

Einführung und Geschichte von Malicious Code

Seminararbeit im Hauptseminar

Heike Lupold

Zusammenfassung Dieser Text liefert eine Einführung in Malware und seine Geschichte. Anhand von Beispielen werden der historische Verlauf und die einzelnen Arten von Schädlingen erklärt.

Diese Seminararbeit deckt die Geschichte der Computerviren von der frühesten Erwähnung bis einschließlich 1989 ab. Weitergeführt wird sie an dieser Stelle in der Arbeit von Fabian Prasser.

1 Kurze Einleitung in die verschiedenen Schädlingsarten

Es gibt leider nicht nur nützliche Software, sondern es gibt auch Programme, die nur entwickelt wurden, um Schaden anzurichten.

Für diese Software steht der Oberbegriff „Computerviren“. Wobei dieser Begriff, als stehender Ausdruck für Schädlinge, zu allgemein ist. Wenn man heute von Viren redet, meint man damit oft alle Schädlinge, also auch Würmer, Trojanische Pferde etc. Hier gibt es aber gravierende Unterschiede. Jeder dieser Schädlinge hat seine Eigenheiten und Tücken und ist von Grund auf anders als ein anderer. Oftmals ist es aber schwierig, einen gegebenen Schädling eindeutig einer Klasse zuzuordnen. Es gibt zum Beispiel Computerschädlinge, die sich einer Eigenschaft des Virus und einer anderen des Wurms bedienen. In der Geschichte der Computerviren lernt man auch solche Fälle kennen.

2 Geschichte der Computerviren

Die Geschichte der Computerviren geht zurück bis in das Jahr 1949. Der ungarische Informatiker John von Neumann (1903-1957) machte sich schon damals Gedanken über ein Programm, welches sich selbst reproduzieren kann. Damals dachte aber noch niemand an schädliche Viren- Programme.

Anfang der 70er Jahre wurde von Mitarbeitern der Bell Laboratories das Spiel „Core Wars“ (übersetzt „Krieg der Kerne“) erfunden. Ziel war es dem Gegner wichtige Rechenzeit zu stehlen. Da dies dem Prinzip eines Virus oder auch Wurms schon sehr nahe kam, kann man heute also behaupten, dass dieses Spiel, zumindest

HEIKE LUPOLD

von der Idee her, der erste Wurm in der Geschichte war. Auch wenn er noch auf die Hilfe der Benutzer angewiesen war. [1]

An dieser Stelle ist eine kurze Definition nötig: [18]

Viren benötigen ein Wirtsprogramm. Sie sind keine eigenständige Programme, sondern Routinen, welche sich selbst reproduzieren und so weitere Programme infizieren können oder Schadroutinen ausführen.

Würmer hingegen sind kleine eigenständige Programme. Sie benötigen also kein Wirtsprogramm, sondern sind selbst in der Lage sich (meist über Netzwerkverbindungen) zu verbreiten.

An der Fakultät für Informatik der Universität in Dortmund verfasste Jürgen Kraus 1980 seine Doktorarbeit mit dem Titel „Selbstreproduktion bei Programmen“. Er dachte damals schon daran, dass sich Programme wie biologische Viren verhalten können. Seine Arbeit wurde aber nie veröffentlicht. [5,7]

So wurde der Begriff des „Computervirus“ 1981 von Professor Adleman eingeführt, wobei der Begriff während eines Gesprächs mit Fred Cohen das erste Mal fiel. [1]

1982 gab es 3 Versionen von Apple II Viren. Man versuchte damals, durch eine minimale Abänderung, aus dem DOS (fast alle Apple Disketten beinhalteten dieses damals) ein virusinfiziertes DOS zu kreieren.

Die erste Version dieses Virus wurde wegen ‚Beeinträchtigungen‘ unter Quarantäne gestellt.

Die zweite Version sollte sich auf den Disketten derer verbreiten, die ihn ‚erfunden‘ hatten. Leider waren deren Sicherheitsvorkehrungen nicht die Besten, was dazu führte, dass sich der Virus auch in der allgemeinen Apple User Umgebung verbreitete. Erst jetzt erkannte man das negative Potenzial des Virus: Die zusätzliche Länge des DOS-Codes veranlasste manche Programme und insbesondere ein Computerspiel zum Abbruch.

