

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP



AVIEN Malware Defense Guide

for the Enterprise

Stop the Stalkers on Your Desktop

- Complete Coverage of the Relationship Between Enterprise Security Professionals, Customers, Vendors, and Researchers
- In-depth Consideration of Key Areas of the 21st Century Threat Landscape
- Systems Security and DIY Defense Using a Range of Specialist Detection and Forensic Techniques and Tools

David Harley CISSP, Antivirus Researcher, former manager of the
Threat Assessment Centre for the U.K.'s National
Health Service

Ken Bechtel
Michael Blanchard
Henk K. Diemer

Andrew Lee
Igor Muttik
Bojan Zdrnja

FOREWORD BY
ROBERT S. VIBERT
AVIEN ADMINISTRATOR

Visit us at

www.syngress.com

Syngress is committed to publishing high-quality books for IT Professionals and delivering those books in media and formats that fit the demands of our customers. We are also committed to extending the utility of the book you purchase via additional materials available from our Web site.

SOLUTIONS WEB SITE

To register your book, visit www.syngress.com/solutions. Once registered, you can access our solutions@syngress.com Web pages. There you may find an assortment of value-added features such as free e-books related to the topic of this book, URLs of related Web sites, FAQs from the book, corrections, and any updates from the author(s).

ULTIMATE CDs

Our Ultimate CD product line offers our readers budget-conscious compilations of some of our best-selling backlist titles in Adobe PDF form. These CDs are the perfect way to extend your reference library on key topics pertaining to your area of expertise, including Cisco Engineering, Microsoft Windows System Administration, CyberCrime Investigation, Open Source Security, and Firewall Configuration, to name a few.

DOWNLOADABLE E-BOOKS

For readers who can't wait for hard copy, we offer most of our titles in downloadable Adobe PDF form. These e-books are often available weeks before hard copies, and are priced affordably.

SYNGRESS OUTLET

Our outlet store at syngress.com features overstocked, out-of-print, or slightly hurt books at significant savings.

SITE LICENSING

Syngress has a well-established program for site licensing our e-books onto servers in corporations, educational institutions, and large organizations. Contact us at sales@syngress.com for more information.

CUSTOM PUBLISHING

Many organizations welcome the ability to combine parts of multiple Syngress books, as well as their own content, into a single volume for their own internal use. Contact us at sales@syngress.com for more information.

SYNGRESS®

This page intentionally left blank

AVIEN Malware Defense Guide for the Enterprise

David Harley, CISSP,

Antivirus Researcher, former manager of the Threat Assessment
Centre for the U.K.'s National Health Service

Foreword by **Robert S. Vibert,** AVIEN Administrator

Ken Bechtel

Michael Blanchard

Henk Diemer

Andrew Lee

Igor Muttik

Bojan Zdrnja

Elsevier, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively “Makers”) of this book (“the Work”) do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media[®], Syngress[®], “Career Advancement Through Skill Enhancement[®],” “Ask the Author UPDATE[®],” and “Hack Proofing[®],” are registered trademarks of Elsevier, Inc. “Syngress: The Definition of a Serious Security Library[™],” “Mission Critical[™],” and “The Only Way to Stop a Hacker is to Think Like One[™]” are trademarks of Elsevier, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	SERIAL NUMBER
001	HJIRTCV764
002	PO9873D5FG
003	829KM8NJH2
004	BAL923457U
005	CVPLQ6WQ23
006	VBP965T5T5
007	HJJJ863WD3E
008	2987GVTWMK
009	629MP5SDJT
010	IMWQ295T6T

PUBLISHED BY

Syngress Publishing, Inc.
Elsevier, Inc.
30 Corporate Drive
Burlington, MA 01803

AVIEN Malware Defense Guide for the Enterprise

Copyright © 2007 by Elsevier, Inc. All rights reserved. Printed in the United States of America.

Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America

1 2 3 4 5 6 7 8 9 0

ISBN 13: 978-1-59749-164-8

Publisher: Amorette Pedersen
Technical Editor: David Harley
Cover Designer: Michael Kavish

Copy Editor: Judith Eby
Indexer: Rich Carlson

For information on rights, translations, and bulk sales, contact Matt Pedersen, Commercial Sales Director and Rights, at Syngress Publishing; email m.pedersen@elsevier.com.



