Article Review 1: Investigating the Intersection of AI and Cybercrime

Caiden Petty

Professor Diwakar Yalpi

CYSE 201S

10/2/2024

Introduction

Sanaika Shetty et al. published their findings of artificial intelligence in the cybersecurity field in the International Journal of Cybersecurity Intelligence and Cybercrime. Their focus was on AI's ability to create widespread, sophisticated attacks that affect as many people as possible. As AI is on the rise a back and forth battle emerges, struggling to find ways of mitigating a new threat to security. The findings suggest innovative approaches and call for a raise of awareness as the new issue grows.

As a society, we are entering the new age of AI, where anyone can create and explore the possibilities artificial intelligence has to offer. This raises some ethical issues as it can be twisted and manipulated for criminal activity. One common use is asking ChatGPT to draft "phishing emails and malware codes" (Getahun, 2023). More effort has been invested in making malicious large language models (LLMs) and a few have already surfaced on the dark web. Shetty et al. study the "intricate relationship between AI and cybercrime, particularly focusing on how AI can be exploited for malicious purposes" where they "employed thematic analysis, drawing insights from a comprehensive review of pertinent literature and expert interviews" (Shetty, 2024). The purpose is to gather information about how cybercriminals optimize AI for their crimes, including both phishing and malware, and find trends that can be used to populate mitigation techniques while simultaneously spreading awareness about the issue.

Research and Findings

Lawrence Cohen and Marcus Felsen founded the Routine Activities Theory (RAT) in 1979 that finds criminal acts necessitate the convergence of space and time of motivated

offenders, suitable targets, and the absence of effective guardians (Cohen and Felson, 1979) and that if any one of these three are entirely absent, the process is to fail. RAT applies to the social sciences as ethics and morals are a key focus of this principle. Neutralization is the justification of malicious acts by finding a scapegoat, or unrelated factors that weren't impacted. Cyberbullies neutralize their actions for example, by saying "at least nobody got hurt". In regards to AI, criminals are driven by a "desire to exploit its capabilities and encounter an infinite pool of suitable targets" (Shetty, 2024). The following research was conducted over both the clear web and the dark web, looking for qualitative and quantitative proof of malicious AI use. 102 malicious prompts were found and verified as AI generated. There were also 8 forums for AI generated prompts with malicious intent, and many other cyber security threats. Several photo examples are included which help the public see what an AI generated phishing email looks like.

Conclusion

These findings help show what to look out for on the internet, and to be aware of suspicious online content. Being aware and cautious is one of the first steps in avoiding victimization of cyber crime. Additionally, this research helps lawmakers and cyber security specialists see where the key issues are as we develop AI further. It shows what we can expect from cyber criminals, and their patterns as well as their tendencies to use AI in new ways for illegal benefits.

Works Cited

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