

Trojaner, Viren, Würmer

Ausbreitungswege und Bekämpfung

Christian Steiner
sichstei@stud.uni-erlangen.de

01.07.2002

Abstract

Vor allem für Windows und DOS-Systeme, aber im zunehmenden Maße auch für Linux existieren eine Vielzahl von verschiedenen Viren, von denen zwar relativ wenige in der freien Wildbahn anzutreffen sind, die jedoch teils Schäden in Millionenhöhe verursachen. Dieser Vortrag soll vor allem über die verschiedenen Arten von Malware, deren Verbreitungswege und Bekämpfungsmöglichkeiten informieren.

1 Einführung - Definitionen

Zur Zeit tauchen beinahe jeden Monat ungefähr 500 neue Spielarten von Computer-Viren, Würmern und Trojanern auf. Insgesamt sind unter dem Strich derzeit ca. 60.000 verschiedene Viren bekannt. Die Auswirkungen und Angriffsziele sind unterschiedlich und reichen von lustigen Bildschirmausgaben über das Löschen bis zum Ausspionieren persönlicher Daten. In freier Wildbahn existiert zwar nur ein kleiner Teil der bekannten Viren, deren Gefährlichkeit ist jedoch nicht zu unterschätzen. Waren anfangs Viren noch auf Apple, Unix und IBM-Systemen beheimatet sind sie heute - aufgrund der schwachen Benutzerrechteverwaltung und der großen Verbreitung- zumeist auf DOS und Windows Systemen zu finden, weshalb sich dieser Vortrag zum Großteil mit Viren in Windows und DOS-Systemen beschäftigt.

1.1 Definition Virus

Der klassische Virus ist ein Schadprogramm, das sich von Datei zu Datei auf einem Computer ausbreitet. Der Virus repliziert sich selbst, zum Beispiel wenn der Benutzer ein bestimmtes Programm ausführt oder den Computer hochfährt. Damit der Virus sich auf dem PC ausbreiten kann, muss er aktiviert werden. Dazu ist menschliche Hilfe nötig, auch wenn der PC-Benutzer natürlich nicht weiß, dass er mit dem Öffnen einer Datei oder dem Starten des Computers seinen Rechner infiziert.

Strategie des Virus: den Wirt beherrschen.

Die Absicht vieler Viren ist es, so viele Dateien wie möglich innerhalb eines Computers zu infizieren oder vitale Funktionen zu blockieren. Viren können nur dann von einem auf den anderen Computer übergreifen, wenn sie zum Beispiel per Diskette übertragen werden. Natürlich können sie auch per E-Mail mit infiziertem Anhang verschickt werden. Das bedeutet aber auch, dass der klassische Virus sich nur so schnell verbreitet, wie Menschen sich untereinander auf digitalem Wege austauschen - den Virus in ihrem Schlepptau. Es kann mitunter Tage oder Wochen dauern, bis eine Virusinfektion von einem auf den anderen PC gelangt.

1.2 Definition Wurm

Ein Wurm ist ein Programm, das sich von Computer zu Computer via Netzwerk selbsttätig weiter verbreitet. Die Absicht der Würmer ist es, so viele Computer wie möglich innerhalb eines Netzwerks zu befallen. Würmer brauchen, sind sie erst einmal auf den Weg gebracht, kein menschliches Zutun, um sich rasend schnell innerhalb eines Firmennetzwerks oder über das Internet zu verbreiten. Sie benutzen beispielsweise die E-Mail-Funktionen eines Rechners, um sich an beliebige Internetadressen zu versenden. Neben ihrer Fähigkeit zur schnellen autonomen Verbreitung haben Würmer eine Ladung(Payload), das eigentliche Schadprogramm, das sich wie ein herkömmlicher Virus innerhalb des befallenen PCs auswirkt.

Strategie des Wurms: die Menge macht's.

Während der *Internet Wurm* im Jahr 1988 es gerade mal auf 2.000-6.000 infizierte Systeme brachte, konnte *Melissa* innerhalb von nur drei Tagen 100.000 Systeme lahm legen. Die Schäden sind dadurch natürlich ungleich höher als noch vor über 10 Jahren. Der große Erfolg von Würmern heutzutage ist auf ihre verbesserten Lebensbedingungen zurückzuführen. Außerdem hat die Programmierbarkeit von Computern stark zugenommen. Kaum ein fortschrittliches Office-Paket verzichtet noch auf Makros, die der Laie bequem nach Handbuch mit z.B. VBS (Visual Basic Script) anfertigen kann. Auch Würmer lassen sich mit dieser einfachen Programmiermethode rasch herstellen. Für den *Loveletter* dürften das Microsoft-Handbuch, ein Nachmittag und eine ordentliche Portion kriminelle Energie genügt haben, um einen Schaden von geschätzten 2,5 Milliarden Dollar weltweit anzurichten. Der Nachteil von Würmern besteht aber eben gerade auch in der verwendeten Skriptsprache, die es Viren häufig unmöglich macht, sich auf anderen Betriebssystemen zu verbreiten, da der Skriptinterpreter eben nur auf einer BS-Familie läuft. (z.B. VBS, VBA,...)

