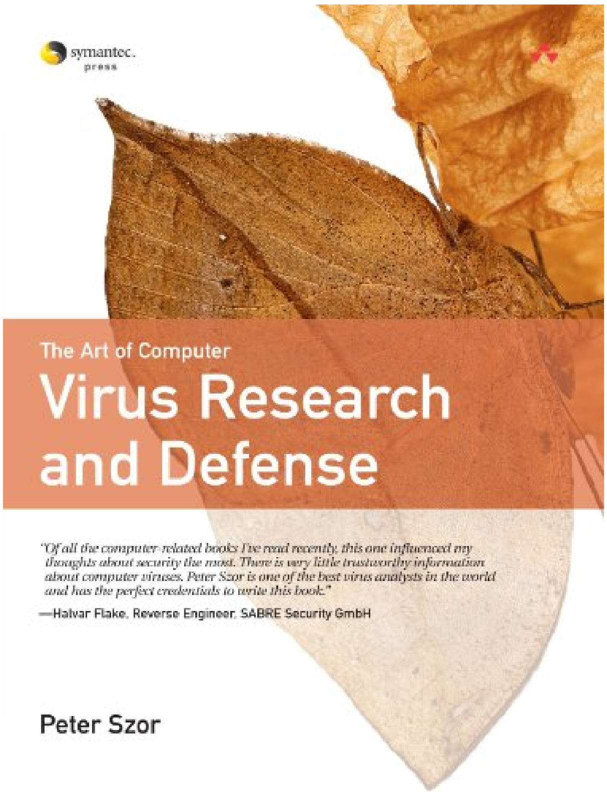
THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE BY PETER SZOR

