stack Pivot

Der Stack einer Anwendung ist ein Speicherbereich, in dem sich unter anderem eine Liste von Speicher-Adresspositionen (sogenannte Rücksprungadressen) befindet. Hier ist der Code gespeichert, den der Prozessor in der nahen Zukunft für seine Ausführung benötigt.

Stack Pivoting wird von Schwachstellen-Exploits häufig genutzt, um Schutzmaßnahmen wie DEP zu umgehen, beispielsweise durch Verkettung von ROP Gadgets in einem Return-Oriented-Programming-Angriff. Mit Stack Pivoting können Angreifer vom echten Stack zum neuen falschen Stack umleiten. Hierbei kann es sich um einen vom Angreifer kontrollierten Puffer wie den Heap, von dem aus Angreifer den zukünftigen Ablauf der Programmausführung steuern können.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Cylance PROTECT, Microsoft EMET, Malwarebytes Anti-Exploit, Palo Alto Networks Traps

Stack Exec (MemProt)

Unter normalen Umständen enthält der Stack Daten und Adressen, die auf Code für den Prozessor verweisen, der in naher Zukunft ausgeführt werden soll. Unter Verwendung eines Stack-Pufferüberlaufs[2] sind Angreifer in der Lage, den Stack mit willkürlichem Code zu überschreiben. Um diesen Code auf dem Prozessor ausführen zu können, muss der Speicherbereich des Stacks ausführbar gemacht werden, um DEP zu überlisten. Sobald der Stack-Speicher ausführbar ist, ist es für einen Angreifer ein Leichtes, den Programmcode einzuschleusen und auszuführen.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Cylance PROTECT, Microsoft EMET

Stack-based ROP Mitigations (Caller)

„Control-Flow Integrity (CFI)"-Technologie soll Angreifer daran hindern, den Control-Flow von Anwendungen, die im Kontakt mit dem Internet stehen (z. B. Web-Browser, Microsoft Office und andere Produktivitäts- und Mediensoftware), zu übernehmen. Um Sicherheitstechnologien wie Data Execution Prevention (DEP) und Address Space Layout Randomization (ASLR) zu überlisten, kommen in letzter Zeit vermehrt Control-Flow-Angriffe zum Einsatz. Diese Angriffe sind für Antivirus-Software, die meisten „Next-Gen"-Produkte und andere Cyber-Abwehrmaßnahmen unsichtbar, da keine schädlichen Dateien zum Einsatz kommen. Stattdessen wird der Angriff während der Laufzeit erstellt. Hierzu werden kurze Abschnitte von harmlosem Code kombiniert, die Teil bestehender Anwendungen wie Internet Explorer oder Adobe Flash Player sind. Man spricht auch von einem Code-Wiederverwendungs- oder „Return-Oriented Programming (ROP)"-Angriff.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Kaspersky Endpoint Security, McAfee Endpoint Security, Microsoft EMET, Malwarebytes Anti-Exploit, Palo Alto Networks Traps

2 https://en.wikipedia.org/wiki/Stack_buffer_overflow

Branch-based ROP Mitigations (Hardware Augmented)

ROP-Angriffe können durch Ausnutzung einer ansonsten ungenutzten Hardware-Funktion in regulären Intel®-Prozessoren (von 2008 und neuer) erreicht werden, um Code-Ausführungen nachzuverfolgen und die Analyse und Erkennung komplexer Exploit-Angriffe während der Laufzeit zu verbessern. Die Anwendung schreibgeschützter Hardware-nachverfolgter (Verzweigungs-) Datensätze hat vom Sicherheitsstandpunkt betrachtet einen wesentlichen Vorteil gegenüber Stack-basierten Ansätzen. Die Verzweigungsinformationen, die aus diesen Datensätzen gewonnen werden können, identifizieren nicht nur das Ziel der Verzweigung, sondern auch die Quelle. Sie geben also Aufschluss darüber, welchen Ursprung die Änderung im Control-Flow hat. Diese spezifischen Informationen können bei Verwendung einer Stack-basierten Lösung nicht mit demselben Grad an Verlässlichkeit erhoben werden.

Verzweigungsinformationen in den Hardware-verfolgten Datensätzen können nicht manipuliert werden; es besteht keine Möglichkeit, sie mit kontrollierten Daten eines Angreifers zu überschreiben. Stack-basierte Lösungen (wie Microsoft EMET und Palo Alto Networks Traps) stützen sich auf Stack-Daten, die sich – insbesondere im Falle eines ROP-Angriffs – in der Kontrolle des Angreifers befinden, der wiederum den Verteidiger in die Irre führen kann. Die von Sophos Intercept X genutzten Hardware-nachverfolgten Daten sind zuverlässiger und manipulationssicherer.

