solarwinds msp

E-Book

Diese 5 Cyberthreats sind zu raffiniert für herkömmliche Antivirenprogramme

Inhaltsverzeichnis

EINFÜHRUNG **3**

1. Polymorphe Malware 4
2. Als Waffe genutzte Dokumente 4
3. Schwache Browser: Drive-by-Downloads 5
4. Dateilose Angriffe 5
5. Perfekt getarnte Malware 6

Wie SolarWinds helfen kann 7

Diese 5 Cyberthreats sind zu raffiniert für herkömmliche Antivirenprogramme

Der erste dokumentierte Computervirus war Creeper im Jahr 1971. Er wurde in einem akademischen Umfeld entwickelt, um die Übertragungsfähigkeit einer Datei in einem Netzwerk zu demonstrieren. Es dauerte geschlagene sechs Monate, bis Computerprogrammierer ein wirksames Antivirenprogramm namens Reaper geschrieben hatten.[1] Die Abwehr hinkte diesem ersten Angriff damit gewaltig hinterher.

Seitdem versuchen Sicherheitsexperten und Computerprogrammierer, mit den Bedrohungen Schritt zu halten. Aufgabe unserer Branche ist es, Bedrohungen zu ermitteln und die Verteidigungsmaßnahmen zu aktualisieren – immer wieder.

Viele herkömmliche Antiviren- oder AV-Programme arbeiten signaturbasiert: Beim Ermitteln bösartiger Software wird eine Signatur mit der Dateibeschreibung erstellt. Diese wird in eine Datenbank geschrieben, die auf die Kundensysteme übertragen wird. Wenn das Antivirenprogramm eine Datei auf Ihrem Rechner erkennt, die zu einer Signatur passt, wird diese Datei in die Quarantäne verschoben oder entfernt. Im Dezember 2018 hatte Malware das bedrohliche Ausmaß von 350.000 neu erkannten Bedrohungen erreicht – pro Tag.[2] Signaturbasierte AV-Lösungen können bei diesem Umfang schnell an ihre Grenzen stoßen, dann sind Geräte nicht umfassend geschützt.

Im Laufe der Zeit wurden zwar neue Verteidigungsmechanismen entwickelt, doch jede dieser Maßnahmen fordert die Cyberkriminellen heraus, ihre Taktik zu ändern. Zu diesen neuen Angriffsmethoden zählt Malware, die nicht nur Schwachstellen ausnutzt, sondern die Abwehr des Antivirenprogramms regelrecht überlistet. Wir haben hier für Sie fünf Angriffsarten aufgeführt, die die Fähigkeiten herkömmlicher Antivirenprogramme übersteigen.

1. „All About Creeper, the First Virus in History“, Softonic. en.softonic.com/articles/all-about-creeper-the-first-virus-in-history (aufgerufen im April 2019).
2. „Malware“, AV-TEST. av-test.org/en/statistics/malware/ (aufgerufen im April 2019).

1. POLYMORPHE MALWARE

Wie eingangs erwähnt, stützen sich gängige AV-Programme auf die signaturbasierte Erkennung von bösartigem Code. Dabei wird eine Datei mit einem bekannten Eintrag (also einer Signatur) in einer Datenbank mit bekannten Bedrohungen verglichen.

Dieser Ansatz weist jedoch einige Schwachstellen auf. Zunächst einmal muss der AV-Nutzer stets die aktuelle Signaturliste haben. Das erfordert also regelmäßige Updates auf Nutzerseite. Wenn ein Nutzer nun die Virendefinitionen nicht auf dem aktuellen Stand hält, ist er gegen neuere Dateien machtlos. Darüber hinaus ist diese Schutzmaßnahme rein reaktiv: Der AV-Anbieter muss die Signatur erst einmal kennen, bevor er sie der Liste hinzufügen kann. Nun verhindert Malware ihrerseits aber oft durch entsprechende Schutzmaßnahmen die Enttarnung durch AV-Unternehmen.

