

Table of Contents

Malware and SPAM

A Case Study on Asprox Infection Dynamics	1
<i>Youngsang Shin, Steven Myers, and Minaxi Gupta</i>	
How Good Are Malware Detectors at Remediating Infected Systems? ...	21
<i>Emanuele Passerini, Roberto Paleari, and Lorenzo Martignoni</i>	
Towards Proactive Spam Filtering (Extended Abstract)	38
<i>Jan Göbel, Thorsten Holz, and Philipp Trinius</i>	

Emulation-Based Detection

Shepherding Loadable Kernel Modules through On-demand Emulation	48
<i>Chaoting Xuan, John Copeland, and Raheem Beyah</i>	
Yataglass: Network-Level Code Emulation for Analyzing Memory-Scanning Attacks	68
<i>Makoto Shimamura and Kenji Kono</i>	
Defending Browsers against Drive-by Downloads: Mitigating Heap-Spraying Code Injection Attacks	88
<i>Manuel Egele, Peter Wurzinger, Christopher Kruegel, and Engin Kirda</i>	

Software Diversity

Polymorphing Software by Randomizing Data Structure Layout	107
<i>Zhiqiang Lin, Ryan D. Riley, and Dongyan Xu</i>	
On the Effectiveness of Software Diversity: A Systematic Study on Real-World Vulnerabilities	127
<i>Jin Han, Debin Gao, and Robert H. Deng</i>	

Harnessing Context

Using Contextual Information for IDS Alarm Classification (Extended Abstract)	147
<i>François Gagnon, Frédéric Massicotte, and Babak Esfandiari</i>	

Browser Fingerprinting from Coarse Traffic Summaries: Techniques and Implications	157
<i>Ting-Fang Yen, Xin Huang, Fabian Monroe, and Michael K. Reiter</i>	
A Service Dependency Modeling Framework for Policy-Based Response Enforcement	176
<i>Nizar Kheir, Hervé Debar, Frédéric Cuppens, Nora Cuppens-Boulahia, and Jouni Viinikka</i>	
 Anomaly Detection	
Learning SQL for Database Intrusion Detection Using Context-Sensitive Modelling (Extended Abstract)	196
<i>Christian Bockermann, Martin Apel, and Michael Meier</i>	
Selecting and Improving System Call Models for Anomaly Detection ...	206
<i>Alessandro Frossi, Federico Maggi, Gian L. Rizzo, and Stefano Zanero</i>	
 Author Index	 225