Sophos Intercept X wendet automatisch Intel MSR Hardware-Register an, wenn es einen Intel® Core™ i3-, i5-, oder i7-Prozessor (CPU) erkennt. Sollte der Endpoint über keinen unterstützten Prozessor verfügen, greift Sophos Intercept X automatisch auf reine Software-orientierte, Stack-basierte Control-Flow-Integrity-Prüfungen zurück.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X

Structured Exception Handler Overwrite Protection (SEHOP)

Ein Angreifer kann den Handler Pointer eines Ausnahmedatensatzes auf dem Stack mit einem kontrollierten Wert überschreiben. Sobald eine Ausnahme eintritt, durchläuft das Betriebssystem die Kette der Ausnahmedatensätze und ruft alle Handler in jedem Ausnahmedatensatz auf. Da der Angreifer einen der Datensätze steuert, springt das Betriebssystem überall dorthin, wo der Angreifer möchte, und verschafft dem Angreifer damit die Kontrolle über den Ablauf der Ausführung.

SEHOP ist eine Opt-in-Option für Windows Vista und höher, die vom Software-Anbieter beim Kompilieren einer Anwendung aktiviert werden muss. Es gibt Angriffe zum Umgehen vom integriertem SEHOP-Schutz. Es ist daher nicht anzuraten, sich auf die Betriebssystemimplementierung zu verlassen.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Symantec Endpoint Protection, Microsoft EMET

Import Address Table Access Filtering (IAF)

Um Schadaktivitäten ausführen zu können, braucht ein Angreifer früher oder später die Adressen bestimmter Systemfunktionen (z. B. kernel32!VirtualProtect). Diese Adressen können von verschiedenen Quellen abgerufen werden, beispielsweise von der Importadresstabelle (IAT) eines geladenen Moduls. Die IAT fungiert als eine Nachschlagetabelle, wenn eine Anwendung eine Funktion in einem anderen Modul aufruft. Da ein kompilliertes Programm den Speicherort der Bibliotheken, auf die es sich stützt, nicht kennen kann, ist bei jedem API-Aufruf ein indirekter Sprung erforderlich. Der dynamische Linker lädt Module und fügt diese zusammen. Dabei schreibt er echte Adressen in die IAT Slots, sodass diese zu den Speicherorten der entsprechenden Library-Funktionen verweisen.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Microsoft EMET

Load Library

Angreifer können versuchen, schädliche Bibliotheken zu laden, indem sie diese auf UNC-Pfaden platzieren. Mittels Überwachung aller Aufrufe der LoadLibrary API kann diese Art von Library Loading unterbunden werden.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Microsoft EMET, Malwarebytes Anti-Exploit, Palo Alto Networks Traps.

Reflective DLL Injection

Wenn Sie eine DLL in Windows laden, rufen Sie normalerweise die API-Funktion LoadLibrary auf. Die LoadLibrary verwendet den Dateipfad der DLL als Eingabe und lädt diese in den Speicher.

Unter Reflective DLL Loading versteht man das Laden einer DLL aus dem Speicher anstelle von der Festplatte. Windows hat keine LoadLibrary-Funktion, die diesen Vorgang unterstützt. Um die Funktion zu nutzen, müssen Sie sie also selbst schreiben. Wenn Sie Ihre eigene Funktion schreiben, besteht ein Vorteil darin, dass Sie auf einige Dinge verzichten können, die bei Windows Standard sind, z. B. Registrieren der DLL als ein geladenes Modul im Prozess, wodurch sich der Reflektive Loader schwieriger analysieren lässt. Das Tool Meterpreter nutzt beispielsweise Reflective Loading, um sich zu verstecken. Als Abwehrmaßnahme wird analysiert, ob eine DLL innerhalb des Speichers reflektierend geladen wird.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Palo Alto Networks Traps

Shellcode

Ein Shellcode ist ein Codeabschnitt, der in einem Exploit als Payload fungiert. Der Shellcode startet eine Kommando-Shell, die vom Angreifer kontrolliert wird. Die Übertragung und Ausführung des Shellcodes kann in vielerlei Form erfolgen und für die Erkennung der unbefugten Bereitstellung von Shellcode sind eine Reihe von Techniken erforderlich, um auf Dinge wie fragmentierten Shellcode, verschlüsselte Payloads und Null Free Encoding einzugehen.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X

VBScript God Mode

Unter Windows kann VBScript in Browsern oder der lokalen Shell verwendet werden. Beim Einsatz im Browser sind die Fähigkeiten von VBScript aus Sicherheitsgründen beschränkt. Diese Beschränkung wird über das Safemode Flag gesteuert. Wird das Flag modifiziert, kann VBScript in HTML genauso wie in der lokalen Shell agieren. Folglich können Angreifer problemlos Schadcode in VBScript schreiben. Das Manipulieren des Safemode Flags auf VBScript im Web-Browser wird als God Mode bezeichnet[3].

