OPINION

Don't Be So Sure AI Is Cybersecurity's Silver Bullet

By Peter S. Vogel and Edward H. Block
Aug 20, 2018 12:03 PM PT

Back
Email

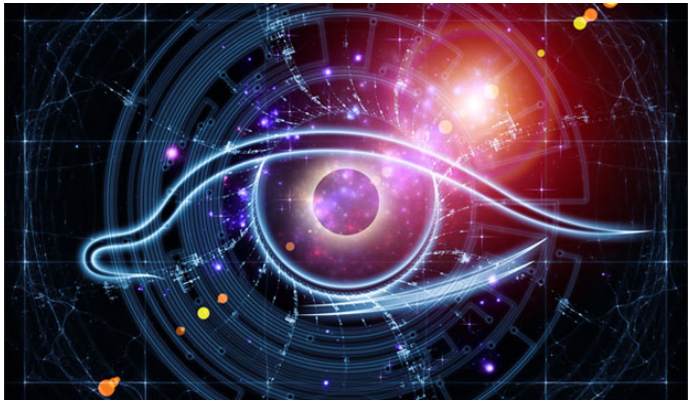

Image: Adobe Stock

There's a lot of hype around artificial intelligence as the greatest thing since sliced bread, but will AI really help with cybersecurity? Criminals who run cybercriminal businesses also are capable of using the AI to commit crimes. It's logical that if one person is smart enough to develop cyberprotection technologies that utilize AI, then thoughtful, creative criminals can use AI to penetrate those AI-created protections.

AI has been around since about 1959. It has had its ups and downs until 2011, when IBM's Watson became a television celebrity by beating *Jeopardy!*'s reigning champs.

Now IBM regularly has television commercials promoting Watson for myriad uses, including detecting problems with aircraft and elevators. At the same time, these ads make AI appear commonplace and part of our current culture, rather than as some esoteric complex computer technology.

AI in Cybersecurity

It is important to understand what machine learning is and how it relates to AI. To oversimplify, machine learning is a computer's ability to recognize things. Artificial intelligence is a computer's ability to mimic human understanding.

However with all the marketing hype found on the Internet, it is oftentimes difficult to understand when someone really is referring to AI or machine learning.

"I actually don't think a lot of these companies are using artificial intelligence," Malwarebytes CEO Marcin Kleczynski told *Wired*. "It's really training machine learning. It's misleading in some ways to call it AI, and it confuses the hell out of customers."

Malwarebytes is a provider of machine learning threat detection software.

Machine learning can be very beneficial in the deployment of cybersecurity detection systems, as it enables devices to learn what to watch for.

Curb Your AI Enthusiasm

No matter what security vendors may say, ask any security profession and they will tell you there is no "Silver Bullet."

"To be fair, AI definitely has a few clear advantages for cybersecurity," wrote Tomas Honzak, director of security and compliance at Good Data, in a recent Dark Reading post. "In reality, like any technology, AI has its limitations."

One of these limitations is our reliance on information the AI has learned. It is clear that an AI has the same learning curve as a human intelligence: Both have to see something or make a mistake before it can learn.

"Even when the malware is detected, security already has been compromised and damage might already have been done," Honzak pointed out.

The first time (at least) that an AI sees something abnormal, it may not react to the change in time to block the action or activity.

Another important limitation of AI is that we view it only from the defenders' side, when in fact the same tools are available to the attackers.

"If you're using AI to better detect threats, there's an attacker out there who had the exact same thought," Honzak cautioned. "Where a company is using AI to detect attacks with greater accuracy, an attacker is using AI to develop malware that's smarter and evolves to avoid detection."

The ability for attackers to make use of products to bypass security measures is most clear with antivirus products. While signature-based antivirus products were effective at detecting malicious software in the early days of the Internet, by some accounts antivirus products are 100 percent ineffective at detecting ransomware. This lack of utility is not because antivirus has gotten worse, but because the virus creators have gotten better.

Attackers use the same types of tools to ensure their malicious software will bypass commercial antivirus products. To address this limitation in signature based antivirus, products came on the market that would run software in a "sandbox" to test whether it was malicious or not.

Attackers then started adding timers into their software to execute only within a window, after which the sandbox would expire. The cat and mouse game continues. We surely will see the same game played with AI.

"Once attackers make it past the company's AI, it's easy for them to remain unnoticed while mapping the environment, behavior that a company's AI would rule out as a statistical error," Honzak wrote in his Dark Reading piece.

One more limitation -- and there are others not discussed here -- is the ubiquity of processing power available. While businesses across the globe have been turning to the cloud for elastic processing, so have attackers.

As far back as 2011, likely before many legitimate businesses were exploring cloud computing, attackers were using the power of AWS elastic compute to crack password files. There is no reason to assume attackers will not take advantage of products developed for legitimate businesses to defeat AI defenses.

Conclusion: AI Offers Hope

While the limitations detailed above may suggest a death knell for cybersecurity AI, that is not the final conclusion to draw. Just as AI needed IBM's Watson to make AI accessible, the development of AI for cybersecurity purposes continues.

We currently use humans for detection. If AI can realize its goal of mimicking human intelligence, then it will equal or surpass the human ability to detect threats. ECT

The opinions expressed in this article are those of the authors and do not necessarily reflect the views of ECT News Network.

Peter Vogel has been an ECT News Network columnist since 2010. His focus is on technology and the law. Vogel is Of Counsel at Foley Gardere, and focuses on cybersecurity, privacy and information management. He tries lawsuits and negotiates contracts dealing with IT and the Internet. Before practicing law, he received a master's in computer science and was a mainframe programmer. His blog covers IT and Internet topics. Email Peter.

Eddie Block has been an ECT News Network columnist since 2017. His focus is on information security and data privacy. Block is an associate at Foley Gardere. Before practicing law, he spent 20 years as an information security professional in a variety of roles, from network security management to chief information security officer for the State of Texas. His blog covers information security and data privacy topics.

Reader Comments

Be the first to comment!