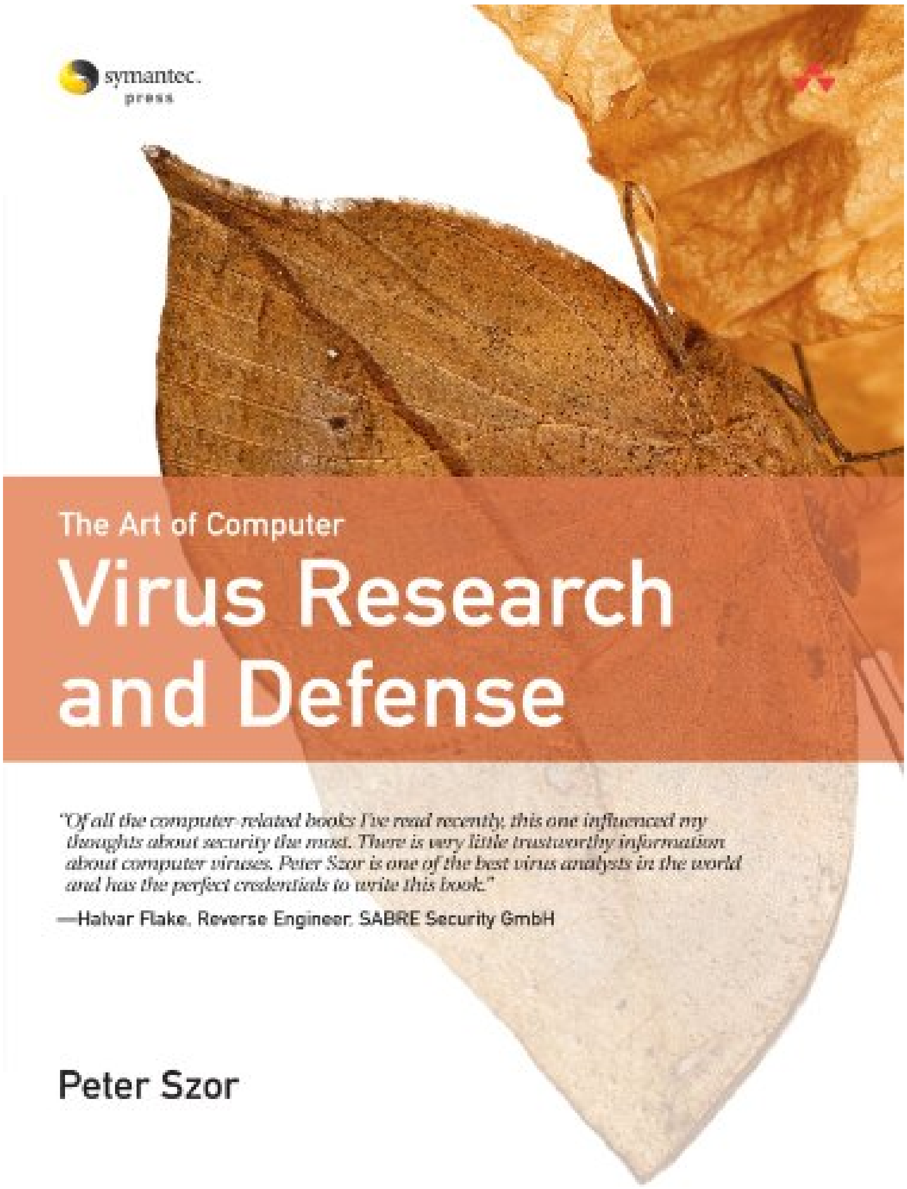


"Of all the computer-related books I've read recently, this one influenced my thoughts about security the most. There is very little trustworthy information about computer viruses. Peter Szor is one of the best virus analysts in the world and has the perfect credentials to write this book."

—Halvar Flake, Reverse Engineer, SABRE Security GmbH

Peter Szor

DOWNLOAD EBOOK : THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE BY PETER SZOR PDF



symantec. press

The Art of Computer

Virus Research and Defense

"Of all the computer-related books I've read recently, this one influenced my thoughts about security the most. There is very little trustworthy information about computer viruses. Peter Szor is one of the best virus analysts in the world and has the perfect credentials to write this book."

—Halvar Flake, Reverse Engineer, SABRE Security GmbH

Peter Szor

THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE BY PETER SZOR PDF

Reviewing habit will consistently lead individuals not to completely satisfied reading *The Art Of Computer Virus Research And Defense By Peter Szor*, an e-book, 10 e-book, hundreds publications, as well as more. One that will make them feel pleased is completing reading this book The Art Of Computer Virus Research And Defense By Peter Szor and also obtaining the notification of the publications, then finding the various other following publication to review. It proceeds an increasing number of. The moment to finish reading an e-book The Art Of Computer Virus Research And Defense By Peter Szor will be constantly various depending upon spar time to spend; one example is this The Art Of Computer Virus Research And Defense By Peter Szor

From the Back Cover

"Of all the computer-related books I've read recently, this one influenced my thoughts about security the most. There is very little trustworthy information about computer viruses. Peter Szor is one of the best virus analysts in the world and has the perfect credentials to write this book."

—Halvar Flake, Reverse Engineer, SABRE Security GmbH

Symantec's chief antivirus researcher has written the definitive guide to contemporary virus threats, defense techniques, and analysis tools. Unlike most books on computer viruses, The Art of Computer Virus Research and Defense is a reference written strictly for white hats: IT and security professionals responsible for protecting their organizations against malware. Peter Szor systematically covers everything you need to know, including virus behavior and classification, protection strategies, antivirus and worm-blocking techniques, and much more.

Szor presents the state-of-the-art in both malware and protection, providing the full technical detail that professionals need to handle increasingly complex attacks. Along the way, he provides extensive information on code metamorphism and other emerging techniques, so you can anticipate and prepare for future threats.

Szor also offers the most thorough and practical primer on virus analysis ever published—addressing everything from creating your own personal laboratory to automating the analysis process. This book's coverage includes

- Discovering how malicious code attacks on a variety of platforms
- Classifying malware strategies for infection, in-memory operation, self-protection, payload delivery, exploitation, and more
- Identifying and responding to code obfuscation threats: encrypted, polymorphic, and metamorphic
- Mastering empirical methods for analyzing malicious code—and what to do with what you learn

- Reverse-engineering malicious code with disassemblers, debuggers, emulators, and virtual machines
- Implementing technical defenses: scanning, code emulation, disinfection, inoculation, integrity checking, sandboxing, honeypots, behavior blocking, and much more
- Using worm blocking, host-based intrusion prevention, and network-level defense strategies

About the Author

Peter Szor is security architect for Symantec Security Response, where he has been designing and building antivirus technologies for the Norton AntiVirus product line since 1999. From 1990 to 1995, Szor wrote and maintained his own antivirus program, Pasteur. A renowned computer virus and security researcher, Szor speaks frequently at the Virus Bulletin, EICAR, ICSA, and RSA conferences, as well as the USENIX Security Symposium. He currently serves on the advisory board of Virus Bulletin magazine, and is a founding member of the AVED (AntiVirus Emergency Discussion) network.

