Viruses Revealed

David Harley, Robert Slade, Urs Gattiker

Osborne/McGraw-Hill

New York Chicago San Francisco
Lisbon London Madrid Mexico City Milan
New Delhi San Juan Seoul Singapore Sydney Toronto

Table of Contents

Foreword. xxi

About the Authors. xxv

Acknowledgments. xxix

Introduction. xxxi

The Problem

Baseline Definitions. 3

Computer Virus Fact and Fantasy. 4

Definitions. 5

Viruses and Virus Mechanisms. 6

Virus Structure. 7

Damage. 7

Damage Versus Infection. 8

Stealth Mechanisms. 9

Polymorphism. 10

What Is This, a UNIX Textbook?. 10

DietofWorms. 12

Trojan Horses. 12

In the Wild. 13

Instant Guide to Anti-Virus Software. 15

Summary. 16

Historical Overview. 17

Virus Prehistory: Jurassic Park to Xerox PARC. 18

Wormholes. 19

CoreWars. 19

The Xerox Worm (Shoch/Hupp Segmented Worm). 20

Real Viruses: Early Days. 22

1981: Early Apple II Viruses. 22
1983: Elk Cloner. 23
1986:©BRAIN. 25
1987: Goodnight Vienna, Hello Lehigh. 26
1988: The Worm Turns. 27
The Internet Age. 30
1989: Worms, Dark Avenger, and AIDS. .30
1990: Polymorphs and Multipartites. 32
1991: Renaissance Virus, Tequila Sunrise. 33
1992: Revenge of the Turtle. 34
1993: Polymorphism Rules. 36
1994: Smoke Me a Kipper. 37
1995: Microsoft Office Macro Viruses. 38
1996: Macs, Macros, the Universe, and Everything. 39
1997: Hoaxes and Chain Letters. 40
1998: It's No Joke. 40
1999: Here Comes Your 19th Server Meltdown. 41
2000: Year of the VBScript Virus/Worm. .43
And So It Goes. 48
Summary. 49

3 Malware Defined. 51

What Computers Do. 52
Virus Functionality. 53
Application Functionality Versus Security. 53
In-the-Wild Versus Absolute Big Numbers. 54
What Do Anti-Virus Programs Actually Detect?. 57
Viruses. 58
Worms. 61
Intendeds. 62
Corruptions. 63
Germs. 64
Droppers. 64
Test Viruses. 65
Generators. 65
Trojans. 66
Password Stealers and Backdoors. 70
Jokes. 71

Remote-Access Tools (RATs). 74
DDoS Agents. 75
Rootkits. 77
False Alarms. 77
Summary. 79

Virus Activity and Operation. 81

How Do You Write a Virus?. 83
Tripartite Structure. 87
Infection Mechanism. 87
Trigger. 88
Payload. 88
Replication. 90
Non-Resident Viruses. 91
Memory-Resident Viruses. 91
Hybrid Viruses. 92
Generality, Extent, Persistence. 93
Payload Versus Reproduction. 94
Damage. 96
Impact of Viral Infection on the Computing Environment 96
Direct Damage from Virus and Trojan Payloads. 97
Psychological and Social Damage. 98
Secondary Damage. 98
Hardware Damage. 99
Ban the Bomb. 100
Logic Bombs. 100
Time Bombs. 101
ANSI Bombs. 101
Mail Bombs and Subscription Bombs. 102
Summary. 102

Virus Mechanisms. 103

Hardware-Specific Viruses. 104
Boot-Sector Infectors. 105
The Boot Zone. 109
File Infectors. 112
Prependers and Appenders. 114
Overwriting Viruses. 115

Misdirection. 117
Companion (Spawning) Viruses. 118
Multipartite Viruses. 119
Interpreted Viruses. 121
Macro Viruses. 121
Scripting Viruses. 122
Concealment Mechanisms. 123
Stealth. 126
Polymorphism. 129
Social Engineering and Malware. 132
Summary. 134

