

HANSER

Eugene Kaspersky

# Malware

Von Viren, Würmern, Hackern und Trojanern und wie man sich vor  
ihnen schützt

ISBN-10: 3-446-41500-9

ISBN-13: 978-3-446-41500-3

Inhaltsverzeichnis

Weitere Informationen oder Bestellungen unter  
<http://www.hanser.de/978-3-446-41500-3>  
sowie im Buchhandel.

# Inhalt

|                  |   |
|------------------|---|
| Einleitung ..... | 1 |
|------------------|---|

## Teil I: Arten, Auftreten und Abwehr von Malware

|  |   |
|--|---|
| Wer schreibt Schadprogramme und weshalb? ..... | 1 |
|--|---|

|                            |    |
|----------------------------|----|
| Computervandalismus .....  | 1  |
| Kleine Betrügereien .....  | 4  |
| Kriminelle Geschäfte ..... | 5  |
| Halblegale Geschäfte ..... | 19 |

|                               |    |
|-------------------------------|----|
| Wissenswertes über Spam ..... | 22 |
|-------------------------------|----|

|  |    |
|--|----|
| Drei Bedingungen für die Existenz von Schadprogrammen..... | 39 |
|--|----|

|                                   |    |
|-----------------------------------|----|
| Schäden durch Virenangriffe ..... | 43 |
|-----------------------------------|----|

|   |    |
|---|----|
| Funktionsfähigkeit von Computern und Netzwerken ..... | 43 |
| Hardware-Ausfälle.....                                | 44 |
| Verlust oder Diebstahl von Daten.....                 | 45 |
| Kein sichtbarer Schaden .....                         | 46 |

|  |    |
|--|----|
| Klassifikation und Verhaltensweisen von schädlichen,<br>unerwünschten und potenziell gefährlichen Programmen ..... | 49 |
|--|----|

|               |    |
|---------------|----|
| Malware ..... | 50 |
|---------------|----|

|              |    |
|--------------|----|
| Würmer ..... | 53 |
|--------------|----|

|                    |    |
|--------------------|----|
| E-Mail-Würmer..... | 53 |
|--------------------|----|

|  |    |
|--|----|
| Würmer in Instant Messengern (IM)..... | 54 |
|--|----|

|  |    |
|--|----|
| Würmer in Internet Relay Chat (IRC)..... | 54 |
|--|----|

|                       |    |
|-----------------------|----|
| Sonstige Würmer ..... | 54 |
|-----------------------|----|

|                                  |    |
|----------------------------------|----|
| Würmer für P2P-Tauschbörsen..... | 56 |
|----------------------------------|----|

|                        |    |
|------------------------|----|
| Klassische Viren ..... | 56 |
|------------------------|----|

|                         |    |
|-------------------------|----|
| Umgebung des Virus..... | 56 |
|-------------------------|----|

|                           |    |
|---------------------------|----|
| Infizierungsmethoden..... | 58 |
|---------------------------|----|

|                                    |    |
|------------------------------------|----|
| Sonstige Infizierungsmethoden..... | 61 |
|------------------------------------|----|

|                |    |
|----------------|----|
| Trojaner ..... | 63 |
|----------------|----|

|  |    |
|--|----|
| Trojan Backdoors – Trojaner zur Fernverwaltung ..... | 63 |
|--|----|

|   |    |
|---|----|
| Trojan PSW – Trojaner zum Kennwortdiebstahl ..... | 64 |
|---|----|