Preface Preface Who Should Read This Book

Over the last two decades, several publications appeared on the subject of computer viruses, but only a few have been written by professionals ("insiders") of computer virus research. Although many books exist that discuss the computer virus problem, they usually target a novice audience and are simply not too interesting for the technical professionals. There are only a few works that have no worries going into the technical details, necessary to understand, to effectively defend against computer viruses.

Part of the problem is that existing books have little—if any—information about the current complexity of computer viruses. For example, they lack serious technical information on fast-spreading computer worms that exploit vulnerabilities to invade target systems, or they do not discuss recent code evolution techniques such as code metamorphism. If you wanted to get all the information I have in this book, you would need to spend a lot of time reading articles and papers that are often hidden somewhere deep inside computer virus and security conference proceedings, and perhaps you would need to dig into malicious code for years to extract the relevant details.

I believe that this book is most useful for IT and security professionals who fight against computer viruses on a daily basis. Nowadays, system administrators as well as individual home users often need to deal with computer worms and other malicious programs on their networks. Unfortunately, security courses have very little training on computer virus protection, and the general public knows very little about how to analyze and defend their network from such attacks. To make things more difficult, computer virus analysis techniques have not been discussed in any existing works in sufficient length before.

I also think that, for anybody interested in information security, being aware of what the computer virus writers have "achieved" so far is an important thing to know.

For years, computer virus researchers used to be "file" or "infected object" oriented. To the contrary, security professionals were excited about suspicious events only on the network level. In addition, threats such as CodeRed worm appeared to inject their code into the memory of vulnerable processes over the network, but did not "infect" objects on the disk. Today, it is important to understand all of these major perspectives—the file (storage), in-memory, and network views—and correlate the events using malicious code analysis techniques.

During the years, I have trained many computer virus and security analysts to effectively analyze and respond to malicious code threats. In this book, I have included information about anything that I ever had to deal with. For example, I have relevant examples of ancient threats, such as 8-bit viruses on the Commodore 64. You will see that techniques such as stealth technology appeared in the earliest computer viruses, and on a variety of platforms. Thus, you will be able to realize that current rootkits do not represent anything new! You will find sufficient coverage on 32-bit Windows worm threats with in-depth exploit discussions, as well as 64-bit viruses and "pocket monsters" on mobile devices. All along the way, my goal is to illustrate how old techniques "reincarnate" in new threats and demonstrate up-to-date attacks with just enough technical details.

I am sure that many of you are interested in joining the fight against malicious code, and perhaps, just like me, some of you will become inventors of defense techniques. All of you should, however, be aware of the pitfalls and the challenges of this field!

That is what this book is all about.

What I Cover

The purpose of this book is to demonstrate the current state of the art of computer virus and antivirus developments and to teach you the methodology of computer virus analysis and protection. I discuss infection techniques of computer viruses from all possible perspectives: file (on storage), in-memory, and network. I classify and tell you all about the dirty little tricks of computer viruses that bad guys developed over the last two decades and tell you what has been done to deal with complexities such as code polymorphism and exploits.

The easiest way to read this book is, well, to read it from chapter to chapter. However, some of the attack chapters have content that can be more relevant after understanding techniques presented in the defense chapters. If you feel that any of the chapters are not your taste, or are too difficult or lengthy, you can always jump to the next chapter. I am sure that everybody will find some parts of this book very difficult and other parts very simple, depending on individual experience.

I expect my readers to be familiar with technology and some level of programming. There are so many things discussed in this book that it is simply impossible to cover everything in sufficient length. However, you will know exactly what you might need to learn from elsewhere to be absolutely successful against malicious threats. To help you, I have created an extensive reference list for each chapter that leads you to the necessary background information.

Indeed, this book could easily have been over 1,000 pages. However, as you can tell, I am not Shakespeare. My knowledge of computer viruses is great, not my English. Most likely, you would have no benefit of my work if this were the other way around.

What I Do Not Cover

I do not cover Trojan horse programs or backdoors in great length. This book is primarily about self-replicating malicious code. There are plenty of great books available on regular malicious programs, but not on computer viruses.

I do not present any virus code in the book that you could directly use to build another virus. This book is not a "virus writing" class. My understanding, however, is that the bad guys already know about most of the techniques that I discuss in this book. So, the good guys need to learn more and start to think (but not act) like a real attacker to develop their defense!

