1. Record Nr. UNINA9910785237703321

Autore	Ligh Michael W
Titolo	Malware analyst's cookbook and dvd [[electronic resource]] : tools and techniques for fighting malicious code / / Michael Ligh ... [et al.]
Pubbl/distr/stampa	Indianapolis, Ind., : Wiley Pub., Inc, 2011
ISBN	1-118-00829-4 1-282-84940-9 9786612849404 1-118-00336-5
Edizione	[1st edition]
Descrizione fisica	1 online resource (746 p.)
Disciplina	005.8 005.84
Soggetti	Malware (Computer software)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Malware Analyst's Cookbook and DVD; Contents; Introduction; On The Book's DVD; Chapter 1: Anonymizing Your Activities; Recipe 1-1: Anonymous Web Browsing with Tor; Recipe 1-2: Wrapping Wget and Network Clients with Torsocks; Recipe 1-3: Multi-platform Tor-enabled Downloader in Python; Recipe 1-4: Forwarding Traffic through Open Proxies; Recipe 1-5: Using SSH Tunnels to Proxy Connections; Recipe 1-6: Privacy-enhanced Web browsing with Privoxy; Recipe 1-7: Anonymous Surfing with Anonymouse.org; Recipe 1-8: Internet Access through Cellular Networks Recipe 1-9: Using VPNs with Anonymizer UniversalChapter 2: Honeypots; Recipe 2-1: Collecting Malware Samples with Nepenthes; Recipe 2-2: Real-Time Attack Monitoring with IRC Logging; Recipe 2-3: Accepting Nepenthes Submissions over HTTP with Python; Recipe 2-4: Collecting Malware Samples with Dionaea; Recipe 2-5: Accepting Dionaea Submissions over HTTP with Python; Recipe 2-6: Real-time Event Notification and Binary Sharing with XMPP; Recipe 2-7: Analyzing and Replaying Attacks Logged by Dionea; Recipe 2-8: Passive Identification of Remote Systems with p0f Recipe 2-9: Graphing Dionaea Attack Patterns with SQLite and

GnuplotChapter 3: Malware Classification; Recipe 3-1: Examining Existing ClamAV Signatures; Recipe 3-2: Creating a Custom ClamAV Database; Recipe 3-3: Converting ClamAV Signatures to YARA; Recipe 3-4: Identifying Packers with YARA and PEiD; Recipe 3-5: Detecting Malware Capabilities with YARA; Recipe 3-6: File Type Identification and Hashing in Python; Recipe 3-7: Writing a Multiple-AV Scanner in Python; Recipe 3-8: Detecting Malicious PE Files in Python; Recipe 3-9: Finding Similar Malware with ssdeep
Recipe 3-10: Detecting Self-modifying Code with ssdeepRecipe 3-11: Comparing Binaries with IDA and BinDiff; Chapter 4: Sandboxes and Multi-AV Scanners; Recipe 4-1: Scanning Files with VirusTotal; Recipe 4-2: Scanning Files with Jotti; Recipe 4-3: Scanning Files with NoVirusThanks; Recipe 4-4: Database-Enabled Multi-AV Uploader in Python; Recipe 4-5: Analyzing Malware with ThreatExpert; Recipe 4-6: Analyzing Malware with CWSandbox; Recipe 4-7: Analyzing Malware with Anubis; Recipe 4-8: Writing AutoIT Scripts for Joebox; Recipe 4-9: Defeating Path-dependent Malware with Joebox
Recipe 4-10: Defeating Process-dependent DLLs with JoeboxRecipe 4-11: Setting an Active HTTP Proxy with Joebox; Recipe 4-12: Scanning for Artifacts with Sandbox Results; Chapter 5: Researching Domains and IP Addresses; Recipe 5-1: Researching Domains with WHOIS; Recipe 5-2: Resolving DNS Hostnames; Recipe 5-3: Obtaining IP WHOIS Records; Recipe 5-4: Querying Passive DNS with BFK; Recipe 5-5: Checking DNS Records with Robtex; Recipe 5-6: Performing a Reverse IP Search with DomainTools; Recipe 5-7: Initiating Zone Transfers with dig; Recipe 5-8: Brute-forcing Subdomains with dnsmap
Recipe 5-9: Mapping IP Addresses to ASNs via Shadowserver

Sommario/riassunto

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