|  |    |
|--|----|
| Trojan Clicker – Internetklicker ..... | 64 |
|--|----|

|  |           |
|--|-----------|
| DDoS Trojans – Trojaner für Massenangriffe .....   | 65        |
| Trojan Downloader – Trojaner zum Herunterladen anderer Schadprogramme .....              | 65        |
| Trojan Dropper – Installationsprogramme für andere Schadprogramme .....                  | 66        |
| Trojan Notifier – Trojaner, die einen erfolgreichen Angriff melden .....                 | 67        |
| Trojan Proxies – Proxy-Server-Trojaner .....   | 67        |
| Trojan Spies – Spionage-Programme .....  | 68        |
| Rootkits – Tools zur Tarnung im System .....   | 68        |
| ArcBombs – Archivbomben .....  | 69        |
| Bad Jokes und Hoaxes – Schlechte Scherze und Irreführung des Nutzers .....               | 70        |
| Potenziell gefährliche Programme .....   | 70        |
| Dialer – Einwahlprogramme .....  | 71        |
| Netzwerk-Installer .....   | 71        |
| FTP-, P2P-, Telnet- und Webserver .....  | 71        |
| Proxy-Server .....   | 72        |
| IRC-Clients .....  | 72        |
| Überwachungsprogramme – Tools zur Systemsteuerung .....                                  | 72        |
| PSW-Tools – Tools zum Wiederherstellen von Kennwörtern .....                             | 72        |
| RemoteAdmin – Fernverwaltungstools .....   | 73        |
| Adware – Werbeprogramme .....  | 73        |
| Eindringen in Systeme .....  | 73        |
| Zustellung von Werbung .....   | 74        |
| Heimliches Erfassen von Informationen .....  | 74        |
| Pornware .....   | 75        |
| Wissenswertes über Spyware .....   | 75        |
| <b>Schutz vor Malware: Herkömmliche Antiviren-Lösungen und neue Technologien .....</b>   | <b>77</b> |
| Auswahl des Viren-Schutzes .....   | 79        |
| Qualität des Viren-Schutzes und Probleme der Antiviren-Programme .....                   | 81        |
| Erkennungsraten für verschiedene Arten von Malware .....                                 | 81        |
| Häufigkeit und Regelmäßigkeit der Updates .....  | 83        |
| Korrektes Entfernen des Virencodes aus dem System .....                                  | 84        |
| Ressourcen-Auslastung: Balance zwischen Leistungsfähigkeit und vollwertigem Schutz ..... | 84        |
| Kompatibilität parallel installierter Antiviren-Programme .....                          | 85        |
| Schutz vor neuen Viren und Trojanern .....   | 85        |
| Unabhängige Tests .....  | 88        |
| Maßnahmen bei einer Infektion des Computers .....  | 90        |

**Teil II: Geschichte der Computerviren und anderer Schadprogramme**

**Geschichte der Computerviren und anderer Schadprogramme .....99**

Die Anfänge – ein wenig Archäologie ..... 100

Anfang der 1970er Jahre..... 100

1975 ..... 101

Anfang der 1980er Jahre..... 102

1981 ..... 103

1983 ..... 104

1986 ..... 104

1987 ..... 105

1988 ..... 107

1989 ..... 109

1990 ..... 111

1991 ..... 112

1992 ..... 114

1993 ..... 115

1994 ..... 116

1995 ..... 117

1996 ..... 118

1997 ..... 120

1998 ..... 122

1999 ..... 126

2000 ..... 129

2001 ..... 131

2002 ..... 136

2003 ..... 138

2004 ..... 140

2005 ..... 145

2006 ..... 147

2007 ..... 149

Ausblick auf zukünftige Entwicklungen..... 149

    Mobile Systeme ..... 150

    Intelligente Häuser ..... 151

Prognosen zu Veränderungen in der Antiviren-Branche ..... 152

    1. Faktor: Fortschreitende Kriminalisierung des Internet..... 153

    2. Faktor: Zunehmende Vielfalt bei den Angriffsarten und  
der Umsetzung der Angriffe..... 154

    3. Faktor: Microsoft ..... 155

|  |     |
|--|-----|
| Schlussfolgerungen .....   | 156 |
| Sollten die Hersteller von Antiviren-Software das Feld einfach räumen? ..... | 157 |
| Schlussbemerkung .....   | 158 |

