DESCRIPTION

A computer forensics "how-to" for fighting malicious code and analyzing incidents

With our ever-increasing reliance on computers comes an ever-growing risk of malware. Security professionals will find plenty of solutions in this book to the problems posed by viruses, Trojan horses, worms, spyware, rootkits, adware, and other invasive software. Written by well-known malware experts, this guide reveals solutions to numerous problems and includes a DVD of custom programs and tools that illustrate the concepts, enhancing your skills.

• Security professionals face a constant battle against malicious software; this practical manual will improve your analytical capabilities and provide dozens of valuable and innovative solutions

• Covers classifying malware, packing and unpacking, dynamic malware analysis, decoding and decrypting, rootkit detection, memory forensics, open source malware research, and much more

• Includes generous amounts of source code in C, Python, and Perl to extend your favorite tools or build new ones, and custom programs on the DVD to demonstrate the solutions

*Malware Analyst's Cookbook* is indispensable to IT security administrators, incident responders, forensic analysts, and malware researchers.
ABOUT THE AUTHOR

Michael Hale Ligh is a malicious code analyst at Verisign iDefense and Chief of Special Projects at MNIN Security.

Steven Adair is a member of the Shadowserver Foundation and frequently analyzes malware and tracks botnets. He also investigates cyber attacks of all kinds with an emphasis on those linked to cyber espionage.

Blake Hartstein is the author of multiple security tools and a Rapid Response Engineer at Verisign iDefense, where he responds to malware incidents.

Matthew Richard has authored numerous security tools and also ran a managed security service for banks and credit unions.

For additional product details, please visit https://www.wiley.com/en-us