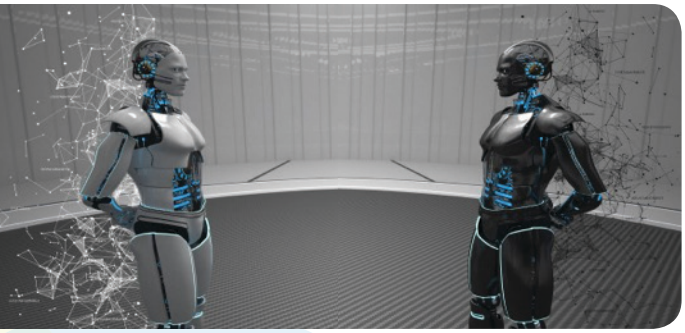
CS CYBER SECURITY & YOU

JULY 2019

WHY IS AI A CYBER SECURITY SUBJECT?

Banks and retailers are investing more money than any other industry into artificial intelligence (AI) and machine learning (ML) capabilities, with each industry expected to spend more than $4 billion this year, according to the International Data Corporation. Banking, in particular, is finding AI capabilities useful for dealing with threat intelligence and prevention systems, fraud analysis, and investigation.

As cyber threats become more complex and sophisticated, AI and ML provide the necessary efficiency and value to keep pace with the changing cyber landscape. A perfect example is ML for virus and malware detection. For decades, antivirus (AV) solutions have relied on signature-based detection. Attackers could make small changes to a virus or malware by changing the signature to bypass AV tools. With ML, algorithms analyze vast data sets of malicious programs to determine consistent features. Rather than specific signatures, ML-based scanners look for characteristics, which makes evading detection more difficult.



QUICK TIP

Artificial intelligence (AI) and machine learning (ML) are the latest buzzwords surrounding general technology trends that have also made their way into cyber security. ML is a subset of AI that relies on algorithms and large data sets to learn and adjust. AI is able to perform specific tasks similar to or better than a human. AI can also generate new conclusions without additional data. Often, AI uses ML algorithms, but may often use other methods too.

Banking apps are great examples as they use the user's location, habits, and more to deter fraud.

AS YOU MAY EXPECT, CYBER CRIME USES AI TOO

While experts have leveraged AI to improve cyber security defenses, there is no doubt cyber criminals also see the value of AI in developing methods to defeat the latest defense tools. This presents a critical threat to organizations, as these AI-based attacks can be even more difficult to detect, and allows attackers to remain inside a network for months without detection.

Malware network penetrations, for example, will be able to adapt-on-the-fly, rendering standard cyber security defenses outdated. AI could potentially be used to automate and quickly discover critical software bugs or support social engineering attacks with algorithmic profiling to achieve a higher likelihood that an unsuspecting user will click on a malicious link or file.

The first known AI-based cyber attack occurred in India in 2017. The attack took place inside a corporate network using ML to observe and apply patterns of normal user behavior. The software was difficult to detect as it behaved like a typical user. In this particular case, it was not entirely clear what the goal of the attack was meant to be, but the number of dangerous scenarios was numerous with AI and ML at play.

LASERS IT
Making Digital Retirement a Reality