Schlussendlich wurde nun die dritte Version geschrieben. Sie strebte danach, dieses Problem zu lösen. So enthielten Teile des Codes Bytes, die sowohl Daten als auch Opcode darstellten. Es sollte nun auch der Teil der Disketten User getroffen werden, welcher sich bislang sicher gefühlt hatte. Eine Reaktion blieb aber aus. [3]

Es gab noch ein weiteres Programm für den Apple II. Der von dem damals 15 Jahre alten Richard Skrenta geschriebene ‚Elk Cloner‘. Er infizierte Disketten des Apple II, löschte dabei aber keine Dateien. Als etwas ‚Besonderes‘ erschien beim 50. Starten der Diskette ein Gedicht auf dem Bildschirm:

EINFÜHRUNG UND GESCHICHTE VON MALICIOUS CODE

It will get on all your disks
It will infiltrate your chips
Yes it's Cloner!

It will stick to you like glue
It will modify ram too
Send in the Cloner!

Dieser ‚Virus‘ verbreitete sich allerdings nicht sehr stark und wurde daher nie als solcher angesehen. [4,5,17]

Im gleichen Jahr wurden von Jon Hepps und John Shock im Xerox Palo Alto Research Center die ersten Würmer programmiert. Diese sollten sich damals kontrolliert verbreiten und für verteilte Rechenoperationen dienen. Ein Programmierfehler hatte allerdings zur Folge, dass der Wurm außer Kontrolle geriet und enormen Schaden anrichtete. Kurz darauf stürzte das komplette System ab. [1,8]

Fred Cohen brachte schließlich im Jahre 1983 den ersten funktionsfähigen Virus an die Öffentlichkeit. Der Virus nistete sich im Befehl VD eines UNIX Betriebssystems ein. Er erbt bei jeder Ausführung die Systemprivilegien eines jeden infizierten Programms und gab diese an andere User weiter.

Mit diesem Virus machte Fred Cohen das möglich, was bis dahin nur als Theorie galt: ein Computerprogramm kann sich selbst reproduzieren. [1,12]

Im folgenden Jahr veröffentlichte er seine Doktorarbeit „Computer-Viruses: Theory and Experiments“ und definierte darin den Begriff Computervirus folgendermaßen:

“We define a **computer Virus** as a program that can "infect" other programs by modifying them to include a possibly evolved copy of itself. With the infection property a virus can spread throughout a computer system or a network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows.” [2]

Von da an gab es in der Welt der Computerschädlinge kein Halten mehr und eine rasante Entwicklung begann.

1985 wurde der Schädling EGABTR über Mailboxen verteilt. Dies stellte das erste Trojanische Pferd dar. Das verteilte Programm gab vor, zur Verbesserung der mangelhaften Graphik zu dienen, in Wirklichkeit wurden aber beim Starten des Programms alle Dateien auf der Festplatte gelöscht und auf dem Bildschirm erschien die Nachricht „Arf, arf, Gotcha!“ (Arf, arf, hab Dich!). [3,5]

Der Brain- Virus, der 1986 in Pakistan sein Unheil begann, war das Werk zweier Brüder, Basit und Amjad Farooq Alvi, die in Pakistan eine Firma namens Brain Computer Services besaßen. An diese Informationen war es nicht sehr schwer zu gelangen, da im Viruscode folgender Text enthalten war: [6]

HEIKE LUPOLD

*"Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt)
Ltd. BRAIN COMPUTER SERVICES 730 NIZAB BLOCK ALLAMA IQBAL
TOWN LAHORE-PAKISTAN PHONE :430791,443248,280530.
Beware of this VIRUS.... Contact us for vaccination..... !!"*

Es gibt verschiedene Annahmen, weswegen die Brüder diesen Virus ins Leben gerufen haben. Da in Pakistan das Raukopieren legal war, wollten sie sich wohl mit dem Virus gegen die Vervielfältigung ihrer eigenen Software wehren. Oder aber sie wollten mit den virusbelasteten Kopien die Kunden an sich binden.

