International Journal of Cyber Warfare and Terrorism
Volume 14 • Issue 1

Perceptual Operating Systems for the Trade Associations of Cyber Criminals to Scrutinize Hazardous Content

Romil Rawat, Department of Computer Science Engineering, Shri Vaishnav Institute of Information Technology, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India*

Anand Rajavat, Department of Computer Science Engineering, Shri Vaishnav Institute of Information Technology, Shri Vaishnav Vidyapeeth Vishwavidyalaya, Indore, India

ABSTRACT

The limits of user visibility have been exceeded by the internet. The "Dark Web" or "Dark Net" refers to certain unknown portions of the internet that cannot be found using standard search methods. A number of computerised techniques are being explored to extract or crawl the concealed data. All users can freely interact on the surface web. Identity identities may be found on the deep web, and the dark web (DW), a hub for anonymous data, is a haven for terrorists and cybercriminals to promote their ideologies and illegal activities. Officials in clandestine surveillance and cyberpolicing are always trying to track down offenders' trails or hints. The search for DW offenders might take five to ten years.The proposed study provides data from a DW mining and online marketplaces situation from a few domains, as well as an overview for investigators to build an automated engine for scraping all dangerous information from related sites.

KEYWORDS

Content Crawling, Cyber Attack, Dark E-Markets, Darkweb, Healthcare, Terrorist, Tor Network, Web Crawler

1. INTRODUCTION

A shadow economy (Gupta et al, 2021) (Weimann,2016) (Tsuchiya & Hiramoto, 2021) by Squires in 2021 A darknet (DN) business website called (Sonmez & Codal, 2022) leverages services like Tor or I2P (Gupta et al., 2021). (Weimann, 2016). They typically act as "black market places (MPS)", selling or brokering deals involving illegal items such as drugs, cyber-arms, weapons, hijacked credit card details, forged documents, anabolic steroids, and other illegal assets (Rawat, 2023). DN marketplaces were the second-most popular Tor sites, per a study by the University of Portsmouth's (Squires, 2021) and (Sonmez & Codal, 2022) researchers.

Numerous evil organisations, including terrorist organisations and hackers, are drawn to the DW's uncontrolled and unregulated character (Gupta et al., 2021). Terrorist organisations may sell their ideas, recruit, share skills, train, market, finance, target, and develop diverse communities without

DOI: 10.4018/IJCWT.343314 *Corresponding Author

concern for location or even the presence of a local leader thanks to the DW's anonymity features (Weimann, 2016) (Sonmez & Codal, 2022).

Similarly, the DW (Wang et al., 2021) enables anonymous information sharing among hackers. DW forums are frequently the subject of many types of surveillance, ranging from manual observation to crawling mixed with natural language processing (NLP) (Saharan et al., 2024) techniques for automated threat intelligence. Terrorism or cybercrime (Gupta et al., 2021) that individuals or well-organised organisations can carry out (Weimann, 2016)(Tsuchiya & Hiramoto, 2021) on the DW. Cybercrime is becoming more accessible to anybody who wants to engage in low-risk illegal activities while still making a difference (for example, launching DDoS (Alshammery & Aljuboori, 2022) assaults on websites is as simple as contracting a botnet that provides DDoS-as-a-Service). These services allow criminals to take advantage of the "low hanging fruit" (targets without adequate security controls or training). Tor's hidden services can let attackers and victims maintain command-and-control (C2) (Gupta et al., 2021)(Weimann, 2016) (Sonmez & Codal, 2022) communications. Tor's anonymity (and difficulties in shutting it down) is excellent for C2 servers, and it is one of the most widely used hidden services.

States are concerned about the necessity of preparing for digital warfare (Saharan et al., 2024), particularly when it impacts critical infrastructure (CI) and industrial control systems (ICS) and has the potential to have negative real-world consequences. Because of the asymmetry of the wartime environment, it is even easier to become a cybercriminal (Fu & Li, 2021). Despite the fact that cybercriminals are not as well-funded or resourced as the organisations they target, they have an edge on the digital battlefield because they can select their tactics, timing, and location, whereas defenders must always be alert. Deterrence and dissuasion have been effective military measures in the past for a variety of reasons, including the high barrier to entry into nuclear weapons (Gupta et al., 2021) (Weimann, 2016)(Tsuchiya & Hiramoto, 2021)(Squires, 2021). This does not apply in cyberspace, because a weapon may be simply coded or purchased on the DW. Deterrence is no longer just the realm of states, since non-state entities become active players in cyber warfare against shared adversaries. Terrorist organisations' activity on the surface web has been reduced by law enforcement authorities and hacktivist groups all across the world. These terrorist organisations have shifted to the DW; their followers may anonymously voice their thoughts; their activities can continue to be supported through virtual currencies; and the DW can be used as a possible recruiting (Alshammery & Aljuboori, 2022) and training ground (Alshammery & Aljuboori, 2022). The latter has been linked to a considerable amount of terrorist activity, and NLP is being used to identify it on DW forums (Mili & Rodin, 2022).

The system has an accessibility feature that allows users to register for DW forums with the assistance of a third party. The solution uses a combination of dynamic proxies and topic-specific spidering parameter setups to assure forum access. The URL Ordering (AlKhatib & Basheer, 2019) component uses language-independent URL ordering features to facilitate spidering of DW forums across languages. It is planned to focus on three separate groups from three different regions: the United States, the Middle East, and Latin America/Spain. Along with BFS and DFS crawling crawling(AlKhatib & Basheer, 2019), a rule-based URL sorting technique (Tsuchiya & Hiramoto, 2021) (Cole et al., 2021) is employed (Fu & Li, 2021) to traverse space. This technique is used to limit the number of unwanted web pages acquired. An incremental crawler that decides which threads need to be collected using forum wrappers. The system will contain a recall improvement mechanism that parses the spidering log (Gupta et al., 2021) (Weimann, 2016) and reinserts incomplete downloads into the crawl area. Finally, the system has a collection analyzer that finds duplicate downloads and generates collection statistics (Cole et al., 2021) at the forum, region, and worldwide levels.

Cybercrime poses a severe threat to the institution and its patients by stealing medical records (Ahmad et al., 2022). In many ransomware (Weimann, 2016)(Tsuchiya & Hiramoto, 2021) cases, the hacker would steal patient information and sell it on the DW, which is a secret section of the internet. In 1971 or 1972, Stanford students (Squires, 2021) and their colleagues at the Massachusetts Institute of Technology (MIT) used ARPANET (Advanced Research Projects Agency Network)