Interestingly, many universities attempt to teach computer virus research courses by offering classes on writing viruses. Would it really help if a student could write a virus to infect millions of systems around the world? Will such students know more about how to develop defense better? Simply, the answer is no...

Instead, classes should focus on the analysis of existing malicious threats. There are so many threats out there waiting for somebody to understand them—and do something against them.

Of course, the knowledge of computer viruses is like the "Force" in Star Wars. Depending on the user of the "Force," the knowledge can turn to good or evil. I cannot force you to stay away from the "Dark Side," but I urge you to do so.

THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE BY PETER SZOR PDF

This is it guide **The Art Of Computer Virus Research And Defense By Peter Szor** to be best seller lately. We give you the most effective deal by getting the magnificent book The Art Of Computer Virus Research And Defense By Peter Szor in this site. This The Art Of Computer Virus Research And Defense By Peter Szor will certainly not just be the sort of book that is hard to find. In this site, all types of books are given. You could look title by title, author by writer, and author by publisher to figure out the best book The Art Of Computer Virus Research And Defense By Peter Szor that you could review currently.

As recognized, many individuals state that e-books are the home windows for the globe. It does not imply that purchasing e-book *The Art Of Computer Virus Research And Defense By Peter Szor* will imply that you could acquire this world. Just for joke! Reviewing a book The Art Of Computer Virus Research And Defense By Peter Szor will opened an individual to think better, to maintain smile, to entertain themselves, as well as to encourage the knowledge. Every publication additionally has their characteristic to affect the reader. Have you recognized why you read this The Art Of Computer Virus Research And Defense By Peter Szor for?

Well, still puzzled of how you can obtain this publication The Art Of Computer Virus Research And Defense By Peter Szor here without going outside? Simply connect your computer or gizmo to the website as well as start downloading and install The Art Of Computer Virus Research And Defense By Peter Szor Where? This page will reveal you the web link page to download and install The Art Of Computer Virus Research And Defense By Peter Szor You never stress, your favourite book will certainly be sooner your own now. It will certainly be much less complicated to delight in reading The Art Of Computer Virus Research And Defense By Peter Szor by on-line or getting the soft file on your gadget. It will despite that you are and what you are. This publication The Art Of Computer Virus Research And Defense By Peter Szor is written for public as well as you are among them which can delight in reading of this publication The Art Of Computer Virus Research And Defense By Peter Szor

THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE BY PETER SZOR PDF

Peter Szor takes you behind the scenes of anti-virus research, showing howthey are analyzed, how they spread, and--most importantly--how to effectivelydefend against them. This book offers an encyclopedic treatment of thecomputer virus, including: a history of computer viruses, virus behavior,classification, protection strategies, anti-virus and worm-blocking techniques,and how to conduct an accurate threat analysis. The Art of Computer VirusResearch and Defense entertains readers with its look at anti-virus research, butmore importantly it truly arms them in the fight against computer viruses.As one of the lead researchers behind Norton AntiVirus, the most popularantivirus program in the industry, Peter Szor studies viruses every day. Byshowing how viruses really work, this book will help security professionals andstudents protect against them, recognize them, and analyze and limit thedamage they can do.

- Sales Rank: #471371 in Books
- Brand: Szor, Peter
- Published on: 2005-02-13
- Original language: English
- Number of items: 1
- Dimensions: 9.00" h x 1.60" w x 6.90" l, 2.58 pounds
- Binding: Paperback
- 744 pages

From the Back Cover

"Of all the computer-related books I've read recently, this one influenced my thoughts about security the most. There is very little trustworthy information about computer viruses. Peter Szor is one of the best virus analysts in the world and has the perfect credentials to write this book."

—Halvar Flake, Reverse Engineer, SABRE Security GmbH

Symantec's chief antivirus researcher has written the definitive guide to contemporary virus threats, defense techniques, and analysis tools. Unlike most books on computer viruses, The Art of Computer Virus Research and Defense is a reference written strictly for white hats: IT and security professionals responsible for protecting their organizations against malware. Peter Szor systematically covers everything you need to know, including virus behavior and classification, protection strategies, antivirus and worm-blocking techniques, and much more.

Szor presents the state-of-the-art in both malware and protection, providing the full technical detail that professionals need to handle increasingly complex attacks. Along the way, he provides extensive information on code metamorphism and other emerging techniques, so you can anticipate and prepare for future threats.

