

COMPUTERVIREN

Virii

Trojaner

Olaf Hölscher

Klasse: SIT04

Fachlehrer: Hr. Priggemeyer
BBS – Berufsbildende Schulen
des Landkreises Osnabrück

Osnabrück Brinkstrasse

Osnabrück, den 12.12.2001

Referat über Computerviren

Inhalt:

1.	Einleitung	Seite 2 - 3
1.1	Geschichte der Computerviren	Seite 3 - 4
1.2	Rechtslage	Seite 5
2.	Vergleich biologischer Viren / Computer Viren	Seite 5
3.	Virenarten	Seite 6 - 11
4.	Funktionsweise	
4.1	Die Infektion	Seite 11 - 12
4.2	Die Reproduktion	Seite 12 - 13
5.	Auswirkungen	Seite 13 - 14
6.	Abwehrmaßnahmen	Seite 14
6.1	Antivirenprogramme	Seite 15
6.2	Prüfsummenprogramme	Seite 16
6.3	Vshield-Programme	Seite 16
6.4	Immunisieren	Seite 16
6.5	Entfernen von Viren	Seite 17
7.	Nachwort	Seite 17 - 18

1. Einleitung

Ein Computervirus ist nichts anderes als ein Programm, das der Sabotage in der EDV dienen soll. Als solches kann es nur Schäden an der Software bzw. an Datenbeständen anrichten. Der Name Virus, der manchmal zur falschen Vorstellung von organischen Lebewesen führt, wurde nur aufgrund der Ähnlichkeit der Wirkungsweise von biologischen und Computerviren gewählt.

Um als Virus bezeichnet werden zu können, muss ein Programm in der Lage sein, einerseits eine Sabotage bzw. Manipulation durchzuführen und andererseits Kopien von sich selbst in andere Programme einzuschleusen. Werden nun diese

infizierten/verseuchten Programme ausgeführt, beginnt mit der darin enthaltenen Kopie des Virus der Kreislauf erneut.

Der „klassische“ Virus war dazu gedacht, ein Unternehmen gezielt über dessen EDV zu schädigen. Die Vorteile, die ein Virus dafür bietet, liegen auf der Hand: Es ist möglich, an sonst unzugängliche Daten heranzukommen, der Täter bleibt mit sehr großer Sicherheit unerkannt und die Zerstörung ist sogar effizienter als eine Löschung der Daten, da eventuell vorhandene Sicherungskopien bei deren Einsatz ebenfalls verseucht werden. Darüber hinaus kann sich ein Virus sehr schnell verbreiten: Selbst wenn eine verseuchte Datei jeweils nur eine Kopie erstellt, wächst die Anzahl der verseuchten Dateien exponentiell.

1.1 Geschichte der Computerviren

Die ersten Ideen zu den Computerviren liegen schon lange Zeit zurück:

- **1950** mathematische Modelle, auf denen Ausbreitung und Wirkung von Viren beruhen, sind bekannt
- **1980** vereinzelte Meldungen über “Worms” und Viren in einigen Großrechnern in den USA
- **1981** der Deutsche J. Kraus stellt Versuche mit Virusprogrammen an und entwickelt eine dahinterstehende Theorie
- **1984** der Amerikaner F. Cohen beschäftigt sich ebenfalls mit Virentheorien und sucht nach sinnvollen Einsatzmöglichkeiten (er schlägt eine Datenkomprimierung durch Viren vor)

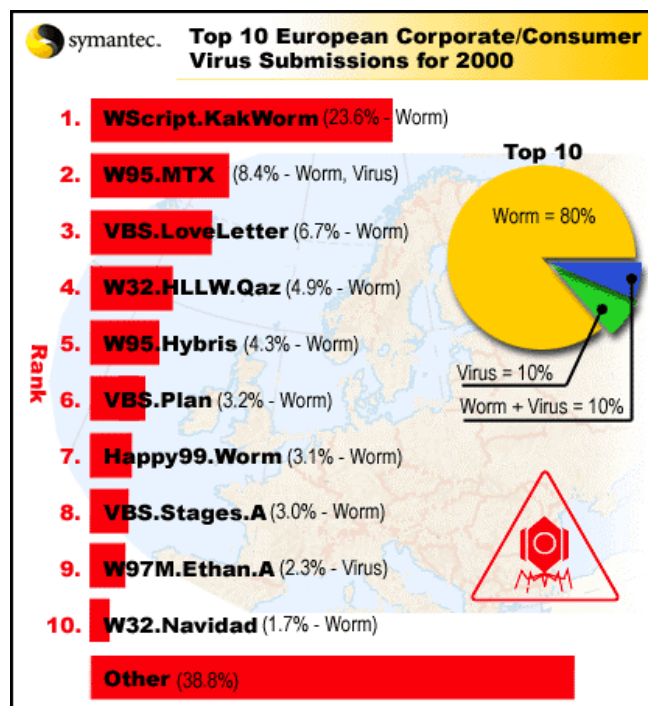
Mitte der achtziger Jahre werden Viren zu einem in den Medien mehr und mehr verbreiteten Thema und es wird auch erstmals ernsthaft über Virenschutz diskutiert.