Der gravierendste Nachteil bei diesem Ansatz besteht jedoch in der zeitlichen Verzögerung, bis der Schutz greift. Und genau hier setzt polymorphe Malware an. Angenommen, die Malware wird von einem Antivirenprogramm erkannt. Dann generiert sie sich neu und hat dann frische Eigenschaften, die keiner bekannten Signatur entsprechen. Dadurch haben signaturbasierte AV-Programme kaum eine Chance, der Infektion Herr zu werden. Außerdem werden Tag für Tag etwa 350.000 neue Malwarevarianten erstellt.[3] Mit signaturbasierter AV kann man also nur hinterherhinken.

2. ALS WAFFE GENUTZTE DOKUMENTE

Kriminelle nutzen oft Schwachstellen in verschiedenen Dokumentformaten aus, um ein System zu entern. Diese Dokumente verwenden in der Regel eingebettete Skripte. Meist verstecken die Verbrecher den Code oder das Skript in diesen zu Waffen umfunktionierten Dokumenten. Selbst für das geübte Auge sieht das harmlos aus. Der AV-Check wird umgangen, da das Antivirenprogramm nur das ursprüngliche Dokument statt den Code oder das Skript nach der Ausführung scannt. Nach dem Start wird der Angriff ohne Wissen des Nutzers im Hintergrund ausgeführt.

Cyberkriminelle können mit Adobe® PDF-Dateien mit eingebettetem JavaScript® Betriebssystembefehle ausführen oder ausführbare Dateien herunterladen, um die geenterten Geräte und Netzwerke zu manipulieren. Anhand von eingebetteten Skripten führen Hacker häufig PowerShell®-Befehle aus. Da PowerShell in das Windows®-Betriebssystem integriert ist, können dieses Angriffe nicht nur Endpunkte, sondern sogar ganze Netzwerke beschädigen. PDFs stellen jedoch bei weitem nicht die einzigen angreifbaren Dateien dar – auch XML-basierte Dokumente, HTML-Dateien und Office®-Dokumente sind häufig mit diesen bösartigen Skripts verseucht. Eine AV-Lösung, die sich auf den Vergleich ausführbarer Signaturen stützt, ist nicht in der Lage, derart manipulierte Dateien zu erkennen. Der Grund: Es wird nur das ursprüngliche Dokument gescannt, nicht der Schadcode, den das Dokument startet.

3. „Malware", AV-TEST. av-test.org/en/statistics/malware/ (aufgerufen im April 2019).

3. SCHWACHE BROWSER: DRIVE-BY-DOWNLOADS

Bei Drive-by-Downloads werden Dateien unter Ausnutzung von Schwachstellen im Browser oder einem Browser-Add-in auf den Endpunkt heruntergeladen – Antivirenprogramm und Nutzer merken nichts. Der Download kann dabei entweder von einer vertrauenswürdigen Website mit einem manipulierten Skript oder Werbedienst oder von einer bösartigen Website stammen, die speziell dafür ausgelegt ist, den Download zu starten. Ausgangspunkt für diese Angriffe: Phishing per E-Mail oder auf sozialen Medien oder auch gut getarnte Popup-Links, die den Nutzer zu einer Website leiten. Die Cyberkriminellen nutzen dann Exploits in Browsern oder Plug-ins, um die Malware herunterzuladen und den Angriff zu starten.

Danach ist dem eigentlichen Schaden der Weg geebnet: Der Angreifer kann einen Cryptominer, einen Remote-Access-Trojaner oder Ransomware installieren. So wurde die Stadt Issaquah im US-Bundesstaat Washington im Oktober 2017 Opfer eines Ransomware-Angriffs, durch den die städtischen Dienste vier Tage offline waren.[4] Verursacht wurde das Ganze durch einen Drive-by-Download, nachdem ein Mitarbeiter eine verseuchte PDF auf einer Website geöffnet hatte.