System Solutions

6 **Anti-Malware Technology Overview. 139**
Great Expectations. 140
How Do We Deal with Viruses and Related Threats?. 143
Pre-emptive Measures. 144
What Does Anti-Virus Software Do?. 151
Beyond the Desktop. 162
Outsourcing. 169
Summary. 170
7 **Malware Management. 171**
Defining Malware Management. 172
Proactive Management. 173
Reactive Management. 184
Cost of Ownership Versus Administration Costs. 186
Summary. 190
8 **Information Gathering. 193**
How Can I Check Whether Advice Is Genuine or Useful?. 194
Books. 196
The Good. 197
The Bad (or Mediocre, at Least). 198
The Really and Truly Ugly. 199
Related Topics. 200
General Security. 201

Legal. 204
Ethics. 205
Fiction. 206
Articles and Papers. 208
Online Resources. 216
Mailing Lists and Newsgroups. 217
Free Scanners. 218
Online Scanners. 218
Encyclopaedias. 219
Virus Hoaxes and False Alerts. 220
Evaluation and Reviews. 221
Anti-Virus Vendors. 222
General Resources. 223
Various Articles. 224
General Advice. 225
Specific Viruses and Vulnerabilities. .225
General Security References. 229

Product Evaluation and Testing. 237

Core Issues. 238
Cost. 239
Performance. 245
It's Not My Default. 251
Disinfection and Repair. 253
Compatibility Issues. 255
Functional Range. 256
Ease of Use. 261
Configurability. 262
Testability. 264
Support Functions. 264
Documentation. 267
Outsourced Services. 269
TestMatch. 269
Detection Versus Usability. 270
Other Ranks. 270
Upconversion. 271
It's All Happening in the Zoo. 273
We Like EICAR. 277

Further Information . . . 280
Summary . . . 281

10 **Risk and Incident Management . . . 283**

Risk Management . . . 285
The Best Form of Defence Is Preparation . . . 286
The Computer . . . 287
The Office . . . 288
Preventive Maintenance . . . 290
First, Do No Harm . . . 293
Reported Virus Incidents . . . 295
Help Desk Investigations . . . 295
Dealing with Virus Incidents . . . 297
Virus Identification . . . 299
General Protective Policies . . . 299
Summary . . . 300

11 **User Management . . . 301**

Managing the Managers . . . 303
Policies Count . . . 303
Security and Insurance . . . 304
Viruses and Insurance . . . 304
Risk/Impact Analysis . . . 305
Management Costs . . . 306
Policy Issues . . . 309
Help Desk Support . . . 311
Other IT Support Staff . . . 314
IT Security and Other Units . . . 314
Training and Education . . . 315
Positive Reinforcement . . . 319
Proactive Malware Management . . . 319
Safe Hex Guidelines . . . 320
Check All Alerts and Warnings with Your IT Department . . . 320
Don't Trust Attachments . . . 320
Take Care in Newsgroups and on the Web . . . 321
Don't Install Unauthorized Programs . . . 322
Be Cautious with Microsoft Office Documents . . . 322

Use and Ask for Safer File Formats. 323

Continue to Use Anti-Virus Software. 323

Keep Your Anti-Virus Software Updated. 323

Up to Date Doesn't Mean Invulnerable. 324

Super-users Aren't Super-human. 324

Disable Floppy Booting. 324

Write-Protect Diskettes. 324

Office Avoidance. 325

Reconsider Your Email and News Software. .325

Show All File Extensions in Windows Explorer. 326

Disable the Windows Script Host. 326

Introduce Generic Mail Screening. 326

Utilize Microsoft Security Resources. 326

Subscribe to Anti-Virus Vendor Lists. 327

Scan Everything. 327

Don't Rely on **Anti-Virus** Software. 327

Back Up, Back Up, Back Up. 328

Hoax Management. 329

Form Response. 329

A Quick Guide to Hoaxes. 330

Summary. 331

Case Studies: What Went Wrong, What Went Right, What Can We Learn?

