1. Record Nr. UNINA9910484521703321

Titolo	Recent advances in intrusion detection : 12th international symposium, RAID 2009, Saint-Malo, France, September 23-25, 2009 : proceedings / / Engin Kirda, Somesh Jha, Davide Balzarotti (eds.)
Pubbl/distr/stampa	Berlin ; ; New York, : Springer, c2009
ISBN	3-642-04342-9
Edizione	[1st ed. 2009.]
Descrizione fisica	1 online resource (XIII, 384 p.)
Collana	Lecture notes in computer science, , 0302-9743 ; ; 5758 LNCS sublibrary. SL 4, Security and cryptology
Classificazione	DAT 055f DAT 460f SS 4800
Altri autori (Persone)	KirdaEngin JhaSomesh BalzarottiDavide
Disciplina	005.8
Soggetti	Computer security Computers - Access control
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	Recent Advances in Intrusion Detection Anomaly and Specification-Based Approaches -- Panacea: Automating Attack Classification for Anomaly-Based Network Intrusion Detection Systems -- Protecting a Moving Target: Addressing Web Application Concept Drift -- Adaptive Anomaly Detection via Self-calibration and Dynamic Updating -- Runtime Monitoring and Dynamic Reconfiguration for Intrusion Detection Systems -- Malware Detection and Prevention (I) -- Malware Behavioral Detection by Attribute-Automata Using Abstraction from Platform and Language -- Automatic Generation of String Signatures for Malware Detection -- PE-Miner: Mining Structural Information to Detect Malicious Executables in Realtime -- Network and Host Intrusion Detection and Prevention -- Automatically Adapting a Trained Anomaly Detector to Software Patches -- Towards Generating High Coverage Vulnerability-Based Signatures with Protocol-Level Constraint-Guided Exploration -- Automated Behavioral Fingerprinting -- Intrusion Detection for Mobile Devices -- SMS-Watchdog: Profiling Social

Behaviors of SMS Users for Anomaly Detection -- Keystroke-Based User Identification on Smart Phones -- VirusMeter: Preventing Your Cellphone from Spies -- High-Performance Intrusion Detection -- Regular Expression Matching on Graphics Hardware for Intrusion Detection -- Multi-byte Regular Expression Matching with Speculation -- Malware Detection and Prevention (II) -- Toward Revealing Kernel Malware Behavior in Virtual Execution Environments -- Exploiting Temporal Persistence to Detect Covert Botnet Channels -- Posters -- An Experimental Study on Instance Selection Schemes for Efficient Network Anomaly Detection -- Automatic Software Instrumentation for the Detection of Non-control-data Attacks -- BLADE: Slashing the Invisible Channel of Drive-by Download Malware -- CERN Investigation of Network Behaviour and Anomaly Detection -- Blare Tools: A Policy-Based Intrusion Detection System Automatically Set by the Security Policy -- Detection, Alert and Response to Malicious Behavior in Mobile Devices: Knowledge-Based Approach -- Autonomic Intrusion Detection System -- ALICE@home: Distributed Framework for Detecting Malicious Sites -- Packet Space Analysis of Intrusion Detection Signatures -- Traffic Behaviour Characterization Using NetMate -- On the Inefficient Use of Entropy for Anomaly Detection -- Browser-Based Intrusion Prevention System -- Using Formal Grammar and Genetic Operators to Evolve Malware -- Method for Detecting Unknown Malicious Executables -- Brave New World: Pervasive Insecurity of Embedded Network Devices -- DAEDALUS: Novel Application of Large-Scale Darknet Monitoring for Practical Protection of Live Networks.

Sommario/riassunto

This book constitutes the refereed proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection, RAID 2009, held in Saint-Malo, Brittany, France, in September 2009. The 17 revised full papers presented together with 16 revised poster papers were carefully reviewed and selected from 59 submissions. The papers are organized in topical sections on anomaly and specification-based approaches, malware detection and prevention, network and host intrusion detection and prvention, intrusion detection for mobile devices, and high-performance intrusion detection.