A Survey of Malware Analysis Using Community Detection Algorithms

ABDELOUAHAB AMIRA, Research Center for Scientific and Technical Information (CERIST), Algeria, and Departement Informatique, Faculté des Sciences Exactes, Universite de Béjaia, Algeria
ABDELOUAHID DERHAB, Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia
ELMOUATEZ BILLAH KARBAB, Security Research Centre, Concordia University, Canada
OMAR NOUALI, Research Center for Scientific and Technical Information (CERIST), Algeria

In recent years, we have witnessed an overwhelming and fast proliferation of different types of malware targeting organizations and individuals, which considerably increased the time required to detect malware. The malware developers make this issue worse by spreading many variants of the same malware [13]. To deal with this issue, graph theory techniques, and particularly community detection algorithms, can be leveraged to achieve bulk detection of malware families and variants to identify malicious communities instead of focusing on the detection of an individual instance of malware, which could significantly reduce the detection time. In this article, we review the state-of-the-art malware analysis solutions that employ community detection algorithms and provide a taxonomy that classifies the solutions with respect to five facets: analysis task, community detection approach, target platform, analysis type, and source of features. We present the solutions with respect to the analysis task, which covers malware detection, malware classification, cyber-threat infrastructure detection, and feature selection. The findings of this survey indicate that there is still room for contributions to further improve the state of the art and address research gaps. Finally, we discuss the advantages and the limitations of the solutions, identify open issues, and provide future research directions.

CCS Concepts: • **Security and privacy → Malware and its mitigation;**

Additional Key Words and Phrases: Malware analysis, community detection, cyber-threat infrastructure, feature selection

ACM Reference format:
Abdelouahab Amira, Abdelouahid Derhab, ElMouatez Billah Karbab, and Omar Nouali. 2023. A Survey of Malware Analysis Using Community Detection Algorithms. *ACM Comput. Surv.* 56, 2, Article 40 (September 2023), 29 pages.
https://doi.org/10.1145/3610223

Authors' addresses: A. Amira, Research Center for Scientific and Technical Information (CERIST), 16000 Algiers, Algeria, and Departement Informatique, Faculté des Sciences Exactes, Universite de Béjaia, 06000 Béjaia, Algeria; email: amira@cerist.dz; A. Derhab, Center of Excellence in Information Assurance (CoEIA), King Saud University, Riyadh, Saudi Arabia, 11451; email: abderhab@ksu.edu.sa; E. B. Karbab, Security Research Centre, Concordia University, Montreal, Canada; email: elmouatez.karbab@concordia.ca; O. Nouali, Research Center for Scientific and Technical Information (CERIST), 16000 Algiers, Algeria; email: onouali@cerist.dz.

0360-0300/2023/09-ART40 $15.00
https://doi.org/10.1145/3610223