1. Record Nr. UNINA9910484264903321

Titolo	Detection of Intrusions and Malware, and Vulnerability Assessment : 12th International Conference, DIMVA 2015, Milan, Italy, July 9-10, 2015, Proceedings / / edited by Magnus Almgren, Vincenzo Gulisano, Federico Maggi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-20550-1
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XII, 351 p. 98 illus.)
Collana	Security and Cryptology ; ; 9148
Disciplina	005.8
Soggetti	Computer security E-commerce Management information systems Computer science Systems and Data Security e-Commerce/e-business Management of Computing and Information Systems
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Attacks -- Cutting the Gordian Knot: A Look Under the Hood of Ransomware Attacks -- 1 Introduction -- 2 Ransomware Data Set -- 2.1 Experimental Setup -- 3 Characterization and Evolution -- 3.1 File System Activity -- 3.2 Mitigation Strategies -- 4 Financial Incentives -- 4.1 Bitcoin as a Charging Method -- 5 Related Work -- 6 Conclusion -- References -- ``Nice Boots!'' - A Large-Scale Analysis of Bootkits and New Ways to Stop Them -- 1 Introduction -- 2 How Bootkits Interfere with the Boot Process -- 3 A Large Scale Analysis of Bootkit Technology -- 3.1 Large-Scale Bootkit Analysis Results -- 3.2 Historic Perspective on the Evolution of Bootkit Technology -- 4 Detecting and Preventing Bootkit Infections -- 4.1 Detecting Bootkit Attacks -- 4.2 Preventing Bootkit Infections -- 5 Bootcamp -- 6 Bootcamp Evaluation -- 6.1 Bootkit Detection Results -- 6.2 Bootkit Prevention Results -- 7 Discussion and

