www.pipelinepub.com
Volume 19, Issue 11

AI in Cybersecurity: The Good News and the Bad News

By: Jacob Ukelson

The impact of AI on our way of life is accelerating and to no one's surprise, AI has become prominent in the opposing realms of cybercrime and cybersecurity. From the beginning of our digital age, the dynamic between these opposing sides has not changed. Each side has always used the capabilities of emerging technologies to achieve their goals. The role of AI in both cyber offense and defense is being played out now. Those responsible for the security of their organizations, from technologists to executives, should stay informed on how AI is being used by their adversaries and how AI can counter these threats.

Tools of the Trade: Machine Learning and Machine Reasoning

To begin, we should clarify some of the terms used when discussing AI. Without going into too much detail, think of AI as an umbrella term encompassing different computer-based technologies that replicate human problem-solving or decision-making. Machine learning and machine reasoning are two types of AI technology that are used to solve different problems.

Machine learning (ML) applies statistical analysis and pattern recognition to large data sets to uncover patterns of behavior. There are several subsets or types of machine learning that are differentiated based on the types of data they use (structured or unstructured), the size of data sets they can work with, and the types of services they provide. Applications of ML are varied; examples include services such as fraud detection, self-driving cars, and customer retention.

Generative AI (for example ChatGPT) is a learning-based AI capable of creating original text, images, audio, and data. Cyber attackers are using Generative AI in several ways that will be described later in this article.

While machine learning is based on the statistical identification of hidden patterns within a large amount of data through correlation, machine reasoning is based on using facts and relationships, and drawing conclusions from them. For example, a reasoning system can differentiate the meaning of the words "put on" in the sentences "I put on my clothes" and "I put on a show." Personal assistants such as Siri and Alexa use machine reasoning to generate answers to the questions we ask—including questions they have never encountered before.

How Attackers Use AI

Cybercrime is big business. One recent estimate is the global annual revenue for cybercrime is $1.5 trillion. The total cost of cybercrime is even greater—about $6 trillion by some estimates. (www.techrepublic.com).

Like any business, cybercrime enterprises strive to grow revenue and reduce costs. Their KPIs (key performance indicators) are cost per attack, success rates, and revenue per attack. Learning AI is proving to be highly effective in driving the success of cybercrime as a business. Learning based AI systems are being used to great effect in the following ways:

1. Generative AI enables attackers to produce more convincing phishing emails quickly and cheaply. These AI systems are well adapted to crafting convincing emails that appear to come from a legitimate source. These generative systems learn and improve over time, growing their input data sets and adjusting based on the effectiveness of past attempts.

2. Generative AI is also used to conduct finely targeted spear-phishing attacks. These attacks are often emails or voicemails based on highly specific information and circumstances pertaining to key individuals at an organization. Many of these are business email compromise (BEC) attacks that convince victims to reveal key information or authorize wire transfers. These attacks involve the impersonation of a trusted party (a company executive, vendor, etc.) to trick a victim into making a financial transaction or sending sensitive data.

3. Attackers are using AI to generate self-learning malware that adapts its course of action in response to the situation, and particularly target its victims' systems. AI-generated malware can avoid detection and adapt to the environment and defenses of its targets.

4. AI tools such as chat bots are used to conduct so called "deep fake" attacks in which the voice of a trusted party is used to convince the victim to perform some action. For example, in 2020, a manager at a Hong Kong bank received a call in the voice of a director he knew well, asking him to authorize a $35M wire transfer. This request was backed up by what appeared to be legitimate emails, and the transfer was carried out. Deep fakes can mimic voices and images, and can be used to interact in conversational mode with victims.

5. A sophisticated, sustained cyberattack known as an advanced persistent threat (APT) occurs when an intruder enters a network undetected and stays there for a long time to steal sensitive data. APTs frequently involve the use of artificial intelligence to avoid detection and target specific organizations or individuals.

Cybercrime statistics bear out the impact AI is having on the ability of criminal enterprises to conduct attacks more cheaply and more effectively than ever before. For example, phishing attacks have grown at a 150% annual rate since 2019 (see *Figure 1* on next page), facilitated by the ability to use AI-driven automation to generate attacks.

The State of AI-Powered Cyber Defense

An effective cyber defense includes a robust prevention strategy in combination with detection and response capabilities. AI plays a key role in both areas.