12 Case Studies: The First Wave. 335

Brainwashing. 336

Who Wrotethe Brain Virus?. 337

Banks of the Ohio. 338

The MacMag Virus. 339

Give Peace a Chance. 340

TheWantonSeed. 342

Macros Mess with Your Mind. 343

Scores. 343

Lehigh. 346

CHRISTMA EXEC. 347

The Morris Worm (Internet Worm). 347
TheWANKWorm. 352
Jerusalem. 353
The "AIDS" Trojan. 355
Everybody Must Get Stoned. 356
Michelangelo, Monkey, and Other Stoned Variants. .357
Don't Monkey with the MBR. 362
Form. 364
The Modem Virus Hoax. 365
The Iraqi Printer Virus. 366
Summary. 370

13 **Case Studies: The Second Wave. 371**

The Black Baron. 373
Good Times Just Around the Corner. 374
Text Appeal. 375
Blowing in the Wind. 375
Loop de Loop. 375
Big Bang. 376
Proof of Concept. 377
Programs Versus Data. 378
The Name of the Game. 379
When Is a Payload Not a Payload?. 380
Auto Macros. 382
The Empire Strikes Back—Slowly. 383
WM/Nuclear. 384
Colors. 387
DMV. 388
Wiederoffnen and FormatC. 389
Diddling: Green Stripe and Wazzu. 389
WM/Atom. 390
WM/Cap. 391
Excel Viruses. 392
Variations on a Theme. 393
Word 97. 395
Thank You for Sharing. 395

Macro Virus Nomenclature. 396
Anti-Macro Techniques. 397
Hare. 399
Chernobyl (CIH.Spacefiller). 400
Esperanto. 401
Summary. 402

14 **Case Studies: Turning the Worm (the Third Wave). 403**

The AutoStart Worm. 404
W97M/Melissa (Mailissa). 406
Consider Her Ways. 406
Infection Versus Dispersal. 407
SansSouci. 408
The Commercial Virus. 409
I Used to Love Her (But It's All Over Now?). 409
W32/Happy99 (Ska), the Value-Added Virus. 410
PrettyPark. 411
Keeping to the Script. 412
VBS/Freelink. 413
I Wrote a Letter to My Love—VBS/LoveLetter. 414
VBS/NewLove-A. 417
Call 911!. 418
VBS/Stages. 419
BubbleBoy and KAKworm. 420
MTX (Matrix, Apology). 421
NakedWife. 425
W32/Navidad. 425
W32/Hybris. 427
VBS/VBSWGJ@mm (Anna Koumikova). 428
VBS/Staple.a@mm. 429
Linux Worms. 430
Ramen. 430
Linux/Lion. 431
Linux/Adore (Linux/Red). 431
Lindose (Winux). 432
W32/Magistr@mm. 432

- BadTrans . . . 434
- Summary . . . 435

IV **Social Aspects**

15 **Virus Origin and Distribution . . . 439**

- Who Writes This Stuff? . . . 441
- Social Engineering . . . 442
- Social Engineering Definitions . . . 444
  - Password Stealers . . . 448
  - This Time It's Personal . . . 449
- *Why* Do They Write This Stuff? . . . 450
- Secondary Distribution . . . 455
- Does Education Work? . . . 456
- Global Education . . . 458
- Summary . . . 459

16 **Metaviruses, Hoaxes, and Related Nuisances . . . 461**

- Chain Letters . . . 463
- Hoaxes . . . 465
- Urban Legends . . . 465
- Chain Letters and Hoaxes . . . 466
- Hoaxes and Virus Alerts . . . 466
- Misinformation under the Microscope . . . 468
  - BIOS, CMOS, and Battery . . . 468
  - The JPEG Hoax . . . 469
  - The Budget Virus . . . 470
  - Rude Awakening . . . 471
  - Wheafand Chaff . . . 471
  - Hoax Identification Heuristics . . . 472
- Spam, Spam, Spam (Part 2) . . . 481
  - Motivations . . . 482
  - Common Themes . . . 484
- Spamology and Virology . . . 484
- Metaviruses and User Management . . . 486
  - What Should I Tell My Customers? . . . 487
  - Handling Spam, Chain Letters, and Hoax Alerts . . . 488