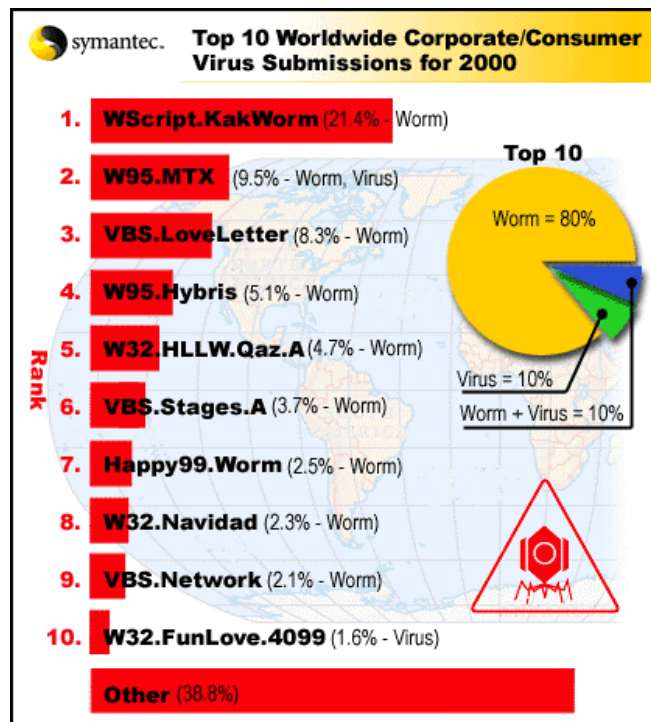
Die heute im Umlauf befindlichen Viren stammen hauptsächlich aus den *Vereinigten Staaten*, den Ländern der *ehemaligen Sowjetunion*, *Deutschland* und überraschenderweise oft aus *Bulgarien* und *Polen*. Sie sind kaum auf die Manipulation eines bestimmten Datenbestandes ausgerichtet; meist geht es dem/den Programmierer(n) darum, ihr Können unter Beweis zu stellen und die oft sehr große Schutz- und Wehrlosigkeit des Anwenders aufzuzeigen. Doch auch wenn ein Virus gezielt auf die Schädigung eines Anwenders ausgerichtet ist, breitet er sich sehr schnell unkontrollierbar aus. Der Schaden, der durch Viren entsteht, beträgt allein in Deutschland jährlich etwa 100 Mio. DM. Obwohl große Netzwerke (vor allem das Internet) immer wieder als Hauptüberträger von Viren genannt werden, wird die Gefahr, die von ihnen ausgeht, meist überschätzt. Der Großteil aller auftretenden Viren wird durch die Weitergabe von Datenträgern, vor allem Disketten, die sehr oft Raubkopien enthalten, übertragen. Durch CD-ROMs können, da sie nicht beschreibbar sind, keine Viren übertragen werden. Es ist jedoch möglich, dass sowohl

kommerzielle CD-ROMs als auch andere WORM-Medien beim einmaligen Beschreiben verseucht werden und so den Virus unauslöschlich in sich tragen. Die zunehmende Vernetzung trägt allerdings dazu bei, dass es auch für Laien immer einfacher wird, an - durchaus sehr gefährliche - Sourcecodes von Viren heranzukommen. Das hat zur Folge, dass die Zahl der in Umlauf befindlichen Viren stark ansteigt. Derzeit sind etwa 54000 Viren verbreitet, wobei jeden Monat etwa 200 – 300 neue hinzukommen.

Das Problem mit diesen Schadenprogrammen ist durchaus nicht lokal bezogen, was man an dem Vergleich des Virenbefalls zwischen Amerika und Europa sehr gut sieht.

Die Gefahr der Viren ist keinesfalls lokaler Natur, sonder Globaler, was man im Vergleich der Befall Quoten leicht erkennen kann:





1.2 Rechtslage

Die Rechtslage im Bereich von Computerviren ist in Deutschland sehr ungenau. Das Programmieren von Computerviren ist demnach nicht ausdrücklich verboten, sehr wohl aber deren - auch nur versuchte - Anwendung und vor allem die daraus resultierende Veränderung von Daten. Strafbar ist die Anwendung jedes Virus, auch wenn er keinen Schaden anrichtet, da in jedem Fall durch das Kopieren des Virusprogramms eine Veränderung von Datenbeständen erfolgt, wenngleich es keine wirklich genauen Bestimmungen zur indirekten Verbreitung von Viren, etwa durch Einschleusen in Netzwerke anstatt durch direkten Einsatz an einem zu manipulierenden Computer, gibt. In der Schweiz hingegen sind alle Schritte, vom Programmieren bis zur Verbreitung, sowie der Anstiftung dazu, mit einer Freiheitsstrafe von bis zu 5 Jahren belegt. Sowohl in der Schweiz als auch in Deutschland und Österreich ist allerdings mit weitreichenden Schadenersatzforderungen sowie einer Bestrafung für andere, durch den Vireneinsatz begangene Delikte, etwa Betrug durch einen Virus, der Bankguthaben verschiebt, zu rechnen.

Immer wieder wird der Einsatz von Viren als Schutz vor Raubkopien diskutiert, d.h. ein illegal benütztes Programm setzt einen Virus frei. Dies ist allerdings rechtlich nur so weit gedeckt, als nur das betroffene Programm - und kein Byte mehr - in Mitleidenschaft gezogen wird.

