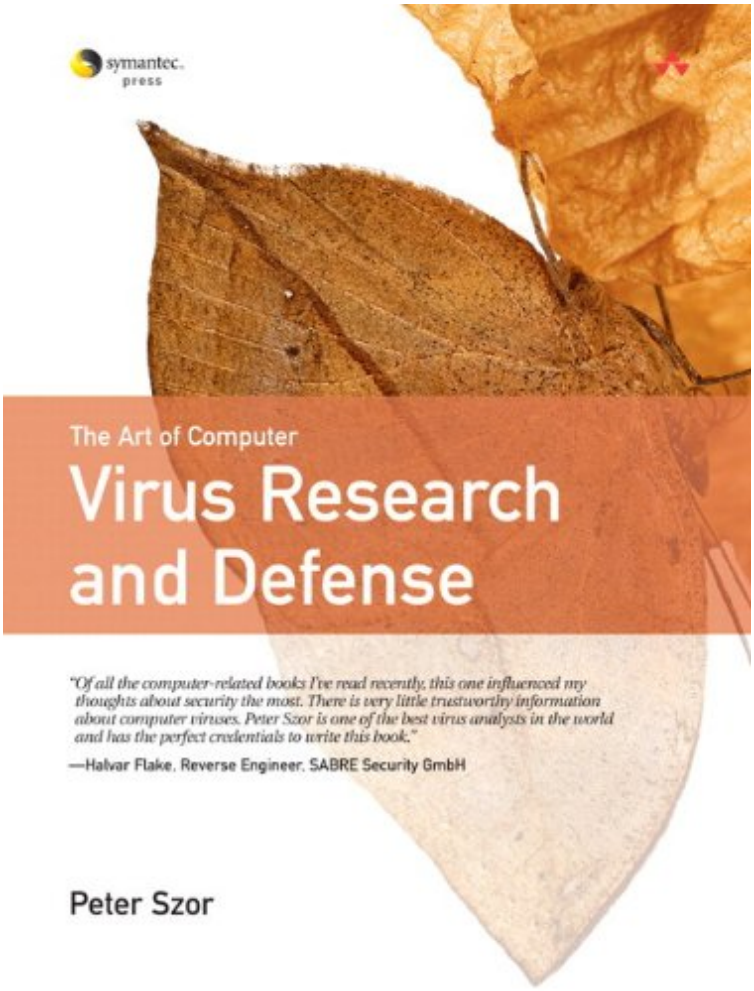
The Art of Computer Virus Research and Defense (Symantec Press)

Von Peter Szor
*DOC | *audiobook | ebooks | Download PDF | ePub*



Produktinformation -Verkaufsrang: #537498 in eBooksVerffentlicht am: 2005-02-03Erscheinungsdatum: 2005-02-03File Name: B003DQ4WLQ | File size: 38.Mb

Von Peter Szor : The Art of Computer Virus Research and Defense (Symantec Press) before purchasing it in order to gage whether or not it would be worth my time, and all praised The Art of Computer Virus Research and Defense (Symantec Press):

KundenrezensionenHilfreichste Kundenrezensionen1 von 1 Kunden fanden die folgende Rezension hilfreich. Eines der besten Bcher zum Thema VirenVon LegasthenikerDa es zu diesem Thema nicht wirklich viele gute Bcher gibt hat Peter Szor mit diesem Buch eine Lcke gefllt. Peter Szor hat etliche Jahre im Bereich der Viren-/Malware-Analyse auf dem Buckel und daher einen sehr tiefen Einblick in das Thema. Das Buch gibt sehr viele Informationen die fr jeden Security-Consultant oder -Administrator ein Must-Have sind. Fr Leute die bereits Erfahrung im Bereich Malware-/Virus-/Binary-Analyse haben geht das Buch jedoch nicht tief genug. Das liegt hauptschlich daran, das Symantec (der Arbeitgeber von Peter Szor) es fr nicht vertretbar hlt Details ber Viren/Malware zu publizieren die einen Leser dazu befhigen knnten Viren zu produzieren. Da aber die wenigsten Leser so tief in die Materie gehen wollen/knnen, ist das

Buch genau richtig! Tendenz zum Standardwerk :)

KurzbeschreibungSymantec'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 publishedaddressing 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 codeand 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 KurzbeschreibungSymantec'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 publishedaddressing 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 codeand 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 Synopsis 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.