Lead Author and Technical Editor

David Harley CISSP (Lead Author, Technical Editor) has written or contributed to over a dozen books in the security and education fields, including “Viruses Revealed” (Osborne). He is a frequent presenter at security conferences and has many research papers to his credit, as well as consumer-level articles in many areas of computing. He runs the Small Blue-Green World security and publishing consultancy, and his roles there include authoring, reviewing and editing, antimalware and security research, and providing consultancy to the antivirus industry. He is also qualified in security audit (BS7799 Lead Auditor) and ITIL Service Management. For five years he ran the Threat Assessment Centre for the UK’s National Health Service, specializing in malware and email abuse management consultancy. He previously worked in systems, application and network support for a major cancer research charity.

David’s academic roots are in Computer Science, Social Sciences and Medical Informatics. His further qualifications include BS7799 Lead Auditor, ITIL Service Management, and Medical Informatics. His affiliations include the Red Team at QuantumLabs, a system testing and validation service, Team Anti-Virus, and the WildList Organization. He is a charter member of AVIEN and AVIEWS, serving as Disciplinary Committee Chairman, Adjunct Administrator of AVIEN, and from mid-2007 will serve as Transitional Administrator and CDO during the restructuring of AVIEN.

David would like to thank all his co-authors, not only for the excellent content they contributed but for their support, suggestions and encouragement. Many other members of AVIEN and AVIEWS also contributed input in the early stages of the book planning (about forty people were subscribed to the book’s dedicated mailing list, over time), and they also deserve thanks. In particular:

- His wife Jude, who not only contributed content and late-night discussion, but put up with the ongoing hormonal changes and mood swings of an expectant author with patience and good humor.
- Andrew Lee and Robert Vibert for their unfailing support during some very rocky moments. Extra brownie points go to Andrew for his timely assistance in proofreading.
- The AVIEN Advisory Board and Disciplinary Committee and their individual members for their support and advice at times of extreme stress.

- Paul Dickens, whose cartoons grace the book's web site at www.smallblue-greenworld.co.uk/pages/avienguide.html.
- Mary Landesman for discussion on chapter planning.
- Jeannette Jarvis, who first suggested the idea of an AVIEN book to him.

He also owes special thanks to Amorette Pedersen and Andrew Williams of Syngress/Elsevier for their unfailing patience and support, even during the occasional prima donna outburst from the technical editor. ☺

There is forensic evidence of David's sticky fingers all over this book, but particularly Chapters 1, 2, 4, 6, 8, 10 and 11.



Foreword Author

Robert S. Vibert is the administrator and CDO of the Anti-Virus Information Exchange Network (AVIEN), the growing network of Security Professionals working in organizations with 1500 or more PCs who discuss Anti-Virus topics and keep each other informed about upcoming malware threats. He also acts as senior advisor to the administrator of AVIEWS (Anti-Virus Information & Early Warning System), AVIEN's sister organization, which brings together security specialists and researchers at both vendor and customer organizations. Robert has worked for more than 25 years as a consultant, mentoring and helping companies and individuals get the most out of their resources.

Author of five books and more than 200 articles on management, computer security and operations, Robert has also worked as a senior consultant for a major international consulting firm, is regularly interviewed by the media for his expert insights on computer security, and serves as an adviser to Canadian government departments. Currently, he acts as a mentor to several entrepreneurs and is developing the *Missing Link* series of books, workbooks, CDs and DVDs to provide practical information and processes to get the success you want in life in the areas of finance, relationships, emotional health, career and personal development.

As well as contributing the foreword on behalf of AVIEN, Robert also co-wrote Chapter 1.



Contributors

Paul Baccas is a researcher at Sophos plc, the UK security company. After reading Engineering Science at Exeter College, Oxford, he worked in various technical roles at Sophos, and is now mainly engaged in spam research. He is a frequent contributor to Virus Bulletin.

Paul assisted with technical editing on a number of chapters.

Ken Bechtel has been involved in corporate malware defense since 1988. His work history includes working in the Virus Lab at NCSA (later ICSA), performing virus analysis and Antivirus Product Certifications, as well as user education. He has worked and consulted for all levels of business, from small businesses to Fortune 500 companies. He is the author of several papers published by Security Focus, Virus Bulletin, and several other trade magazines. He has appeared 26 times on local and national news for interviews concerning various malicious code threats. Ken is a Founding Member and Adjunct Administrator of the Anti-Virus Information Exchange Network (AVIEN), member of Association Anti-Virus Asian Researchers (AAVAR), WildList Reporter since 1998, Founder of Team Anti-Virus, and member of several unofficial associations. Several of his papers and articles have been printed in Security Focus, Virus Bulletin, and several other trade magazines. His biggest literary contribution so far has been the “Handbook of Corporate Malware Protection.”

