

Worms & Co – Malicious Code

- Antivirenprogramme -

Wolfgang Zejda

Ausarbeitung zum Hauptseminar

Abstract: Viren breiten sich immer weiter aus und werden immer stärker zum Problem. Diese Ausarbeitung zeigt die Methoden der Viren und der Antivirenprogramme. Es werden die Methoden wie Viren versuchen die Antivirenprogramme zu überlisten (Stealth, Polymorphie, Verschlüsselung) und die Gegenmaßnahmen der Antivirenhersteller (Heuristik, Sandboxing) gezeigt. Es zeigt sich, dass eine Kombination der bestehenden Idee der Antivirenhersteller bereits einen akzeptablen Schutz bieten kann. Besonders effektiv ist hierbei die Analyse von Viren in Netzen und die Verbreitung der daraus gewonnenen Daten, die jedoch flächendeckend an dem Konkurrenzdenken der Hersteller scheitert.

Inhalt:

1. Viren und Antivirenprogramme
2. Was sind Viren
 - 2.1. Arten von Viren
 - 2.2. Methoden von Viren
 - 2.2.1. Bootsektorviren
 - 2.2.2. Dateiviren
 - 2.2.3. Tarnkappenviren (stealth virus)
 - 2.2.4. Polymorphe Viren
 - 2.2.5. Programmierbare Viren
 - 2.2.6. Makroviren
 - 2.2.7. Verschlüsselung
3. Maßnahmen von Antivirenprogrammen
 - 3.1. Abwehrmaßnahmen gegen Viren
 - 3.2. Angriffsmaßnahmen gegen Viren
 - 3.2.1. Maßnahmen gegen bekannte Viren
 - 3.2.1.1. Signaturen
 - 3.2.1.2. Impfungen
 - 3.2.1.3. Viren-Profilanalyse
 - 3.2.2. Maßnahmen gegen unbekannte Viren
 - 3.2.2.1. Prüfsummen
 - 3.2.2.2. Heuristik
 - 3.2.2.3. Überwachung kritischer Bereiche
 - 3.2.2.4. Sandboxing
 - 3.2.2.5. Heuristische Entschlüsselung
 - 3.2.2.6. Statische und dynamische heuristische Verfahren
4. Ausblick in die Zukunft
 - 4.1. weitere Methoden von Antivirenherstellern
 - 4.2. Ausblick im Kampf gegen Viren
5. Quellen

1 Viren und Antivirenprogramme

Viren verbreiten sich immer stärker und verursachen immer größere Kosten. Viren können ganze Rechnersysteme ausschalten und auf diese Art sogar Firmen in ihrer Existenz bedrohen. Der Kampf gegen Viren durch Antivirenprogramme und die Weiterentwicklung dieser, gewinnt deshalb immer mehr an Bedeutung.

2 Was sind Viren

Viren sind Kleinprogramme, die ohne Einverständnis des jeweiligen Benutzers arbeiten, sich verbreiten oder Schaden anrichten.

2.1 Arten von Viren

Viren kann man nach mehreren Kriterien unterscheiden. Man kann diese nach ihrer Schadwirkung klassifizieren:

- Reine Verbreitung
- Verbreitung und Zerstörung von Programmen
- Verbreitung und Zerstörung von Rechnern
- Verbreitung und Ausschalten ganzer Systemgruppen

Eine Andere Möglichkeit ist es, Viren nach der Methode ihrer Verbreitung einzustufen:

- Per E-Mail
- Durch infizierte Dateien
- Durch manipulierte Webseiten
- Durch Angriffe auf Systemdienste

2.2 Methoden von Viren

Viren werden immer fortschrittlicher programmiert und es ist ein ständiger Kampf zwischen Virenprogrammierern und den Herstellern von Antivirenprogrammen, wer die Methoden schneller versteht und weiter fortschreitet. In der Regel sind die Virenprogrammierer etwas weiter und ihr Vorsprung wird erst dann geschmälert, wenn ihr Virus eine gewisse Verbreitung besitzt, dieser von Antivirenherstellern untersucht und ihre Methoden der Verschleierung herausgefunden wurde.

Einige Viren spezialisieren sich sogar darauf, Antivirenprogramme zu finden und zu deaktivieren.