Summary. 490

17 **Legal and Quasilegal Imperatives. 491**

Malware and the Law. 492

Grounds for Criminal Proceedings. 493

The Computer Misuse Act 495

Some Broad Concepts. 496

Data Protection Legislation. 497

Data Protection Principles. 498

BS7799 and Virus Controls. 500

ISO 9000. 505

Security Architecture. 505

Who Is Responsible for Security in a Given Context?. 509

What Systems Are Protected?. 509

What Are the Details of Implementation and Configuration?. 510

Policy Outlines. 511

Acceptable Use of Facilities and Resources. 512

Acceptable Use of Email. 512

Anti-Chain Mail Policy. 515

Anti-Spam Policy. 515

Acceptable Use of the World Wide Web and USENET. 516

Anti-Virus Policy. 516

Summary. 518

18 **Responsibility, Morality, and Ethics. 519**

The Two-Minute Guide to Ethics. 520

Demographics. 523

Age. 523

Gender. 525

Cultural and National Norms. 526

National Issues. 527

Motivational Factors. 530

Cross-National Differences. 531

Familiarity and Ethics. 532

End Users and Responsibility. 533

Is Anti-Virus a Profession?. 535

Vendors and Ethics. 536

Commercial Ethics. 538
Do No Harm. 539
Developing Codes of Conduct 540
A Minimum Code of Conduct 540
EICAR. 541
Article 1: **The** Public Interest 542
Article 2: Legal Compliance. 542
Article 3: Duty to Employers, Clients, and Colleagues. 543
Article 4: Duty to the Profession. 543
Article 5: Specialist Competence. 543
Do Codes of Conduct Make a Difference?. 544
Summary. 547

19 Wrap Up. 551

Predictions. 552
Closing Comments. 553
Bad News: Security Specialists Don't Know Much—About Viruses. 553
Good News: A Little Education and Basic Policies Can Really Help. 554
Bad News: Convergence Is Going to Get Worse. 555
Good News: Just the Same, but More. 555
Bad News: Multiple Points of Attack Can Scale the Problem. 556
Good News: Existing Tools and Some Diligence Can Work. 557
Stop Press. 557
RTF Is Not a Panacea. 558
Poly/Noped. 559
Mandragore. 559
SULFNBK Hoax. 560
Sadmind. 561
Cheese. 561
Lindose/Winux. 561
MacSimpsons. 562
Outlook View Control. 562
Code Red/Bady. 562
Sircam. 563
Summary. 564

V Appendixes

A Frequently Asked Questions on VIRUS-L/comp.virus. 567

Primary Contributors. 568

What are the known viruses?. 568

Where can I get more information on viruses and related topics?. 569

What are computer viruses?. 570

Whatisaworm?. 572

What is a Trojan horse?. 572

What are the indications of a virus infection?. 573

What steps should be taken in diagnosing and identifying viruses?. 574

What is the best way to remove a virus?. 574

What are "false positives" and "false negatives"?. .576

Could an anti-virus program itself be infected?. 577

Where can I get a virus scanner for my UNIX system?. 578

Why does my scanner report an infection only sometimes?. 579

I think I have detected a new virus; what do I do?. 579

CHKDSK reports 639KB (or less) total memory on my DOS system; am I infected?. 580

