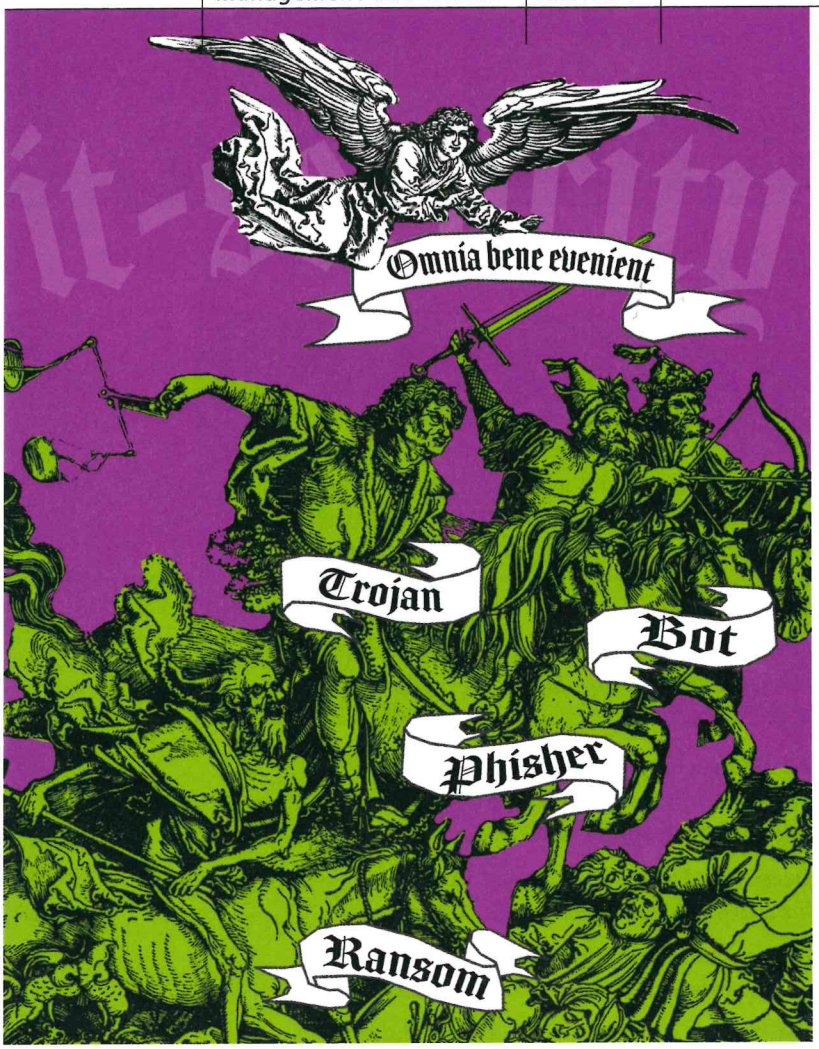

Dasselbe in Grün?

Trends im Malwareschutz

Bisweilen könnte man denken, in Sachen Malware gilt das Motto „Same Procedure as every Year": Schwerpunkte und Taktiken verschieben sich, aber das ewige Katz-und-Maus-Spielchen geht immer weiter und so richtig kriegen Anbieter und Security-Abteilungen das Problem nicht in den Griff. Tatsächlich haben viele Techniken in Angriff und Abwehr recht alte Wurzeln und werden über die Jahre hinweg verfeinert oder in neue Modelle gegossen – doch auch „echter" Fortschritt ist auf beiden Seiten zu beobachten.

Von Stefan Strobel, Heilbronn

Die Malwareschutzbranche ist in den letzten Jahren stark in Bewegung. Die immer aggressiveren Angriffe durch Ransomware mit Emotet als bekanntestes Beispiel (s. a. S. 66), aber auch die stärker werdende Rolle von Microsoft in den letzten Jahren haben dies maßgeblich beeinflusst. Natürlich gab es schon immer Bewegung in diesem Technologiesegment: Während die ersten Virenschutzlösungen in den 80er-Jahren primär nach bekannten Mustern in Dateien gesucht haben, kam man bald auf die Idee, dies mit Heuristiken zu ergänzen und so auch Varianten von Malware zu erkennen, die ähnlichen aber doch neuen Code enthalten.

Frühe Ursprünge

Neben der statischen Analyse des Codes kamen die Hersteller recht früh schon auf die Idee, das Verhalten potenzieller Malware zur Laufzeit zu beobachten, um so bösartiges Verhalten erkennen zu können. Zunächst waren diese Eingriffe in den Ablauf von Programmen relativ einfach. Die frühen Sandbox-Lösungen, aber auch erste Host-Intrusion-Prevention-Produkte von Herstellern wie Okena oder auch Platform Logic brachten die Idee auf eine neue Ebene, indem sie nahezu alle Ressourcenzugriffe von Programmen kontrolliert haben.

