

Contents

Attacks

Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks	3
<i>Amin Kharraz, William Robertson, Davide Balzarotti, Leyla Bilge, and Engin Kirda</i>	
“Nice Boots!” - A Large-Scale Analysis of Bootkits and New Ways to Stop Them	25
<i>Bernhard Grill, Andrei Bacs, Christian Platzer, and Herbert Bos</i>	
C5: Cross-Cores Cache Covert Channel	46
<i>Clémentine Maurice, Christoph Neumann, Olivier Heen, and Aurélien Francillon</i>	

Attack Detection

Intrusion Detection for Airborne Communication Using PHY-Layer Information	67
<i>Martin Strohmeier, Vincent Lenders, and Ivan Martinovic</i>	
That Ain’t You: Blocking Spearphishing Through Behavioral Modelling	78
<i>Gianluca Stringhini and Olivier Thonnard</i>	
Robust and Effective Malware Detection Through Quantitative Data Flow Graph Metrics.	98
<i>Tobias Wüchner, Martín Ochoa, and Alexander Pretschner</i>	

Binary Analysis and Mobile Malware Protection

Jackdaw: Towards Automatic Reverse Engineering of Large Datasets of Binaries	121
<i>Mario Polino, Andrea Scorti, Federico Maggi, and Stefano Zanero</i>	
Fine-Grained Control-Flow Integrity Through Binary Hardening	144
<i>Mathias Payer, Antonio Barresi, and Thomas R. Gross</i>	
Powerslave: Analyzing the Energy Consumption of Mobile Antivirus Software	165
<i>Iasonas Polakis, Michalis Diamantaris, Thanasis Petsas, Federico Maggi, and Sotiris Ioannidis</i>	

Social Networks and Large-Scale Attacks

The Role of Cloud Services in Malicious Software: Trends and Insights	187
<i>Xiao Han, Nizar Kheir, and Davide Balzarotti</i>	
Capturing DDoS Attack Dynamics Behind the Scenes	205
<i>An Wang, Aziz Mohaisen, Wentao Chang, and Songqing Chen</i>	
Quit Playing Games with My Heart: Understanding Online Dating Scams . . .	216
<i>JingMin Huang, Gianluca Stringhini, and Peng Yong</i>	

Web and Mobile Security

More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations	239
<i>Ethan Shernan, Henry Carter, Dave Tian, Patrick Traynor, and Kevin Butler</i>	
May I? - Content Security Policy Endorsement for Browser Extensions	261
<i>Daniel Hausknecht, Jonas Magazinius, and Andrei Sabelfeld</i>	
On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users	282
<i>Yanick Fratantonio, Antonio Bianchi, William Robertson, Manuel Egele, Christopher Kruegel, Engin Kirda, and Giovanni Vigna</i>	

Provenance and Data Sharing

Identifying Intrusion Infections via Probabilistic Inference on Bayesian Network	307
<i>Yuan Yang, Zhongmin Cai, Weixuan Mao, and Zhihai Yang</i>	
Controlled Data Sharing for Collaborative Predictive Blacklisting	327
<i>Julien Freudiger, Emiliano De Cristofaro, and Alejandro E. Brito</i>	

Author Index	351
-------------------------------	-----

Detection of Intrusions and Malware, and Vulnerability
Assessment

12th International Conference, DIMVA 2015, Milan, Italy,
July 9-10, 2015, Proceedings

Almgren, M.; Gulisano, V.; Maggi, F. (Eds.)

2015, XII, 351 p. 98 illus., Softcover

ISBN: 978-3-319-20549-6