Egal weswegen dieser Virus geschrieben wurde, dachte man doch damals noch nicht über die Folgen nach und hatte auch noch nicht die heutige, vorsichtige Einstellung diesen Schadprogrammen gegenüber.

Fakt ist, dass der Brain- oder auch Pakistan- Virus der erste MS-DOS Virus war. Es handelte sich hierbei um einen speicherresidenten Bootsektor Virus, der Tarnkappentechnik benutzte.

Er überschrieb den Bootsektor einer Diskette, verschob den originalen Bootsektor an eine andere Stelle auf der Diskette und schrieb sich selbst an zwei ergänzende Sektoren. Er besetzte also 3 Sektoren und bediente sich dafür des ungenutzten Platzes auf der Diskette.

Wenn der Bootsektor beispielsweise beim Starten gebraucht wurde, las der Virus den originalen Bootsektor, dort wo er ihn gespeichert hatte, ab und wurde so getarnt.

Dann änderte er noch die Bezeichnung der Diskette auf ©Brain und wartete, resident im Speicher stehend, auf neue, noch zu infizierende Disketten.

Der originale Brain- Virus war also relativ harmlos, da er die Festplatte nicht infizierte. [1,3,6,15]

Im gleichen Jahr wurde der erste Dateivirus „Viridem“, welcher aus Deutschland kam, entdeckt. Es handelte sich um einen Virus, der Programmdateien infiziert. Diese Art von Viren hatte auf PCs neben den Bootviren ursprünglich die größte Bedeutung. [8,9]

1987 entstand an der Lehigh-University ein neuer Virustyp, der erste Virus, der COMMAND.COM infizierte. Der Lehigh- Virus verlängerte die COMMAND.COM um 555 Bytes und überschrieb dadurch den Stackbereich. Er verwendete daher eine neue Technik beim Infizieren. Man spricht auch von einem Stackbereich-Infector. Bei jedem Lesen einer Diskette überprüfte der Virus, ob die Datei COMMAND.COM bereits infiziert ist oder nicht und nach jeder vierten Infektion wurde ein Teil der Diskette überschrieben.

Entdeckt wurde dieser Virus, da mehrere hundert Studenten der Universität die Systemdisketten zurückgaben, weil sie nicht mehr bootfähig waren. Bei Untersuchungen ergab sich, dass überall Größe und Datum der COMMAND.COM verschieden waren, obwohl alle Disketten die gleiche Betriebssystemversion enthielten.

Dieser Virus kursierte, soweit man das sagen kann, nur auf dem Campus der Universität. [5,10,11]

EINFÜHRUNG UND GESCHICHTE VON MALICIOUS CODE

Kurz vor Weihnachten im selben Jahr, legte der Wurm „Christmas Tree“ das weltweite IBM-Netzwerk lahm. Der Wurm wurde von einem deutschen Studenten als Weihnachtsgruß in Form eines aus Buchstaben gezeichneten Weihnachtsbaums verschickt. Der Wurm suchte sich alle Email Adressen des Empfängers und versendete sich selbst an alle weiter. Erstaunlich ist, dass der Wurm es schaffte, innerhalb von 4 Minuten 12 Rechner in 6 Staaten auf 4 Kontinenten zu infizieren. Die Ausbreitung im gesamten IBM-Netz war enorm. [11]

Der Virus mit den meisten Varianten und der klare ‚Sieger‘ unter den Dateiviren ist der Jerusalem Virus. Er tauchte Ende des Jahres 1987 erstmals in Israel auf.

Der Dateivirus hängt sich an COM und EXE Dateien. Wenn eine der infizierten Dateien ausgeführt wurde, ging der Virus resident in den Speicher und infizierte von nun an alle laufenden Programme indem er seinen Code anhängte. Viele dieser Viren hatten eine Art ‚date logic bomb payload‘, das meist auf Freitag den 13ten ausgerichtet war.