Die ersten **Sandboxing-Systeme** kamen schon in den 90er-Jahren von Firmen wie Aladdin und Finjan auf den Markt. Die Grundidee war dabei, dass potenziell gefährliche Programme auf dem Endgerät wie beispielsweise der Web-Browser und Programme, die von diesem heruntergeladen werden, keinen vollen Zugriff mehr auf die Ressourcen des Betriebssystems haben, sondern in einem „Sandkasten" eingesperrt werden, in dem sie keinen Schaden anrichten können.

Eine Sandbox fängt dazu beispielsweise schreibende Zugriffe auf die Festplatte ab und speichert Änderungen in einem eigenen Bereich. Aus Sicht des schreibenden Programms war die Änderung erfolgreich, aber außerhalb der Sandbox ist davon nichts sichtbar und die Sandbox kann jederzeit in den ursprünglichen Zustand zurückgesetzt werden, indem man die zwischengespeicherten Änderungen einfach löscht. Eine Sandbox verhindert somit Schaden und ermöglicht dennoch die nahezu störungsfreie Ausführung von Programmen.

Auch **Host-Intrusion-Prevention-Systeme (HIPS)** greifen in alle Zugriffe von Programmen auf Ressourcen, wie das Dateisystem oder die Registry von Windows, ein. Allerdings täuschen sie Änderungen nicht

vor, sondern erlauben oder verhindern diese anhand einer komplexen Regelbasis für jedes einzelne Programm.

Heutige Implementierung

Beide Techniken waren ihrer Zeit weit voraus, als sie auf den Markt kamen – und deshalb zunächst recht erfolglos. Die ersten Hersteller wurden rasch von größeren Firmen aufgekauft. In modernen Malwareschutzlösungen findet man heute mehrere Verfahren, die von diesen ursprünglichen Ideen abstammen.

Sie verwenden Sandboxing allerdings meist nicht mehr, um potenziell gefährliche Programme dauerhaft zu isolieren, sondern um eine gesicherte Analyseumgebung bereitzustellen, in der verdächtige Programme für einen gewissen Zeitraum beobachtet werden, um sie dann anhand ihres Verhaltens zu klassifizieren. Manchmal sind die Sandboxes dabei eigene Gateways, die eingehende E-Mail-Attachments oder per Web heruntergeladene Dateien auf dem Weg zum Endgerät in einer Isolationsumgebung analysieren, manchmal laufen sie in der Cloud des Herstellers und die Malwareschutz-Agenten auf den Endgeräten laden verdächtige Dateien bei Bedarf in diese Sandboxes hoch oder sie sind ein Teil des Virenschutz-Agenten auf dem Endgerät selbst.

Aus den ursprünglichen HIPS-Ideen sind heute meist einfachere und gezieltere Regeln geworden, die von Malwareschutzlösungen oder vom Betriebssystem selbst umgesetzt werden. Ein beliebtes Beispiel ist eine Regel, die verhindert, externe Programme aus Office-Makros heraus zu starten. Die Lösung von Cylance hatte dies 2016 unter dem Titel *Macro Script Control* eingeführt und in Windows 10 kann man solche Regeln mit dem Feature *Attack Surface Reduction* aktivieren.

Generell haben Windows 10 und die im Jahr 2017 von Microsoft eingeführte neue Version des kostenlosen Malwareschutzprodukts *Defender-Antivirus (AV)* die Branche stark beeinflusst. Während Virenschutz von Microsoft zuvor meist belächelt wurde, nimmt seither fast jeder das Produkt ernst und viele Unternehmen ersetzen bisherige Zusatzsoftware durch die Funktionen, die kostenlos in Windows enthalten sind. Malwareschutz ist damit kein zusätzlicher Agent mehr, der installiert und aktualisiert werden muss, sondern ein **integraler Bestandteil des Betriebssystems.**

Dabei sollte man Defender-AV jedoch nicht einzeln betrachten, sondern im Zusammenspiel mit den Exploit-Mitigation-Funktionen des *Defender Exploit Guard Exploit Protection, Attack Surface Reduction, AppLocker* und den anderen Sicherheitsfeatures des Betriebssystems einsetzen. Für etablierte Hersteller von Speziallösungen ergab sich daraus dennoch eine höhere Dringlichkeit, sich mit zusätzlichen Features, besserem Management oder nochmals höherer Sicherheit gegen die kostenlose Konkurrenz abzugrenzen.

