How does AI interact with the Dark Web?

Student
Course
Professor
Date

Introduction

Like any other part of the internet, AI can interact with the dark web differently. The dark web is known to be a part of internet intentionally hidden and can only be accessed with specific software such as Tor (Rawat et al. 1). Although dark web is often linked with illegal activities, it also has some legitimate purposes such as privacy, anonymity, and free expression. AI interacts with the dark web in monitoring and surveillance. AI systems can monitor the dark web for illegal activities, including drug sales, hacking tools, stolen data, and illicit goods and services. It can help law enforcement agencies and cyber security firms combat cybercrime since AI automated systems can analyze large amounts of data and identify patterns, hence detecting any possible threat. AI can interact with the dark web in dark web markets. Cybersecurity firms can use AI to understand trends, track the flows of cryptocurrencies, and identify cyber threats. The interaction of AI and the dark web comes with benefits, such as helping individuals understand what the dark web is and how we can use AI to exploit its advantages and regulate its use to avoid its adverse impacts.

Background

The dark web is a small part of the deep web, which contains harmless sites such as email account protection with passwords, some part subscriptions that you must pay for, such as Netflix, and other sites you can only access through online forms. The identities of those who visit these websites are hidden by anonymizing software on their computers, and the dark web will require passwords for access. The main purpose of the dark web is to encrypt any data sent through it by hiding both where the data originated and its destination. Since the launch of AI, forums on the dark web have been trying to find how they can exhaust all the ways they can make use of this technology. Dark web users have been trying to enlighten each other on how to use AI to make their deals look ethical and ensure their safety. The dark web has produced new AI-powered tools and applications designed to cater to cybercriminals' illegal needs. These tools are WormGPT and FraudGPT, which appeared on the dark web and were marketed as an alternative for ChatGPT with no ethical boundaries. As per their anonymous sellers, WormGPT and FraudGPT have a range of features, including unlimited character inputs, memory retention and coding abilities. They are used for offensive purposes such as writing malicious codes, hacking, creating undetectable malware, writing scam content, finding security vulnerabilities, and business email attacks. Research has it that more

than 94% of illegal deals are completed through the dark web (Rawat et al. 1).

Literature Review

According to Basheer et al (2021), the interaction of AI and the dark web poses a big challenge to cybersecurity firms and law enforcement officers. Due to the rapid development being experienced in technology today, dark web activities are advancing from individual acts of theft and vandalism to well-organized acts aiming at high profits (Basheer et al. 1). Companies and cybersecurity firms should consider using more sophisticated techniques to cope with this transformation pace to prevent cyberattacks. AI-driven tools can be used to monitor and survey the dark web for illegal activities, which may include the sale of stolen data, weapons, hacking services, illegal substances, and malware. AI-powered machine learning algorithms can scan and analyze the dark web's hidden forums, websites, and marketplaces. These machines are designed to highlight any suspicious activities or content. It makes it easy to identify potential cyber threats or even criminal activities.

Research by Aloqaily et al (2022) suggests that, though the interaction of AI and the dark web has developed great cybersecurity threats, AI has the potential to evolve cyber threat detection. Various intelligent learning techniques are now integrated into cybersecurity systems (Aloqaily et al. 1). They provide secure and strong ways to preserve private data and delicate systems from cyber-attacks. Some individual and societal data kept by institutions such as hospitals and schools can be at risk of cyberattacks. Cybersecurity firms can use AI to secure individuals, organizations, and society at large data from cyberattacks.

However, research by Musumeci et al (2022) differs from the other authors on the importance of AI in cybersecurity. Their research shows that even with the incorporation of AI in the system of plane known as the Software Defined Networking (SDN), the system is still vulnerable to cyber-attacks (Musumeci et al. 1). A malicious cyber-attack known as Distributed Denial of Service can still affect the operations of SDN either directly or indirectly. It can impair the ability of this controller to function or interfere with its switches' ability to function properly. To improve the situation, these authors believe the developers should improve their incorporation by using AI tools such as Machine learning algorithms. The ML algorithms can slow down plane data forwarding and provide faster availability of network features. It helps the

program detect the attack quicker, hence minimizing the damage it can cause.