Ken is devoted to his family, and enjoys all manner of outdoor sports, from fishing and camping to several shooting sports.

Ken co-wrote Chapters 1, 2 and 6.

Michael P. Blanchard, CISSP, GCIH (gold), CCSA-NGX and MCSE, has been an IT professional for over 16 years, and is currently a member of AVIEN. His current major duties include Malware analysis/protection and assessment, vulnerability analysis and assessment, and other daily activities. Apart from some in-house training documents, Mike is also the author of the definitive whitepaper on the FunLove virus

that he wrote to achieve his SANS GCIH gold certification (#350) in 2002, at www.giac.org/certified_professionals/practicals/GCIH/0350.php. Mike takes pride in his current professional role serving in the CIO's Office of Information Security and Risk Management as the Senior Antivirus Security Engineer overseeing the malware protection on a global scale at EMC² Corporation in Westborough, Mass, a role that he's had since 1999.

Before that, it was Mike's father who introduced him to the wonders of computers and building electronic devices back in the mid to late 1970's and up to programming in Fortran and Pascal in the mid 1980's on his father's Atari 800 and his High School's PDP-11. To this day, Mike says that he learned everything he knows from his Dad, and is happy to still be learning from him now that Mike is a Dad with his own two children.

In his spare time, Mike can be seen wandering around Renaissance faires, making Chainmaille armor and jewelry, spending time with his family, performing CubMaster duties for his local CubScout pack, or leveling up with friends in the computer MMORPG Everquest 2. Mike would like to thank his parents and his wife and two children for bearing with him and being very supportive while he locked himself in his computer room with his headphones on for months to complete his contribution to this project. Mike wishes to dedicate his contribution to his loving wife and children, and his late best friend Jim: he would have been proud.

Mike co-wrote Chapter 9.

Tony Bradley (CISSP-ISSAP) is the author of Essential Computer Security, co-author of *Hacker's Challenge 3*, and has contributed chapters to many other books. Tony is the Guide for the Internet/Network Security site on About.com, a part of the New York Times Company, where he has more than 30,000 subscribers to his weekly newsletter. He has written for a variety of other Web sites and publications, including PC World, SearchSecurity.com, WindowsNetworking.com, Smart Computing Magazine and Information Security Magazine. Currently a Security Consultant with BT INS, Tony has driven security policies and technologies for endpoint security and incident response for Fortune 500 companies for over 6 years. Tony is a CISSP (Certified Information Systems Security Professional) and ISSAP (Information Systems Security Architecture Professional). He is Microsoft Certified as an MCSE (Microsoft Certified

Systems Engineer) and MCSA (Microsoft Certified Systems Administrator) in Windows 2000, and he is recognized by Microsoft as an MVP (Most Valuable Professional) in Windows security.

Other books to which Tony has contributed include *Winternals: Defragmentation, Recovery, and Administration Field Guide*, *Combating Spyware in the Enterprise*, *Emerging Threat Analysis*, and *Botnets: The Killer Web App*. He is the lead technical editor and contributing author to the upcoming *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance*.

Tony co-wrote Chapter 4.

Henk K. Diemer (CISSP, MSC in Bio Physics) lives in Utrecht, in the Netherlands, with his wife Ieneke and three school age children. He brought to this book his experience as an independent AV management specialist with over 28 years – mostly – international ICT management experience in both the private and public sectors. Using computers and programming for his research since 1972, he has dedicated himself since 1996 to limiting the losses related to malicious code. Henk currently works for a large global Fortune 500 IT services company, as a senior IT security advisory specialist. Before that, he worked for a large Dutch multinational bank for 20 years, until IT there was largely outsourced in 2005.

Henk initiated, among other things, a workgroup for Dutch AV experts under the authority of the FI –ISAC NL and Dutch Banker Association, for sharing lessons learned and to help manage high profile malware incidents in banking. Today, his focus is primarily on improving local, regional and global services in the context of outsourced IT AV services, and to assist security management functions in creating and maintaining optimal conditions for success in outsourcing AV services.

Henk has had the pleasure of working with many other independent and dedicated AV specialists in AVIEN, Virus Bulletin and the Anti-Phishing Working Group, and many others committed to the sharing of best practices or lessons learned. He wishes to express his warm gratitude to all who made his contribution to this book possible.

