Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2019, 6(6):19-21**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

The Impact of Artificial Intelligence (AI) on Cybersecurity

Nik Tehrani, Mamoun Samaha

International Technological University, 2711 N 1st St. San Jose, CA 95134

Abstract Artificial Intelligence (AI) use for cyber defense can be based on existing patterns, so a combination of learning approaches can be used to predict new threats and malware. Behavior analytics compiled by machine learning techniques can be used to monitor system and human activity for detection of potential malicious abnormalities. Attackers can anticipate AI defense techniques, so AI development to protect data must be constantly monitored to credibly predict malicious intent. Users can prevent social engineering attacks by eliminating re-use of passwords and using two-factor authentication. AI is used for data- analysis and protection, threat detection, and authentication using a variety of solutions, to include blockchain technology.

Keywords AI protection, threat detection, authentication, AI solutions, blockchain

Introduction

At the heart of cybercrime is data, which is considered to be the new currency of the digital world. Data is a key asset of any organization, and safeguarding it is top priority [1]. It is predicted that, by 2021, cybercrime losses will reach $6 trillion annually. A recent joint report by the FBI and the U.S. Department of Homeland Security joint report expressed concerns that Russian associated threat hackers attempted to infiltrate and inflict damage on critical U.S. infrastructure, energy and nuclear sectors, water facilities, and the aviation industry [2]. Increasing AI-enabled cyberattacks is causing a barrage of personal data thefts, network penetrations, and an epidemic of intelligent computer viruses [3]. 845.37 million malwares were created in 2018 and around 10 million new malwares are created every month. Traditional cybersecurity systems are no longer effective in handling new varieties of malware. AI for cybersecurity is the only viable solution to handle this challenge[3].

AI is being deployed for malicious purposes by clever, anonymous hi-tech attackers because AI systems are inexpensive and easy to use. Therefore, the cybersecurity industry is increasingly finding solutions to protect the systems and networks that organizations use to store data. Cybersecurity companies are turning to artificial intelligence (AI) to ensure that defensive aspects of cybersecurity can effectively combat spam, cybercrime, and detect malware [4-5].

A prevalent attack is a click on a on a seemingly innocent social media link that introduces malware into the unsuspecting user's computer. Attackers can prioritize their victims by analyzing large data sets (predictive models) that indicate online behavior. All of the data in the public domain is now available in seconds and can be used for victim profiling. E-mails and sites can be tailored to seduce a user to click on them. The sophistication of such attacks can increase by exceeding human capabilities of deception, such as mimicking voices through speech synthesis or creating realistic voice recordings using chatbots that interact with humans by impersonating live contacts [6].

Defensive Strategies using AI

AI use for cyber defense can be based on existing patterns, so a combination of learning approaches can be used to predict new threats and malware. Behavior analytics compiled by machine learning techniques can be used to monitor system and human activity for detection of potential malicious abnormalities. Since attackers can

anticipate AI defense techniques, AI development to protect data must be constantly monitored to credibly predict malicious intent. Users can prevent social engineering attacks by eliminating re-use of passwords and using two-factor authentication [5].

Data- Analysis and Protection

The immense volume of sensitive data that modern networks produce needs to be identified, classified, and tracked. AI uses computer vision and machine learning for data analysis at the pixel and byte levels to categorize data to identify where data is stored. AI also determines which device is compliant with data rules, such as the EU General Data Protection Regulation (GDPR)which identifies suspicious and unusual data activity. Redundant data can be identified, saving companies huge costs for storage [5].

Threat Detection

AI facilitates the detection of malware (malicious software) by using a *good-behavior* model that is generated from data examples used to classify suspicious activity [8]. Using an Intrusion Detection System (IDS) can detect anomalies. AI identifies patterns of excessive resource use, such as CPU or memory, unusual host connections, data transfers, incorrect logins, or suspicious traffic. Such threats are classified into types such as Trojans, worms, ransomware, viruses, backdoors, bots, adware, and spyware [7]. Malware is specifically designed to disrupt, damage, steal, or perpetrate some criminalaction on networks, hosts, or data [7]. Malware has also evolved to damage the physical systems hardware [7].