According to Smuha & Nathalie (2021), the interaction of AI and the dark web comes with benefits and some notable ethical and legal risks. For example, the technology could breach fundamental rights like privacy and non-discrimination. It can manipulate people to hinder their self-determination, which can result in harming their safety and security (Smuha & Nathalie 1). These authors suggest that governments should not only accept the brighter side of this program but also look at the dark side of it. It is the government's responsibility to protect its people; therefore, they are urged to safeguard their people against the risks that come with AI. The potential way to control the negativities that come with the interaction of AI with the dark web is to have regulations on its application. While maximizing the benefits of the interaction, all governments worldwide should have regulations at all levels to minimize future adverse impacts. Having a proper regulatory regime that can bring balance between these needs and legal certainty can build trust for the technology and facilitate its uptake.

Results and Findings

After reviewing the existing literature, it is clear that the interaction of AI and the dark web does not only have positive but also negative effects. Data has it that more than 94% of illegal deals are completed through the dark web. Research by Basheer et al (2021) shows that the interaction of AI with the dark web creates a big challenge for cybersecurity firms. However, AI has the potential to bring solutions to these cyber-attacks. Organizations can make use of more sophisticated techniques to prevent cyberattacks. AI-driven tools can be used to monitor and survey the dark web for illegal activities, which may include the sale of stolen data, weapons, hacking services, illegal substances, and malware. Research by Aloqaily et al. (2022) shows that interaction between AI and the dark web not only creates problems for cybersecurity firms but also brings solutions to the existing challenges that come with the existence of the dark web. AI can be used to secure individual and organization data at risk of being stolen and misused by dark web users without a trace.

Musumeci et al. (2022) suggest in their research that AI has severely failed to defend against cyber-attacks. When incorporated with plane data security programs, AI may not fully protect the plane's program from being attacked. However, the improvements in AI and the introduction of ML algorithms

can help the plane data security program detect in advance and slow down the attack, hence minimizing the damage it can cause. Smuha & Nathalie (2021) also suggest that the interaction of AI and the dark web comes with benefits and some notable ethical and legal risks. The program can cause a potential breach of fundamental rights like privacy and non-discrimination. Governments should be careful when accepting the incorporation of AI not to face its future impaired consequences on its citizens. They should have regulations at all levels to regulate the utilization of AI as they enjoy its benefits. In future the developers should ensure that the interaction of AI and dark web is safer for all users.

Conclusion

The interaction between AI and the dark web positively and negatively impacts everyone involved. It helps cybersecurity firms control challenges created by the dark web, such as cyber-attacks, by helping intelligence officers monitor and trace the movement of information in the dark web. However, without regulations, the interaction between AI and the dark web can adversely affect individuals by interfering with their privacy rights. Therefore, governments have a duty to put a regime that will regulate the application of AI in the dark web to ensure that its future adverse impacts are avoided or minimized.

Works Cited

Aloqaily, Moayad, et al. "Special issue on cybersecurity management in the era of AI." *Journal of Network and Systems Management* 30.3 (2022): 39. https://link.springer.com/article/10.1007/s10922-022-09659-3

Basheer, Randa, and Bassel Alkhatib. "Threats from the dark: A review over dark web investigation research for cyber threat intelligence." *Journal of Computer Networks and Communications* 2021 (2021): 1-21.https://doi.org/10.1155/2021/1302999

Musumeci, Francesco, et al. "Machine-learning-enabled DDoS attacks detection in p4 programmable networks." *Journal of Network and Systems Management* 30 (2022): 1-27. https://link.springer.com/article/10.1007/s10922-021-09633-5

Rawat,Romil, et al. "Organ trafficking on the dark web—the data security and privacy concern in healthcare systems." *Internet of Healthcare Things: Machine Learning for Security and Privacy* (2022): 189-216.https://doi.org/10.1002/9781119792468.ch9

Smuha, Nathalie A. "From a ‘race to AI’to a ‘race to AI regulation’: regulatory competition for artificial intelligence." *Law, Innovation and Technology* 13.1 (2021): 57-84. https://doi.org/10.1080/17579961.2021.1898300