Contents

Botnet Detection Based on Network Behavior
W. Timothy Strayer, David Lapsely, Robert Walsh, and Carl Livadas ........ 1

Honeynet-based Botnet Scan Traffic Analysis
Zhichun Li, Anup Goyal, and Yan Chen ................................. 25

Characterizing Bots’ Remote Control Behavior
Elizabeth Stinson and John C. Mitchell .................................. 45

Automatically Identifying Trigger-based Behavior in Malware
David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Dawn Song,
and Heng Yin .................................................................. 65

Towards Sound Detection of Virtual Machines
Jason Franklin, Mark Luk, Jonathan M. McCune, Arvind Seshadri, Adrian
Perrig, Leendert van Doorn .................................................. 89

Botnets and Proactive System Defense
John Bambenek and Agnes Klus .......................................... 117

Detecting Botnet Membership with DNSBL Counterintelligence
Anirudh Ramachandran, Nick Feamster, and David Dagon .............. 131

A Taxonomy of Botnet Structures
David Dagon, Guofei Gu, Christopher P. Lee .......................... 143
Botnet Detection
Countering the Largest Security Threat
Lee, W.; Wang, C.; Dagon, D. (Eds.)
2008, XII, 168 p., Hardcover
ISBN: 978-0-387-68766-7