Der Virus wurde in einigen Fällen schon vor dem richtigen Schaden, den er anrichten konnte, entdeckt. Das Problem war, dass der Virus wohl durch einen Programmierfehler nicht mit nur einer Infektion zufrieden war, sondern die EXE Dateien immer wieder infizierte und so die Größe dieser enorm wuchs. Befallene Rechner wurden dadurch erheblich langsamer.

Wie eine Bombe schlug der Jerusalem Virus dann erstmals am Freitag, 13.Mai 1988 ein. Er löschte an diesem Tag alle COM und EXE Dateien der infizierten Rechner.

Zusammenfassend war Jerusalem ein Virus, der zwei Virenprogramme kombinierte. Er erfreute sich großer Popularität - wahrscheinlich, weil er recht einfach programmiert war und für jemanden, der Erfahrung mit Assemblerprogrammierung hat, einen optimalen ‚Grundstein‘ darstellte, um neue Viren zu kreieren, die COM und EXE Dateien befallen. [8,12,13,14]

Der Stoned- Virus war der erste MBR- Virus (Master Boot Record); er stammte von einem Studenten der Universität von Wellington, Neuseeland. Er infizierte den Bootsektor einer Diskette. Wurde der Rechner über eine infizierte Diskette gestartet, wurde der Virus speicherresident.

Die Meldung "Your Computer is now stoned. Legalize Marijuana." erschien bei jedem achten Programmaufruf. [11]

Im gleichen Jahr gab es den ersten Virus für Macintosh-Rechner. Apple stattet darauf hin alle Rechner mit einem Virensuchprogramm aus. Dieses Programm konnte allerdings nur diesen einen Virus erkennen, war also für weitere Schädlingserkennung nutzlos. [1]

HEIKE LUPOLD

MacMag stellt dann den ersten massenhaft vervielfältigten Computervirus dar. Er verbreitete sich nicht nur über Disketten, sondern erstmals auch über das Netzwerk. Es handelte sich hierbei um eine Datei (Stapel) für das Apple- Programm Hypercard. Sie tauchte am 7. Februar 1988 in einem Forum von Compuserve auf und sorgte für viel Ärger.

Sobald diese Datei vom Benutzer geöffnet wurde, kopierte sich der Virus als INIT, als eine Systemerweiterung, in den Systemordner. Viele INITs sind ‚background‘ oder residente Programme, die besondere Hardware unterstützen oder das System um besondere Funktionen erweitern. Also ein perfekter Standort für Viren.

Davon machte auch der nicht sehr anspruchsvoll programmierte MacMag Virus Gebrauch. Er verbreitete sich bis zum 2.März 1988 sehr schnell und so weit wie möglich; und wenn ein infizierter Computer an diesem Tag gebootet wurde, so zeigte der Virus eine „UNIVERSAL MESSAGE OF PEACE“ an. Glücklicherweise löschte sich der Virus nach dieser Anzeige selbst. [3]

Der Student Robert Morris wollte 1988 lediglich einige Schwachstellen des Betriebssystems UNIX aufdecken. Durch seinen Virus und den Programmierfehler, der sich eingeschlichen hatte, legte er aber innerhalb von kürzester Zeit tausende Computer lahm. Durch den Fehler kopierte sich der Virus nämlich sooft, dass die Speicherkapazitäten des jeweiligen Systems nicht mehr reichten.

Der Schaden, den der Student mit seinem Wurm anrichtete, wird auf 96 Millionen Dollar geschätzt. [5,11]

Der Dark Avenger war der erste Virus, der aus Bulgarien kam. Es handelte sich hierbei wieder um einen residenten Virus, der COM und EXE Dateien befahl. Allerdings befahl er, resident im Speicher, nicht nur Programme, welche ausgeführt wurden, sondern auch wenn nur die Programmdatei gelesen wurde. Das heißt, dass ein einfaches Programm, das jede COM und EXE Datei öffnete, um diese beispielsweise auf eine Virusinfektion zu prüfen, leicht eine Epidemie auslösen konnte. [5,16]

Cascade stellte den ersten sich selbst verschlüsselnden und speicherresidenten Virus dar. Wenn der Computer erfolgreich infiziert wurde, regneten Buchstaben wie ein Wasserfall über den Bildschirm. [5]

1989 war das Jahr, in dem der erste polymorphe Virus gefunden wurde, der V2Px oder auch Washburn.

