

2009 European Conference on Computer Network Defense

(EC2ND 2009)

**Milano, Italy
9 – 10 November 2009**



IEEE Catalog Number: CFP0936F-PRT
ISBN: 978-1-4244-6049-6

2009 European Conference on Computer Network Defense

EC2ND 2009

Table of Contents

Message from the Chair	vi
Organization	vii
Reviewers	viii

EC2ND 2009

Gone Rogue: An Analysis of Rogue Security Software Campaigns	1
<i>Marco Cova, Corrado Leita, Olivier Thonnard, Angelos Keromytis, and Marc Dacier</i>	
Racewalk: Fast Instruction Frequency Analysis and Classification for Shellcode Detection in Network Flow	4
<i>Dennis Gamayunov, Nguyen Thoi Minh Quan, Fedor Sakharov, and Edward Toroshchin</i>	
Walowdac - Analysis of a Peer-to-Peer Botnet	13
<i>Ben Stock, Jan Göbel, Markus Engelberth, Felix C. Freiling, and Thorsten Holz</i>	
Effectiveness Metrics for Intrusion Detection in Wireless Sensor Networks	21
<i>Andriy Stetsko and Vashek Matyas</i>	
Visualization and Explanation of Payload-Based Anomaly Detection	29
<i>Konrad Rieck and Pavel Laskov</i>	
Integrated Detection of Attacks Against Browsers, Web Applications and Databases	37
<i>C. Criscione, G. Salvaneschi, F. Maggi, and S. Zanero</i>	
Self-Routing Denial-of-Service Resistant Capabilities Using In-packet Bloom Filters	46
<i>Christian Esteve Rothenberg, Petri Jokela, Pekka Nikander, Mikko Sarela, and Jukka Ylitalo</i>	
The Dorothy Project: An Open Botnet Analysis Framework for Automatic Tracking and Activity Visualization	52
<i>Marco Cremonini and Marco Riccardi</i>	
Author Index	55