### Teil III: Beschreibung einiger Schadprogramme

|   |            |
|---|------------|
| <b>Beschreibungen einiger Schadprogramme.....</b> | <b>161</b> |
| Viren für MS-DOS .....                            | 161        |
| DOS.April1st.COM .....                            | 161        |
| DOS.April1st.EXE.....                             | 162        |
| DOS.ArjVirus .....                                | 163        |
| DOS.AsmVir-Familie .....                          | 164        |
| DOS.Badboy-Familie.....                           | 164        |
| DOS.Beast-Familie .....                           | 165        |
| DOS.Carbuncle .....                               | 166        |
| DOS.Casino.2330 .....                             | 167        |
| DOS.Chameleon-Familie.....                        | 168        |
| DOS.Cruncher-Familie .....                        | 168        |
| DOS.Mutant-Familie .....                          | 170        |
| DOS.Ply-Familie.....                              | 171        |
| DOS.RMNS.MW-Familie .....                         | 172        |
| DOS.Shifter.....                                  | 173        |
| Hybridviren für MS-DOS .....                      | 174        |
| OneHalf-Familie .....                             | 174        |
| Tequila-Familie.....                              | 175        |
| Viren für MS-DOS in der BAT-Befehlssprache.....   | 176        |
| BAT.Batalia6 .....                                | 176        |
| BAT.Batman.186 .....                              | 178        |
| BAT.Combat.....                                   | 179        |
| Makroviren .....                                  | 180        |
| Macro.MSVisio.Radiant .....                       | 180        |
| Macro.MSWord.Cap.....                             | 181        |
| Macro.MSWord.Concept.....                         | 182        |
| Macro.MSExcel.Laroux.....                         | 182        |
| Viren für Microsoft Windows .....                 | 183        |
| Win9x.CIH.....                                    | 183        |
| Win32.Donut.....                                  | 187        |
| Win32.Driller.....                                | 187        |
| Win32.FunLove.3662 .....                          | 189        |
| Win32.InvictusDLL .....                           | 190        |
| Win32.Kriz .....                                  | 191        |

|                                    |            |
|------------------------------------|------------|
| Win32.Libertine .....              | 193        |
| Win32.Perrun .....                 | 195        |
| Würmer für Microsoft Windows ..... | 196        |
| Net-Worm.Win32.CodeRed.a .....     | 196        |
| I-Worm.VBS.LoveLetter .....        | 198        |
| Net-Worm.Win32.Lovesan.a .....     | 201        |
| Email-Worm.MSWord.Melissa .....    | 203        |
| Email-Worm.Win32.Mydoom.a .....    | 205        |
| Net-Worm.Win32.Nimda.a .....       | 209        |
| Net-Worm.Win32.Opasoft.a .....     | 212        |
| Net-Worm.Win32.Sasser .....        | 214        |
| Net-Worm.Win32.Slammer .....       | 216        |
| Würmer für Linux.....              | 217        |
| Net-Worm.Linux.Adm.....            | 217        |
| Net-Worm.Linux.Lupper .....        | 219        |
| Net-Worm.Linux.Ramen .....         | 220        |
| Net-Worm.Linux.Slapper.....        | 224        |
| Sonstige Würmer .....              | 226        |
| IRC-Worm.DOS.Septic .....          | 226        |
| Worm.FreeBSD.Scalper.....          | 229        |
| Worm.OSX.Inqtana .....             | 231        |
| Net-Worm.Perl.Santy .....          | 231        |
| P2P-Worm.Win32.Benjamin .....      | 232        |
| P2P-Worm.Win32.Mandragore .....    | 233        |
| Würmer für Smartphones .....       | 234        |
| Worm.SymbOS.Cabir.a .....          | 234        |
| Worm.SymbOS.Comwar.a.....          | 236        |
| Trojaner .....                     | 239        |
| Backdoor.Win32.BO.....             | 239        |
| Trojan-Spy.SymbOS.Pbstealer .....  | 241        |
| Trojan-SMS.J2ME.RedBrowser .....   | 242        |
| Trojan-Spy.Win32.Small.q .....     | 243        |
| <b>Quellennachweis .....</b>       | <b>245</b> |