Henk wrote most of Chapter 7.

Ken Dunham is Director of the Rapid Response Team at iDefense, a VeriSign company, overseeing all Rapid Response and global cyber-threat operations. He frequently briefs upper levels of federal cyber security authorities on emerging threats, and regularly interfaces with vulnerability and geopolitical experts to assemble comprehensive malicious code intelligence and to inform the media of significant cyber-threats. Ken is regularly rated as a top speaker at events including the Forrester Security Summit, GFIRST, ISSA, Pentagon and others. He regularly discovers new malicious code, has written anti-virus software for Macintosh, and has written about malicious code for About.com, SecurityPortal, AtomicTangerine and Ubizen. He is a member of AVIEWS, InfraGard, an RCG Information Security Think Tank, CME, International High Tech Crime Investigation Association, the WildList Organization and others. He is also a certified reverse engineer and regularly analyzes top threats of concern for top tier clients.

Ken authored Bigelow's Virus Troubleshooting Pocket Reference, "The HyperCard Roundup" (on HyperText programming), and is a regular columnist for two information security magazines. He is also the founder and President of the Boise, Idaho, Information Systems Security Association chapter. He is also the founder and President of the Idaho InfraGard chapter, in conjunction with the FBI. He holds several security certifications, serves as the VeriSign Forum for Incident Response and Security Teams (FIRST) lead representative, and is a member of the North American Incident Response Team (NAIRT).

Ken co-wrote Chapter 5.

Enrique González is a Senior Virus Researcher at Microsoft Corporation. Before joining Microsoft, Enrique was a Senior Security Researcher with Websense where he lead Websense Security Labs' EMEA team, being also spokesperson for the Lab in the EMEA region. Enrique's background includes positions at Panda Software where he analyzed and researched malware from old DOS viruses to the latest threats. He is a frequent presenter at conferences and events such as APWG, AVAR, CISCI, and so on. His presenting work includes malware cases and technologies, research on future attack vectors such as VoIP, as well as current and upcoming threats. Enrique also co-founded a security systems company in Spain. Enrique's

contribution to the book would have not been possible without his parents' hard work and support of his education. His wife and his children have also played a key role, supporting him and bringing him the joy he needs to keep working hard for them.

Enrique co-wrote Chapter 5.

Judith Harley teaches ICT and business communications at a secondary school in the UK. Even before qualifying as a teacher, she was a qualified adult training instructor and assessor, and also worked in user support and systems and security administration in the public sector. She has many years of experience in writing training manuals, policies, FAQs and other documentation, and has published articles in educational periodicals. She was co-author, with David Harley and Eddy Willems, of "Teach your children well" for the 2005 Virus Bulletin International Conference, and also co-wrote two chapters for "Coming of Age – an introduction to the new world wide web", 2nd Edition (Freedman).

Judith co-wrote Chapter 8.

Andrew Lee (CISSP) is Chief Research Officer of ESET LLC. He was a founding member of the Anti-Virus Information Exchange Network (AVIEN) and its sister group AVIEWS (AVIEN Information & Early Warning System), is a member of AVAR and a reporter for the WildList organisation. He was previously at the sharp end of malware defense as a systems administrator in a large government organisation.

Andrew is author of numerous articles on malware issues, and is a frequent speaker at conferences and events including ISC2 Seminars, AVAR, Virus Bulletin and EICAR. When he is not sitting at the computer or in an airport somewhere, he enjoys reading, photography, playing guitar, and the martial art of Ki-Aikido.

Andrew co-wrote Chapters 10 and 11.

Jim Melnick is Director of Threat Intelligence at iDefense, leading the global threat intelligence group that focuses on cyber threats around the world, from nation states and hacker groups to new technologies. His "Weekly Threat Report" on cyber threats, which he founded and

edits for iDefense/VeriSign, was dubbed by Business Week in 2005 as including “some of the most incisive analysis in the business.” Prior to joining iDefense, Jim served with distinction as a civilian analyst for more than 16 years in the U.S. Army and the Defense Intelligence Agency in a variety of roles, including intelligence, psychological operations, international warning issues, information operations and Russian affairs.

Jim has been published in numerous military and foreign affairs journals, and has received numerous military and related awards, including a Presidential Commission medal for his work on the Y2K problem in support of the National Intelligence Council. He also recently retired from the U.S. Army Reserves as a Colonel in Military Intelligence. His last military assignment was with the Office of the Assistant Secretary of Defense for Networks and Information Integration. Jim has a Master of Arts in National Security and Strategic Studies from the U.S. Naval War College, a Master of Arts in Russian studies from Harvard University, and a Bachelor of Arts with Honors in Political Science from Westminster College.

