8-10-2022

A Systematic Review on Using Hacker Forums on the Dark Web for Cyber Threat Intelligence

Abdullah Albizri
Montclair State University, albizria@montclair.edu

Alaa Nehme
Mississippi State University, a.nehme@msstate.edu

Antoine Harfouche
Univ Paris Nanterre, harfoant@yahoo.com

A Systematic Review on Using Hacker Forums on the Dark Web for Cyber Threat Intelligence

TREO Talk Paper

Abdullah Albizri
Montclair State University
albizria@montclair.edu

Alaa Nehme
Mississippi State University
a.nehme@msstate.edu

Antoine Harfouche
Université Paris Nanterre
antoine.h@parisnanterre.fr

Abstract

Urgent warnings for private businesses and public organizations to monitor and predict disruptive cyberattacks have been on the rise. The annual cost of cyber-attacks in the worldwide economy is expected to be more than $10.5 trillion in 2025. To that end, new methods are being developed to fight cyberattacks.

One such method builds upon leveraging cybercriminal/hacker forums on the dark web to design 'cyberthreat intelligence' solutions. The dark web, which is not accessible by the conventional browsers that are normally used to access the surface web, is the part of the web where most of the illegal and illicit content is hosted. It is a major market resource for cybercriminal-hackers for trading and developing cyberthreat content (e.g., malware; novel hacking methods; malicious source code). Therefore, the study of designing cyber threat intelligence solutions (i.e., methods; artifacts) based upon analyzing hacker forums has been undertaken in the literature. To enhance this structured inquiry and to formulate new research directions, we conduct a systematic literature review on leveraging hacker forums and designing 'threat intelligence' solutions.

In our systematic review, we report our findings based on the PRISMA - Preferred Reporting Items for Systematic Reviews and Meta-Analyses - checklist. We conducted our search on Scopus and Ebscohost, and our search query was the following: ("dark web" OR "dark net" OR "darknet" OR "hacker* forum" OR "underground forum") AND ("security" OR "threat intelligence"). Our search included abstracts and English-language documents published in peer-reviewed journals and conferences. We extracted a total of 295 papers and retained 69 papers.

Our findings indicate the proposed threat intelligence solutions have been built upon the analysis of different forms of unstructured data, including text, videos, and images. Different solutions had different objectives, including: (1) key actor (hacker) identification (i.e., identifying the key active hackers on the forum who actively engage in and lead discussions and posts), (2) hacker ranking according to expertise (i.e., ranking the forum participant hackers based on their hacking domain-knowledge expertise reflected in their posts), (3) malware identification (i.e., identifying novel malware from hackers' posts on the forums), and (4) organizational information security risk management and mitigation (i.e., identifying organizational vulnerabilities and developing strategies to mitigate them based on the knowledge retrieved from hacker forums). We found that as of now, the proposed solutions do not consider the factor of temporality, or temporal-based dynamism, in the forums. Key hackers may change, expertise may change, and vulnerabilities may evolve in organizations. We hope that our review catalyzes future research in this area.