Ein Angreifer kann beispielsweise den Wert des Safemode Flags modifizieren, indem er die Schwachstelle CVE-2014-6332 ausnutzt[4], einen durch unsachgemäße Handhabung bei der Größenanpassung eines Arrays in der Internet Explorer VBScript Engine verursachten Bug. Im God Mode kann willkürlicher, in VBScript geschriebener Code aus der Browser-Sandbox ausbrechen. Dank Gode Mode greifen Schutzmaßnahmen wie Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR) und Control-Flow Guard (CFG) nicht.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Microsoft EMET, Malwarebytes Anti-Exploit

WoW64

Microsoft bietet Abwärtskompatibilität für 32-Bit-Software auf 64-Bit-Editionen von Windows durch den „Windows on Windows" (WoW) Layer. Bestimmte Aspekte der WoW-Implementierung liefern Angreifern interessante Methoden zum Verkomplizieren dynamischer Analysen, Entpacken von Binärdateien und zum Umgehen von Exploit-Abwehrmaßnahmen.

Das Verhalten einer 32-Bit-Anwendung in der WoW64-Umgebung unterscheidet sich in vielen Punkten von einem echten 32-Bit-System. Die Möglichkeit, während der Laufzeit zwischen Ausführungsmodi umzuschalten, kann Angreifern Methoden zur Ausnutzung, Verschleierung und Anti-Emulation liefern, z. B.:

- Zusätzliche ROP Gadgets, die im 32-Bit-Code nicht vorhanden sind
- Mixed Execution Mode Payload Encoder
- Ausführungsumgebungsfunktionen, die Abwehrmaßnahmen weniger effektiv machen können
- Umgehen von Hooks, die von Sicherheitssoftware eingerichtet wurden (nur 32-Bit-Benutzerbereich)

Endpoint-Protection-Software hookt meist nur sensible API-Funktionen im 32-Bit-Benutzer-Speicherbereich, wenn ein Prozess unter WoW64 ausgeführt wird. Falls ein Angreifer in der Lage ist, in den 64-Bit-Modus umzuschalten, kann er sich Zugriff auf ungehookte 64-Bit-Versionen sensibler API-Funktionen verschaffen, die im 32-Bit-Modus gehookt sind.

In 64-Bit-Editionen von Windows verbietet Sophos Intercept X dem Programmcode, direkt vom 32-Bit- in den 64-Bit-Modus umzuschalten (z. B. unter Verwendung von ROP), ermöglicht dem WoW64 Layer jedoch weiterhin, diese Umstellung durchzuführen.

3 https://en.wikipedia.org/wiki/Glossary_of_video_game_terms#God_mode
4 https://www.rapid7.com/db/modules/exploit/windows/browser/ms14_064_ole_code_execution

Weitere Informationen über die missbräuchliche Nutzung von WoW64 finden Sie in diesem Forschungsbeitrag von Duo Security: „WoW64 and So Can You5 and Mitigating Wow64 Exploit Attacks“[6].

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X

Syscall

Syscalls können für Zugriffe auf kritische Systemfunktionen im Kernel genutzt werden, um gehookte Windows-APIs, Sandbox-Analysen und die meiste Schutzsoftware zu umgehen.

Die meisten Endpoint-Security-Produkte verwenden User-Mode-Hooks, um sensible API-Aufrufe abzufangen und zu überwachen. Um diese Hooks zu umgehen, kann ein Angreifer sich die Tatsache zu Nutze machen, dass:

- nicht alle API-Funktionen, sondern nur sensible API-Funktionen gehookt sind
- die zum Aufruf von Kernel-Funktionen genutzten Stubs sind sehr ähnlich sind, nur der Funktionsindex ist einmalig

Nähere Informationen über die missbräuchliche Nutzung von Syscalls finden Sie in dem BreakDev.org-Blogeintrag „Defeating Antivirus Real-time Protection From The Inside“[7].