Authentication

AI uses biometrics, the science of establishing a person's identity, by increasing cyber and physical security [8]. Users frequently use weak passwords that are used across multiple platforms, allowing ease if guessing these passwords to access accounts that have the same username/password combinations. To combat this, AI biometrics requires validation for a characteristic that is hard to copy and analyzes two types of characteristics about a user: physical and behavioral. Physical biometrics consists of unique characteristics, such as fingerprints, facial recognition, eyes, or DNA. Behavioral characteristics are unique, such as voice, or the way a user types and interacts with a device, which are harder to mimic because they are unique factors. Landwehr Behavioral biometrics can be used in banking apps and ATM's requiring voice or facial recognition for validation.

Types of AI Solutions

- AI can be integrated with other advanced technologies, such as Blockchain, to guarantee better security protocols [9].
- The Versive Security Engine (VSE) uses artificial intelligence to differentiate critical risks from routine network activity, identifying chains of activities that result in attacks [4].
- LogRhythm uses machine learning to profile and detect compromised accounts and other anomalies [4].
- Anomali identifies suspicious activity before it reaches networks using threat intelligence solutions that allow security teams and analysts identify threats and adversaries and collaborate with other organizations [4].
- Crowdstrike provides cloud-native endpoint protection software called Falcon for prevention and proactive threat hunting in finance, healthcare and retail. Falcon automatically investigates threats, removing guesswork of threat analysis [4].
- Shape Security from SentinelOne provides software that combats imitation attacks, such as fake accounts and credit application fraud used in retail, finance, government, tech and travel. Shape uses machine learning models enabling the system to learn what human activity looks like against fraud [4].
- Symantec uses a cloud-based threat intelligence platform to help governments and organizations to defend clouds, endpoints and infrastructures against threats [4].

- CUJO AI's platform uses machine learning to secure browsers, smartphones and IoT devices using algorithms that recognize patterns and proactively predict attacks to thwart malicious malware and phishing schemes [4].

Conclusion

While AI is a valuable solution for security and will continue to advance, AI is also giving power to the wrong hands to threaten data security. Malware is increasing, threat actors are becoming more cunning, and traditional cybersecurity systems are no longer effective in handling these new varieties. AI for cybersecurity is the only viable solution to handle this challenge by integrating with other advanced technologies, such as Blockchain, to guarantee better security protocols.

References

[1]. Powell, M. (2019). CPO. Artificial Intelligence: A Cybersecurity Solution or the Greatest Risk of All? Retrieved from https://www.cpomagazine.com/cyber-security/artificial-intelligence-a-cybersecurity-solution-or-the-greatest-risk-of-all/

[2]. CISA. (2018). Alert (TA18-074A). Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-074A

[3]. Yampolsky, R. (2017). AI Is the Future of Cybersecurity, for Better and for Worse. Retrieved from https://hbr.org/2017/05/ai-is-the-future-of-cybersecurity-for-better-and-for-worse

[4]. Built-in. (2019). 25 companies merging AI and cybersecurity to keep us safe and sound. Retrieved from https://builtin.com/artificial-intelligence/artificial-intelligence-cybersecurity

[5]. Zinatullin, L. (2019). Artificial Intelligence and Cybersecurity: Attacking and Defending. Tripwire. The State of Security. Retrieved from https://www.tripwire.com/state-of-security/featured/artificial-intelligence-cybersecurity-attacking-defending/

[6]. NJCCIC. (2019). Seeing AI to AI: Artificial Intelligence and its Impact on Cybersecurityhttps://www.cyber.nj.gov/be-sure-to-secure/seeing-ai-to-ai

[7]. Cisco. (2019). What Is the Difference: Viruses, Worms, Trojans, and Bots? Retrieved from https://www.cisco.com/c/en/us/about/security-center/virus-differences.html

[8]. Landwehr, C. (2019). Cybersecurity and Artificial Intelligence. From Fixing the Plumbing to Smart Water. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4639011

[9]. Naveen, J. (2019). Forbes. Can AI Become Our New Cybersecurity Sheriff? Retrieved from https://www.forbes.com/sites/cognitiveworld/2019/02/04/can-ai-become-our-new-cybersecurity-sheriff/#cb94b2036a8e