THE EVOLUTION OF CYBER THREATS IN THE AGE OF ARTIFICIAL INTELLIGENCE: AN ANALYSIS OF HOW AI IS TRANSFORMING THE CYBERSECURITY LANDSCAPE, FROM ENHANCING DEFENSE SYSTEMS TO THE CREATION OF NEW FORMS OF INTELLIGENT MALWARE

Adrian MANOLE

Software Engineering and Automation, SI-232, Faculty of Computing, Informatics and Microelectronics, Technical University, Chișinău, Moldova

Corresponding author: Manole Adrian, adrian.manole@isa.utm.md

Tutor/coordinator: **Ala ȘIȘIANU**, university assistant, TUM

Abstract. *In today's developing digital age, cybersecurity sits at the core of every aspect of our use of technology. The revolution of Artificial Intelligence has opened a "Pandora's box" in the cybersecurity realm. Nowadays's AI can be used to monitor dangerous behaviors, and abnormal incoming traffic, so as to predict incoming cyber-attacks using the machine learning aspect of its means. It is because the AI is continuously learning with the help of a wide range of cyber-attacks from the past and about the vulnerabilities that caused those attacks. This research paper dives into the current state of the Artificial Intelligence implementations in cybersecurity, and how it can overcome the threats in this day and age of technology. It also expands into its vulnerabilities and how hackers can exploit Artificial intelligence for their own benefits, implementing it for their own attacks. Lastly, it directs attention to the responsible and ethical use of AI, as it's becoming a more powerful tool every day.*

Keywords: *cybersecurity, artificial intelligence (AI), cyber-attacks, machine learning, vulnerabilities, digital age*

Introduction

Cybersecurity is the term used for the technology and protocols used for protecting our data that travels through networks and it's stored in devices from malicious attacks from the outside. With the current advancements of Artificial Intelligence such as pattern recognition and procedure automation, it is progressively being implemented in solving cyber threats such as bot detection, attack detection, data protection and automating the procedure used in responding in case of a cyber-attack, ending the need of human interaction that comes with its late response and in some cases human-errors. But the Artificial Intelligence has opened the gates for a new age of cyber-attacks, with the use of Machine Learning, AI can learn from patterns and find vulnerabilities in the software, especially when an application has been recently updated, making the possibility of day zero attacks go up substantially. Attackers can also use AI in social-engineering attacks such as phishing with the use of its ability to generate highly realistic images, cloning of a human's voice, and to analyze and replicate its speaking patterns and mannerism.

The use of AI in developing sophisticated cyber threats

Machine Learning Powered Malware is a new type of malware that uses the power of Machine Learning in analyzing a vast amount of data from past software vulnerabilities so that it can adapt its behavior in the moment of the attack. Unlike the tradition malware which is written to follow a straight protocol of actions, ML Powered Malware can adapt and overcome the challenges imposed by security rules, the current security measures designed to identify malware are challenged by this malware's abilities really adjust itself based on the current situation of an attack, and by the in-depth analysis it does on software it targets, such as its past vulnerabilities, it's architecture and even the type of security measures it has implemented. The most powerful

aspect of this type of malware is that it has its own decision-making power, during an attack it can analyze the risk and its priorities so it can move its focus on other key aspects of a software, the most polarizing thing is that those decisions are made instantly, making the time window for humans to intercept the attack practically inexistent.

Cyber-attacks such as identity theft and fraud, disinformation and manipulation can be implemented using social engineering with the help of Deepfakes and Generative Content. Deepfakes are a result of Machine Learning models trained on a database of videos and images of a person. In result the malware generates content that imitates a person's aspect, voice and mannerism, the content is so impressively accurate because of the two neural network it uses, first there is the one that generates the false content while the second neural network is comparing it to the original dataset of videos/photos of the original photos, making adjustments in real time to the fake, making it to look exactly like the original.

AI Phishing also is a genuine cyber security threat, compared to the original phishing methods which involves targeting a considerable number of people of all ages, incomes and interests the new method which involves Artificial Inteligence (AI) and Machine Learning (ML) can target a specific person, by automatically analyzing his social media activity and imitating a real communication between the target and the person the malware disguises as. The malware also has contextual awareness, it can change the interaction based on recent events, and other useful information.