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X

Hollow Process

Process Hollowing ist eine Technik, bei der ein legitimer Prozess auf dem System ausschließlich geladen wird, um als Container für bösartigen Code zu dienen; beispielsweise svchost.exe und explorer.exe. Beim Starten wird der Verweis auf den legitimen Code durch einen Verweis auf Schadcode ersetzt, woraufhin der Prozess beginnt, den Schadcode auszuführen. Auf diese Weise kann sich der Prozess zwischen normalen Prozessen verbergen.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Palo Alto Networks Traps

DLL Hijacking

Aufgrund einer Schwachstelle, die oft als DLL Hijacking, DLL Spoofing, DLL Preloading oder Binary Planting bezeichnet wird, können viele Programme dazu gebracht werden, dass sie eine schädliche DLL ausführen, die sich im selben Ordner befindet wie andere von diesen Programmen geöffnete Dateien.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Palo Alto Networks Traps

5 https://duo.com/blog/wow64-and-so-can-you
6 https://hitmanpro.wordpress.com/2015/11/10/mitigating-wow64-exploit-attacks
7 https://breakdev.org/defeating-antivirus-real-time-protection-from-the-inside/

Application Lockdown

Für den Fall, dass es einem Angreifer gelingen sollte, alle Abwehrmaßnahmen auf Speicher- und Code-Ebene auszunutzen und auszuhebeln, beschränkt Sophos Intercept X die Möglichkeiten des Angreifers, Schaden anzurichten. Dieses Feature heißt Application Lockdown und soll verhindern, dass Angreifer unerwünschten Code einschleusen.

Application Lockdown stoppt Angriffe, die sich in der Regel nicht auf Software-Bugs in Anwendungen stützen. Ein solcher Angriff kann beispielsweise der Einsatz eines speziell entwickelten (schädlichen) Makros in einem Office-Dokument sein, das an eine (Spear-)Phishing-E-Mail angehängt wird. Makros in Dokumenten sind potenziell gefährlich, weil sie in der Programmiersprache Visual Basic for Applications (VBA) erstellt werden. Diese ermöglicht das Herunterladen und Ausführen von Binärdateien aus dem Internet und erlaubt außerdem den Einsatz von PowerShell und anderen vertrauenswürdigen Anwendungen.

Diese unerwartete Funktion (oder „Logic-Flaw Exploit") bietet Angreifern einen offensichtlichen Vorteil, da sie keinen Software-Bug ausnutzen oder Abwehrmaßnahmen auf Code- und Speicherebene aushebeln müssen, um Computer zu infizieren. Sie müssen lediglich Standardfunktionen ausnutzen, die von einer vertrauenswürdigen, weit verbreiteten Anwendung angeboten werden, und das Opfer mittels Social Engineering überzeugen, das speziell für diesen Zweck erstellte Dokument zu öffnen.

Ohne dass eine Blacklist von Ordnern gepflegt werden muss, beendet Sophos Intercept X eine geschützte Anwendung automatisch auf Basis ihres Verhaltens: Wenn beispielsweise eine Office-Anwendung genutzt wird, um PowerShell zu starten, auf den WMI zuzugreifen und ein Makro zur Installation von willkürlichem Code oder zur Manipulation kritischer Systembereiche auszuführen, blockiert Sophos Intercept X diesen schädlichen Vorgang – selbst wenn der Angriff keinen untergeordneten Prozess erstellt.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Malwarebytes Anti Exploit, Palo Alto Networks Traps

Java Lockdown

Java-Anwendungen haben Zugriff auf leistungsstarke und nützliche Tools, die für Angriffe genutzt werden können, z. B. die Fähigkeit, auf die Festplatte zu schreiben und die Registry zu aktualisieren.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X, Malwarebytes Anti Exploit, Palo Alto Networks Traps

Squiblydoo AppLocker Bypass

Ähnlich wie bei anderen Whitelist-bezogenen Angriffen nutzt Squibydoo Funktionen des Betriebssystems zur Ausführung beliebiger Skripte – selbst auf Systemen im vollständigen Lockdown, auf denen eigentlich nur autorisierte Skripte ausgeführt werden dürfen.

Lösungen, die vor dieser Exploit-Technik schützen: Sophos Intercept X

Vergleich

Im Folgenden finden Sie eine Übersicht der Anti-Exploit-Funktionen verschiedener Security-Produkte, die wir aus Datenblättern, Handbüchern und den Produkten selbst zusammengetragen haben.

