1. Record Nr. UNINA9910451034703321

Autore	Boyce David George <1942->
Titolo	Nationalism in Ireland [[electronic resource]]
Pubbl/distr/stampa	London, : Routledge, 1995
Edizione	[3rd ed.]
Descrizione fisica	1 online resource (502 p.)
Disciplina	320.509415 320.5409415
Soggetti	Nationalism Nationalism - Ireland Political Science Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di contenuto	Book Cover; Title; Contents; Introduction: Nationalism and Ireland; Colony and Nation; Intimations of Nationalism in Tudor Ireland; For God, King and Country; From English Colony to Irish Nation: The Protestant Experience; 'The Irish, Properly So Called'; Patterns of Nationalism, 1842 1870; The Making of Parnellism and Its Undoing; The Battle of Three Civilizations; What Home Rule Stood For, 1891 1918; Nationalism, Socialism and the Irish Revolution; State and Nation in Modern Ireland; Conclusion: Ireland and Nationalism; Epilogues: History, Politics and Nationalism Contemporary Ireland: Nationalist and Post-Nationalist?Appendix; Maps; Bibliography; Supplementary Bibliography; Index;
Sommario/riassunto	Boyce examines the relationship between ideas and political and social reality. A new final chapter considers the development of nationalism in both parts of Ireland, and places the phenomenon of nationalism in a contemporary and European setting

2. Record Nr. UNINA9910760297803321

Titolo	Cyber Malware : Offensive and Defensive Systems / / edited by Iman Almomani, Leandros A. Maglaras, Mohamed Amine Ferrag, Nick Ayres
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2024
ISBN	3-031-34969-5 9783031349690
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (xxxvi, 280 pages) : illustrations
Collana	Security Informatics and Law Enforcement, , 2523-8515
Disciplina	929.605 005.88
Soggetti	Telecommunication Computer crimes Data protection Security systems Communications Engineering, Networks Cybercrime Data and Information Security Security Science and Technology
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Part 1. Android Malware Analysis -- Chapter 1. A Deep Vision-based Multi-Class Classification System of Android Malware Apps -- Chapter 2. Android Malware detection based on network analysis and federated learning -- Chapter 3. ASParseV3: Auto Static Parser & Customizable Visualizer -- Part 2. Network Malware Analysis -- Chapter 4. Fast Flux Service Networks: Architecture, Characteristics and Detection Mechanisms -- Chapter 5. Efficient Graph-based Malware Detection using Minimized Kernel and SVM -- Chapter. 6 Deep Learning for Windows Malware Analysis -- Part 3. IoT Malware Analysis -- Chapter 7. Malware analysis for IoT and Smart AI-based Applications -- Chapter 8. A Multi-Class Classification Approach for IoT Intrusion Detection Based on Feature Selection and Oversampling -- Chapter 9. Malware Mitigation in Cloud Computing Architecture.

Sommario/riassunto

This book provides the foundational aspects of malware attack vectors and appropriate defense mechanisms against malware. The book equips readers with the necessary knowledge and techniques to successfully lower the risk against emergent malware attacks. Topics cover protections against malware using machine learning algorithms, Blockchain and AI technologies, smart AI-based applications, automated detection-based AI tools, forensics tools, and much more. The authors discuss theoretical, technical, and practical issues related to cyber malware attacks and defense, making it ideal reading material for students, researchers, and developers. Presents theoretical, technical, and practical knowledge on defending against malware attacks; Covers malware applications using machine learning algorithms, Blockchain and AI, forensics tools, and much more; Includes perspectives from experts in cybersecurity at different institutions, including academia, research centers, and companies.