

1. Record Nr.	UNINA9910484247803321
Titolo	Detection of intrusions and malware, and vulnerability assessment : second international conference, DIMVA 2005, Vienna, Austria, July 7-8, 2005 : proceedings // Klaus Julisch, Christopher Kruegel (eds.)
Pubbl/distr/stampa	Berlin ; ; New York, : Springer, c2005
Edizione	[1st ed. 2005.]
Descrizione fisica	1 online resource (X, 241 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 3548
Altri autori (Persone)	JulischKlaus KruegelChristopher <1976->
Disciplina	005.8
Soggetti	Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and author index.
Nota di contenuto	Obfuscated Code Detection -- Analyzing Memory Accesses in Obfuscated x86 Executables -- Hybrid Engine for Polymorphic Shellcode Detection -- Honeypots -- Experiences Using Minos as a Tool for Capturing and Analyzing Novel Worms for Unknown Vulnerabilities -- A Pointillist Approach for Comparing Honeypots -- Vulnerability Assessment and Exploit Analysis -- Automatic Detection of Attacks on Cryptographic Protocols: A Case Study -- METAL -- A Tool for Extracting Attack Manifestations -- Flow-Level Traffic Analysis of the Blaster and Sobig Worm Outbreaks in an Internet Backbone -- Anomaly Detection -- A Learning-Based Approach to the Detection of SQL Attacks -- Masquerade Detection via Customized Grammars -- A Prevention Model for Algorithmic Complexity Attacks -- Misuse Detection -- Detecting Malicious Code by Model Checking -- Improving the Efficiency of Misuse Detection -- Distributed Intrusion Detection and IDS Testing -- Enhancing the Accuracy of Network-Based Intrusion Detection with Host-Based Context -- TCPtransform: Property-Oriented TCP Traffic Transformation.
Sommario/riassunto	On behalf of the Program Committee, it is our pleasure to present to you the proceedings of the 2nd GI SIG SIDAR Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA). DIMVA is organized by the Special Interest Group Security — Intrusion Detection and Response (SIDAR) of the German Informatics Society (GI)

as an annual conference that brings together experts from throughout the world to discuss the state of the art in the areas of intrusion detection, detection of malware, and assessment of vulnerabilities. The DIMVA 2005 Program Committee received 51 submissions from 18 countries. This represents an increase of approximately 25% compared with the number of submissions last year. All submissions were carefully reviewed by at least three Program Committee members or external experts according to the criteria of scientific novelty, importance to the field, and technical quality. The final selection took place at a meeting held on March 18, 2005, in Zurich, Switzerland. Fourteen full papers were selected for presentation and publication in the conference proceedings. In addition, three papers were selected for presentation in the industry track of the conference. The program featured both theoretical and practical research results, which were grouped into six sessions. Philip Attfield from the Northwest Security Institute gave the opening keynote speech. The slides presented by the authors are available on the DIMVA 2005 Web site at <http://www.dimva.org/dimva2005>. We sincerely thank all those who submitted papers as well as the Program Committee members and the external reviewers for their valuable contributions.