2.2.1 Bootsektorviren

Diese Art der Viren versteckt sich im Bootsektor der infizierten Systeme. Der Vorteil an dieser Methode ist, dass die Viren so direkt bei Systemstart geladen werden und noch vor dem Betriebssystem aktiv werden können. Auf diese Weise können sie Gegenmaßnahmen rechtzeitig erkennen und sich zum Beispiel gegen Antivirenprogramme verteidigen.

2.2.2 Dateiviren

Diese Viren suchen das infizierte System gezielt nach Dateien ab, die sie infizieren können. Dies sind meist ausführbare Dateien (zum Beispiel .com oder .exe unter Windows- / Dosssystemen) in die sich der Virus einnistet. Sobald diese so genannten Wirtsprogramme gestartet werden, wird erst der Virus geladen und dieser startet das eigentliche Programm erst danach.

2.2.3 Tarnkappenviren (stealth virus)

Diese Viren enthalten eine Methode, die das infizierte System überwacht und Antivirenprogramme erkennen kann. Dies geschieht zum einen über eine Liste bekannter Prozesse, zum anderen über das Erkennen von Scanvorgängen.

Stellt ein solcher Virus ein aktives Antivirenprogramm fest, so beginnt er sich aus den jeweiligen Bereichen zu entfernen und die Originale der jeweiligen Dateien wieder herzustellen um sich so einem Erkennen zu entziehen.

2.2.4 Polymorphe Viren

Diese Viren können ihren eigenen Programmcode ändern. Jedes Mal wenn sich ein solcher Virus vermehrt, beginnt er eine Transformation seines eigenen Programms. Dies geschieht zum Beispiel durch Einfügen von NOP Operationen oder durch Ändern der Reihenfolge der Codeblöcke durch unbedingte Sprünge.

2.2.5 Programmierbare Viren

Diese Viren können sich selbst updaten, in dem sie Code von vorgegebenen Quellen nachladen können. Dies können zum einen neue Schadroutinen, aber auch Methoden des Verschleierns sein. Der Virus kann dadurch seine Gestalt nahezu komplett verändern.

2.2.6 Makroviren

Diese Viren befallen keine Programme sondern nisten sich in Makros von Dokumenten ein. Sie können erst aktiv werden, wenn sie von dem Dokument verarbeitendem Programm interpretiert werden.

2.2.7 Verschlüsselung

Diese Viren speichern sich nur verschlüsselt ab. Sobald sich diese Viren speichern, zum Beispiel auf der Festplatte oder in E-Mails, verschlüsselt sich der Virus selbst. Er fügt auch noch eine Routine zum Entschlüsseln hinzu. Wird das Programm nun aufgerufen, so wird erst zur Laufzeit der Virus ausgepackt. Diese Methode verhindert, dass ein Virus in seiner abgespeicherten Form identifiziert und entfernt werden kann.

3 Maßnahmen von Antivirenprogrammen

In dem vorherigen Kapitel wurden die Methoden von Viren geschrieben, wie sie versuchen die Antivirenprogramme zu überlisten. In diesem Kapitel wird nun beschrieben, wie Antivirenprogramme versuchen diese Tricks zu überlisten.

3.1 Abwehrmaßnahmen gegen Viren

Viele Viren versuchen gegen Antivirenprogramme vorzugehen um ihrer Entdeckung und Entfernung zu entgehen. Deshalb müssen Programmierer von Antivirenprogrammen auch Strategien entwickeln um sich gegen direkte Angriffe von Viren zu wehren. Antivirenprogramme versuchen deshalb möglichst früh geladen zu werden und scannen jedes Programm das ausgeführt werden soll. Einige Programme verwenden auch zwei oder mehrere Prozesse, die sich gegenseitig überwachen und darauf achten, dass noch alle Prozesse laufen.

3.2 Angriffsmaßnahmen gegen Viren

Um Viren zu entdecken verwenden Antivirenprogramme folgende Methoden:

3.2.1 Maßnahmen gegen bekannte Viren

Die folgenden Maßnahmen der Antivirenprogramme können nur gegen bereits bekannte Viren angewandt werden

3.2.1.1 Signaturen

Jeder Virus kann anhand seiner Signatur identifiziert werden. Die Signatur eines Virus unterscheidet sich bei verschiedenen Antivirenprogrammen zum Teil erheblich. So kommen einige Hersteller mit kleinen Ausschnitten von Viren aus, während andere den gesamten Rumpf eines Virus speichern müssen.