Limitations -- 8 Related Work -- 9 Conclusion -- References -- C5: Cross-Cores Cache Covert Channel -- 1 Introduction -- 2 Background -- 2.1 Cache Fundamentals -- 2.2 Playing with Caches for Fun and Profit -- 2.3 The Problem of Addressing Uncertainty -- 3 C5 Covert Channel -- 3.1 Sender -- 3.2 Receiver -- 4 Experiments -- 4.1 Testbed -- 4.2 Native Environment -- 4.3 Virtualized Environment -- 4.4 Complex Addressing Matters -- 5 Discussion -- 5.1 Performance -- 5.2 Mitigation -- 6 Related Work -- 7 Conclusion -- References -- Attack Detection -- Intrusion Detection for Airborne Communication Using PHY-Layer Information -- 1 Introduction -- 2 Overview of ADS-B Security Concerns -- 3 Modeling False-Data Injection Attackers -- 4 Intrusion Detection -- 5 Experimental Design -- 6 Results -- 7 Conclusion and Future Work -- References -- That Ain't You: Blocking Spearphishing Through Behavioral Modelling.
1 Introduction -- 2 Behavioral Profiles -- 2.1 Features Characterizing an Email -- 2.2 Building Behavioral Profiles -- 3 Detecting Anomalous Emails -- 4 Evaluation -- 4.1 Evaluation Datasets -- 4.2 Analysis of the Classifier -- 4.3 Detecting Attack Emails -- 4.4 Performance of IdentityMailer -- 5 Discussion and Limitations -- 6 Related Work -- 7 Conclusions -- References -- Robust and Effective Malware Detection Through Quantitative Data Flow Graph Metrics -- 1 Introduction -- 2 Preliminaries -- 2.1 Quantitative Data Flow Model -- 2.2 Windows Instantiation -- 3 Approach -- 3.1 Features -- 3.2 Training and Model Building Phase -- 3.3 Detection Phase -- 4 Evaluation -- 4.1 Prototype -- 4.2 Effectiveness -- 4.3 Efficiency -- 4.4 Summary and Threats to Validity -- 5 Related Work -- 6 Discussion and Conclusion -- References -- Binary Analysis and Mobile Malware Protection -- Jackdaw: Towards Automatic Reverse Engineering of Large Datasets of Binaries -- 1 Introduction -- 2 Binary Analysis and Reverse Engineering -- 3 System Details -- 3.1 Step 1: Data Collection -- 3.2 Step 2: Clustering of Data-Flow Information -- 3.3 Step 3: Behavior Extraction -- 3.4 Step 4: Semantic Tagging -- 4 Experimental Evaluation -- 4.1 Dataset and Ground Truth -- 4.2 Parameter Estimation -- 4.3 Clustering Validation (Step 2) -- 4.4 Behavior Evaluation (Step 3) -- 5 Limitations and Future Work. -- 6 Related Work -- 7 Conclusions -- References -- Fine-Grained Control-Flow Integrity Through Binary Hardening -- 1 Introduction -- 2 Attack Model -- 3 Background and Related Work -- 3.1 Control-Flow Integrity -- 3.2 Dynamic Binary Translation -- 4 Lockdown Design -- 4.1 Rules for Control Transfers -- 4.2 Control Transfer Guards -- 4.3 Handling Stripped Binaries -- 5 Prototype Implementation -- 5.1 Runtime Optimizations -- 5.2 Control-Flow Particularities.
5.3 Implementation Heuristics -- 5.4 Binary Compatibility -- 6 Evaluation -- 6.1 Performance -- 6.2 Apache Case Study -- 6.3 Security and CFI Effectiveness Case-Study -- 6.4 Security Guarantees -- 7 Conclusion -- References -- Powerslave: Analyzing the Energy Consumption of Mobile Antivirus Software -- 1 Introduction -- 2 Energy Measurements -- 3 Experimental Setup and Datasets -- 4 Experimental Results -- 4.1 Energy Consumption vs. Scan Duration -- 4.2 Energy Consumption vs. Detection Outcome -- 4.3 Upon Installation vs. on Demand Detection -- 4.4 Size Does Matter -- 4.5 Display vs. CPU Energy Consumption -- 4.6 Internet Connectivity (WiFi) -- 5 Efficiency Guidelines -- 5.1 Detection Heuristics and Behavior -- 5.2 Visual Design -- 6 Limitations and Future Work -- 7 Related Work -- 8 Conclusion -- References -- Social Networks and Large-Scale Attacks -- The Role of Cloud Services in Malicious Software: Trends and Insights -- 1 Introduction -- 2 Approach -- 2.1 Platform Description -- 3 Experiments -- 3.1 Role of Public Cloud Services in Malware

