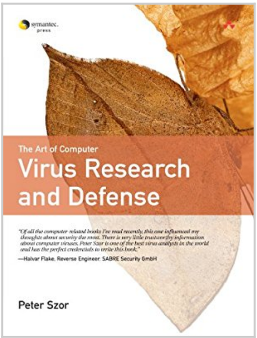

The Art of Computer Virus Research and Defense

By Peter Szor

Download now

Read Online

The Art of Computer Virus Research and Defense By Peter Szor

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.

Download The Art of Computer Virus Research and Defense ...pdf

Read Online The Art of Computer Virus Research and Defense ...pdf

The Art of Computer Virus Research and Defense

By Peter Szor

The Art of Computer Virus Research and Defense By Peter Szor

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.

The Art of Computer Virus Research and Defense By Peter Szor Bibliography

- Sales Rank: #303774 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

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.

Read The Art of Computer Virus Research and Defense By Peter Szor for online ebook

The Art of Computer Virus Research and Defense By Peter Szor Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read The Art of Computer Virus Research and Defense By Peter Szor books to read online.

Online The Art of Computer Virus Research and Defense By Peter Szor ebook PDF download

The Art of Computer Virus Research and Defense By Peter Szor Doc

The Art of Computer Virus Research and Defense By Peter Szor Mobipocket

The Art of Computer Virus Research and Defense By Peter Szor EPub

WQO4FLI7ZGK: The Art of Computer Virus Research and Defense By Peter Szor