Wichtig bei dieser Methode ist, dass die Daten der Signaturen immer aktuell sind. Viele Antivirenprogramme werden deshalb täglich, mindestens jedoch wöchentlich, aktualisiert.

Ein Nachteil dieser Methode ist, dass bereits geringe Veränderungen am Virus selbst es dem Antivirenprogramm sehr schwer oder gar unmöglich machen, den Virus zu identifizieren. Bei manchen Viren reicht hierfür bereits das Verändern eines einzigen Zeichens aus.

3.2.1.2 Impfungen von Dateien

Dabei handelt es sich um Versuche der Hersteller von Antivirenprogrammen Kennzeichen in Dateien zu integrieren, wie sie auch Viren verwenden um zu erkennen, ob diese bereits infiziert sind.

6 Wolfgang Zejda

Der Vorteil dieser Methode ist, dass Viren an der Verbreitung gehindert werden und sich gar nicht erst in dem System einnisten.

Jedoch hat diese Methode einige Nachteile, so verweigern einige Programme danach ihre Ausführung. Weitere Probleme gibt es bei dem Verwenden mit Virencannern, da diese Signaturen auch ausreichen können um diese Datei gegenüber dem Virencanner als infiziert auszuzeichnen. Auch ist diese Variante bei der Masse an Viren äußerst unökonomisch, da sich diese Signaturen nicht mit vertretbarem Aufwand herstellen lassen.

3.2.1.3 *Viren-Profilanalyse*

Die Viren-Profilanalyse ist die Antwort der Antivirenhersteller auf polymorphe Viren. Diese Analyse beruht auf ausgiebigen Tests des Virus in einer Sandbox. Dabei wird versucht alle möglichen Erscheinungsformen des Virus durch geeignete Algorithmen darzustellen. Dies muss solange durchgeführt werden, bis der Virus keine Form von sich mehr erschaffen kann, die nicht durch Algorithmen abgedeckt ist.

Besonders effektiv kann man mit dieser Methode gegen Viren aus Virenkits vorgehen, bei denen sich die Erschaffer von Viren diese einfach zusammenstellen können. Die so erzeugten Viren unterscheiden sich zwar deutlich in ihrer Signatur, jedoch bestehen diese Viren aus der gleichen Basis und werden meist auch nur aus bereits vorbereitetem Assemblercode zusammengefügt. Diese lassen sich durch gezieltes Aufstellen der Algorithmen gut identifizieren.

3.2.2 **Maßnahmen gegen unbekannte Viren**

Da ständig neue Viren entstehen und es eine Zeit dauert, bis die Hersteller von Antivirenprogrammen darauf reagieren können, versuchen moderne Antivirenprogramme Viren bereits zu erkennen bevor der Virus bekannt ist.

3.2.2.1 *Prüfsummen*

Bei dieser Methode werden nicht die Viren direkt entdeckt. Für jede Datei die infiziert werden kann, meist sind dies Programmdateien, wird eine Prüfsumme erstellt und hinterlegt. Sollte nun die entsprechende Datei verändert werden, so ändert sich die Prüfsumme und das Antivirenprogramm kann dies erkennen. Die Prüfsummen müssen hinreichend kompliziert und geschützt sein, damit diese Prüfsummen nicht durch Viren gefälscht werden können. In die Prüfsumme gehen unter anderem der Hashwert sowie das Erstellungs- unter Änderungsdatum der Datei ein.

Der Vorteil darin besteht, dass jede Änderung bemerkt werden kann, ohne dass der Virus dahinter bekannt sein muss.

Der Nachteil dieser Methode ist, dass die Datei nicht wiederhergestellt werden kann und auch der Virus nicht gelöscht wird. Auch haben sich Tarnkappenviren genau auf diese Methode spezialisiert und können Antivirenprogramme täuschen.

