1. Record Nr. UNINA9910824210803321

Autore	Koret Joxean
Titolo	The Antivirus hacker's handbook / / Joxean Koret, Elias Bachaalany
Pubbl/distr/stampa	Indianapolis, IN : , : John Wiley and Sons, , [2015] ©2015
ISBN	1-119-18352-9 1-119-02878-7 1-119-02876-0
Edizione	[First edition.]
Descrizione fisica	1 online resource (384 p.)
Disciplina	005.84
Soggetti	Hackers Computer viruses
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Cover; Title Page; Copyright; Contents; Introduction; Part I Antivirus Basics; Chapter 1 Introduction to Antivirus Software; What Is Antivirus Software?; Antivirus Software: Past and Present; Antivirus Scanners, Kernels, and Products; Typical Misconceptions about Antivirus Software; Antivirus Features; Basic Features; Making Use of Native Languages; Scanners; Signatures; Compressors and Archives; Unpackers; Emulators; Miscellaneous File Formats; Advanced Features; Packet Filters and Firewalls; Self-Protection; Anti-Exploiting; Summary; Chapter 2 Reverse-Engineering the Core Reverse-Engineering ToolsCommand-Line Tools versus GUI Tools; Debugging Symbols; Tricks for Retrieving Debugging Symbols; Debugging Tricks; Backdoors and Configuration Settings; Kernel Debugging; Debugging User-Mode Processes with a Kernel-Mode Debugger; Analyzing AV Software with Command-Line Tools; Porting the Core; A Practical Example: Writing Basic Python Bindings for Avast for Linux; A Brief Look at Avast for Linux; Writing Simple Python Bindings for Avast for Linux; The Final Version of the Python Bindings; A Practical Example: Writing Native C/C++ Tools for Comodo Antivirus for Linux Other Components Loaded by the KernelSummary; Chapter 3 The Plug-

ins System; Understanding How Plug-ins Are Loaded; A Full-Featured Linker in Antivirus Software; Understanding Dynamic Loading; Advantages and Disadvantages of the Approaches for Packaging Plug-ins; Types of Plug-ins; Scanners and Generic Routines; File Format and Protocol Support; Heuristics; Bayesian Networks; Bloom Filters; Weights-Based Heuristics; Some Advanced Plug-ins; Memory Scanners; Non-native Code; Scripting Languages; Emulators; Summary; Chapter 4 Understanding Antivirus Signatures; Typical Signatures; Byte-Streams ChecksumsCustom Checksums; Cryptographic Hashes; Advanced Signatures; Fuzzy Hashing; Graph-Based Hashes for Executable Files; Summary; Chapter 5 The Update System; Understanding the Update Protocols; Support for SSL/TLS; Verifying the Update Files; Dissecting an Update Protocol; When Protection Is Done Wrong; Summary; Part II Antivirus Software Evasion; Chapter 6 Antivirus Software Evasion; Who Uses Antivirus Evasion Techniques?; Discovering Where and How Malware Is Detected; Old Tricks for Determining Where Malware Is Detected: Divide and Conquer
Evading a Simple Signature-Based Detection with the Divide and Conquer TrickBinary Instrumentation and Taint Analysis; Summary; Chapter 7 Evading Signatures; File Formats: Corner Cases and Undocumented Cases; Evading a Real Signature; Evasion Tips and Tricks for Specific File Formats; PE Files; JavaScript; String Encoding; Executing Code on the Fly; Hiding the Logic: Opaque Predicates and Junk Code; PDF; Summary; Chapter 8 Evading Scanners; Generic Evasion Tips and Tricks; Fingerprinting Emulators; Advanced Evasion Tricks; Taking Advantage of File Format Weaknesses
Using Anti-emulation Techniques

Sommario/riassunto

Hack your antivirus software to stamp out future vulnerabilities The Antivirus Hacker's Handbook guides you through the process of reverse engineering antivirus software. You explore how to detect and exploit vulnerabilities that can be leveraged to improve future software design, protect your network, and anticipate attacks that may sneak through your antivirus' line of defense. You'll begin building your knowledge by diving into the reverse engineering process, which details how to start from a finished antivirus software program and work your way back through its development using the func