Szor also offers the most thorough and practical primer on virus analysis ever published—addressing everything from creating your own personal laboratory to automating the analysis process. This book's coverage includes

- Discovering how malicious code attacks on a variety of platforms
- Classifying malware strategies for infection, in-memory operation, self-protection, payload delivery, exploitation, and more
- Identifying and responding to code obfuscation threats: encrypted, polymorphic, and metamorphic
- Mastering empirical methods for analyzing malicious code—and what to do with what you learn
- Reverse-engineering malicious code with disassemblers, debuggers, emulators, and virtual machines
- Implementing technical defenses: scanning, code emulation, disinfection, inoculation, integrity checking, sandboxing, honeypots, behavior blocking, and much more
- Using worm blocking, host-based intrusion prevention, and network-level defense strategies

About the Author

Peter Szor is security architect for Symantec Security Response, where he has been designing and building antivirus technologies for the Norton AntiVirus product line since 1999. From 1990 to 1995, Szor wrote and maintained his own antivirus program, Pasteur. A renowned computer virus and security researcher, Szor speaks frequently at the Virus Bulletin, EICAR, ICSA, and RSA conferences, as well as the USENIX Security Symposium. He currently serves on the advisory board of Virus Bulletin magazine, and is a founding member of the AVED (AntiVirus Emergency Discussion) network.

Preface Preface Who Should Read This Book

Over the last two decades, several publications appeared on the subject of computer viruses, but only a few have been written by professionals ("insiders") of computer virus research. Although many books exist that discuss the computer virus problem, they usually target a novice audience and are simply not too interesting for the technical professionals. There are only a few works that have no worries going into the technical details, necessary to understand, to effectively defend against computer viruses.

Part of the problem is that existing books have little—if any—information about the current complexity of computer viruses. For example, they lack serious technical information on fast-spreading computer worms that exploit vulnerabilities to invade target systems, or they do not discuss recent code evolution techniques such as code metamorphism. If you wanted to get all the information I have in this book, you would need to spend a lot of time reading articles and papers that are often hidden somewhere deep inside computer virus and security conference proceedings, and perhaps you would need to dig into malicious code for years to extract the relevant details.

I believe that this book is most useful for IT and security professionals who fight against computer viruses on a daily basis. Nowadays, system administrators as well as individual home users often need to deal with computer worms and other malicious programs on their networks. Unfortunately, security courses have very little training on computer virus protection, and the general public knows very little about how to analyze and defend their network from such attacks. To make things more difficult, computer virus analysis techniques have not been discussed in any existing works in sufficient length before.

I also think that, for anybody interested in information security, being aware of what the computer virus writers have "achieved" so far is an important thing to know.

For years, computer virus researchers used to be "file" or "infected object" oriented. To the contrary, security professionals were excited about suspicious events only on the network level. In addition, threats such as CodeRed worm appeared to inject their code into the memory of vulnerable processes over the network, but did not "infect" objects on the disk. Today, it is important to understand all of these major perspectives—the file (storage), in-memory, and network views—and correlate the events using malicious code analysis techniques.

During the years, I have trained many computer virus and security analysts to effectively analyze and respond to malicious code threats. In this book, I have included information about anything that I ever had to deal with. For example, I have relevant examples of ancient threats, such as 8-bit viruses on the Commodore 64. You will see that techniques such as stealth technology appeared in the earliest computer viruses, and on a variety of platforms. Thus, you will be able to realize that current rootkits do not represent anything new! You will find sufficient coverage on 32-bit Windows worm threats with in-depth exploit discussions, as well as 64-bit viruses and "pocket monsters" on mobile devices. All along the way, my goal is to illustrate how old techniques "reincarnate" in new threats and demonstrate up-to-date attacks with just enough technical details.

I am sure that many of you are interested in joining the fight against malicious code, and perhaps, just like me, some of you will become inventors of defense techniques. All of you should, however, be aware of the pitfalls and the challenges of this field!

That is what this book is all about.

What I Cover

The purpose of this book is to demonstrate the current state of the art of computer virus and antivirus developments and to teach you the methodology of computer virus analysis and protection. I discuss infection techniques of computer viruses from all possible perspectives: file (on storage), in-memory, and network. I classify and tell you all about the dirty little tricks of computer viruses that bad guys developed over the last two decades and tell you what has been done to deal with complexities such as code polymorphism and exploits.