2. Vergleich Biologischer Viren / Computer Viren

Biologische Viren	Computerviren
Greifen bestimmte Zellen an	Greifen best. Dateien (z.B. *.COM, *.EXE) an
Erbinformation der Zelle wird verändert	Datei wird manipuliert
In befallenen Zellen entwickeln sich neue Viren	Befallene Dateien erzeugen weitere Kopien des Virus
Krankheiten treten nicht unmittelbar nach dem Befall auf	Infizierte Programme können längere Zeit fehlerfrei ablaufen
Jede Zelle wird nur einmal infiziert	Viren legen in der Regel in jedem Programm nur eine Kopie an
Viren können mutieren	Bestimmte Viren verändern ihre Struktur

3. Virenarten

Viren kann man in verschiedene Arten unterteilen. Die Art bestimmt hierbei was der Virus überhaupt infiziert, wie er es infiziert und welche Techniken er einsetzt, um sich ungestört verbreiten zu können und nicht von irgendeinem Programm aufgespürt zu werden. Oft fallen Computerviren nicht nur in eine Kategorie. Sie verwenden natürlich die besten Techniken, um sich möglichst oft zu vermehren und dabei nicht entdeckt zu werden.

Makroviren:

Ein Makro ist eine Zusammenfassung einer Abfolge von Befehlen. Sie werden zur Arbeitserleichterung in Programmen wie MS-Word eingesetzt. Makroviren sind die neueste Generation von Computerviren und sehr effektiv, da Makros an normale Dokumentdateien gebunden sind und somit leicht verbreitet werden. So ist es z. B. möglich von Word aus unbemerkt die Festplatte zu formatieren.

Dateiviren / Linkviren:

Sie werden so genannt, da sie, wie der Name schon sagt, EXE-, COM- und andere Dateien infizieren. Diese Viren "linken" sich an das Wirtsprogramm an.

Es gibt verschiedene Infektionsmechanismen. Jeder Virus verwendet jeweils nur eine der folgenden Mechanismen.

- **Überschreibender Virus:** Das ist die einfachste Art der Infektion. Der Virus überlagert schlicht und einfach das Wirtsprogramm mit seinem Code. Das Programm wird dabei natürlich zerstört und ist nicht mehr ausführbar. Startet man ein solches Programm, wird der Virencode ausgeführt und danach das Programm. Da dieses aber verstümmelt ist, kommt es unweigerlich zum Absturz oder mindestens zu Fehlermeldungen. Diese einfachen Viren treten heute in der Praxis kaum noch auf, da sie sehr leicht zu erkennen sind. Das Programm bleibt jedoch auch nach der Entfernung des Virus zerstört.
- **Überschreibender Virus - zweite Variante:** Diese neuere Entwicklung von überschreibenden Viren zeichnet sich durch einen sehr kurzen Code aus. Ein solcher Virus sucht nach Wirtsprogrammen mit statischen Daten. Diese können mehrere Kilobyte groß sein und sind zum Beispiel bei C-Programmen mit Nullen gefüllt. Hierher schreibt der Virus seinen Code und ändert noch den Startup-Code. Das Programm wird nicht zerstört und außerdem ändert sich dessen Länge auch nicht. Unter Umständen kann man bemerken, dass bei der Ausführung des Programms die statischen Daten falsche Werte aufweisen (die Bytes des Virencodes).
- **Nichtüberschreibender Virus:** Hier wird der erste Teil des Programms in der Länge des Virencodes an das Ende der Datei verschoben. Danach überlagert der Virus den ersten Teil mit seinem Code und einer Verschieberoutine. Wird das Programm gestartet, wird zuerst der Virus abgearbeitet. Dann tritt die Verschieberoutine in Aktion. Sie kopiert den verschobenen Programmteil wieder an seinen ursprünglichen Platz und startet ihn. Der Virus wird dabei überschrieben, er hat jedoch seine Arbeit schon längst getan.
- **Nichtüberschreibender Virus - zweite Variante:** Hier versteckt der Virus seinen Code irgendwo - sehr oft auch zufallsgesteuert - im Programm. Der Teil des Programms, wo jetzt der Virencode steht, wird wieder an das Ende verschoben. Ein Sprungbefehl am Anfang führt zum Virencode, an dessen Ende ein weiterer Sprung zurück zum eigentlichen Programm steht. In der Regel kann man solche Viren entfernen.
- **Anlagernder Virus:** Dieser Virus lagert sich am Ende des Wirtsprogramms an und setzt an den Programmanfang eine Sprung auf den Virencode. Am Ende des Virus geht es wieder mit einem Sprung zum eigentlichen Programm zurück. Diese Struktur wird auch von vielen

Hochsprachencompilern verwendet - sie übersetzen Quelltext auf die gleiche Art und Weise.

- Begleitender oder Companion-Virus: Diese Viren stellen die Ausnahme von der Regel dar - sie sind ein komplettes, ausführbares Programm. Sie brauchen jedoch ebenfalls einen Wirt und nutzen eine Eigenart von DOS aus: Wenn nämlich ein Programm sowohl als EXE- als auch COM-File vorliegt, wird prinzipiell bei Aufruf ohne Angabe der Extension nur das COM-File ausgeführt. Solche Viren infizieren daher immer nur EXE-Dateien. Der Virus erstellt ein COM-File, welches den Virus selbst darstellt. Wird das Programm gestartet, wird der Virus (COM-Datei) ausgeführt. Dieser startet dann das eigentliche Programm (EXE-Datei).
- Längentreuer Virus: Dieser Virus lagert den Code des Wirtsprogramms in eine externe Datei aus, die dann versteckt wird. Der Virus kopiert sich in das Wirtsprogramm. Dabei bleibt die Länge der Datei gleich. Der Virus sorgt bei der Abarbeitung noch dafür, dass das ausgelagerte Programmstück richtig eingebunden wird. Sollte das ausgelagerte Stück des Programms "verloren gehen", wird der Virus korrekt gestartet, da er sich ja im Originalprogramm befindet. Das Wirtsprogramm wird aber sehr wahrscheinlich abstürzen.

