Exploiting Artificial Intelligence Within Cybercrime

Alexander Berrios

CYSE 201S

Exploiting Artificial Intelligence Within Cybercrime

Recent developments in artificial intelligence (AI) have taken society by storm. The large language model (LLM) ChatGPT has transformed AI into a novelty that is easily accessible to virtually anyone and has quickly become a popular tool for various purposes. However, this powerful tool has introduced new risks and has significant implications for cybercrime when used maliciously. As this technology continues to grow in complexity, it'll become increasingly popular among cybercriminals as an instrument to help carry out attacks.

AI's ability to generate text sophisticatedly can enhance social engineering tactics by drafting convincing phishing texts or generating malware codes. Experienced cybercriminals are even utilizing the structure of the LLM to develop and disseminate malicious versions of ChatGPT on the dark web. The article chosen investigates the intersection of AI and cybercrime and addresses challenges associated with mitigating these risks as a modernized society.

Experiment

This study did not conduct a traditional experiment to generate any fixed conclusions. Alternatively, thematic analysis was employed by drawing insights from archival research and SME interviews. The information collected was thematically analyzed to understand the problems more comprehensively and draw practical and theoretical insights concerning the implications of the misuse of AI concerning cybercrime.

Data Collection & Analysis

Utilizing quantitative analysis, evidence of malicious AI-generated prompts on the clear and dark web were collected and categorized. Their database consisted of screenshots and details about the software used for input. This data, which consisted of 102 prompts, was retrieved through an open-source browser called TOR (The Onion Router).

Forums that discussed AI-generated prompts for malicious purposes on platforms such as Reddit, Dark Net Army, YouTube, Dread, and others, were collected and added to their database which, notably, were mostly in English, Russian, and Portuguese. These forums were observed to have user bases ranging from 4,430 to 4,600,00 individuals.

Six subject matter experts across various fields such as criminal justice, cybersecurity, and cybercrime were also interviewed. These interviews offered views that are essential to understanding and addressing the challenges and complexities of the malicious use of artificial intelligence and the respective policies.

Results

The discussion forums provided evidence that various communities and linguistic backgrounds are engaging in AI-driven cybercrime, reinforcing the narrative that cybercrime is a global issue with increasing importance to address. The quantitative data measured demonstrated the escalation of AI utilization, bringing up concerns about the challenges associated with regulation, especially on the dark web.

An overwhelming need for increased public education about AI and its ethical implications was highlighted in the SME interviews. These experts believed that increasing risks of victimization can be correlated to society's current narrative and the media's portrayal of AI, shifting the focus to the anxieties of automation instead of highlighting security risks. The information gained from mass media directly influences decisions on AI's regulation, adoption, and ethical considerations.

Recommendations to combat this new dimension of crime and to reduce susceptibility involve proactive measures, such as cyber awareness training, developing AI-driven cyber defense tactics, and adopting best practices for online safety.

In conclusion, the findings of this article suggest that the use of AI within cybercrime is a multifaceted and widespread phenomenon with global implications. This study demonstrated the validity of AI-derived cybercrime and encouraged the inclusion of the practice in future cybersecurity studies and developing theories, such as the Cyber RAT theory.

References

Shetty, S. , Choi, K. & Park, I. (2024). Investigating the Intersection of AI and Cybercrime: Risks, Trends, and Countermeasures . *International Journal of Cybersecurity Intelligence & Cybercrime, 7(2)*, - . DOI: https://doi.org/10.52306/2578-3289.1187