The easiest way to read this book is, well, to read it from chapter to chapter. However, some of the attack chapters have content that can be more relevant after understanding techniques presented in the defense chapters. If you feel that any of the chapters are not your taste, or are too difficult or lengthy, you can always jump to the next chapter. I am sure that everybody will find some parts of this book very difficult and other parts very simple, depending on individual experience.

I expect my readers to be familiar with technology and some level of programming. There are so many things discussed in this book that it is simply impossible to cover everything in sufficient length. However, you will know exactly what you might need to learn from elsewhere to be absolutely successful against malicious threats. To help you, I have created an extensive reference list for each chapter that leads you to the necessary background information.

Indeed, this book could easily have been over 1,000 pages. However, as you can tell, I am not Shakespeare.

My knowledge of computer viruses is great, not my English. Most likely, you would have no benefit of my work if this were the other way around.

What I Do Not Cover

I do not cover Trojan horse programs or backdoors in great length. This book is primarily about self-replicating malicious code. There are plenty of great books available on regular malicious programs, but not on computer viruses.

I do not present any virus code in the book that you could directly use to build another virus. This book is not a "virus writing" class. My understanding, however, is that the bad guys already know about most of the techniques that I discuss in this book. So, the good guys need to learn more and start to think (but not act) like a real attacker to develop their defense!

Interestingly, many universities attempt to teach computer virus research courses by offering classes on writing viruses. Would it really help if a student could write a virus to infect millions of systems around the world? Will such students know more about how to develop defense better? Simply, the answer is no...

Instead, classes should focus on the analysis of existing malicious threats. There are so many threats out there waiting for somebody to understand them—and do something against them.

Of course, the knowledge of computer viruses is like the "Force" in Star Wars. Depending on the user of the "Force," the knowledge can turn to good or evil. I cannot force you to stay away from the "Dark Side," but I urge you to do so.

Most helpful customer reviews

52 of 55 people found the following review helpful.
One of the best technical books I've ever read
By Richard Bejtlich
Peter Szor's 'The Art of Computer Virus Research and Defense' (TAOCVRAD) is one of the best technical books I've ever read, and I've reviewed over 150 security and networking books during the past 5 years. This book so thoroughly owns the subject of computer viruses that I recommend any authors seeking to write their own virus book find a new topic. Every technical computing professional needs to read this book, fast.

I read this book from cover to cover. The author does not lie when he says acquiring the same amount of information requires digging in obscure virus journals and analyzing malicious code. TAOCVRAD's single most powerful aspect is the author's persistence in naming one or more sample viruses that exemplify whatever concept he is discussing. In other words, all of his theory is backed by, or builds on, real-life examples. Each chapter contains moderate end-notes that provide pointers for additional research.

A truly great book has the power to change deeply-entrenched opinions, or make readers look at old problems in a new light. In my case, I altered my perception of the virus problem and ways to fight it. First, I changed my concept of viruses and worms. Peter builds on Fred Cohen's virus definition to say 'a computer virus is a program that recursively and explicitly copies a possibly evolved version of itself.' He calls worms a 'subclass of computer viruses.' I used to disagree with Peter; I believed a virus infects files and requires user interaction, and a worm spreads by itself via the network. Now I agree with Peter's viewpoint: 'worms are network viruses, primarily replicating on networks... If the primary vector of the virus is the network, it should be classified as a worm.' The distinction is subtle, but it makes sense to consider worms a subclass of viruses given Peter's extensive analysis of both types of malware.

Second, I recognized I held an opinion Peter considers unfortunate: 'some computer security people do not seem to consider computer viruses as a serious aspect of security, or they ignore the relationship between computer security and computer viruses.' I was guilty as charged. I used to positively detest viruses because they seemed like mindless automated code that did little but replicate. After reading about scores of real viruses, I have a profound appreciation for virus technology. Viruses introduced techniques for obfuscation, stealth, and exploitation a decade earlier, in some cases, than the single-shot exploit code we see today.

Third, Peter put a human face on the problems associated with closed-source operating systems like Microsoft Windows. Many so-called Native API calls are undocumented, and as such make life difficult for anti-virus developers. (Virus writers tend to know them.) With Microsoft entering the anti-virus market, will it leverage these secrets to outperform competitors lacking this internal knowledge?

