1. Record Nr. UNISA996464517003316

Autore	Alvari Hamidreza
Titolo	Identification of pathogenic social media accounts : from data to intelligence to prediction / / Hamidreza Alvari, Elham Shaabani, Paulo Shakarian
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2021] Â©2021
ISBN	3-030-61431-X
Edizione	[1st ed. 2021.]
Descrizione fisica	1 online resource (IX, 95 p. 25 illus., 19 illus. in color.)
Collana	SpringerBriefs in Computer Science
Disciplina	006.754
Soggetti	Online social networks - Security measures Computer networks - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Sommario/riassunto	This book sheds light on the challenges facing social media in combating malicious accounts, and aims to introduce current practices to address the challenges. It further provides an in-depth investigation regarding characteristics of “Pathogenic Social Media (PSM),”by focusing on how they differ from other social bots (e.g., trolls, sybils and cyborgs) and normal users as well as how PSMs communicate to achieve their malicious goals. This book leverages sophisticated data mining and machine learning techniques for early identification of PSMs, using the relevant information produced by these bad actors. It also presents proactive intelligence with a multidisciplinary approach that combines machine learning, data mining, causality analysis and social network analysis, providing defenders with the ability to detect these actors that are more likely to form malicious campaigns and spread harmful disinformation. Over the past years, social media has played a major role in massive dissemination of misinformation online. Political events and public opinion on the Web have been allegedly manipulated by several forms of accounts including “Pathogenic Social Media (PSM)” accounts (e.g., ISIS supporters and fake news writers). PSMs are key users in spreading misinformation on social media - in

viral proportions. Early identification of PSMs is thus of utmost importance for social media authorities in an effort toward stopping their propaganda. The burden falls to automatic approaches that can identify these accounts shortly after they began their harmful activities. Researchers and advanced-level students studying and working in cybersecurity, data mining, machine learning, social network analysis and sociology will find this book useful. Practitioners of proactive cyber threat intelligence and social media authorities will also find this book interesting and insightful, as it presents an important and emerging type of threat intelligence facing social media and the general public.