Jim co-wrote Chapter 5.

Igor Muttik, PhD is a senior architect with McAfee Avert™. He started researching computer malware in 1980s when anti-virus industry was in its infancy. He is based in the UK and worked as a virus researcher for Dr. Solomon’s Software where he later headed the anti-virus research team. Since 1998 he has run Avert Research in EMEA and switched to his architectural role in 2002. Igor is a key contributor to the core security technology at McAfee. He takes particular interest in new emerging malware techniques, and in the design of security software and hardware appliances. Igor holds a PhD degree in physics and mathematics from Moscow University. He is a regular speaker at major international security conferences and a member of the Computer Antivirus Research Organization.

Igor wrote Chapter 3.

David Phillips has been working at The Open University (OU) since 1986, transferring into computer support full time in mid-1996. He has spent over 14 years in the antivirus field, involved in the implementation and support of staff and students at the OU. A speaker at the 1998, 1999,

2001 and 2003 Virus Bulletin conferences, he has also presented for SecureIT Europe and others including workshops at NetFocus2006. In 2003 he created a short course at the OU, T187 Vandalism in Cyberspace aimed at educating the home users in malware and malware protection issues which is currently being presented two times a year, until 2009.

David co-wrote Chapter 8.

Paul Schmehl is Senior Information Security Analyst at the University of Texas at Dallas, and has many years of experience in antimalware administration. A number of his articles have been published by SecurityFocus and Claymania, on such topics as AV software evaluation, firewall and AV product reviews, and protection for the enterprise and for small businesses. He is a frequent contributor to security lists, and a founder member of AVIEN. His presentation on “Barbarians at the Gateways: Defeating Viruses in EDU” has been featured at SIGUCCS and EDUTEX.

Paul co-wrote Chapter 6.

James M. Wolfe, CHS-V is the Technical Director of the European Institute for Computer Anti-Virus Research (EICAR). His other memberships include AVIEN, Team Anti-Virus, the US-CERT CME project, and he is a reporter for the WildList Organization. He is an Associate Member of the prestigious Computer Anti-Virus Research Organization (CARO). He is also an Adjunct Professor at the University of Central Florida and Webster University, teaching Information Security, Ethics, Counter-Terrorism and Homeland Security. He has a Bachelor of Science degree in Management Information Systems and a Master of Science degree in Change Management from the University of Florida. He holds a Level 5 Certification in Homeland Security from the American College of Forensic Examiners Institute. Currently, he is working on a Bachelor's degree in Anthropology. He plans to begin his Doctorate soon.

He has published articles in the Virus Bulletin and EICAR magazines. He co-authored a chapter in the 2003–2005 editions of the Handbook of Information Security Management by Micki Krause and Hal Tipton. He is a five-time honoree in “Who's Who in America.” He routinely presents at conferences all over the world, usually in the Anti-Virus, Terrorism, and Security arena.

James would like to dedicate his contribution to Krista and Cymoril, who never waver in their support even when the trolls are attacking at 3am, and to Mom for giving her wisdom and strength.

James co-wrote chapter 1.

Bojan Zdrnja (GCIA, CISSP, RHCE) is Security Implementation Specialist at the University of Auckland, New Zealand. He previously worked as a security consultant and security team leader at the Faculty of Electrical Engineering and Computing, University of Zagreb, as part of a commercial team working on external projects. He was also a member of several Incident Response Teams for the Croatian CERT. He is a handler for the Internet Storm Center (ISC) and is also on the SANS Advisory Board and one of the GIAC Gold Advisors. Specialized areas of interest include analyzing malware, forensic analysis, incident handling. His publications include a security column for a Croatian computer magazine, the book *What Are Computer Viruses?* (Syspring), and diaries for the Internet Storm Center.

Bojan co-wrote Chapter 9.