1.3 Definition Trojaner

Trojaner sind Programme, die sich als nützliche Anwendungen tarnen, im Hintergrund aber ohne das Wissen des Anwenders eine Schadensroutine ausführen. Nach dem Start des Tarn-Programms wird auch die schädliche Ladung auf dem PC aktiviert.

Strategie des Trojaners: sensible Daten ausspionieren, den Rechner kontrollieren

Die Absicht vieler Trojaner ist es, unbemerkt so viele sensible Benutzerdaten wie möglich auszuspähen. Wenn der Internetbenutzer persönliche Daten wie zum Beispiel Passwörter für das Onlinebanking oder für Mailaccounts, Kreditkartennummern und Ähnliches übermittelt, schreibt der Trojaner mit(keylogging). Die Leistungsfähigsten unter ihnen sind in der Lage, die wirklich interessantesten Informationen herauszufiltern, und übermitteln diese dann per E-Mail an den Hacker, sprich den Absender des Trojaners.

Attacke durchs Hintertürchen.

Eine besonders aggressive Form des trojanischen Pferdes sind so genannte *Backdoor-Trojaner*. Diese richten auf dem Wirtssystem Ports (Backdoors) ein, durch die der Hacker einfallen kann. Mit Hilfe von Backdoor-Trojanern oder auch *RAT-Trojanern* kann der Hacker auf fremde Rechner zugreifen und hat dann die Fernkontrolle über praktisch alle Funktionen.

2 Viren

2.1 Arten von Computerviren

Nicht residente Viren: Werden nur bei Ausführung des infizierten Programmes aktiv und infizieren dann andere Programme bzw. führen ihr Payload aus. z.B. Shell-Skripte, Batches...

Speicherresidente Viren: Nisten sich resident im Hauptspeicher ein, um auf niedriger Systemebene die Abläufe im Rechner zu überwachen und ggf. zu verändern. Dem Benutzer geht der Zusammenhang zwischen Auftreten des Virus und Ausführung des befallenen Programmes verloren, da dazwischen mehrere andere Programme ausgeführt werden können.

Eine Sonderart der speicherresidenten Viren sind die **Stealth-Viren**. Diese versuchen sich durch verschiedene Tricks zu verstecken z.B. werden Zugriffe auf Dateien und Inhaltsverzeichnisse überwacht und derart manipuliert, dass dem Benutzer und evtl. auch Virencannern ein sauberes System vorgespielt wird.

Dateiviren: hängen sich an bestehende Programmdateien an, das Programm wird dadurch verändert und teilweise verlängert oder überschrieben. Während der Ausführung des Programms wird der Virus aktiv. Unter Linux sind nur sehr wenige Dateiviren bekannt (ca. 50 gegenüber ca. 50.000 für Windows/Dos), da hier die Benutzerrechte und die -bisher- relativ geringe Verbreitung des Betriebssystems überhaupt den Virenprogrammieren keinen Anreiz boten.

Bootviren: Diese Virusart befällt Systembereiche von Disketten und Festplatten. Sie legt sich im Bootsektor bzw. im Masterbootsektor ab und wird dadurch bei jedem Booten vom befallenen Medium aktiv. Prinzipiell also vom Betriebssystem unanständig (da vorher gestartet), sind sie jedoch trotzdem z.B. vom verwendeten Dateisystem etc. abhängig.

Companion-Viren: erzeugen neue Programme, die dem Benutzer nicht bekannt sind, jedoch zumeist die gleichen Namen tragen, wie bereits vorhandene. Laut Systemdefinition werden z.B. unter Windows „.com“-Dateien immer vor „.exe“-Dateien ausgeführt...

Makrovirus: Makroviren sind neuere Viren. Viele Applikationen bringen mittlerweile eine umfangreiche Makroprogrammiersprache mit, in der diese Viren geschrieben sind. Dem Virus steht der gesamte Umfang der Applikations-Programmiersprache zur Verfügung, was sie zu einer ernsthaften Gefahr werden lässt. Prinzipiell sind solche Viren eigentlich auch plattformübergreifend möglich, nämlich dann, wenn der Dokumenttyp, an den der Virus gebunden ist, auch auf anderen Plattformen existiert.

