Trojaner, Viren, Würmer – Ausbreitungswege und Bekämpfung

Christian Steiner
sichstei@stud.uni-erlangen.de

8. Juli 2002

Gliederung

1. Geschichtliche Entwicklung
2. Viren
   - Grundtypen
   - Arten
     - Verbreitungswege von Bootsektor und Dateiviren
     - Beispiel Michelangelo
     - Beispiel 1260 Virus
3. Würmer
     - Beispiel Loveletter.a
4. Trojaner
     - Beispiel Sub7
5. Viren unter Linux
     - Beispiel Bliss
6. Schäden
7. Vermeidung und Bekämpfung von Viren
8. Gesetze gegen Viren
9. Zusammenfassung

1. Geschichtliche Entwicklung - 1

1949	John v. Neumann (1903-1957): Theorie der selbstreproduzierbaren Automaten
1970	Spiel „Core Wars“ in Bell Laboratories entwickelt.
1981	Erstmalige Verwendung des Begriffes „Computervirus“ durch Prof. Adleman im Gespräch mit seinem Doktoranden Fred Cohen
1981	„Elk Cloner“-Virus verbreitet sich über Apple][-Disketten
1983	Fred Cohen schreibt ersten richtigen Virus, der unter Unix den VD-Befehl befällt
1985	Virus „EGABTR“ wird über Mailboxen verbreitet.
1986	Erster MsDOS-Virus: „Pakistani“- oder „Brain“- Virus
1986	Sharewareprogramm „PCWrite“ enthält den 1. Trojaner
1986	Erster Dateivirus „Virdem“
1987	19 verschiedene Viren bekannt
1987	Erster richtiger Macintosh Virus „MacMag“
1987	IBM-Virus „X-Mas“ verbreitet sich an alle Empfänger in Mailingliste des Opfers
1988	2.000-6.000 Rechner durch „Internet-Wurm“ befallen

1. Geschichtliche Entwicklung - 2

1989	44 Virenfamilien bekannt
1989	„AIDS“-Trojaner
1990	VX „Virus Exchange“ BBS geht in Bulgarien Online
1991	„Tequila“ ist der 1. polymorphe Virus
1992	„Michelangelo“ geht durch die Medien
1995	„Word Concept“ erster Makro-Virus, ein Jahr später „Laroux“ für Excel
1998	„Back Orifice“, einer der ersten RAT-Trojaner
1999	„Mellisa“ Kombination aus Word-Makro-Virus und Wurm, verbreitet sich via E-Mail
2000	Erste DoS-Attaken gegen Yahoo! Und andere große Firmen
2000	„Love Letter“ wird am schnellsten verbreiteter Wurm
2001	„Peachy Pdf“ verbreitet sich über PDF-Dokumente **(Vollversion von Acrobat nötig!)**
2002	„LFM-926“ erster Shockwave-Virus
2002	„Benjamin.Kazaa“ verbreitet sich - medienwirksam -über das p2p-Netzwerk von Kazaa

Viren

Virus: Ein Computer Virus ist eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt (bsi)

Aufbau eines Computervirus:

- Reproduktionsteil
- Erkennungsteil
- Schadensteil(Payload), optional
- Bedingungsteil, optional
- Tarnungsteil, optional

Viren- Grundtypen

Nicht residente Viren – nur bei Ausführung des infizierten Programmes aktiv

Speicherresidente Viren – resident im Hauptspeicher um Programmabläufe zu überwachen und zu steuern

Stealth-Viren – anderen Programmen wird ein sauberes System vorgespiegelt.

Viren- Arten

Dateiviren	werden beim Start eines Programmes oder bei der Ausführung einer Datei mitgestartet
Bootsektorviren	der Virencode liegt im Bootsektor des Mediums und wird i.A. unabhängig vom Betriebssystem ausgeführt
Companionviren	der Viruscode liegt in einer eigenem Datei, die dem Benutzer verborgen bleiben soll.
Makroviren	haben die selbe Funktionalität wie „normale“ Viren, sind aber in einer Makrosprache geschrieben und somit auch von der Ausführung im zugehörigen Makrointerpreter abhängig.

