

Bernhard M. Hämmerli Robin Sommer (Eds.)

Detection of Intrusions and Malware, and Vulnerability Assessment

4th International Conference, DIMVA 2007
Lucerne, Switzerland, July 12-13, 2007
Proceedings

 Springer

Table of Contents

Web Security

Extensible Web Browser Security	1
<i>Mike Ter Louw, Jin Soon Lim, and V.N. Venkatakrishnan</i>	
On the Effectiveness of Techniques to Detect Phishing Sites	20
<i>Christian Ludl, Sean McAllister, Engin Kirda, and Christopher Kruegel</i>	
Protecting the Intranet Against “JavaScript Malware” and Related Attacks	40
<i>Martin Johns and Justus Winter</i>	

Intrusion Detection

On the Effects of Learning Set Corruption in Anomaly-Based Detection of Web Defacements	60
<i>Eric Medvet and Alberto Bartoli</i>	
Intrusion Detection as Passive Testing: Linguistic Support with TTCN-3 (Extended Abstract)	79
<i>Krzysztof M. Brzezinski</i>	
Characterizing Bots’ Remote Control Behavior	89
<i>Elizabeth Stinson and John C. Mitchell</i>	

Traffic Analysis

Measurement and Analysis of Autonomous Spreading Malware in a University Environment	109
<i>Jan Goebel, Thorsten Holz, and Carsten Willems</i>	
Passive Monitoring of DNS Anomalies (Extended Abstract)	129
<i>Bojan Zdrnja, Nevil Brownlee, and Duane Wessels</i>	
Characterizing Dark DNS Behavior	140
<i>Jon Oberheide, Manish Karir, and Z. Morley Mao</i>	

Network Security

Distributed Evasive Scan Techniques and Countermeasures	157
<i>Min Gyung Kang, Juan Caballero, and Dawn Song</i>	

On the Adaptive Real-Time Detection of Fast-Propagating Network
Worms 175
Jaeyeon Jung, Rodolfo A. Milito, and Vern Paxson

Host Security

Targeting Physically Addressable Memory 193
David R. Piegdon and Lexi Pimenidis

Static Analysis on x86 Executables for Preventing Automatic Mimicry
Attacks 213
Danilo Bruschi, Lorenzo Cavallaro, and Andrea Lanzi

A Study of Malcode-Bearing Documents 231
*Wei-Jen Li, Salvatore Stolfo, Angelos Stavrou, Elli Androulaki, and
Angelos D. Keromytis*

Author Index 251