2.2 Verbreitungswege

Die größte Zahl der Viren verbreiteten sich über den Tausch von Disketten und Programmen. Im Unterschied zu Dateiviren sind Bootsektorviren nur dann infektiös, wenn von einem befallenen Medium gebootet wird, da sonst der Virencode gar nicht erst ausgeführt wird. Dateiviren und Makroviren verbreiten sich zusammen mit den infizierten Programmen/Dateien, an die sie sich angeheftet haben, bzw. in denen sie sich verstecken.

2.3 Bekämpfung

Je nach Virustyp gibt es verschiedene Möglichkeiten, Viren loszuwerden. Bootsektorviren unter Dos/Windows lassen sich am einfachsten mit Fdisk /mbr entfernen, indem man einfach den Master-Boot-Sektor überschreibt. Partitionsviren werden relativ gut durch Antivirenprogramme entfernt, Dateiviren sind ebenfalls durch Virencanner auffindbar, jedoch betreiben diese in der Regel nur reines Pattern-Matching, d.h. sie suchen nach bestimmten, signifikanten Strings, die typisch für einen Virus sind. Das Problem hierbei ist, das z.B. Stealth-Viren, poly-

morphe Viren oder verschlüsselte Viren durch Änderung des eigenen Codes diesen so ändern, dass die Such-Strings nicht mehr zum Viruscode passen und somit das Auffinden dieser erschwert wird. Andere Möglichkeiten sind Virenschilde oder das Abschalten der Makro-Option in Programmen.

3 Würmer

3.1 Script Viren oder Würmer

Scriptviren/Würmer sind eigenständige Programme die auf die Verbreitung in Netzwerken, beispielsweise als Anhang von E-Mails, ausgerichtet sind. Viren brauchen im Gegensatz dazu ein Wirtsprogramm. Die bekanntesten Würmer sind Code Red und Nimda. Würmer sind meist äußerst einfach in einer Script-Sprache programmiert und verbreiten sich häufig innerhalb weniger Stunden selbstständig per E-Mail um den ganzen Erdball. Da durch einfaches Ändern einiger Programmtextzeilen ein neuer Virus erzeugt werden kann, tauchen auch immer wieder veränderte Ableger auf, die dann den Antivirenprogrammen Probleme bereiten. Allein von VBS/Loveletter sind über hundert Varianten bekannt. Die verbreitetsten Script-Sprachen sind Visual Basic Script, mIRC und Visual Basic for Applications (VBA). Visual Basic Script kann sogar fast alle Funktionen des Betriebssystems aufrufen und ausführen. Damit lassen sich dann die Programme (Word, Excel , PowerPoint) steuern, E-Mails versenden, richtige Programme ausführen und auch Würmer und Viren programmieren. Diese Würmer können sich selbst per E-Mail oder an Dateien angehängt versenden. Auch Schadensfunktionen wie das Verstellen der Uhr, das Starten eines externen Programms oder gar das Formatieren der Festplatte lassen sich auslösen. Die meisten Viren sind - der Einfachheit wegen - für Windows und DOS-Systeme geschrieben. die Aussage „Würmer sind unter Linux kein Problem...“ ist allerdings falsch, da hier zumeist nur noch keine geeigneten Scriptsprachen existieren, in denen Viren geschrieben werden können.

3.2 Bekämpfung

Bei der Bekämpfung gelten die gleichen Dinge wie auch für Dateiviren: Regelmäßig nach Viren scannen und nach Möglichkeit keine unbekanntes Skripte starten. Ist das System einmal infiziert, lässt es sich mit einem aktuellen Virenschanner relativ gut wieder vom Virus befreien. Nach Möglichkeit sollte ganz auf die Verwendung von Skripten verzichtet werden.

4 Trojaner

4.1 Arten von Trojanern

Ein Trojaner im klassischen Sinn ist Software, die sich auf dem Wirtsrechner als normales Programm ausgibt, das aber unter bestimmten Bedingungen anderen Programmcode ausführen kann... Hierzu gehören im weitesten Sinn auch sogenannte *logische Bomben*, die bei Erreichen einer bestimmten Triggerbedingung anderen, als den vorgesehenen Programmcode ausführen, also auch Programme, in die die Programmierer Creditscreens eingebaut haben, die bei bestimmten Eingaben, Klicks, oder zu bestimmten Zeitpunkten aktiv werden. Derartige logische Bomben müssen nicht unbedingt gefährlich sein. Sogenannte Dropper sind Trojaner, die den Wirtsrechner mit Viren infizieren, also durchaus schlechte Absichten haben. Eine andere Art der Trojaner betätigt sich auf dem Wirtsrechner als *Keylogger* und *Passwort-Sniffer*. Gefundene Passworte und Eingaben, sowie Screenshots werden über das Internet z.B. an eine bestimmte Mailadresse versandt. Der Sinn solcher Trojaner ist also nicht das Zerstören der Software, sondern viel mehr das Ausspionieren des Benutzers. Desweiteren gibt es noch eine 4. Art von Trojanern, die *RAT-Trojaner* (Remote Access Tools), diese bestehen in der Regel aus einem Client und einem Server. Der Server wird auf dem Rechner des Opfers installiert und bietet nach außen hin Dienste an, auf die man über den Client zugreifen kann... Dadurch ist es einer 2. Person möglich, den Rechner des Opfers zu belauschen, Bildschirmfotos zu machen, diesen komplett fernzusteuern, Dateien zu kopieren oder zu löschen und den Rechner für DoS-Attacken gegen 3. Rechner zu missbrauchen.