4. DATEILOSE ANGRIFFE

Die meisten Antivirenprogramme untersuchen die Dateien, wenn sie auf das Gerät gelangen. Wenn jedoch der Ausgangspunkt keine Datei ist, ist das AV-Programm nicht in der Lage, das bösartige Verhalten aufzuspüren.

Da bei dateilosen Angriffen kein Payload, kein Schadcode auf dem System installiert wird, ist es für AV-Programme so extrem schwierig, sie zu erkennen. Ausgeführt werden sie meist im Arbeitsspeicher des Endpunktgeräts. Zum Infizieren dienen dabei PowerShell, rundll32.exe oder andere integrierte Systemressourcen.

Dateilose Angriffe gehen häufig mit Dokumenten oder bösartigen Skripts auf einer Website einher, aber das ist längst nicht die einzige Möglichkeit, Geräte zu infizieren. Wenn beispielsweise ein Endpunkt RDP (Remote Desktop Protocol) aktiviert hat, bleibt ein Listening-Port offen, mit dem jemand eine Verbindung zum Gerät herstellen und bösartige Prozesse ausführen kann – also tatsächlich dateibasierte Malware herunterladen, Registryeinträge ändern oder Daten stehlen.

Und damit nicht genug: SentinelOne ermittelte für das erste Halbjahr 2018 für dateilose Angriffe einen Anstieg um satte 91 %.[5] Da sich diese Angriffe häufen, müssen Unternehmen mehr als nur dateibasierte Angriffe ermitteln, um ihre Daten und Systeme besser zu schützen.

4. „How a Drive-by Download Attack Locked Down Entire City for 4 Days", The Hacker News. thehackernews.com/2017/10/drive-by-download-ransomware.html (aufgerufen im April 2019).
5. „Fileless Malware Attacks | How They Can Be Detected and Mitigated", SentinelOne. sentinelone.com/blog/fileless-malware-attacks-can-detected-mitigated/ (aufgerufen im April 2019).

5. PERFEKT GETARNTE MALWARE

Wie geschildert versuchen Sicherheitsexperten und Programmierer unentwegt, mit den Cyberkriminellen Schritt zu halten. AV-Unternehmen setzen für die Malware-Erkennung verschiedene Verfahren ein. Ein häufig genutztes Verfahren, besteht darin, die Dateien in abgeschotteten Sandbox-Umgebungen auszuführen und auf bösartiges Verhalten zu untersuchen. Eine weitere gängige Maßnahme ist, den Code auf typische Anzeichen für bösartige Absichten zu scannen.

Cyberkriminelle haben jedoch auch hier Mittel und Wege gefunden, diese Abwehrmaßnahmen zu umgehen. Genauso wie Sicherheitsexperten ihre Daten und Anlagen immer besser schützen, rüsten Hacker auf, um ihrerseits den bösartigen Payload in Malware zu schützen.

Neuere Malware erkennt Sandbox-Umgebungen und bleibt dort inaktiv; der Angriff erfolgt ausschließlich in Produktivsystemen. Dadurch ist es für das AV-Programm schlicht unmöglich, eine Erkennung anhand von Verhaltensanalysen in der Sandbox-Umgebung durchzuführen.

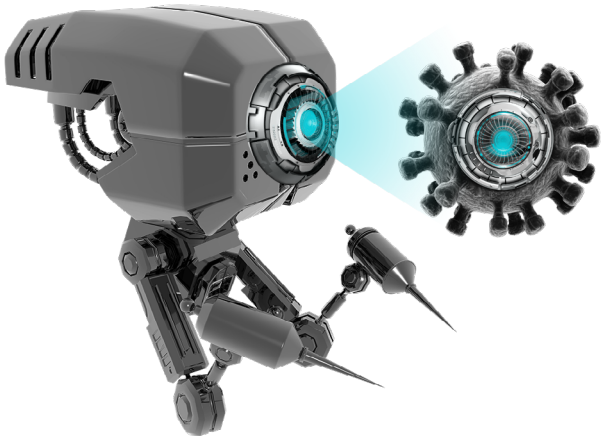
Antivirenprogramme können auch mit sogenannten Packern umgangen werden, die durch Verschlüsselung oder Komprimierung verhindern, dass das Innere der Datei betrachtet werden kann. Die Ersteller von Malware können darüber hinaus den Schadcode in harmlosen Code einbetten, um ihn zu verbergen.