Abwehrmaßnahmen auf Speicherebene

	Sophos Intercept X	ESET Endpoint Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Micro OfficeScan	Webroot Endpoint Protection	CylancePROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	CrowdStrike Falcon
Enforce Data Execution Prevention (DEP) Unterbindet die missbräuchliche Nutzung von Pufferüberläufen	■			■					■	■	■	■
Mandatory Address Space Layout Randomization (ASLR) Verhindert vorhersagbare Code-Speicherorte	■								■[1]		■	■[1]
Bottom Up ASLR Optimiert die Randomisierung von Code-Speicherorten	■								■	■		
Null Page (Null Dereference Protection) Stoppt Exploits, die Sprungbefehle über die Zero-Page beinhalten	■		■						■			
Heap Spray Allocation Reserviert beim Programmstart Speicherbereiche, die häufig für das Einbringen von Schadcode verwendet werden, um solche Angriffe abzuwehren	■				■				■	■	■	■
Dynamic Heap Spray Stoppt Angriffe, die verdächtige Sequenzen an verschiedene Stellen des Heaps schreiben	■										■[2]	

Abwehrmaßnahmen auf Code-Ebene

	Sophos Intercept X	ESET Endpoint Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Micro OfficeScan	Webroot Endpoint Protection	CylancePROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	CrowdStrike Falcon
Stack Pivot Stoppt missbräuchliche Nutzungen des Stack Pointers	■			■		■		■	■	■	■	
Stack Exec (MemProt) Stoppt Code von Angreifern auf dem Stack	■					■		■	■			
Stack-based ROP Mitigations (Caller) Stoppt „Return-Oriented Programming"-Standardangriffe	■		■ 3	■ 1		■			■	■	■	
Branch-based ROP Mitigations (Hardware Augmented) Stoppt komplexe „Return-Oriented Programming"-Angriffe	■											
Structured Exception Handler Overwrite Protection (SEHOP) Stoppt missbräuchliche Nutzungen des Ausnahmehandlers	■				■ 4				■ 2			
Import Address Table Filtering (IAF) (Hardware Augmented) Stoppt Angriffe, die nach API-Adressen in der IAT suchen	■								EAF EAF+			
Load Library Unterbindet das Laden von Libraries von UNC-Pfaden	■								■	■	■	
Reflective DLL Injection Verhindert das Laden einer Library vom Speicher in einen Host-Prozess	■										■	
VBScript God Mode Verhindert die Ausnutzung von VBScript in IE zur Ausführung von Schadcode	■								■	■	■ 5	
WoW64 Stoppt Angriffe, die auf die 64-Bit-Funktion des WoW64-Prozesses abzielen	■											
Syscall Stoppt Angreifer, die versuchen, Sicherheitsmaßnahmen zu umgehen	■											

Exploits unter der Lupe: Welche Security-Produkte wehren Exploits zuverlässig ab?

	Sophos Intercept X	ESET Endpoint Security	Kaspersky Endpoint Security	McAfee Endpoint Security	Symantec Endpoint Protection	Trend Micro OfficeScan	Webroot Endpoint Protection	CylancePROTECT	Microsoft EMET	Malwarebytes Anti-Exploit	Palo Alto Networks Traps	CrowdStrike Falcon
Hollow Process Stoppt Angriffe, die legitime Prozesse nutzen, um Schadecode zu verbergen	■										■	
DLL Hijacking Gibt System-Libraries für heruntergeladene Anwendungen Priorität	■											
Application Lockdown Stoppt Logic-Flaw-Angriffe, die Abwehrmaßnahmen umgehen	■									■	■ 1	
Java Lockdown Verhindert Angriffe, die Java ausnutzen, um ausführbare Windows-Dateien zu starten	■									■	■	
Squiblydoo AppLocker Bypass Verhindert die Ausführung von Remote-Skripte und -Code durch regsvr32	■				■							
CVE-2013-5331 & CVE-2014-4113 via Metasploit In-Memory Payloads: Meterpreter & Mimikatz	■	■	■						■		■	

1 Auf Basis der ASLR-Funktion von Windows (nur in Windows Vista und neueren Windows-Versionen verfügbar)

2 Nur 32-Bit-NOP-Schlitten und polymorpher NOP-Schlitten; keine Erkennung von Flash Vector Heap Spray und nicht auf 64-Bit-Versionen von Windows

3 32-Bit-ROP-Abwehr nur mit WinExec()-Funktion, nicht für 64-Bit-Versionen von Windows

4 Auf Basis der SEHOP-Funktion von Windows (nur verfügbar in Windows Vista Service Pack 1 und neueren Windows-Versionen)

5 Manuell definierte Beschränkungen auf Basis von Ordnern und untergeordneten Prozessen; wartungsintensiv, nicht verhaltensbasiert

Testen Sie Sophos Intercept X kostenfrei

unter www.sophos.de/intercept-x

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

01.12.2017 WP-DE (MP)

SOPHOS