Viele Linkviren sind durch illegale Einträge in der FAT (= File-Allocation-Table) erkennbar. So setzt zum Beispiel der Lisbon-Virus den Sekundeneintrag auf den Wert 62. Da bei fast allen Linkviren die Datei um den entsprechenden Virencode länger wird, installieren sich manche Linkviren im Hauptspeicher resident und manipulieren von dort die Ausgabe des „DIR-Kommandos“, so dass die Dateilänge normal erscheint.

Bootsektorviren:

Diese Viren schreiben ihren Code in den Bootsektor von Disketten bzw. Festplatten, wo er nicht nur schwer zu entdecken ist, sondern auch bei jedem Bootvorgang von einem infizierten Datenträger in den Speicher geladen wird und dort meist resident bleibt. Daher werden viele Bootsektorviren bei nahezu jedem Schreibvorgang auf einem verseuchten System übertragen.

Hybridviren:

Sie werden auch Doppelviren genannt. Diese Viren infizieren sowohl Dateien (Linkviren) als auch die Systembereiche (Systemviren). Der Vorteil dieser Viren

ist folgender: hat ein System-Virus das System infiziert, wird er bei jedem Start geladen. Durch Booten von einer (sauberen !) Diskette kann man jedoch das Laden umgehen. Hybridviren werden so zwar nicht beim Starten geladen, aber ein Aufruf eines infizierten Programms führt zur Verbreitung des Virus. Geschieht dies auf der Diskette, so wird auch diese infiziert. Das ist eine doppelte Absicherung für den Virus.

Polymorphe (mutierende) Viren:

Diese Art von Viren ändert ihren Code in jeder neuen Generation, d.h. sie kopieren einen mehr oder weniger stark veränderte Version weiter. Manchmal wird auch die Wirkungsweise des Virus modifiziert. Sie sind die am schwersten zu erkennende Art von Viren.

Tunnelnde Viren:

Diese Viren benutzen das so genannte Interrupt Tracing. Sie belegen Interrupts, die überwacht werden, warten auf einen Aufruf, der sich zurückverfolgen lässt, und sucht dann den Eintrittspunkt, den das Monitorprogramm, der Virenschanner, nicht mehr überwacht. Manche Virenschanner habe arge Probleme mit diesen Viren, da sie immer neue Tunnel-Methoden wie das Ersetzen des Block-Device-Treibers für die Laufwerke entdecken, auf die sich Antivirenprogramme erst einmal einstellen müssen.

Stealth-Viren:

Viele der Viren verwenden bestimmte Tarnmechanismen, um in aller Ruhe "arbeiten" zu können.

- Der Virus kann den Rückgabewert von Interrupt 12hex manipulieren, um den tatsächlich freien Speicher zu verfälschen.
- Manche Viren ermitteln die absolute Adresse eines Interruptvektors. Damit können sie diese benutzen ohne einen Interrupt aufrufen zu

müssen. Sie springen die ermittelte Adresse an und unterlaufen so Programme, die Interruptroutinen überwachen (=Tunneling).

- Viren können auch diverse Diskettenzugriffe überprüfen. So kann der Virus einen lesenden Zugriff auf eine Datei erkennen und die Infizierung rückgängig machen, bis zum Beispiel ein Scan-Programm die Datei überprüft, aber keine Virensignatur erkannt hat. Danach wird die Datei wieder infiziert.
- Durch überprüfen des Interrupts 13hex können Bootsektorviren einen ganz normalen Zugriff auf den Masterbootrekord, die Partitionstabelle und den Partitionsbootrekord gewähren, indem sie den Aufruf in die ausgelagerten Sektoren umleiten.
- Auch können Viren mit falschen Dateilängeneinträgen in der FAT die Ausgabe des DIR-Befehls fälschen.
- Viren verstecken natürlich die von ihnen erzeugten Dateien mit Attributen wie HIDDEN oder SYSTEM. Diese können auch Bitmuster darstellen, mit denen DOS nichts anfangen kann. Sie stellen dann für DOS unbekannte Daten dar.
- Viren verschlüsseln auch ihren Code in den Dateien. Hier wird vor dem eigentlichen Virus eine Ent- und Verschlüsselungsroutine ausgeführt, die den Code wiederherstellt. Auch das zerwürfeln des Codes ist eine wirksame Technik, um nicht gefunden zu werden. Auch ein solcher Code wird natürlich wieder zusammengesetzt.
- Einige Viren enthalten Signaturen von anderen Viren. Wird ein solch infiziertes Programm gefunden, entfernt der Virens Scanner den vermeintlichen Virus und zerstört so die Datei.
- Andere überprüfen, ob ein Interrupt von einem Virenprogramm "verbogen" ist, um Viren aufzuspüren. Ist dies der Fall, wird keine Infektion durchgeführt.

Wie sich ein Virus tarnt bleibt einzig und allein der Phantasie des Programmierers überlassen (je besser, desto geringer ist die Möglichkeit, gefunden zu werden).