Readers of Ed Skoudis' 'Malware' or Jose Nazario's 'Defense and Detection Strategies against Internet Worms' will find this new book greatly complements those two works. Those wishing to get the most value from TAOCVRAD should have Intel assembly coding skills and several years of hands-on security experience.

I had almost no issues with this book, which is striking given it is nearly 700 pages long. In a few places I found the language a little rough, but not enough to bother me. I believe a code listing on p. 372 should show a '

THE ART OF COMPUTER VIRUS RESEARCH AND DEFENSE BY PETER SZOR PDF

Spending the extra time by checking out **The Art Of Computer Virus Research And Defense By Peter Szor** could offer such great encounter even you are only sitting on your chair in the workplace or in your bed. It will not curse your time. This The Art Of Computer Virus Research And Defense By Peter Szor will certainly assist you to have more priceless time while taking remainder. It is quite enjoyable when at the midday, with a mug of coffee or tea and an e-book The Art Of Computer Virus Research And Defense By Peter Szor in your device or computer system screen. By taking pleasure in the sights around, right here you could begin reading.

From the Back Cover

"Of all the computer-related books I've read recently, this one influenced my thoughts about security the most. There is very little trustworthy information about computer viruses. Peter Szor is one of the best virus analysts in the world and has the perfect credentials to write this book."

—Halvar Flake, Reverse Engineer, SABRE Security GmbH

Symantec's chief antivirus researcher has written the definitive guide to contemporary virus threats, defense techniques, and analysis tools. Unlike most books on computer viruses, The Art of Computer Virus Research and Defense is a reference written strictly for white hats: IT and security professionals responsible for protecting their organizations against malware. Peter Szor systematically covers everything you need to know, including virus behavior and classification, protection strategies, antivirus and worm-blocking techniques, and much more.

Szor presents the state-of-the-art in both malware and protection, providing the full technical detail that professionals need to handle increasingly complex attacks. Along the way, he provides extensive information on code metamorphism and other emerging techniques, so you can anticipate and prepare for future threats.

Szor also offers the most thorough and practical primer on virus analysis ever published—addressing everything from creating your own personal laboratory to automating the analysis process. This book's coverage includes

- Discovering how malicious code attacks on a variety of platforms
- Classifying malware strategies for infection, in-memory operation, self-protection, payload delivery, exploitation, and more
- Identifying and responding to code obfuscation threats: encrypted, polymorphic, and metamorphic
- Mastering empirical methods for analyzing malicious code—and what to do with what you learn
- Reverse-engineering malicious code with disassemblers, debuggers, emulators, and virtual machines
- Implementing technical defenses: scanning, code emulation, disinfection, inoculation, integrity checking, sandboxing, honeypots, behavior blocking, and much more
- Using worm blocking, host-based intrusion prevention, and network-level defense strategies

About the Author

Peter Szor is security architect for Symantec Security Response, where he has been designing and building antivirus technologies for the Norton AntiVirus product line since 1999. From 1990 to 1995, Szor wrote and maintained his own antivirus program, Pasteur. A renowned computer virus and security researcher, Szor speaks frequently at the Virus Bulletin, EICAR, ICSA, and RSA conferences, as well as the USENIX Security Symposium. He currently serves on the advisory board of Virus Bulletin magazine, and is a founding member of the AVED (AntiVirus Emergency Discussion) network.

Preface Preface Who Should Read This Book

Over the last two decades, several publications appeared on the subject of computer viruses, but only a few have been written by professionals ("insiders") of computer virus research. Although many books exist that discuss the computer virus problem, they usually target a novice audience and are simply not too interesting for the technical professionals. There are only a few works that have no worries going into the technical details, necessary to understand, to effectively defend against computer viruses.

Part of the problem is that existing books have little—if any—information about the current complexity of computer viruses. For example, they lack serious technical information on fast-spreading computer worms that exploit vulnerabilities to invade target systems, or they do not discuss recent code evolution techniques such as code metamorphism. If you wanted to get all the information I have in this book, you would need to spend a lot of time reading articles and papers that are often hidden somewhere deep inside computer virus and security conference proceedings, and perhaps you would need to dig into malicious code for years to extract the relevant details.

I believe that this book is most useful for IT and security professionals who fight against computer viruses on a daily basis. Nowadays, system administrators as well as individual home users often need to deal with computer worms and other malicious programs on their networks. Unfortunately, security courses have very little training on computer virus protection, and the general public knows very little about how to analyze and defend their network from such attacks. To make things more difficult, computer virus analysis techniques have not been discussed in any existing works in sufficient length before.