Verbreitung:

Bootsektorviren	▪ durch Austausch von befallen Medien und Booten von diesen
Datei-/Makroviren	▪ durch Austausch und Aufruf von infizierten Dateien ▪ durch „Dropper“ gesetzt ▪ als Bestandteile von Würmern

WO VIEL UND MIT UNBEKANNTEN GETAUSCHT WIRD
ERHÖHT SICH DIE GEFAHR DES VIRENBEFALLS

Beispiel: Michelangelo

- Einfache Abart des Stoned-Virus, ohne Stealth oder Polymorphie-Eigenschaften
- Bootsektor-Virus, der nur 5.25“ Disketten einwandfrei infizieren kann
- Wird Michelangelo geladen, fängt er Interrupt 13h ab und überwacht die Schreib-/Lesezugriffe auf den Datenträger.
- Sobald ein nicht infiziertes Medium benutzt wird, wird es infiziert.
- Schaden: Michelangelo löscht am 6.3. eines jeden Jahres Dateien.

Bootsektoren

```
000000      ·<·MSDOS5.0·····
000010      ···@············
000020      ·····)··H·VOLUM
000030      E-NAMEFAT12   ·3
000040      ·····|···x·6·7·V
          . . . . . . .
          . . . . . . .
          . . . . . . .
000190      ·····$|·6%|·····
0001A0      Kein System oder
0001B0       Laufwerksfehler
0001C0      ··Wechseln und T
0001D0      aste drücken···I
0001E0       O      SYSMSDOS
0001F0        SYS·····U·
```

Normaler Bootsektor (DOS 5.0)

```
000000      ···········.···P
000010      ··u·3·····?··u·X
000020      ··.···········X
000030      ·.·.··PSQR··VW··
000040      ·············3·
          . . . . . . . .
          . . . . . . . .
          . . . . . . . .
000190      ·····r······!
0001A0      ·····3·····
0001B0      ·····er
0001C0      ··Wechseln und T
0001D0      aste drücken···I
0001E0       O      SYSMSDOS
0001F0        SYS·····U·
```

Michelangelo befallene Diskette

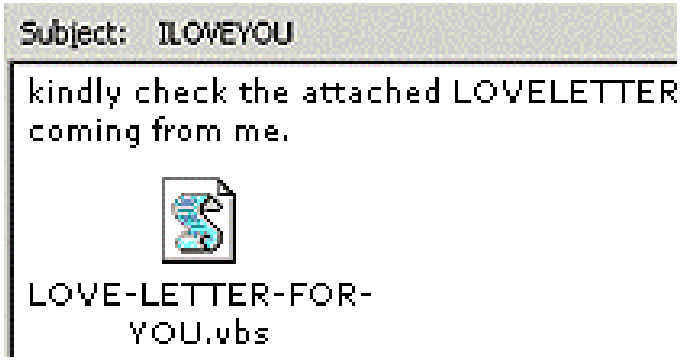
Beispiel: 1260

- DOS-Dateivirus
- Stealth-Virus
- Fügt 1260 Byte an jedes befallene Programm an
- Ersten 39 Byte enthalten einfache Entschlüsselungsrouting
- Mehrere 1-2 Byte lange nonsense-Instruktionen (variabel viele!)
- Infiziert .com-Dateien und zerstört Programme.
- Setzt TimeStamp der befallenen Dateien auf 62 Sekunden!