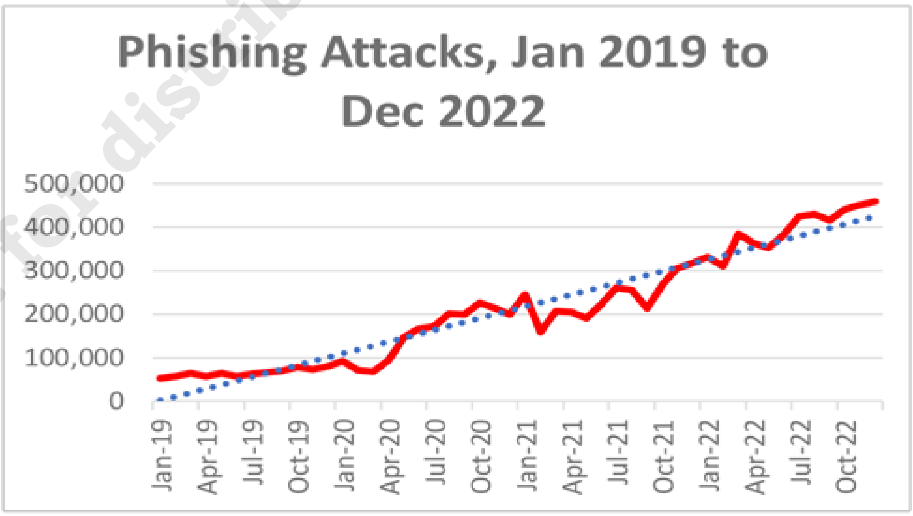
Learning-based AI cyber defense systems are most effective in attack detection, often using behavioral, pattern-matching, and contextual approaches to spot malicious activity hidden within vast amounts of legitimate activity. Some areas where learning-based AI is showing the most value are:

1. **Malware Identification.** Machine-learning AI can analyze the signatures of known malware and use this information to identify similar malware. They can also identify unusual or anomalous behavior, such as a file attempting to access a resource it does not typically use.

2. **Intrusion Detection.** At this point, learning-based systems are essential for coping with the vast amount of activity-logging data in modern networks to find anomalous behavior—and to reduce the chronically high number of alerts that bog down response teams with false positives.

3. **Phishing, BEC, and Spam Detection.**AI-powered detection systems use a multidimensional approach, combining learned knowledge of content, context, behavior, sources, and so on to identify malicious emails. This is an ongoing contest as bad actors keep improving on their methods and adapt to defenses.

These applications of AI mostly pertain to attack detection—not robust prevention strategy. The challenge in attack prevention is organizations have only limited and partial visibility into the state of their defenses. They can only test their defenses in piecemeal fashion and under constraints against operational disruption. The security of a complex system can only be assured if it is thoroughly and realistically tested. Thus far, the only real-world tests of cyber defenses have come from the cyber attackers themselves—resulting in breaches where the defenses are found to be lacking. Thankfully, this is changing.



Source: APWG Phishing Activity Trends Report 4th Quarter 2022

Figure 1. Phishing Activity Trends Report 4th Quarter 2022, www.apwg.org

AI in Attack Prevention

AI can play a key role in ensuring organizations are both well defended from attacks and that the potential impacts of a successful attack are minimized. This gets back to the need for robust prevention processes and tools such as those described in Gartner’s Continuous Threat Exposure Management (CTEM) program.

This is where reasoning-based AI defenses are most effective. While machine learning is based on the statistical identification of hidden patterns within a large amount of data, machine reasoning is based on using facts and relationships, and drawing conclusions from them.

This has great value in the cyber world. A semantic graph for cyber threats can be produced by using information and concepts found in standard information sources, such as MITRE ATT&CK and NVD CVE. By combining a semantic graph of cyber threats with a graph describing features of an organization’s IT systems (a “digital cyber twin” of the IT environment) the reasoning system has all the information it needs to sort through millions of simulated cyberattacks. It can identify which specific attack scenarios represent exposures to the organization and calculate the risk from those exposures. It shows the steps an organization can take to reduce exposures to an acceptable level. A CTEM process of continuous threat exposure management is made possible by AI-powered technology.

Who is Winning?

While the current state of play indicates cyber attackers are maintaining and even widening their lead, there are reasons for optimism. AI is providing organizations tools that automate many of the tasks of cybersecurity that are both costly and prone to error. AI is also enabling a more holistic approach to cyber defense, allowing businesses to better integrate security strategy and operations, thus reducing dependence on disparate point solutions. AI-powered cybersecurity is showing that organizations can improve both the effectiveness and efficiency of their security operations—lowering costs while reducing risk.