Aktuelle Entwicklungen

Ein weiteres neues Hypethema der letzten Jahre war **künstliche Intelligenz (KI)** beziehungsweise „maschinelles Lernen". Da solche Ansätze im Bereich Malwareschutz zur Klassifikation von Dateien keine Signaturen, sondern vom Hersteller trainierte neuronale Netzwerke verwenden, erreichen sie bei neuer Malware deutlich höhere Erkennungsraten als signaturbasierte Ansätze.

Allerdings sind neuronale Netze meist nur für exe-Dateien trainiert und können daher kaum Malware auf Basis von Exploits oder Office-Makros erkennen. Für Organisationen, die bereits den kostenlosen AppLocker von Windows verwenden, um sich vor Bedrohungen durch ausführbare Programme zu schützen, ist der Zusatznutzen daher begrenzt – denn heruntergeladene oder

per E-Mail empfangene Programme können dann sowieso nicht ohne Weiteres gestartet werden.

Inzwischen nehmen fast alle Hersteller für sich in Anspruch, dass sie KI-Methoden beziehungsweise maschinelles Lernen in ihren Produkten verwenden. Die Unterschiede liegen dabei jedoch im Detail. Maschinelles Lernen allein sagt kaum etwas darüber aus, ob der Mechanismus wirklich zu einer höheren Erkennungsrate führt.

Ebenso gibt es heute kaum noch Malwareschutzlösungen, die ohne eine **Cloud-Anbindung** auskommen, was auch technisch einfach nachvollziehbar ist: Die Menge neuer Malware, die heute täglich verarbeitet werden muss, lässt sich nicht mehr sinnvoll in Signaturlisten abbilden und verteilen. In einer Cloud-Datenbank kann man hingegen problemlos immense Datenmengen ablegen – und so verwenden nahezu alle Hersteller zumindest Abfragen von Hashwerten über ihre Cloud-Services. Darüber hinaus kommen oft noch KI-Mechanismen, die nicht auf dem Endgerät selbst, sondern in der Cloud bestimmte Daten analysieren oder Sandboxes, in denen die Ausführung von verdächtigem Code in der Cloud isoliert beobachtet wird.

Endpoint Discovery and Response (EDR)

Unabhängig von präventiven Mechanismen haben Hersteller auch ihre Verfahren zur Erkennung von bösartigem Verhalten immer weiter ausgebaut. Eine Herausforderung besteht dabei darin, dass sich ein auffälliges Verhalten oft nicht eindeutig als bösartig klassifizieren lässt. Wenn ein Malwareschutzprogramm im Zweifel einschreitet und den auffälligen Prozess stoppt, führt dies gelegentlich aber dazu, dass legitime Anwendungen nicht mehr richtig funktionieren, was Benutzer in der Praxis nicht akzeptieren – daher sind Hersteller in diesem Bereich sehr vorsichtig.

Ergänzend zu den normalen Malwareschutz-Suiten haben sich deshalb Zusatzprodukte etabliert, die meist als **Endpoint Discovery and Response (EDR)** vermarktet werden. Im Bereich der Erkennung zeichnen solche Lösungen möglichst viele Einzelheiten zum Verhalten von Prozessen auf, stellen diese auch grafisch dar und enthalten in der Regel eine Komponente, die auf der Basis maschinellen Lernens Zusammenhänge erkennt und Alarme auslöst.

Bei diesen Lösungen steht nicht mehr das automatische Blockieren im Vordergrund, sondern die möglichst umfassende und qualifizierte Alarmierung im Verdachtsfall. Wenn beispielsweise ein Anwender aus einem Browser heraus ein Programm herunterlädt und startet und dieses Programm danach eine Verbindung zu einem Server in China oder Russland aufbaut, weitere Programmteile nachlädt, seine Rechte erweitert, die Registry manipuliert und Dateien verschlüsselt, dann zeigt ein EDR-Programm idealerweise den kompletten Ablauf grafisch an und bewertet ihn im Gesamtkontext.

Zusätzlich haben Hersteller meist auch Funktionen implementiert, mit denen man auf einen solchen Alarm reagieren kann. Bei manchen Anbietern können beispielsweise relevante Prozesse beendet und sogar Änderungen rückgängig gemacht werden, welche die mutmaßliche Malware am System durchgeführt hat.

Da mit einer EDR-Lösung eine umfassende Sicht auf die technischen Vorgänge auf Endgeräten erreicht wird, kann man sich natürlich fragen, ob zusätzliche Erkennungstechniken im Netzwerk jetzt überhaupt noch notwendig sind. Hier kommt es sicher auf den Einzelfall an: Einerseits sieht ein EDR-Produkt auch die Kommunikation von und zum betroffenen Endgerät, andererseits gibt es möglicherweise Endgeräte, Server oder Internet-of-Things-(IoT)-Devices im Netzwerk, die nicht mit EDR-Software bestückt sind und deren Verhalten sich dann nicht beobachten ließe.