Infrastructures -- 3.2 Dedicated Domains Lifetime Estimation -- 4 Discussion -- 5 Related Work -- 6 Conclusion -- References -- Capturing DDoS Attack Dynamics Behind the Scenes -- 1 Introduction -- 2 Dataset Collection -- 3 Attack Dynamics -- 3.1 Bots Shift Pattern Analysis -- 3.2 Mathematical Representation of Shift Patterns -- 4 Related Work -- 5 Conclusion -- References -- Quit Playing Games with My Heart: Understanding Online Dating Scams -- 1 Introduction -- 2 Background and Problem Study -- 2.1 Online Dating Sites -- 2.2 Case Study: Jiayuan -- 2.3 Threat Model: Online Dating Scams -- 3 Methodology -- 3.1 Behavioral-Based Detection System -- 3.2 IP Address-Based Detection System -- 3.3 Photograph-Based Detection System -- 3.4 Text-Based Detection System -- 4 Description of the Scam Account Dataset.
5 A Taxonomy of Online Dating Scammers -- 6 Analysis of the Scam Account Dataset -- 6.1 Demographics of Different Scam Account Types -- 6.2 Strategies Used by Different Scam Account Types -- 7 Discussion -- 7.1 Scammers Are Perseverant -- 7.2 Future Work -- 8 Related Work -- 9 Conclusions -- References -- Web and Mobile Security -- More Guidelines Than Rules: CSRF Vulnerabilities from Noncompliant OAuth 2.0 Implementations -- 1 Introduction -- 2 Background -- 2.1 Authorization Code Flow -- 2.2 Cross Site Request Forgery -- 3 Attack -- 3.1 CSRF in OAuth -- 3.2 Developer Implementation Problems -- 3.3 Mitigation -- 4 CSRF in the Wild -- 4.1 Web Crawler Design and Implementation -- 4.2 Data Collection Setup -- 4.3 Results -- 5 Case Studies -- 5.1 Missing Documentation -- 5.2 Incorrect Code Samples -- 5.3 Inconsistent Requirements -- 5.4 Lack of Enforcement -- 5.5 Recommended Approaches to Mitigation -- 6 Discussion -- 6.1 Comparison to HTTPS Use -- 6.2 OAuth 1.0 -- 7 Related Work -- 8 Conclusion -- References -- May I? - Content Security Policy Endorsement for Browser Extensions -- 1 Introduction -- 2 Empirical Study -- 2.1 Extension Analysis -- 3 Extension Framework Analysis -- 3.1 Resource Loading Through Content Scripts -- 3.2 Case Study: Rapportive -- 4 CSP Endorsement -- 4.1 Endorsement Workflow -- 4.2 Prototype Implementation -- 5 Evaluation -- 5.1 Experiment Set-Up -- 5.2 Results -- 6 Related Work -- 7 Conclusion -- References -- On the Security and Engineering Implications of Finer-Grained Access Controls for Android Developers and Users -- 1 Introduction -- 2 Overview -- 3 System Details -- 3.1 Symbolic Executor -- 3.2 Policy Extractor -- 3.3 Application Rewriter -- 4 Practicality Evaluation -- 4.1 Results and Quality of Static Analysis -- 4.2 Quality of the Security Policies -- 4.3 Size of the Security Policies.
4.4 Discussion and Limitations -- 5 Viable Workflows -- 6 Security Implications and Benefits -- 7 Related Work -- 8 Conclusion and Future Work -- References -- Provenance and Data Sharing -- Identifying Intrusion Infections via Probabilistic Inference on Bayesian Network -- 1 Introduction -- 2 Related Work -- 3 Temporal Dependency Network -- 3.1 Dependency Relationships -- 3.2 Temporal Dependency Network -- 4 Proposed Method -- 4.1 Problem Description -- 4.2 Overview -- 4.3 Probabilistic Bayesian Network Model -- 4.4 Probabilistic Inference -- 5 Experimental Evaluation -- 5.1 Data Set -- 5.2 Methodology -- 5.3 Experiment Results -- 6 Conclusion -- References -- Controlled Data Sharing for Collaborative Predictive Blacklisting -- 1 Introduction -- 1.1 Problem Statement -- 1.2 Roadmap -- 2 Related Work -- 3 Preliminaries -- 3.1 System Model -- 3.2 Cryptographic Tools -- 3.3 Predictive Blacklisting -- 4 Collaborative Predictive Blacklisting via Controlled Data Sharing -- 4.1 Benefit Estimation -- 4.2 Establishing Partnerships -- 4.3 Data Sharing -- 5 The DShield Dataset -- 5.1

Original Dataset -- 5.2 Measurements and Observations -- 5.3 Final Dataset -- 6 Experimental Analysis -- 6.1 Experimental Setup -- 6.2 Different Benefit Estimation Metrics -- 6.3 Analysis -- 6.4 Different Sharing Strategies -- 6.5 Performance of Cryptographic Tools -- 6.6 Take-Aways -- 7 Conclusion -- References -- Author Index.

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, DIMVA 2015, held in Milan, Italy, in July 2015. The 17 revised full papers presented were carefully reviewed and selected from 75 submissions. The papers are organized in topical sections on attacks, attack detection, binary analysis and mobile malware protection, social networks and large-scale attacks, Web and mobile security, and provenance and data sharing.