Wie funktionieren Virenscanner

Gregor Faiman
BIT 19
Fachhochschule Wiener Neustadt

Wiener Neustadt, Österreich
Gregor.Faiman@fhwn.ac.at

***Abstract*—Dieses Dokument befasst sich mit dem Begriff der Malware, und weiterführend mit den Begriffen Anti Viren Software, sowie Anti Malware Software. Der Autor setzt es sich zum Ziel, dem Leser einen Überblick über die gängigsten Arten von Malware, sowie der Funktionsweise von Software, die es sich zum Ziel setzt, Malware die Stirn zu bieten, zu verschaffen. So wird nach einer einleitenden Definition von Malware über die zwei Arten von Anti Viren sowie Anti Malware Software gesprochen, wonach eine Erläuterung der bekanntesten Strategien zur Erkennung bösartiger Software führt. (*Abstract*)**

I. Einleitung

Dieses Dokument setzt es sich zum Ziel, dem Leser einen Überblick über die Funktionsweise von Antiviren Software zu verschaffen. Den Beginn des Dokuments bildet die Definition des Begriffs Malware, ein Begriff der gleichzeitig als Verständnisbasis für den Rest des Dokuments anzusehen ist. Anschließend wird über die gängigsten Antiviren Softwarelösungen und deren Vorgehensweise um Malware zu identifizieren, gesprochen. Der letzte Abschnitt dieses Schreibens, soll einen Überblick bieten, was die jeweiligen Vor- sowie Nachteile der diversen Antiviren Strategien sind. Nach ausgiebigem Studieren dieses Schreibens, soll es dem Leser möglich sein, den Begriff der Malware zu definieren, ihre gängigsten Vertreter sowie deren Funktionsweise zu nennen, und über Strategien zu sprechen, die zur Bekämpfung eben jener eingesetzt werden.

II. Definition Malware

Bevor über Antivirus Software gesprochen wird, sollte zunächst geklärt sein, worum es sich bei einem Virus überhaupt handelt. Im alltäglichen Sprachgebrauch fällt das Wort Computervirus überall dort, wo ein Computersystem sich aufgrund eines oder mehrerer Schadprogramme unnatürlich verhält. Beispiele von Situationen, in denen von einem Virus gesprochen wird, sind etwa PopUps die den Benutzer davon in Kenntnis setzen, dass die gesamte Festplatte verschlüsselt wurde und eine Geldsumme bezahlt werden muss, um sämtliche daten nicht zu verlieren; ein Programm, welches vorgibt harmlos zu sein aber im Hintergrund private Daten eruiert und weiterschickt; oder ein Programm welches sämtliche Daten auf der Festplatte löscht.

Tatsächlich ist hier die einheitliche Verwendung der Bezeichnung Virus eine Ungenauigkeit. Vielmehr ist hier von Malware zu sprechen. Diese ominöse Malware kann verschiedenste Formen annehmen. Auf die gängigsten Vertreter wird nachfolgend eingegangen.

A. Malware - Virus

Beginnen wird die Runde der Computervirus. Ein Virus ist kein eigenständiges Programm. Stattdessen bezeichnet der Begriff Virus Code Snippets, die sich in den Code einer anderen Applikation einschleusen, um dort beim Ausführen der Applikation, neben dem nativen Programmcode ausgeführt zu werden.

B. Malware - Trojaner

Ein Trojaner ist ein eigenständiges Programm, das sich dadurch auszeichnet, nach Außen den Anschein zu erwecken, ein harmloses, legitimes Programm zu sein. Allerdings beruht das Innenleben darauf, dir durch das Ausspionieren deiner persönlichen Daten Schaden zuzufügen. Der größte Unterschied zum Virus ist jener, dass es sich beim Trojaner anders als beim Virus, um ein eigenständiges Programm handelt.

C. Malware – Wurm

Ein Wurm kann als eine Art großer Bruder des Virus angesehen werden. Ein Wurm vermehrt sich ähnlich wie ein Virus, indem er Kopien von sich erstellt, und diese auf dem sich zu vermehrendem System verteilt. Jedoch benötigt ein Wurm dafür keine Host Programme, weil der Wurm selbst, anders als der Virus, ein eigenständiges Programm ist.

D. Malware – Ransomware

Unter dem Begriff Ransomware versteht man Software, die die eigene Festplatte, oder Teile von dieser, verschlüsselt und den Benutzer auf diese Weise zu erpressen versucht. Um die verschlüsselten Daten wieder zu entschlüsseln, ist es notwendig, eine oftmals beträchtliche Summe an Geld zu bezahlen.