Würmer

- Eigenständige Programme
- Ausgelegt auf Verbreitung in Netzwerken z.B. E-Mail-Anhänge
- In zumeist sehr mächtigen, dennoch einfachen Skript-Sprachen geschrieben (z.B. VBA, VBSkript...)
- Mächtige Skriptsprachen ➡ große Schäden möglich
- Benutzen teils Sicherheitslücken in Software zur Ausführung des Codes

Beispiel: Loveletter



- Windows-Wurm
- Loveletter.a ist ein VBS-Skript
- Nur auf Windows-Rechnern mit Windows-Scripting-Host ausführbar
- Verschickt sich selbst als E-Mail
- Kopiert sich selbst unter verschiedenen Namen in zahlreiche Verzeichnisse:
  - \windows\win32dll.vbs
  - \windows\system\mskernel32.vbs
  - \Love-Letter-For-You.txt.vbs
- Überschreibt verschiedene Dateien mit eigenem Code
  Versucht sich via IRC weiter zu verschicken

Trojaner

- Bei Erreichen einer Triggerbedingung wird „gefährlicher“ Programmcode ausgeführt
- Sind i.d.R. Bestandteil anderer Programme, die für den Benutzer normal zu arbeiten scheinen
- Creditscreens, logische Bomben, ...
  sind definitionsgemäß alles Trojaner
  („es steckt was drin, was nicht drin sein sollte“)
- „Dropper“: Infizieren ein Opfersystem mit Viren
- Werden normalerweise als Keylogger, Passwordsniffer und Remote-Access-Tools verwendet
- DoS-Attaken

- Verbreiten sich i.A. nicht selbstständig
- Werden teils durch andere Programme mitinstalliert oder auch durch Würmer heruntergeladen
- Start normalerweise durch Eintrag in Autostart-Zeilen (windows: „run“/“run-services“ – Schlüssel der Registry, win.ini“)
- Stellen v.a. als RATs Serverdienste auf spezifischen Ports zur Verfügung und teilen anderen mit, dass sie aktiv sind.
- Von Spionage bis Rechnersteuerung ziemlich alles möglich

Beispiel: Sub7

- Windows-Trojaner
- Erstmals 1999 entdeckt
- Verbreitet durch E-Mails und Newsgroups
- Kopiert sich ins Windows-Verzeichnis und benennt sich in den Namen der Datei um, von der er ausgeführt wurde.
- Ändert Registry und win.ini so, daß er bei jedem Start mitgeladen wird
- Sucht nach TCP/IP-Verbindungen und lauscht auf bestimmten Ports
- Unterstützt ca. 113 verschiedene Befehle:
  „restart windows“, „enable keylogger“,
  „open ftp-server“, „disable keyboard“,
  „screen capture“, „download/upload“...

- Fertige Konfigurations-Utilities erhältlich
- Frei konfigurierbar, von Verbreitungsart bis Programmicon alles einstellbar

Viren und Linux

- vier Virentypen für Linux: Shell-Skript-, Perl-, Makroviren (z.B. in StarBasic, StarScript und JavaScript von StarOffice geschrieben)

  und

- ELF-Viren. (Executable Linking Format):

  Patchen von ELF-Binaries ist kein Problem.

  Sich im Speicher selbst modifizierender Code nicht ohne weiteres möglich

  Daemonen (z.B. sendmail etc.) sind evtl. infizierbar

- W32.Winux-Virus. Zeigt Möglichkeit, Windows- **und** Linux-Systeme gleichermaßen zu infizieren.

Beispiel: Bliss

- Linux Virus, der ELF-Binaries infiziert.
- Februar 1997 erstmals entdeckt
- 2. bekannter Linux Virus
- Überschreibt Binaries auf die er Schreibrecht hat mit seinem eigenem Programmcode
- Infizierte Programme starten nicht, eine Wiederherstellung ist möglich
- Sucht sich neue Opfer auf anderen Rechnern über die /etc/hosts.equiv

Schäden durch Viren & Co

- Beabsichtigte, programmierte Zerstörfunktionen
- Unbeabsichtigte Seiteneffekte
- Inanspruchnahme von Speicherplatz und Rechenzeit
- Materieller und personeller Aufwand für Suche und Entfernung
- Panik-Reaktionen und Verunsicherung

...