Slow-Viren:

Diese Viren gehen, wie ihr Name schon sagt, sehr langsam vor. Sie verändern Daten so minimal, dass der Nutzer den Befall nicht bemerkt. Stellt der Nutzer nun Datensicherungen her, sind diese auch schon mit dem Virus befallen und nutzen dem Anwender nichts mehr.

Windows-Viren:

Der bekannteste dieser Viren, der CIH-Virus, konnte sich sehr schnell in Taiwan, seinem Ursprungsland, und in Deutschland verbreiten. Er hat sich auf Windows spezialisiert und zerstört an jedem 26. des Monats nicht nur sämtliche Daten auf der Festplatte durch Überschreiben, sondern mitunter auch den Inhalt des Flash-BIOS. Der Virus kann nur schwer entfernt werden, da er sich direkt im Windows-Kernel versteckt und sich dabei über mehrere Bruchstücke in EXE-Dateien verteilt.

Trojanische Pferde:

Trojanische Pferde, auch Trojaner genannt, sind in dem Sinne keine Viren, da sie sich nicht von alleine reproduzieren. Sie können aber an jede beliebige ausführbare Datei angehängt werden. Wird diese Datei ausgeführt, installiert sich der Trojaner. Im Grunde genommen ist es ein Fernsteuerungsprogramm. Ist auf einem PC ein Trojaner installiert, stehen dem mutmaßlichen „Hacker“ alle Türen und Tore offen. Es steht der Phantasie offen, was man alles machen kann. Sei es z. B., das CD-Rom Laufwerk zu öffnen, oder diverse gespeicherte Passwörter auslesen. Man kann wirklich alles machen. Wenn das „Opfer“ sich ins Internet einwählt, erhält der „Hacker“ eine Nachricht, in der die dynamisch vergebene IP Adresse steht. Die bekanntesten Trojaner sind wohl „Back Orifice“ und „SubSeven“, welche man sich auch einfach im Internet runterladen kann.

Würmer:

In sehr entfernter Form ist auch der Wurm ein Trojaner. Das Opfer muss das befallene Programm auch selber starten. Der Wurm ist in der Lage, sich selber z. B. über E-Mail an neue Empfänger zu verschicken. Hat sich der Wurm einmal installiert, wartet er auf den Start des E-Mail-Programms, scant den ganzen Posteingang durch, und verschickt sich an jeden Absender. Es ist wirklich enorm, was dieses Schadenprogramm anrichten kann, was man z. B. an dem Wurm „ExploreZip“ sieht. Es durchsucht gezielt alle verfügbaren Laufwerke nach Dateien des Typs asm, c, cpp, doc, h, xls, und ppt, sprich Quelldateien von Programmiersprachen und Dokumente von Officeanwendungen. Die Länge dieser Dateien wird auf Null gesetzt, was ein Wiederherstellen sehr erschwert.

4. Funktionsweise

4.1 Die Infektion

Natürlich erhebt sich jetzt die Frage, von wo aus die Festplatte oder Diskette infiziert wird.

Gefährlich sind vor allem Raubkopien, Spiele, Shareware, Public-Domain-Software und Demonstrationssoftware. Auch kann man sich bei seltsamen Utilities nie sicher sein, ob sich nicht ein Trojaner oder Dropper hinter dem Namen verbirgt. Festplatten werden sehr oft von Disketten aus infiziert (über 80%). Es gibt aber auch noch andere Wege.

- Diskettenlaufwerke: Sie stellen die größte Gefahr für Infektionen dar. Ob nun ein Bootsektorvirus, ein Linkvirus oder ein anderer - auf Disketten ist alles möglich. Hier gibt es jedoch auch verschiedene Infektionswege, die speziell auf den Virus zutreffen.
 1. Booten von Diskette: Das Starten mit einer infizierten Diskette führt dazu, dass sich Bootsektorenviren auch über die Festplatte hermachen.
 2. Lesen des Datenträgerinhaltes: Manche Viren können sich zum Beispiel bloß durch Aufrufen eines DIR-Kommandos weiterverbreiten.
 3. Lesen und Schreiben von Systeminformationen: Hier können sich vor allem Viren die den Interrupt 13hex überwachen reproduzieren, wenn zum Beispiel durch Programme wie PCTools oder anderen Systeminformationen geschrieben oder gelesen werden.
 4. Kopieren von Programmdateien: Das Kopieren stellt natürlich die größte Gefahr einer Infektion dar. Meistens sind Viren nach dem Kopiervorgang inaktiv. Jedoch andere wie zum Beispiel der Dark-Avanger-Virus werden schon durch das Kopieren eines Wirtes aktiv.
 5. Starten von Programmen des Laufwerks: Wird ein infiziertes Programm ausgeführt, wird der Virus verbreitet.
- Festplatten: Hier verbreiten sich Computerviren auf die bereits beschriebene Art und Weise (Aufruf eines infizierten Programms, booten, ...).
- Kommunikationsadapter: In der heutigen Zeit stellt vor allem das Internet eine Gefahr dar. Über Modem werden die verschiedensten Programme und mit denen sehr oft auch ein Virus heruntergeladen. Aber auch durch einfache Verbindung über serielle/parallele Schnittstelle können zu einer Infektion führen, wenn eine infizierte Datei kopiert wird.
- Backup: Disketten, Streamer-Bänder, CDs und andere Medien sind ideal für ein Backup wichtiger Dateien. Es kann aber passieren, dass ein infiziertes File auf eine CD-R gebrannt wird. Dieser Virus lässt sich natürlich nicht mehr entfernen (außer man vernichtet die CD). Kopiert man diese infizierte Datei zurück auf die Festplatte und startet diese Programm, so kommt es zu einer Infektion. Man sollte daher besonders aufpassen, dass auf keinen Fall Viren auf dem Medium sind.