III. Virenscanner und deren Funktionalität

Im vorigen Kapitel wurde der Begriff der Malware definiert, und auf gängige Vertreter und deren Auswirkungen auf ein Computersystem eingegangen. Jedoch bleibt noch die Frage offen, wie es möglich ist, die Auswirkungen von Schadsoftware zu minimieren oder gänzlich zu eliminieren. An diesem Punkt kommen Antiviren, sowie Anti Malware Software ins Spiel. Bei diesen Softwares wird grundsätzlich zwischen zwei verschiedenen Methodiken der Gefahrenbekämpfung unterschieden, der reaktiven Strategie sowie der proaktiven Strategie. Die Unterschiede zwischen Anti Virus und Anti Malware Software, sowie zwischen reaktiver Erkennung und proaktiver Erkennung, werden in diesem Kapitel behandelt.

A. *Anti Virus Software*

Ein Virenscanner, oftmals auch Antiviren Software genannt, ist eine Software, die Möglichkeiten bietet, die gängigsten Arten von Malware zu erkennen und zu verhindern, dass diese Schäden an einer Maschine anrichten. Aus der Verwendung des Begriffs Malware geht hervor, dass eine Antiviren Software, trotz des Namens, der vermuten lassen würde, sie würde rein gegen Viren ein angemessenes Effektivitätsniveau besitzen, auch andere Formen von Malware erkennen und bekämpfen kann. Die Kompetenzen der Antiviren Software beschränken sich hier jedoch auf die häufigsten Vertreter von Malware, mit Viren, Trojanern und Würmern. Eine gewöhnliche Antiviren Software ist in der Regel gegen anspruchsvollere Malware, wie etwa Ransomware oder Rootkits machtlos. Daher bietet Antiviren Software auch beispielsweise keinen Schutz gegen Phishing Seiten. Um bestmöglichsten Schutz gegen ein breiteres Spektrum an Malware zu bieten, gibt es neben Antivirus Software auch noch Anti Malware Software.

B. *Anti Malware Software*

Im Gegensatz zu einer Antivirus Software, ist eine Anti Malware Software gegen ein weitaus breiteres Spektrum an Gefahren effektiv einzusetzen. So kann Anti Malware Software beispielsweise vor Ransomware schützen, indem sie bei Ausführung dieser interveniert, bevor die Ransomware die Chance hat, die Festplatte zu verschlüsseln. Eine weitere Handlungsmöglichkeit von Anti Malware Software ist es, vor Phishing Seiten zu schützen, indem beim Besuchen einer Website, diese Seite analysiert wird, und sofern sie als Phishing Seite erkannt wird, jene Seite schnellstmöglich blockiert wird. Wenn es jedoch um die Erkennung und Bekämpfung von Klassikern wie Viren, Trojanern und Würmern geht, steht eine Anti Malware Software einer Antiviren Software sowohl was Performanz als auch was Effektivität angeht, weit nach. Eine Anti Malware Software setzt es sich auch nicht zum Ziel, eine Anti Viren Software gänzlich abzulösen, sondern stellt eine Ergänzung für die eigene Sicherheit dar. Zusammenfassend lässt sich also hierzu sagen, dass eine Anti Malware Software Strategien gegen ein breites Spektrum an selteneren, dafür potentiell komplexeren Malware Arten bietet, während eine Antiviren Software gegen ein kleines Spektrum an besonders häufig auftretenden Problemen, höchst effizient arbeiten kann.

C. *Reaktive Strategie*

Bei einer reaktiven Strategie wird nach dem Prinzip vorgegangen, auf eine Bedrohung erst dann zu reagieren, wenn sich diese tatsächlich als Bedrohung entpuppt. So würde bei einer rein reaktiven Lösung, eine Anwendung vor der Ausführung nicht gescannt. Genauso würden nicht im Hintergrund immer wieder proaktive Systemchecks durchgeführt werden, um nach bösartig wirkenden Signaturen zu suchen.

D. *Proaktive Strategie*

Bei einer proaktiven Strategie, werden sämtliche Dateien und Programme im Vorhinein gescannt, beispielsweise bei dem Download einer Datei, oder vor der Ausführung eines Programms, um potentielle Bedrohungen möglichst früh zu erkennen, und terminieren zu können, ohne ihnen überhaupt die Chance zu bieten, Schaden anzurichten. Die Devise lautet hier: „Besser vorher Arbeit investieren, damit nachher auch garantiert nichts passiert“.