I have an infinite loop of subdirectories on my hard drive; am I infected?. 581

Can a PC not running DOS be infected with a common DOS virus?. 581

My hard disk's file system has been garbled; do I have a virus?. 582

Is it possible to protect a computer system with only software?. 582

Is it possible to write-protect the hard disk with software only?. 583

What can be done with hardware protection?. 583

Does setting a file's attributes to read-only protect it from viruses?. 584

Do password/access control systems protect my files from viruses?. 584

Do the protection systems in DR DOS work against viruses?. 585

Does a write-protect tab on a floppy disk stop viruses?. 586

Do local area networks (LANs) help to stop viruses, or do they facilitate their spread? 586

What is the proper way to make backups?. 587

Can boot-sector viruses infect nonbootable DOS floppy disks?. 589

Can a virus hide in a PC's CMOS memory?. 590

Can a PC virus hide in Extended or in Expanded RAM in a PC?. 591

Can a virus hide in a PC's Upper Memory or in High Memory Area?. 591

Can a virus infect data files?. 591

Can viruses spread from one type of computer to another?. 592
Are mainframe computers susceptible to computer viruses?. 592
Some people say that disinfecting is a bad idea. Is that true?. 594
Can I avoid viruses by avoiding shareware, free software, or games?. 595
Can I contract a virus on my PC by performing a DIR of an infected floppy disk?. 596
Is there any risk in copying data files from an infected floppy disk to a clean PC's hard disk?. 597
Can a DOS virus survive and spread on an OS/2 system using the HPFS file system?. 597
Under OS/2 2.0+, could a virus-infected DOS session infect another DOS session?. 597
Can normal DOS viruses work under MS Windows?. 598
Can I get a virus from reading email?. 598
Can a virus "hide" in a.GIF or JPEG file?. 599
How often should we upgrade our anti-virus tools?. 600
Is it possible to use a computer virus for something useful?. 600
Wouldn't adding self-checking code to your programs be a good idea?. 601
Is my disk infected with the Stoned virus?. 602
I was infected by both Stoned and Michelangelo. Why has my computer become unbootable?. 603
I was infected with Flip, and now a large part of my hard disk seems to have disappeared. What has happened?. 604
What does the GenB and/or the GenP virus do?. 604
How do I "boot from a clean floppy"?. 604
My PC diagnostic utility lists "Cascade" among the hardware interrupts (IRQs). Does this mean I have the Cascade virus?. 606
When I do a DIR I MORE, I see two files with random names that are not there when I just use DIR. On my friend's system, they cannot be seen. Do I have a virus?. . . . .'. 606

Viruses and the Macintosh. 609

How Many Viruses Affect the Macintosh?. 610
Mac-Specific Viruses. 610
Mac-Specific System and File Infectors. 611
HyperCard Infectors. 614
Mac Trojan Horses. 615
Macro Viruses, Trojans, and Variants. 616
PC Viruses on Emulated PCs. 617
Esperanto.4733. 618
PC Scripting Viruses. 618
Welcome Datacomp. 618

The EICAR Installation Test File. 618
Information Resources. 619
Mac-Related Newsgroups. 619
Books. 619
WebSites. 620
Virus Bulletin. 621
Macro Virus Information Resources. 622
Other Virus Resources. 622
Mac Troubleshooting. 623
Questions Received at Mac Virus. 624

Social Engineering. 629

ITSecurity. 630
What the Intruder Wants to Know. 631
People Hacking. 632
Shouldersurfing. 632
Eavesdropping/Surveillance. 633
Inappropriate Access. 633
Being Sociable. 633
Phone Phonies. 633
Dumpster Diving. 634
Electronic Leftovers. 634
Targeting the Help Desk. 634
Attacks on the Help Desk. 635
Do I Need to Disclose My Password?. 635
Wouldn't I Notice Unwarranted Interest in Security Issues?. 635
How Big Is the Risk?. 636
What Are the Solutions?. 636
Good Password Practice. 638
Why Do Password Practices Matter?. 638
Passwords: Good Systems Enforcement Practice. 638
Best Practice. 639
Where Do I Get Further Information?. 640

Glossary. 641

Index. 667