Using AI for cybersecurity measures

Companies can also benefit from the power of Artificial Intelligence (AI), involving the Machine Learning (ML) and Deep Neural Network aspects the AI can learn from the vast number of attacks in the past, making a great analysis on the patterns of those cyber threats alongside the vulnerabilities that caused them.AI can replace the human aspect with its power of automating repetitive tasks, analyzing a big chunk of data in a short period of time and making assessments and changes to its protocols based on that. The benefits that companies and organizations can benefit from using this technology are the Improved more accurate and fast detection, because of its upgraded algorithm that constantly changes based on the most recent events and threats, this type of algorithm can use the large amount of data of past events it can send warnings of incoming threats and recommend fast changes for eliminating the risk. Implementing this type of AI in Cybersecurity can also reduce the response time significatively, it can automatically recognize the type of attack and the most efficient procedures for neutralizing the threat, it can compare in real time the past response to a type of cyber-attack and decide for itself the most efficient decision. This eliminates the human aspect of threat-response that is often slow and biased. Another wonderful use of Artificial Intelligence is its behavior analysis, it can detect anomalies in the network usage, such as high spikes of traffic from specific location or types of users, AI uses a large database of user's interaction on the web for creating a baseline profile healthy user, when this type of attack occurs the AI can find the patterns in the traffic, comparing it to its baseline profile for a normal user, and make decisions from there. With the use of Machine Learning it can constantly improve and change the profile of its normal user, ensuring the number of false positives stay low, the AI can also use its Deep Neural Network to understand the context of the current situation, such as current events across the world, the types of users there are on the Internet, ensuring its effectiveness in any time of day.

The challenges that come with the use of AI in Cybersecurity

AI revolutionizes the cybersecurity industry, but also it can come with many limitations and challenges we need to overcome for increasing its benefits. One of the biggest limitations of Artificial Intelligence is that its response quality is linked to the quality of data it is being fed. There is a lot of misinformation in the data right now, and companies need to invest a lot of resources to filter out and process the data, ensuring the quality of information the AI uses. Another issue is the privacy aspect of processing our sensitive information by the Artificial Intelligence, many times it often violates data privacy regulations such as GDPR and CCPA. Companies that invest the use of AI in their security

need to also invest in good encryption techniques alongside a well-structured privacy term of use. AI can also suffer from a bias, the information it uses to learn is not all the time the fairest one, for example the historical data, current news. There needs to be a well thought out system that filters out the AI's bias and unfairness in term of assessing which type of user should not access the service. Also, AI can suffer from bias in the moment of threat response, the decision it makes can be the least efficient one. This technology can also suffer from scalability issues, the Machine Learning aspect requires a large computational power, as the cyber threats continue to grow, companies need to invest in their infrastructure, ensuring that the AI is not limited by the lack of computational resources.

Conclusion

AI is the innovative technology that can reinvent Cybersecurity, a huge improvement for real-time threat detection, attack response automation and risk assessment. Companies can leverage this power for the benefit of the user, making the internet a safer space for all of us. But it that also comes with great challenges such as the quality of data the Machine Learning uses for its learning aspect, the bias and fairness aspect of the decisions it makes in real time. In order to benefit from the protentional this technology brings, companies need to invest in data scientist that can filter the data they feed the AI with, alongside cybersecurity experts that can evaluate the responses the AI makes in the time of an attack, and legal professionals that can help with the legal aspect of data processing and fairness of decisions. Companies need to keep in mind that AI is also a powerful tool that the malicious users also have access to, so they need to continuously invest in improving the technology. Improving the AI's transparency of data usage, computing infrastructure and ensuring the legal aspect is on point, this tool can revolutionize the safety of the internet and it's users.

AI is the innovative technology that can reinvent Cybersecurity, a huge improvement for real-time threat detection, attack response automation and risk assessment. Companies can leverage this power for the benefit of the user, making the internet a safer space for all of us. But it that also comes with great challenges such as the quality of data the Machine Learning uses for its learning aspect, the bias and fairness aspect of the decisions it makes in real time. In order to benefit from the protentional this technology brings, companies need to invest in data scientist that can filter the data they feed the AI with, alongside cybersecurity experts that can evaluate the responses the AI makes in the time of an attack, and legal professionals that can help with the legal aspect of data processing and fairness of decisions. Companies need to keep in mind that AI is also a powerful tool that the malicious users also have access to, so they need to continuously invest in improving the technology. Improving the AI's transparency of data usage, computing infrastructure and ensuring the legal aspect is on point, this tool can revolutionize the safety of the internet and it's users.

Bibliography

[1] A. Rege-Patwardhan and J. Zhou, "Artificial Intelligence in Cybersecurity: Applications and Implications for Governance," IEEE Security & Privacy, vol. 18, no. 4, pp. 24-33, Jul./Aug. 2020, doi: 10.1109/MSEC.2020.2998516.

[2] J. Lin, R. Ballard, and Y. Zhang, "Deep Learning for Intrusion Detection: A Review and Analysis," Journal of Information Security and Applications, vol. 54, pp. 102620, Sep. 2020, doi: 10.1016/j.jisa.2020.102620.

[3] L. Yang, Y. Li, and Q. Zhang, "Challenges and Opportunities in Using AI for Cybersecurity," IEEE Internet of Things Journal, vol. 8, no. 4, pp. 2401-2411, Feb. 2021, doi: 10.1109/JIOT.2020.3022175.