Diese Vorgehensweisen machen es Sicherheitsexperten schwer, diese bösartigen Dateien überhaupt zu erkennen (und den verborgenen Mechanismen zu begreifen). Und bei AV-Programmen mit heuristischen Scans in einer Sandbox-Umgebung helfen sie der Malware, sich bis zum Einschleusen in das Produktivsystem zu tarnen.

WIE SOLARWINDS HELFEN KANN

Zum Schutz vor modernen Bedrohungen brauchen Anbieter von Managed Services (MSPs) mehrstufige Sicherheitsmaßnahmen. Durch überlappende Sicherheitselemente lässt sich die Gefahr, zum Opfer zu werden, auf ein Minimum reduzieren. SolarWinds MSP hat zwei Plattformen für das Remote-Monitoring und -Management im Angebot: SolarWinds® RMM und SolarWinds N-central®. Damit können Sie mehrstufige Sicherheitsmaßnahmen bei Ihren Kunden implementieren. Wenn eine AV-Lösung eine Bedrohung nicht erkennen kann, können Sie mit Web Protection bösartige Links auf die Schwarze Liste setzen. E-Mail-Schutz schiebt Spam einen Riegel vor und unterbindet Phishing-Versuche, während Patch-Management Schwachstellen kittet – sowohl im Betriebssystem als auch in externer Software. Und sollte ein Angriff doch einmal erfolgreich sein, lassen sich Ihre Dateien oder Systeme mit der integrierten Backup- und Wiederherstellungsfunktion wiederherstellen.

Beide Plattformen verfügen zudem über SolarWinds Endpoint Detection and Response (EDR) mit SentinelOne®. SolarWinds EDR sorgt zuverlässig für die Vermeidung, Erkennung und Bekämpfung von Cyberangriffen auf die Endpunkte Ihrer Kunden. Der signaturlose Ansatz ist herkömmlichen Antivirenprogrammen weit überlegen: Wartezeiten für regelmäßige Scans oder Aktualisierungen der Signaturdefinitionen entfallen. Im Falle eines Angriffs kann EDR die erforderlichen Schritte einleiten, um die Bedrohung einzudämmen, die Angriffsspuren zu beseitigen und den Endpunkt bzw. die befallenen Dateien in einen früheren einwandfreien Zustand zurückzuversetzen.



Weitere Informationen finden Sie unter solarwindsmsp.com/de

SolarWinds ist ein führender Anbieter von leistungsfähiger und erschwinglicher Software zum IT-Infrastrukturmanagement, mit der Unternehmen unabhängig von ihrer Größe und der Komplexität ihrer IT-Infrastruktur die Leistung ihrer IT-Umgebungen überwachen und verwalten können – on-premise, in der Cloud oder in hybriden Umgebungen. Durch fortlaufenden Kontakt mit Spezialisten der Bereiche IT Operations, DevOps und Managed Services kennen wir die Anforderungen bei der Wartung leistungsstarker und hochverfügbarer IT-Infrastrukturen genau. Das Angebot von SolarWinds MSP richtet sich an Anbieter von Managed Services (MSPs). Wir bieten vielseitige, skalierbare Lösungen für das IT-Servicemanagement mit integrierter mehrschichtiger Sicherheit, kollektiver Intelligenz und intelligenter Automatisierung. Unsere Produkte unterstützen MSPs dabei, kleinen und mittleren Unternehmen überzeugende IT-Dienstleistungen anzubieten und ihren eigenen Betrieb effizienter zu verwalten.