Vermeidung und Bekämpfung

- Aktuelle Virenscanner erkennen 60-80% aller Viren
  (suche über – evtl. uneindeutige – Virensignaturen: False Positives)
- Um unbekannte Viren zu „erkennen“: Prüfsummenprogramme
- Selbsttests von Programmen:
  Fast alle bekannten File-Viren hätten keine Chance zur Ausbreitung, wenn alle Programme bei ihrem Start einen Selbsttest ausführen würden
- Virenschilde, On Access-Scanner

  ...

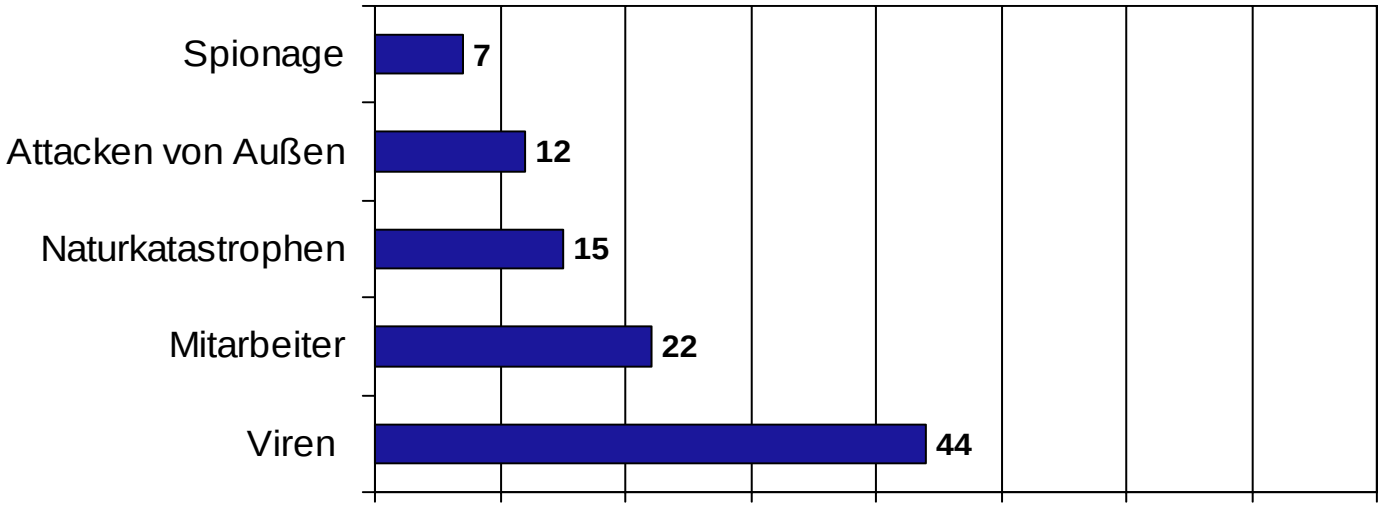
Gesetze

- Keine expliziten Gesetze gegen Viren oder Schadprogramme in der BRD
- Zuständig: § 202a, 303a und 303b StGB
  - Wer sich oder anderen besonders gesicherte Daten verschafft wird mit Freiheitsstrafe bis 3 Jahre oder Geldstrafe bestraft
  - Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert oder dies versucht wird mit Freiheitsstrafe bis 2 Jahren oder Geldstrafe bestraft

Im Zeitalter des Internets und fast grenzenloser Kommunikation richten Computerviren und ihre Unterarten mittlerweile enormen wirtschaftlichen Schaden an.

Von den ersten bekannten Viren aus dem Jahr 1980, damals noch ein Experiment, bis heute, sind mittlerweile über 60.000 verschiedenste Arten und Unterarten bekannt.

Schäden im IT-Bereich, verursacht durch: (Angaben in %)



www.ca.com