I also think that, for anybody interested in information security, being aware of what the computer virus writers have "achieved" so far is an important thing to know.

For years, computer virus researchers used to be "file" or "infected object" oriented. To the contrary, security professionals were excited about suspicious events only on the network level. In addition, threats such as CodeRed worm appeared to inject their code into the memory of vulnerable processes over the network, but did not "infect" objects on the disk. Today, it is important to understand all of these major perspectives—the file (storage), in-memory, and network views—and correlate the events using malicious code analysis techniques.

During the years, I have trained many computer virus and security analysts to effectively analyze and respond to malicious code threats. In this book, I have included information about anything that I ever had to deal with. For example, I have relevant examples of ancient threats, such as 8-bit viruses on the Commodore 64. You will see that techniques such as stealth technology appeared in the earliest computer viruses, and on a variety of platforms. Thus, you will be able to realize that current rootkits do not represent anything new! You will find sufficient coverage on 32-bit Windows worm threats with in-depth exploit discussions, as well as 64-bit viruses and "pocket monsters" on mobile devices. All along the way, my goal is to illustrate how old techniques "reincarnate" in new threats and demonstrate up-to-date attacks with just enough technical details.

I am sure that many of you are interested in joining the fight against malicious code, and perhaps, just like me, some of you will become inventors of defense techniques. All of you should, however, be aware of the pitfalls and the challenges of this field!

That is what this book is all about.

What I Cover

The purpose of this book is to demonstrate the current state of the art of computer virus and antivirus developments and to teach you the methodology of computer virus analysis and protection. I discuss infection techniques of computer viruses from all possible perspectives: file (on storage), in-memory, and network. I classify and tell you all about the dirty little tricks of computer viruses that bad guys developed over the last two decades and tell you what has been done to deal with complexities such as code polymorphism and exploits.

The easiest way to read this book is, well, to read it from chapter to chapter. However, some of the attack chapters have content that can be more relevant after understanding techniques presented in the defense chapters. If you feel that any of the chapters are not your taste, or are too difficult or lengthy, you can always jump to the next chapter. I am sure that everybody will find some parts of this book very difficult and other parts very simple, depending on individual experience.

I expect my readers to be familiar with technology and some level of programming. There are so many things discussed in this book that it is simply impossible to cover everything in sufficient length. However, you will know exactly what you might need to learn from elsewhere to be absolutely successful against malicious threats. To help you, I have created an extensive reference list for each chapter that leads you to the necessary background information.

Indeed, this book could easily have been over 1,000 pages. However, as you can tell, I am not Shakespeare. My knowledge of computer viruses is great, not my English. Most likely, you would have no benefit of my work if this were the other way around.

What I Do Not Cover

I do not cover Trojan horse programs or backdoors in great length. This book is primarily about self-replicating malicious code. There are plenty of great books available on regular malicious programs, but not on computer viruses.

I do not present any virus code in the book that you could directly use to build another virus. This book is not a "virus writing" class. My understanding, however, is that the bad guys already know about most of the techniques that I discuss in this book. So, the good guys need to learn more and start to think (but not act) like a real attacker to develop their defense!

Interestingly, many universities attempt to teach computer virus research courses by offering classes on writing viruses. Would it really help if a student could write a virus to infect millions of systems around the world? Will such students know more about how to develop defense better? Simply, the answer is no...

Instead, classes should focus on the analysis of existing malicious threats. There are so many threats out there waiting for somebody to understand them—and do something against them.

Of course, the knowledge of computer viruses is like the "Force" in Star Wars. Depending on the user of the "Force," the knowledge can turn to good or evil. I cannot force you to stay away from the "Dark Side," but I urge you to do so.

Reviewing habit will consistently lead individuals not to completely satisfied reading *The Art Of Computer Virus Research And Defense By Peter Szor*, an e-book, 10 e-book, hundreds publications, as well as more. One that will make them feel pleased is completing reading this book The Art Of Computer Virus Research And Defense By Peter Szor and also obtaining the notification of the publications, then finding the various other following publication to review. It proceeds an increasing number of. The moment to finish reading an e-book The Art Of Computer Virus Research And Defense By Peter Szor will be constantly various depending upon spar time to spend; one example is this The Art Of Computer Virus Research And Defense By Peter Szor