4.2 Die Reproduktion

4.2.1 Linkviren:

Wie schon erwähnt, hängen sich Linkviren an eine bestimmte Datei oder erzeugen eine. Nach dem Aufruf der infizierten Datei wird der Virus im Speicher resident (nicht alle Viren). Danach sucht er eine Datei, welche er infizieren kann. Wird eine gefunden, wird zuerst einmal das Datum, die Zeit und das Attribut der Datei gesichert. Danach wird die Datei geöffnet und der Virencode geschrieben (am Anfang oder am Ende ist von Datei abhängig, da es Unterschiede zwischen EXE- und COM-Dateien gibt). Ist dies geschehen, werden noch nötige Änderungen im Startupcode gemacht. Um nun noch seine Spuren zu verwischen, wird das gespeicherte Datum, die Zeit und das Attribut wieder in die Datei geschrieben und diese danach geschlossen. Nun kann der Virus auch noch nötige Änderungen in der FAT vornehmen, wie zum Beispiel den Eintrag der Dateilänge ändern oder auch unsinnige Werte für Zeit (62 Sekunden) oder Datum (13. Monat) schreiben.

Viren, die nicht entdeckt werden wollen, verschlüsseln sich nach der Infektion oft selbst.

Eine andere Technik der Infektion ist das Erstellen einer temporären Datei. In diese Datei wird dann zuerst der Virencode und dann das eigentlich zu infizierende Programm geschrieben. Am Schluss wird diese Datei in das Original umbenannt und das Original wird gelöscht.

4.2.2 Systemviren:

Man muss davon ausgehen, dass mit einer infizierten Diskette gestartet worden ist. Der Virus installierte sich so im Hauptspeicher. Sehr oft "verbiegen" solche Viren auch noch diverse Interruptvektoren, wie zum Beispiel den Interrupt 13hex. Nun kann der Virus mit Hilfe dieses Interrupts nach anderen Laufwerken suchen. Wird eines gefunden (zum Beispiel Laufwerk C:), installiert sich der Virus im Startbereich und ist ab nun bei jedem Start present.

Von einem so infiziertem Laufwerk kann der Virus natürlich wieder andere Disketten infizieren. Da er ja den Interrupt 13hex überwacht, kann er schon durch ein simples "DIR A:" Informationen über die Diskette bekommen (zum Beispiel HD- oder DD-Diskette) und diese dann infizieren.

5. Auswirkungen

Die meisten Viren beinhalten sehr oft Schadensroutinen die Dateien löschen, verstecken oder andere gemeine Sachen vollbringen. Manche Viren werden

auch nur geschrieben, um die Verletzlichkeit des Computersystems aufzuzeigen, indem sie die Dateien mit einer Routine infizieren, die einfach zum Beispiel den Text "Virus was here !!" auf den Bildschirm schreibt. Von dieser Art gibt es jedoch eher wenige. Die meisten sind dafür geschrieben worden, um Beeinträchtigungen oder Schäden hervorzurufen. Hier sollen nun einige der Möglichkeiten aufgezählt werden.

- Es gibt eine bestimmte Art von Viren, die nur ein einziges Ziel verfolgen - sie erzeugen Systemfehler. Genannt werden sie Crasher-Viren, nach dem allbekannten Systemcrash. Der Computer arbeitet nicht mehr, über die Eingabegeräte wird keine Eingabe mehr angenommen und gar nichts reagiert mehr. Das einzige, was in solch einer Situation hilft, ist die Reset-Taste. Natürlich ist das eine Methode, um den Anwender in die Verzweiflung zu treiben, wenn dieser "Fehler" bei jedem Programmstart wieder auftritt.
- Eine Frage taucht immer wieder auf: "Können Viren die Hardware eines Computers zerstören?" Die Antwort ist "Ja", wenn auch nur in begrenztem Ausmaß. So kann man durch wiederholt kritische Bewegungen der Schreib- und Leseköpfe eine mechanische Zerstörung erreichen. Auch der Monitor stellt für die Zerstörung ein wertvolles Ziel dar. Soweit bekannt sind aber keine solchen Viren im Umlauf, was nicht heißen soll, dass sie nicht existieren.
- Eine von Viren gern verwendete Funktion ist das Formatieren der Festplatte(n). Ob nun eine High- oder Low-Level-Formatierung, ärgerlich ist es auf jeden Fall.
- Weitere nette Dinge sind das Überschreiben der Systembereiche, das "Zerwürfeln" der FAT, das Löschen von Dateien (obwohl man bei bestimmten Arten des Löschens die Datei wiederherstellen kann) oder das wahllose Überschreiben von Sektoren auf der Festplatte. Manchen Viren verstecken auch Programme oder sogar ganze Verzeichnisse, wieder andere verschlüsseln diese, so dass sie unbrauchbar sind.
- Wenn Viren resident im Hauptspeicher installiert sind und einen Interrupt überwachen (zum Beispiel Interrupt 13hex), können sie einfach jeden Schreibzugriff in eine Verify-Operation umwandeln. Solange der Virus installiert ist, werden keine Daten auf die Festplatte oder andere Medien geschrieben.