Contents

Forewordxxvii
Prefacexxix
Introductionxxxiii
Chapter 1 Customer Power and AV Wannabes	1
Introduction	2
History of AVIEN and AVIEWS	2
Background: So Who Is Robert Vibert?	2
AV Vendor/Researcher Lists and Groups	3
VB 2000: A Star is Born	4
Cocktails For Two — and More	5
After the Hangover	5
One Day at a Time	5
Oh No, The Users Are Ganging Up On Us!!!	6
The Objectives of AVIEN and AVIEWS	7
AVIEN Membership Benefits	7
Alerts and Advisories	7
Peer Discussions	8
AVIEN Projects	8
Anti-virus Vendor Image	9
AVIEN & AVIEWS: Independents and Vendors in Anti-Malware Research	9
Favorite Myths	12
“Anti-virus Only Catches Known Viruses”	13
“Vendors Protect Their Own Revenue Stream, Not Their Customers”	16
“Vendors Only Know About and Detect Viruses”	17
“They Write All the Viruses”	18
“Anti-virus Should Be a Free Service: After All, There Are Free Services That Do a Better Job”	18
AV Wannabe	19
So You Want to Be a <i>Bona Fide</i> Computer Anti-Malware Researcher?	19
In the Beginning... ..	20
Anti-virus Company Analysts	21

Independent Researchers	21
Technical and Psychological Analysts	21
Corporate Anti-virus Specialist	22
What is a Researcher?	22
Researcher Skill-Set	23
What Makes a Researcher?	23
In The End	24
You Should Be Certified	25
(ISC) ²	25
SSCP	27
CISSP	28
CISSP Concentrations	28
SANS GIAC/GSM Certifications	30
Other Certifications and Qualifications	33
Vendor-Dependent Training	34
McAfee	34
Sophos	35
Symantec	37
Should There Be a Vendor-independent	
Malware Specialist Certification?	38
Levels of Certification and Associated Knowledge Bases	39
Certified Anti-Virus Administrator (CAVA)	39
Certified Anti-virus Specialist (CAVS)	39
Certified Enterprise Anti-virus Architect (CEAVA)	40
Updating the Certifications	42
Summary	43
Solutions Fast Track	44
Frequently Asked Questions	47
Chapter 2 Stalkers on Your Desktop	51
Introduction	52
Malware Nomenclature	53
21st Century Paranoid Man	56
In The Beginning	56
The Current Threatscape	58
The Rise of Troy	59
Rootkits	60
Kernel Mode and User Mode	62
Persistency and Non-Persistency	62
Rootkit Detection	63

Words Can Hurt You64
Spam, Spam, Spam64
Fraudian Slips66
Advance Fee Fraud (419s)66
Phishing Scams67
Or Would You Rather Be a Mule?70
Pump and Dump Scams74
Hoaxes and Chain Letters76
Why Do People Pass Hoaxes and Chain Letters On?77
Summary78
Solutions Fast Track78
Frequently Asked Questions81
Chapter 3 A Tangled Web85
Introduction86
Attacks on the Web86
Hacking into Web Sites88
Index Hijacking90
DNS Poisoning (Pharming)95
Malware and the Web: What, Where, and How to Scan100
What to Scan100
Where to Scan104
How to Scan105
Parsing and Emulating HTML107
Browser Vulnerabilities110
Testing HTTP-scanning Solutions112
Tangled Legal Web113
Summary115
Solutions Fast Track115
Frequently Asked Questions120
Chapter 4 Big Bad Botnets123
Introduction124
Bot Taxonomy127
How Botnets are Used135
DoS and DDoS ATTACKS136
SYNs and Sensibility137
UDP Flooding138
ICMP Attacks139
DNS Reflector Attacks141

Managing DoS and DDoS Attacks	142
The Botnet as Spam Tool	142
Click Fraud	143
Click Fraud Detection	144
Bot Families	144
The Early Bot Catches the Worm	146
Pretty Park	146
SubSeven	147
GT Bot	147
TFN, Trinoo, and Stacheldraht	147
SDBot	150
Infection and Propagation	150
Rbot	152
Infection and Propagation	153
Known Vulnerability Exploits	155
Exploiting Malware Backdoors	156
Terminated Processes	157
Agobot (Gaobot) and Phatbot	158
Infection and Propagation	158
Terminated Processes	161
Spybot	162
Keystroke Logging and Data Capture	165
Mytob	165
Bot/Botnet Detection and Eradication	167
Summary	171
Solutions Fast Track	171
Frequently Asked Questions	176
Chapter 5 Crème de la Cybercrime	181
Introduction	182
Old School Virus Writing	182
Generic Virus Writers	183
The Black Economy	187
Spam	188
A Word about Dialers	191
Botnets for Fun and for Profit	192
“Wicked Rose” and the NCPH Hacking Group	193
Introduction to NCPH	193
Public Knowledge of a Zero-day Word Exploit	193