Um noch einen Schritt weiter zu gehen, bieten einige Hersteller, die nicht nur Malwareschutz auf Endgeräten, sondern auch im Netzwerk verkaufen, eine Integration beider Bereiche an. Eine beliebte Bezeichnung dafür lautet **Extendend Detection and Response (XDR)**, um deutlich zu machen, dass hier mehr als EDR drinsteckt – auch von **Cross Layer Detection and Response (XDR)** ist die Rede, um die ebenenübergreifende Analyse zu betonen. Meist findet die Analyse dann auch nicht mehr auf einem Server in der eigenen Organisation statt, sondern in einem KI-basierten Cloud-Service des Herstellers, teils optional mit Analysten, welche die KI durch menschliche Intelligenz ergänzen.

Solche Services konkurrieren dann durchaus mit Services eines Security-Operations-Centers (SOC), die noch auf klassische Art ohne EDR die Logs und Events von möglichst vielen Geräten in einem Security-Information- and -Event-Management (SIEM) sammeln und mit Regeln korrelieren. Die moderne Variante auf Basis von EDR-Daten oder sogar zusätzlich Netzwerk-Anomalien ist nicht zuletzt bei der Erkennung von Malware-Aktivitäten einem einfachen klassischen SOC oft überlegen. Denn bei vielen Datenquellen eines klassischen SIEM fehlt Kontext, den man dann erst im SIEM-System durch aufwendige Korrelation zu rekonstruieren versucht. EDR-Systeme bringen dagegen diesen Kontext prinzipbedingt mit, da sie die tatsächlichen Vorgänge auf den Endgeräten in ihrer Verkettung sehen.

Eine interessante Bewertung dieses Marktsegments findet man in den Produkt-Evaluationen gegen

das **Mitre ATT&CK-Framework**, die von Mitre selbst publiziert werden (https://attackevals.mitre.org). Das ATT&CK-Framework gliedert das Verhalten eines professionellen Angreifers in Taktiken und Techniken (s. a. S. 15). Der Fokus liegt dabei auf dem Vorgehen nach einer ersten Kompromittierung und entsprechend sind die Produkte, die an der Evaluation teilgenommen haben, vor allem EDR-Produkte.

Für diese Evaluationen von Produkten hat Mitre im Labor Angriffe von bekannten APT-Gruppen simuliert und dabei einen Teil der Techniken des Frameworks verwendet – ein Test gegen alle denkbaren Techniken wäre laut Mitre allerdings unpraktikabel. Man kann den veröffentlichten Ergebnissen entnehmen, welches Produkt bei welchem Schritt des Angriffs Informationen geliefert oder Alarme erzeugt hat. Dazu muss man jedoch die als JSON-Dateien verfügbaren Rohdaten herunterladen und diese selbst auswerten, denn die Ergebnisgrafiken auf der Website von Mitre sind wenig aussagekräftig und eignen sich nicht dafür, Produkte miteinander zu vergleichen. Bisher hat Mitre zwei Testrunden durchgeführt und veröffentlicht: einmal mit einer Simulation von APT-3 und einmal mit einer Simulation von APT-29. Eine dritte Runde ist laut Website derzeit in Vorbereitung.

Ausblick

Eine spannende Frage für die nächsten Jahre wird die Zukunft von Nischentechniken wie Mikrovirtualisierung oder Sanitisation sein.

Bei **Mikrovirtualisierung** versucht man Malware nicht mehr zu erkennen, sondern ihre Ausführung in einer speziellen virtuellen Maschine vom eigentlichen Arbeitsplatz zu isolieren. Neben der Firma Bromium, die diese Idee auf den Markt gebracht hat, inzwischen aber von HP aufgekauft wurde, hat auch Microsoft schon einige Funktionen aus dem Bereich Mikrovirtualisierung in Windows 10 eingebaut. Unter dem Namen *Windows Defender Application Guard* kann der Edge-Browser in einer isolierten VM ablaufen. Die Technik überzeugt zwar in der Praxis noch nicht so ganz, hat aber das Potenzial, in zukünftigen Versionen den Malwareschutz von Windows nochmal stark zu verbessern.

Auch **Sanitisation** – bisweilen auch altenativ als „Content Disarm and Reconstruction (CDR)" oder Datenwäsche bezeichnet – könnte die Abwehr von Malware in Zukunft stärker beeinflussen. Dabei werden Dokumente in ihre Einzelbestandteile zerlegt und daraus neue Dateien erzeugt, die im Idealfall keinen Schadcode mehr enthalten können.

Beide Verfahrensweisen sind heute noch sehr wenig verbreitet, bieten aber prinzipiell einen sehr hohen Schutz, allem voran vor neuer und noch unbekannter Malware. ■

Stefan Strobel ist Geschäftsführer der cirosec GmbH.