2010 European Conference on Computer Network Defense

(EC2ND 2010)

Berlin, Germany
28-29 October 2010

IEEE Catalog Number: CFP1036F-PRT
ISBN: 978-1-4244-9377-7

2010 European Conference on Computer Network Defense

EC2ND 2010

Table of Contents

Message from the Program Chair....................vii

Organizing Committee....................viii

Malicious Software

Embedded Malware - An Analysis of the Chuck Norris Botnet 3
Pavel Čeleda, Radek Krejčí, Jan Vykopal, and Martin Drašar

Experiences and Observations from the NoAH Infrastructure 11
Georgios Kontaxis, Iasonas Polakis, Spiros Antonatos, and Evangelos P. Markatos

Privacy and Availability

iLeak: A Lightweight System for Detecting Inadvertent Information Leaks 21
Vasileios P. Kemerlis, Vasilis Pappas, Georgios Portokalidis, and Angelos D. Keromytis

HTTPreject: Handling Overload Situations without Losing the Contact to the User 29
Joerg Schneider and Sebastian Koch

Vulnerability Discovery

An Evolutionary Computing Approach for Hunting Buffer Overflow Vulnerabilities: A Case of Aiming in Dim Light 37
Sanjay Rawat and Laurent Mounier

USB Device Drivers: A Stepping Stone into Your Kernel 46
Moritz Jodeit and Martin Johns

Intrusion Detection

Response Initiation in Distributed Intrusion Response Systems for Tactical MANETs 55
Gabriel Klein, Henning Rogge, Felix Schneider, Jens Toelle, Marko Jahnke, and Stefan Karsch

Empirical Evaluation of the Internet Analysis System for Application in the Field of Anomaly Detection 63
Harald Lampesberger

Author Index 71