The GinWui Backdoor Rootkit Payload	194
June 21, 2006–2007 – Continued US Targeted Attacks	195
Backtracking Targeted Attacks: RipGof	196
Timeline of Events	197
Introduction to Wicked Rose and NCPH	198
How Did NCPH Begin?	200
WZT	203
The Jiangsu Connection?	203
The China Syndrome	203
Lurkers in Your Crystal Ball	205
Things That Will Not Change (Much)	205
Social Engineering	205
Back in Fashion	207
Botnets	208
The Shape of Things to Come	208
Communication: A Common Problem	208
Automobiles	210
VoIP	211
RSS	212
Podcast	212
Home Media Systems	213
Cell Phones	214
Credit Cards	216
Operating Systems	217
Summary	218
Solutions Fast Track	218
Frequently Asked Questions	221
Chapter 6 Defense-in-depth	225
Introduction	226
Enterprise Defense-in-Depth	227
Getting to Know Your Network	229
Choosing Your Network-Knowledge Tools	229
Designing An Effective Protection Strategy	231
Secure Individual Hosts First	231
Purchase Host-based Protective Software	232
Carefully Examine All Points of Access to Hosts	233
Malware Detection	234
Intrusion Detection	234
SNORT	236

Virus Detection	240
Generic Anti-virus	241
Planning, Testing, Revising	243
Develop Contingency Plans	244
Perform an “After Action Review”	244
Designate a Conference Room or Office as a “War Room”	245
Personnel	246
Look Beyond the Borders	247
Documentation	248
Malware Laboratory Procedures	249
Summary	252
Solutions Fast Track	252
Frequently Asked Questions	254
Chapter 7 Perilous Outsorcery	257
Introduction	258
Key Concepts: Outsourcing AV Services and Risk Management	260
Key Building Blocks for Managing Outsourced Security	261
What Do “Security Activities” Imply for a Business Manager?	262
What does “Outsourcing AV Services” Mean?	263
What Drives the Success or Failure of Outsourced Operational AV?	265
First Law	266
Second Law	266
Third Law	266
Fourth Law	266
Fifth Law	267
Sixth Law	269
Seventh Law	270
What Common Phases does the Project Manager Encounter when Outsourcing AV Services?	270
What Are The Most Common Problems Seen During AV Outsourcing?	272
Miscommunication Between Customer and Vendor	272
Lack of Responsive and Flexible Threat/ Change Management Mechanisms	274
Procurement and Tendering Conflicts	274
A Vendor-Centric Worldview	275
Overestimation of a Vendor’s Competence	275

The Perils of Outsourcing AV Activities	276
Why Do More and More Companies Outsource AV Services?	277
The ‘Perilous Outsorcery’ Management Matrix	280
The First Dimension: Use The Job Descriptions, Roles, and Functions of People You Meet	280
The Second Dimension: AV Function Types from Risk and Systems Management Perspectives	281
The Third Dimension: Type of Governance Role Using The RACI Model	282
An Example of the “Perils of Outsourcing” Matrix	284
Critical Success Factors for Surviving AV Outsourcing	285
Sources of CSFs: the More Explicit, the Better!	286
Open Peer Communication Lines Between Both Companies	287
Use a Questionnaire to Match People to AV Functions	289
Align as Soon as Possible with Monitoring Services (SOC) and Incident Management Teams	290
Outline the AV infrastructure (as Seen by the Customer and the Vendor) and Discuss Differences	291
Align or Prepare the Reporting on Compliance Issues of Outsourced AV Services	292
Putting the Pieces Together	293
Roles and Responsibilities	295
Sample AV Skills and Experience Questionnaire for an AV Service Provider.	296
Summary	301
Solutions Fast Track	301
Frequently Asked Questions	304
Chapter 8 Education in Education	307
Introduction	308
User Education from an Educationalist’s Perspective	309
Some True Stories	313
The Grandmother	314
The Sister	315
The Father	315
The Young Girl	315
The Self-employed Professional	316
The Unwitting Spammers	316