Das sind natürlich nicht alle Schädigungen die Viren verursachen können. Manchmal erfreuen sie auch ihren "Nutzer" auch mit einem netten Bild oder einer kleinen Melodie, um auf sich aufmerksam zu machen. Viele Viren führen solche Schadensroutinen nicht immer aus. So gibt es Viren (Friday 13th, Father Christmas, Halloween, ...) die nur zu einem bestimmten Zeitpunkt, Datum oder einem anderen Ereignis aktiv werden und dann zuschlagen. Die restliche Zeit wird nur zur Ausbreitung benutzt.

6. Abwehrmaßnahmen

Äußerst wichtig bei neuen Dateien, Disketten, CDs, und anderen ist die Überprüfung der Daten beziehungsweise Datenträger auf eine mögliche Infektion. Viele Leute gehen viel zu unachtsam mit diesem Thema um und kopieren dann eine infizierte Datei auf die Festplatte und wundern sich danach über eine Infektion.

Für solche Untersuchungen eignen sich Antivirenprogramme wie zum Beispiel Scan™ von McAfee, Norton Anti Virus, Microsoft Anti-Virus oder viele mehr. Sehr wichtig ist auch, immer das neueste Update zu bekommen, denn der Scanner wird mit einem veralteten Daten-File keine neue Mutation eines Virus erkennen.

Außer diesen Programmen dienen auch noch Vshield-Programme oder das Immunisieren der Dateien zur Vorbeugung.

6.1 Antivirenprogramme:

Sie sind für die Suche und Entfernung von Viren geschrieben worden und bedienen sich zwei Methoden

1. **Auffinden von Viren-Strings:** Mit dieser Methode werden Dateien durchsucht, um Virensignaturen zu finden. Diese Signaturen werden von den Viren selbst verwendet, um eine bereits erfolgte Infektion zu erkennen. Es ist jedoch nicht die beste Methode, da sich die Signaturen durch Verschlüsselung und/oder Mutation ändern können, aber auch gar keine Signaturen vorhanden sein müssen (zum Beispiel überprüft ein Virus, ob der Sekundeneintrag der Datei 62 Sekunden beträgt. Ist das so, ist die Datei bereits infiziert.). Ein einfaches Beispiel kann verwendet werden, um den Scanner zu testen. In einem Text-Editor geben sie folgenden Zeile ein und speichern dann die Datei mit einer .COM Extension:

» X5O!P% @AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H* « Wenn die Datei ausgeführt wird gibt sie eine Meldung

am Bildschirm aus. Jetzt muss nur noch der Scanner gestartet werden, um den "Virus" aufzuspüren. Sowohl Scan™ als auch F-Prot sollten ihn finden.

2. **Heuristische Analyse:** Diese, noch sehr junge, Form der Analyse dient vor allem dazu, neue Viren zu entdecken. Hier werden keine Signaturen gesucht, sondern es werden bestimmte Regeln für die Beschreibung eines Virus festgelegt und nach diesen werden die Dateien untersucht. Bei dieser Methode werden nicht alle Viren gefunden und es kann auch häufig zu Fehlalarmen kommen.

Bei fast allen Antivirenpaketen sind sehr oft Textdateien dabei, die über neu gefundene Viren berichten oder auf die sich im Moment im Umlauf befindlichen Viren hinweisen. Mit den Programmen kann man auch eine Virenliste abfragen. Diese enthält die verschiedensten Viren aufgelistet mit Informationen über Länge, Art der Infektion, Möglichkeit der Entfernung und so weiter. Zum Beispiel entdeckt F-PROT aus dem Jahr 1996 insgesamt 8427 Viren von denen es 6219 entfernen kann. Heutzutage erkennt das neue Norton Anti Virus 2002 von der Firma Symantec bereits 54.000 verschiedene Viren. Dieses, sowie das McAfee gehören zu den bekanntesten.



6.2 Prüfsummenprogramme:

Diese Programme benötigen keine Updates. Sie können jedoch auch nur Veränderungen in Dateien oder im Bootsektor erkennen.

6.3 Vshield-Programme:

Diese Speicherresidenten Programme arbeiten im Grunde wie Scan-Programme und werden sehr oft mit diesen geliefert. Sie sind im Speicher und überprüfen dort Programme, die ebenfalls dorthin geladen werden. Sie sind ebenfalls in der Lage, Viren zu entfernen.

6.4 Immunisieren:

Diese Methode funktioniert auf drei verschiedene Arten:

- **Immunisieren mittels Kennbyte:** In ein Programm wird ein bestimmtes Kennbyte eines Virus eingebaut. Sollte der Virus jetzt diese Datei

infizieren wollen, erkennt er das Kennbyte und verschont die Datei. Diese Methode bildet jedoch nur geringen Schutz, da nicht alle Kennbytes aller Viren eingebaut werden können. Außerdem gibt es Viren, die bei infizierten Dateien die Version des Virus überprüfen. Ist es ein älterer wird die Datei neu infiziert.

