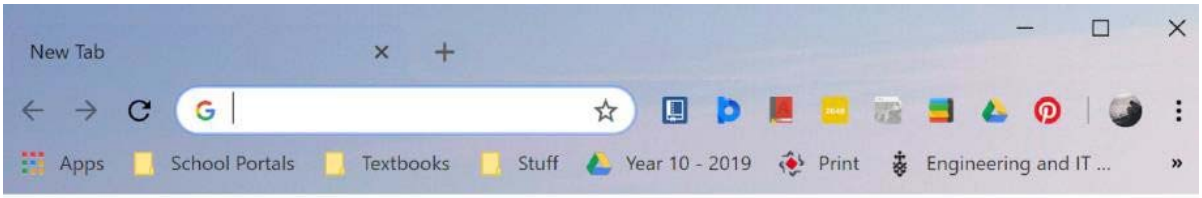

AI And Cybersecurity: Are We Fueling Hackers' Fire?

Juliette Rizkallah Forbes Councils
Forbes Technology Council CommunityVoice

POST WRITTEN BY

Juliette Rizkallah

Chief Marketing Officer at **SailPoint**, overseeing all aspects of the company marketing strategy, positioning and execution.

To present the risks of AI in malware and cyber-attacks IBM created a proof of concept a decade ago with an aim of analysing and learning from the program to create new and more robust anti-virus software. To this notion many professionals within the cybersecurity community scoffed at the idea of a program like it being a real threat. When the superior concept was presented the idea that a program could evolve to detect endpoints, attack their targets and run without detection of our modern cybersecurity software, even behavioural based defences, although worrying was largely dismissed. It seems with recent developments that we should've listened.

Through recent research many reports indicate that the use of AI in malware and other malicious programs is now widespread. Through use of AI these malware systems run separate to their developer with no traceable links through the web allowing the hackers to keep their anonymity. Since many of these programs are sitting camouflaged by benign applications hackers have created a sophisticated and widespread surveillance system which is, we believe, constantly feeding data through the algorithms and to databases off your computer.

The AI-powered malware software model that has been examined takes evasive abilities of malware to the next level. Through using a deep neural network to protect its data from being reverse engineered analysers are left scratching their heads on how they are supposed to understand and neutralise this threat.

When the proof of concept was presented a decade ago one of the biggest reasons t was dismissed was that cybersecurity professionals believed that behaviour-based anti-virus would be able to detect these programs due to their executors and general activity. This seems not to be the case, hindsight and revising previous iterations of common-use programs analysis has shown that a high-percentage of common-use programs can be found to have been compromised.

The biggest question in this ever-evolving tech landscape is what do we do now to protect ourselves against this new threat. The response that we are getting from many professionals is that they don't know. By avoiding and ignoring a proof of concept a decade ago the cybersecurity industry now finds themselves in a tough bind where they are investigating a complete unknown. All we can hope is that the upcoming generation of cybersecurity professionals, white-hat hackers and open-source developers can find a way to combat this new threat.