And the Point is...	316
Where Do You Come In?	317
Security and Education in the UK	320
Evaluating Security Advice	321
Information Sharing and the WARP factor	321
The Myth of Teenage Literacy	324
Teaching Security in the Classroom	325
Duty of Care	331
Surfing the Darkside Economy	332
Duty of Care Issues (Again)	333
Cross-Curricular Security	334
Technical Areas Checklist	337
Not Exactly a Case Study: The Julie Amero Affair	339
Summary	342
Solutions Fast Track	342
Frequently Asked Questions	345
Chapter 9 DIY Malware Analysis	349
Introduction	350
Anti-Malware Tools of the Trade 101	350
The Basics: Identifying a Malicious File	351
Process and Network Service Detection Tools	359
Web-based Inspection and Virus Analysis Tools	367
AV Vendors Accept Submissions	367
Using an Online Malware Inspection Sandbox	374
Using Packet Analyzers to Gather Information	383
Results of Running <i>windump</i> at the Command Line	
to Show Proper Syntax Formatting	384
Examining Your Malware Sample with Executable Inspection Tools	388
Using Vulnerability Assessment and Port Scanning Tools	394
Advanced Tools: An Overview of Windows Code Debuggers	401
Advanced Analysis and Forensics	405
Advanced Malware Analysis	406
Static (Code) Analysis	406
Packers and Memory Dumping	408
Quick Assessment	411
Disassembling Malware	413
Debugging Malware	414
Dynamic (Behavior) Analysis	416
Isolated Environments	416

Behavior Monitoring418
Forensic Analysis420
Collecting Volatile Data421
Rootkits422
Collecting Process and Network Data423
Collecting Non-volatile Data425
Determining the Initial Vector425
A Lesson from History426
Case Study: An IRCbot-infected Machine428
Summary432
Solutions Fast Track432
Frequently Asked Questions437
Chapter 10 Antimalware Evaluation and Testing441
Introduction442
Antimalware Product Evaluation443
Configurability445
Cost445
Ease of Use447
Functionality448
Performance448
Support Issues451
Upgrades and Updates452
Information Flow and Documentation452
Evaluation Checklist453
Core Issues454
Testing Antimalware Products462
Replicating Malware464
Why is Sample Verification Important?464
Polymorphic Replicative Malware466
Environment468
In the Wild Testing468
Non-Replicating Malware470
Is It or Isn't It?470
Does it work?474
Time To Update Testing476
Defining the Problems476
Problem 1: Time to Update as a Measure	
of Protection Capability477
Problem 2: Baseline Setting for Heuristic/Proactive Detections478

Problem 3: Time of Release vs. Time of First Detection	481
Frozen Update (Retrospective) Testing	483
A Few Words on False Positives	484
A Checklist of Do's and Don'ts in Testing	484
First of All, Here's What Not to Do!	485
How to Do it Right!	486
Non-detection Testing Parameters	486
Conclusion	487
Independent Testing and Certification Bodies	487
VB100 Awards	488
ICSA Labs (a Division of Cybertrust)	489
Checkmark Certification	489
Anti-virus Level 1	489
Anti-virus Level 2	490
Trojan	490
Anti-Spyware	490
AV-Test.org	490
AV-Comparatives.org	490
Summary	491
Solutions Fast Track	493
Frequently Asked Questions	496
Chapter 11 AVIEN and AVIEWS: the Future	499
Appendix A Resources	503
Introduction	504
Customer Power	505
Stalkers on Your Desktop	505
A Tangled Web	507
Big Bad Bots	508
Crème de la CyberCrime	508
Defense in Depth	509
Perilous Outsorcery	509
Education in Education	509
DIY Malware Analysis	511
Antivirus Evaluation and Testing	512
Additional Resources	512
Books	512
Additional Resources	513
Linux:	514

Macintosh:514
Network Tools:514
SANS:515
Security Focus Newsletters515
Appendix B Glossary517
Introduction518
Index527

This page intentionally left blank

Foreword

This book recognizes that the combined membership of AVIEN and AVIEWS are uniquely qualified to pass on their combined knowledge and the benefits of their experience at the leading edge of anti-malware defense to others facing the challenges of new generations of malware.

The collective membership of the two organizations comprises many of the brightest minds working on malware-related issues.

This book also demonstrates the value of combining the practical research skills of some members with the writing experience of others. The end result is a wonderful blend of deeply researched and yet easily accessible information.

David Harley was the logical choice for heading up this project, not only because he has been involved with AVIEN since its earliest days, but also due to his extensive experience in managing very large installations of anti-virus defenses and his impeccable credentials in writing and editing in the security arena, especially in antivirus.

David has also extensive research experience, independence from commercial influence and the respect of his peers in the anti-malware field, a field that has seen his contributions for many years.

—Robert S. Vibert
Administrator, Anti-Virus Information Exchange Network

This page intentionally left blank