3.2.2.2 *Heuristik*

Es wird virentypischer Code gesucht. Viren enthalten meist typische Funktionen, die von Antivirenprogrammen gefunden werden können. Diese können zum einen Schadfunktionen (zum Beispiel das Löschen von Dateien), Infektionsmethoden (zum

Beispiel das Hinzufügen von Schlüsseln in die Registrierung) oder Verbreitungsmethoden sein (zum Beispiel das Versenden von infizierten E-Mails). Diese Methoden sind meist ähnlich und können so in Antivirenprogramme eingebaut werden, dass sie diese Methoden in einem großen Spektrum erkennen können.

3.2.2.3 *Überwachung kritischer Bereiche*

Diese Methode überwacht kritische Systemressourcen. Dabei werden Systemaufrufe, wie zum Beispiel das Verändern der Registrierung oder Schreiben in den Bootsektor, überwacht und gegebenenfalls von dem Antivirenprogramm unterbunden werden. Die Methode funktioniert natürlich nur in Bereichen, die nicht häufig verwendet werden. Es gibt jedoch keine Methode, mit der das Programm erkennen kann, ob der Zugriff eines fremden Programms als Virusbefall zu werten ist oder zum Normalbetrieb gehört und die Datei nur deshalb nicht erkannt wird, weil sie erneuert wurde.

3.2.2.4 *Sandboxing*

Diese Methode ist die Verbesserung der „Überwachung kritischer Bereiche“. Dabei werden grundsätzlich alle kritischen Systemaufrufe durch das Antivirenprogramm abgefangen und es wird anhand einer Tabelle überprüft, ob dieser Systemaufruf zulässig ist oder nicht. Neuere Antivirenprogramme sorgen dabei dafür, dass weitere Systemaufrufe jedoch nicht von einem Blockierten behindert werden.

Der Vorteil darin besteht, dass es unerheblich ist, ob der Virus versucht sich zu verstecken oder seine Spuren zu verwischen, denn bei dieser Methode wird das Virenprogramm ihn finden.

Ein Nachteil dieser Variante ist, dass die Systemleistung darunter leidet.

Diese Methode wird sehr erfolgreich von „Norman Virus Control“ eingesetzt.

3.2.2.5 *Heuristische Entschlüsselung*

Verschlüsselte Viren können von Antivirenprogrammen nicht identifiziert werden. Um an den entschlüsselten Code eines Virus zu gelangen, muss man den Virus dazu bringen, sich selbst zu entschlüsseln. Die Antivirensoftware kann hierzu ein verdächtiges Programm in einer Sandbox verlangsamt ablaufen lassen und auf verdächtiges Verhalten hin überprüfen.

3.2.2.6 *Statische und dynamische heuristische Verfahren*

Wenn ein Antivirenprogramm das komplette Programm analysieren würde, könnte es unter Umständen sehr lange dauern. Bei der Analyse von Dateien werden hauptsächlich der Anfang und das Ende von Dateien untersucht, da dies die Bereiche sind, in denen sich hauptsächlich Viren befinden. Bei diesen Analysen werden Bytesequenzen des Programms in Sequenzen übersetzt und nach typischen Befehlen von Viren gesucht, wie zum Beispiel Zugriffe auf Datenträger oder das Abschicken einer Mail.

Bei der statistischen heuristischen Analyse kann das Antivirenprogramm seine Entscheidung mit Hilfe einer Datenbank fällen. In dieser werden Bytefolgen gespeichert, die virentypische Aktionen durchführen. Dies ist ähnlich der Analyse

anhand von Signaturen, jedoch deutlich flexibler, da hier Aktionen und nicht nur reine Strukturen untersucht werden.

Der Vorteil dieser Methode ist, dass man unbekannte Viren finden kann, die nur anhand ihrer Aktionen erkannt werden. Man kann so auch Varianten von Viren erkennen, die sich gegenüber dem Stammvirus nur leicht verändert haben.

Der Nachteil dieser Methode ist die Abhängigkeit von einer Datenbank. Sollte ein Virus eine Möglichkeit gefunden haben, eine Schadfunktion mit einer unbekanntenen Methode aufzurufen, so wird diese Analyse den Virus nicht als solchen identifizieren können.

