An Overview on Artificial Intelligence Applied in Offensive Cybersecurity

Gabriela TOD-RĂILEANU, Ioan BACIVAROV
Faculty of Electronics, Telecommunications, and Information Technology
National University of Science and Technology POLITEHNICA Bucharest, Romania
gabriela.tod@stud.etti.upb.ro, ioan.bacivarov@upb.ro

Abstract

As of the onset of 2023, ChatGPT has emerged as the predominant Artificial Intelligence (AI) tool, finding extensive application across various sectors and rapidly becoming an integral part of everyday work and domestic activities. However, the widespread adoption of ChatGPT has been accompanied by instances of misuse, wherein individuals have utilized the tool for unauthorized data access or engaged in activities deemed disruptive or malicious in nature. Consequently, a discernible trend has emerged wherein cyberattacks are increasingly being propelled by the capabilities of AI. This escalation in AI-driven cyber threats is evidenced by the misuse of generative AI tools, which are now being harnessed by attackers for activities such as crafting deceptive phishing emails, deploying malware designed for keystroke monitoring, and developing rudimentary yet effective ransomware code. This shift underscores the growing sophistication of cyber threats facilitated by the misuse of advanced AI technologies, necessitating a comprehensive understanding of the associated risks and the implementation of robust cybersecurity measures to mitigate potential harms.

Index terms: chatGPT, artificial intelligence, WormGPT, information technology, phishing

References

[1]. Europol Public Information, "Tech Watch Flash - The Impact of Large Language Models on Law Enforcement.pdf," March 2023. [Online]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf. [Accessed October 2023].

[2]. Darktrace, "The Next Paradigm Shift: AI-Driven Cyber-Attacks," 2018. [Online]. Available: https://www.oixio.ee/sites/default/files/the_next_paradigm_shift_-_ai_driven_cyber_attacks.pdf. [Accessed October 2023].

[3]. "ChatGPT," OpenAI, 2022. [Online]. Available: https://chat.openai.com/. [Accessed October 2023].

[4]. K. Huang, M. Siegel, K. Pearlson and S. Madnick, "Casting the Dark Web in a New Light," Cybersecurity Interdisciplinary Systems Laboratory (CISL), Cambridge, MA, 2019.

[5]. "WormGPT official website," 2021. [Online]. Available: wormgpt[.]com[.]co. [Accessed September 2023].

[6]. D. Kelley, "WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks," AlashNext, 2023. [Online]. Available: https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/. [Accessed September 2023].

.