4.2 Verbreitungswege

Trojaner verbreiten sich im allgemeinen nicht selbstständig, werden aber teilweise durch andere Programme mitinstalliert, oder durch Würmer heruntergeladen.

4.3 Ausführung der Schadensroutinen

Normalerweise starten sich Trojaner selbstständig, indem sie sich bei ihrem ersten Start oder aber durch den zugehörigen Wurm in die Autostart-Variablen des Systems eintragen. Dadurch werden sie bei jedem Systemstart mitgeladen, was unter Umständen erhebliche Verzögerungen mit sich bringen kann. Wird der Trojaner ausgeführt, startet er entweder selbst mit dem Versenden der abgefangenen Daten an ein vorher festgelegtes Ziel bzw. mit der Schadensroutine oder stellt einen Serverdienst bereit, der auf einem bestimmten Port auf Befehle wartet.

4.4 Bekämpfung

Ist der Trojaner in Programmen versteckt ist es besonders schwierig, ihn festzustellen. Besonders bei logischen Bomben, die nur auf einen bestimmten Trigger hin zu wirken anfangen, ist es schwierig diese ausfindig zu machen. Deshalb sollte man v.a. bei Downloads eventuell zur Verfügung gestellte Checksummen benützen, um sicherzustellen, dass das Programm nicht mehr enthält, als man will. Bei RATools ist die schon erheblich einfacher, da diese in der Regel selbstständige Programme sind, die automatisch beim Laden mitgestartet werden. Oftmals reicht es einfach, den betreffenden Start-Eintrag und die zugehörige Datei zu löschen, um den Trojaner loszuwerden. Es gibt mittlerweile viele Trojaner-Bau-Kits, mit denen aus vorgefertigten Bausteinen eigene Trojaner erzeugt werden können. Viele davon werden jedoch durch neuere Antivirensoftware erkannt und entfernt.

5 Zusammenfassung

Sowohl die bereits bekannten ca. 55.000 bis 60.000 Viren für Windows/DOS-Systeme als auch die zunehmende Zahl von Linux-Viren zeugen davon, wie wichtig umfassender Schutz vor Viren ist. Prüfsummenprogramme, Virens Scanner sowie andere Sicherheitsmaßnahmen sollten wahrgenommen werden, um die Verbreitung von Viren zu verhindern oder zumindest einzudämmen. Jeden Tag werden 10 bis 15 neue Viren registriert. Die meisten davon erreichen allerdings niemals die privaten PCs. Nur ca. 200 Computerviren führen zu ernsthafter Unruhe. Allein die zehn meist verbreiteten Computerviren sind für ein Drittel aller Schäden verantwortlich - mit teilweise verheerenden Folgen. Nach Untersuchungen der International Computer Security Association (ICSA) richtet jede einzelne Virenattacke durchschnittlich 15.000 Mark Schaden an. 44 Stunden dauert es laut Statistik, die Folgen eines Virenbefalls zu beheben. Die monatliche Infektionsrate liegt laut ICSA-Studie bei 3,3 Prozent monatlich, was bedeutet: Drei von hundert PCs kommen jeden Monat mit einem Computervirus in Berührung.

Literatur

- [1] <http://www.datafellows.com/v-descs/>
- [2] <http://www.symantec.de/> Symantec Corporation
- [3] <http://www.avp.ch/avpve/worms/lovelet.stm> - Kaspersky labs
- [4] <http://www.trendmicro.de/>
- [5] <http://www.skrenta.com/cloner/> - Informationen zu Elk Cloner
- [6] <http://www.all.net/books/virus/> - Fred Cohen's Computer Viruses - Theory and Experiments
- [7] Mark Ludwig's - The Little Black Book of Computer Viruses (1990)
- [8] <http://www.bsi.de/av/> und <http://www.bsi.de/literat/faltbl/trojaner.htm> Bundesamt für Sicherheit in der Informationstechnik
- [9] <http://www.datafellows.com/v-descs/> F-Secure Virendatenbank
- [10] <http://vil.mcafee.com/> McAfee Virus Library
- [11] <http://www.th-security.de/virusarten.php3>
- [12] <http://www.trusecure.com/>