Die dynamische Heuristik arbeitet ähnlich zu einer Sandbox. Das Antivirenprogramm startet einen virtuellen Computer im Computer den das Virus nicht erkennen darf. In diesem geschützten Bereich lässt das Antivirenprogramm nun den Virus laufen und protokolliert jede Aktion des vermeintlichen Virus.

Als sehr effektiv hat sich die Verknüpfung beider Varianten gezeigt. Dies wendet zum Beispiel die Firma Symantec in ihren Produkten als „Bloodhound“ Funktion an.

4 Ausblick in die Zukunft

4.1 weitere Methoden von Antivirenherstellern

IBM entwickelte bereits vor einiger Zeit sein DIS, das Digital Immunsystem. Dieses wurde entwickelt um Viren innerhalb von Netzen (bestenfalls das Internet) automatisch zu erkennen und an einen zentralen Server zu schicken. Dieser versucht diese Datei zu analysieren und für alle Clients die Rezepte für die Erkennung und Entfernung zu entwickeln. Scheitert dies, so schickt dieser Rechner die Datei verschlüsselt an einen speziellen Rechner weiter, der dem potenziellen Virus die Möglichkeit gibt sich auszubreiten und seine Schadwirkung und Struktur zu zeigen. Daraus kann dann dieser Rechner die Rezepte entwickeln und den Servern zur Verfügung stellen.

Dieses Prinzip wurde von allen größeren Antivirenherstellern übernommen und es wird derzeit entwickelt, dieses weiter zu automatisieren um so Erkennungs- und Abwehrmaßnahmen nahezu in Echtzeit, zumindest aber möglichst schnell bereitzustellen.

Diese Methode kann durch geschickte Kombination der bereits bestehenden Analyse einen sehr schnellen und umfassenden Schutz zur Verfügung stellen, da es den Viren nahezu unmöglich ist, dieses Analysensystem zu erkennen. So wird dieser Virus seine Schad- und Verbreitungsmethoden zeigen und es können Gegenmittel entwickelt werden. Es spielt dabei auch keine Rolle, ob der Virus sich verschlüsselt oder polymorph ist, da dies analysiert werden kann. Auch gegenüber modularen Viren wäre man so schneller in der Lage die Gegenmittel zu erzeugen und zu verbreiten.

4.2 Ausblick im Kampf gegen Viren

Viren werden weiter ein Problem bleiben, besonders solange die größte Schwachstelle noch vor dem Computer sitzt und Anhänge aus E-Mails ungeprüft öffnet. Auch müssen die Hersteller von Programmen und Betriebssystemen an ihren Entwicklungen nachbessern und die Eintrittstellen für Viren versuchen zu schließen. Es wird ein Kampf um Techniken aber auch um Zeit werden, ob es Hersteller von Antivirenprogrammen schaffen, dem Druck der Virenhersteller rechtzeitig entgegenzuwirken oder sogar Methoden vorher absichern können. Ein umfassender Schutz wird sich aber sicher nur durch den Ausbau von Netzen bilden lassen, wenn dafür gesorgt wird, dass Computer möglichst schnell die Informationen über Viren erhalten. Dazu ist es allerdings notwendig, dass die Hersteller von Antivirenprogrammen stärker miteinander arbeiten und nicht, wie bisher, den gleichen Viren sogar andere Namen geben.

5 Quellen

Sandeep Kumar, Eugene H. Spafford
A Generic Virus Scanner in C++

Mihai Christodorescu, Somesh Jha
Testing Malware Detectors

Max Doll:
(eMail-) Viren
www.informatik.uni-augsburg.de/lehrstuehle/info1/lehre/ss04/internetsicherheit/02.pdf

Martin Zollhuber:
Destruktive Programme und Gegenmaßnahmen am Beispiel Viren und Virenschanner
stud3.tuwien.ac.at/~e9826031/download/swa_Viren.pdf

Conny Estermann, Martin Waldburger:
Computerviren
www.ifi.unizh.ch/ikm/Vorlesungen/Sem_Sich01/Estermann.pdf

Kathleen Platzk:
Viren
www-rnks.informatik.tu-cottbus.de/de/materials/ss2001psSicherheit/file5_2.pdf