Diese Viren verschlüsseln sich bei jeder Infektion neu, was das Erkennen des Viruses bzw das Entwickeln von Anti-Virus-Software erheblich erschwert.

Auch neu in diesem Jahr waren Tarnkappen- Viren (Stealth- Viren). Sie infizierten Dateien, waren aber in der Lage, die gemachten Änderungen zu verstecken. Und das sehr erfolgreich.

EINFÜHRUNG UND GESCHICHTE VON MALICIOUS CODE

Das heißt, wenn der Virus resident im Speicher war und ein Programm eine infizierte Datei lesen wollte, sah es nur die Bytes, die vor der Infektion darin enthalten waren. Ein Beispiel hierfür war der Frodo- Virus, welcher am 22. September die Meldung „FRODO LIVES!“ ausgab. [5,8,14]

Zuletzt sollte in diesem Abschnitt der Geschichte der Computerviren auf jeden Fall der AIDS- Trojaner erwähnt werden.

Ein Trojanisches Pferd ist ein scheinbar nützliches Programm, welches aber versteckte Schadroutinen enthält.

Im Dezember 1989 wurden auf einer internationalen AIDS-Konferenz Disketten, von der Firma PC Cyborg Corp, mit angeblich wichtigen Informationen zum Thema verteilt. Hierbei handelte es sich aber um einen Trojaner, der, nachdem die Dateien auf den Computer gespielt wurden, nach dem 90. Starten des Systems alle Dateien der Festplatte verschlüsselte; ausgenommen eine: Eine Rechnung mit der Aufforderung, 189 US-Dollar zu zahlen, um den Entschlüsselungscode zu bekommen. Die Firmeninhaber wurden kurz darauf in eine geschlossene psychiatrische Anstalt eingewiesen. [1,3,14]

Literatur

1. <http://www.vhm.haitec.de/konferenz/1997/history.htm> zuletzt besucht am: 15.12.04
2. <http://www.infnet.verein.de/arbeitsgruppe/sicherheit/schadensprogramme/typen.html> zuletzt besucht am: 15.12.04
3. Robert M. Slade, History of Computer Viruses http://www.claws-and-paws.com/virus/papers/slade_history.shtml#C01 zuletzt besucht am: 20.10.04
4. <http://www.ph-studio.de/module-subjects-viewpage-pageid-136.html?POSTNUKESID=22e9da6051607a0ae6fc27179df8091f> zuletzt besucht am: 15.12.04
5. http://www.digitalcraft.org/index.php?artikel_id=281 zuletzt besucht am: 15.12.04
6. http://freenet.meome.de/app/fn/artcont_portal_news_article.jsp?catId=78466 zuletzt besucht am: 15.12.04
7. <http://de.wikipedia.org/wiki/Computervirus> zuletzt besucht am: 15.12.04
8. http://symantec.com/region/de/avcenter/regeln_de.html zuletzt besucht am: 15.12.04
9. http://www.dr-klotz.de/Glossar/glossar_d.html zuletzt besucht am: 15.12.04
10. <http://www.pinguhuhn.de/text.php?id=140&s=read> zuletzt besucht am: 15.12.04
11. <http://www.covitec.de/seiten/index.php?haupt=http://www.covitec.de/frames/main/firma/viren/virengeschichte.html> zuletzt besucht am: 15.12.04
12. <http://www.freecity.de/special/viren/geschichte2.phtml> zuletzt besucht am: 15.12.04
13. <http://www.pc-special.net/?idart=2147> zuletzt besucht am: 15.12.04
14. <http://www.computerviren-info.de/Geschichte.html> zuletzt besucht am: 15.12.04
15. <http://www.michael-berndt.de/ie/sou/viren.htm#14> zuletzt besucht am: 15.12.04
16. <http://www.f-secure.com/v-descs/eddie.shtml> zuletzt besucht am: 15.12.04
17. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci989616.00.html zuletzt besucht am: 15.12.04
18. <http://www.oid.lu.ch/index/vireninfo.htm> zuletzt besucht am: 15.12.04