IV. Erkennungsverfahren

Neben der Frage, wie eine Schutzsoftware vorgehen kann wenn es um das Suchen nach Malware geht, ist es auch notwendig darüber zu sprechen, wie ein Programm überhaupt als gefährlich erkannt wird. Für die Identifikation von Malware setzen diese Softwarelösungen auf verschiedene Strategien. Diese Strategien, und ihre generelle Funktionsweise darzulegen, ist das Ziel dieses Abschnitts.

A. *Erkennungsstrategien – Signaturen*

Wenn bei Malware von einer Signatur die Rede ist, wird damit eine Art Fingerabdruck des spezifischen Programms oder Files gemeint, anhand dessen es zu identifizieren ist. Die Signatur selbst kann mehrere Formen annehmen, beispielsweise könnte sie eine Folge an spezifischen Bytes welche oft in Verbindung mit Malware zu finden sind, ein Hash, oder spezielle Strings sein. Signaturen von bekannter Malware werden in eine Datenbank gespeichert. Wird jetzt ein bestimmtes File, oder ein bestimmtes Executable auf seine Signatur überprüft, wird diese Signatur mit der Sammlung von bekannten Signaturen in den diversen Datenbanken abgeglichen, um so festzustellen, ob es sich bei dem File oder Programm um bekannte Malware handelt oder nicht.

B. *Erkennungsstrategien – Heuristics*

Wenn in Kombination mit Anti Viren Software von Heuristics die Rede ist, werden damit gewisse Regeln gemeint, anhand derer es möglich ist, Malware, oder zumindest verdächtiges Verhalten zu erkennen. Solche Regeln können beispielsweise sein, dass ein Programm versucht sich selbst zu replizieren, Code in andere Programme zu injizieren, oder versucht, nach seiner vermeintlichen Terminierung im Arbeitsspeicher aktiv zu bleiben.

C. *Erkennungsstrategien – Sandboxing*

Eine Sandbox im technischen Sinn, beschreibt einen virtuellen, vom System logisch abgetrennten Bereich, in dem ein Programm ausgeführt werden kann, um sein Verhalten zu analysieren. Sandboxing ist eine weitere Methode, die von Anti Viren und Anti Malware Programmen verwendet werden kann, um potentiell bösartige Software als solche zu entlarven, da davon ausgegangen werden kann, dass ein Programm, welches sich im Sandbox Testing verdächtig verhält, mit hoher Wahrscheinlichkeit nichts für den Benutzer Förderliches im Schilde führt.

V. Die Strategien im Kontrast

Abschließend ist noch über die Vor- sowie Nachteile von den genannten Strategien zur Malware Erkennung zu sprechen. Während die Signatur basierte Strategie weitläufig Anwendung findet, da sie vergleichsweise schnell durchführbar ist, und bereits eine umfassende Datenbank an

Software Signaturen die zu Schädlingen gehören besteht, darf nicht außer Acht gelassen werden, dass diese Strategie darauf angewiesen ist, dass die Signatur einer bösartigen Software bereits in einer Datenbank vorzufinden, also bekannt ist. Somit ist diese Strategie machtlos, gegen sogenannte „Zero Day Malware“, womit neuartige Malware gemeint ist, die bislang unbekannt und somit auch undokumentiert ist. Heuristics bieten hier bereits besseren Schutz, da hierbei nicht die Signatur, sondern das Verhalten der zu überprüfenden Software selbst bewertet wird. Allerdings besteht bei der Verwendung von Heuristics die Gefahr, aufgrund von schlecht konfigurierten Regeln, entweder Malware nicht als solche zu erkennen, oder ehrliche, nicht bösartige Software als Malware einzustufen.

Sandboxing scheint zunächst eine perfekte Lösung zu sein. Tatsächlich ist es eine gute Idee, ein Programm dem nicht vertraut werden kann, in einer sicheren Umgebung zu testen, und sein Verhalten zu analysieren. Allerdings steht es jedem Programm nach Verlassen der Sandbox, sofern es als sicher eingestuft wurde, ungehindert zu arbeiten. Dadurch entsteht ein Problem, welches „Sandbox Evading“ genannt wird. Dabei wird ein Programm so geschrieben, dass es sich im Falle dessen, dass es in einer virtuellen Umgebung ausgeführt wird, anders verhält als es sich verhalten würde, wenn es auf einem realen System gestartet wird, wodurch im Sandboxing die Gefahr nicht erkannt, und das Programm anschließend normal ausgeführt werden würde.