- **Immunisieren mittels ASR-Routine:** Hier wird ein “Antivirus”, eine sogenannte ASR-Routine (=Auto Self Reconstruct), in die Datei eingebaut, die bei Start des Programms wichtige Daten (Länge, ...) ermittelt und mit bereits zuvor gespeicherten vergleicht. Werden Änderungen festgestellt, wird das Programm sofort abgebrochen. Diese Möglichkeit der Immunisierung hat jedoch einige entscheidende Nachteile:
 1. WINDOWS-Programme funktionieren oft nicht mehr
 2. Ist die Datei infiziert, meldet die ASR-Routine zwar eine Änderung des Codes und beendet die Ausführung. Der Virencode ist jedoch schon längst abgearbeitet.
 3.
- **Self-Integrity-Test:** Vor allem Virens Scanner überprüfen mit dieser Methode den eigenen Code auf Modifikationen. Es wäre ja verheerend, wenn das Antivirenprogramm selbst andere Dateien mit einem Virus infizieren würde.

Den besten Schutz gewährt aber noch immer eine Überprüfung durch ein Antivirenprogramm, da selbst die Immunisierungsmethoden nicht genug Schutz bieten.

6.5 Entfernen von Viren:

Sollte trotz aller Sicherheitsmaßnahmen ein Virus das System infizieren, muss man diesen so schnell es geht entfernen, um keine Schäden zu riskieren.

6.5.1 Systemviren:

Antivirenprogramme können infizierte Bootsektoren oder den MBR oft erfolgreich wiederherstellen. Ist der MBR infiziert reicht sogar der Befehl `FDISK /MBR`. Dieses Kommando schreibt einen neuen MBR und zerstört so den Virus.

Eine vollständige Beseitigung erfolgt natürlich über ein Low-Level-Format, bei dem aber auch alle restlichen Daten am Datenträger zerstört werden.

Antivirenprogramme leisten aber meistens gute Arbeit.

6.5.2 Linkviren:

Bei überschreibenden Viren besteht zur Wiederherstellung keine Chance mehr. Alle anderen Viren können aber oft entfernt und der Wirt restauriert werden. Die Gefahr dabei kann sein, dass der Wirt "kaputt repariert" wird. Grundsätzlich können Stealthviren, Viren mit veränderlicher Länge oder mit getrennten Codeteilen oft nicht oder nur sehr schwer entfernt werden. Die sicherste Methode einen Linkvirus loszuwerden ist natürlich die entsprechende Datei zu löschen.

7. Nachwort:

Die Gefahr der Computerviren ist auch heute noch akut. Noch immer versuchen die verschiedensten Programmierer den besten Virus zu schreiben. Manchmal gibt es sogar Wettbewerbe für Viren. Die größte Gefahr stellen heutzutage sicherlich die Virengeneratoren dar. Ohne jegliches Programmierwissen kann praktisch jedermann, der das Programm besitzt, sich seinen eigenen Virus basteln. Leute, die solche Programme und Trojaner benutzen, werden unter den richtigen „Hackern“ auch „Script Kiddis“ genannt. Man gibt einfach den gewünschten Schaden, den Aktivierungsgrund, aber auch ob der Virus mutieren soll oder nicht an. Auch Verschlüsselung wird natürlich eingebaut. So soll zum Beispiel die "Dark-Avanger-Mutation-Engine" mehrere Millionen Abarten von Viren erzeugen können. Dies ist aber nicht der einzige Generator. Es existieren bereits verschiedenste. Alleine wenn man in der Internet Suchmaschine „Google“ den Suchbegriff „Virii“ eingibt, erhält man auf Anhieb die umfangreichsten Seiten, auf denen Sourcecodes von tausenden Viren erhält sind. Ein Beispiel dafür ist die Seite von „Virii Argentina“.





Virii Argentina-The biggest Virii resource in the net - Microsoft Internet Explorer

Datei Bearbeiten Ansicht Favoriten Extras ?

Zurück Suchen Favoriten Medien Wechselt zu Links Norton AntiVirus

Adresse <http://www.550m.com/usuarios/viriar/home2.htm>





Virii Argentina Top 50

Site of the Week

Virii collection

- Macro virus
- Search
- Antivirus
- Creation labs
- Bulletin Board
- Top 50
- Others collections
- Lotus virus
- Our Virii
- Mac virus
- Linux-Unix virus
- Virus exchange
- Source codes
- Virii groups
- Virii tutorials
- Trojans
- Credits
- Recommended sites
- Send virus

Virus Index Contact us

VBSWG 2 Beta Fix


Contact us [here](#)

Send us virii to virus@virii.com.ar

www.voodoo600.net - Great site

Can't find what you want? [Search](#)


Please click [HERE](#)



VIRII ARGENTINA TOP 50
 PLEASE VOTE

- **100.000 VISITS!!** THANK ALL OF YOU WHO HELPED TO MAKE THAT.
- **WE DON'T HAVE VBSWG ANYMORE, YOU CAN FIND IT IN VX.NETLUX.ORG, SO DON'T ASK FOR IT ANYMORE.**
- **Virii Argentina Board Reopened**
- **Virii Argentina Top 50 Reopened**
- **[K] has started his personal site where you can find all his work. <http://www.kvirii.com.ar>**

- CYBERARMY
- ASTALAVISTA
- LINKWORLD
- WEBFRINGE
- TOP 999
- ELITE TOP LIST
- BLACK CODE
- REAL TOP 69
- SECURED ONLINE
- SECURITY ROOT
- SPYMODEN
- NOVA
- T188.TD
- SUB-LIST.COM
- NO FUTURE
- RED DEMONZ



PLEASE CLICK HERE

[Virii Argentina] <http://www.virii.com.ar> [The biggest Virii resource in the net]

Internet