Hackers Now Deploying AI To Break The Best Computer Defenses

Technocracy promises Scientific Dictatorship in the end. If IBM now admits that their engineers can do it, you can be certain that U.S. Intelligence agencies have been doing it for some time. Targeted hacking is potentially the most malicious and destructive type of surveillance in history. In the hands of rogue intel, all details are laid bare before them. TN Editor

The nightmare scenario for computer security – artificial intelligence programs that can learn how to evade even the best defenses – may already have arrived.

That warning from security researchers is driven home by a team from IBM Corp. who have used the artificial intelligence technique known as machine learning to build hacking programs that could slip past top-tier defensive measures. The group will unveil details of its experiment at the Black Hat security conference in Las Vegas on Wednesday.

State-of-the-art defenses generally rely on examining what the attack

software is doing, rather than the more commonplace technique of analyzing software code for danger signs. But the new genre of AI-driven programs can be trained to stay dormant until they reach a very specific target, making them exceptionally hard to stop.

No one has yet boasted of catching any malicious software that clearly relied on machine learning or other variants of artificial intelligence, but that may just be because the attack programs are too good to be caught.

Researchers say that, at best, it's only a matter of time. Free artificial intelligence building blocks for training programs are readily available from Alphabet Inc's Google and others, and the ideas work all too well in practice.

"I absolutely do believe we're going there," said Jon DiMaggio, a senior threat analyst at cybersecurity firm Symantec Corp. "It's going to make it a lot harder to detect."

The most advanced nation-state hackers have already shown that they can build attack programs that activate only when they have reached a target. The best-known example is Stuxnet, which was deployed by U.S. and Israeli intelligence agencies against a uranium enrichment facility in Iran.

The IBM effort, named DeepLocker, showed that a similar level of precision can be available to those with far fewer resources than a national government.

In a demonstration using publicly available photos of a sample target, the team used a hacked version of videoconferencing software that swung into action only when it detected the face of a target.

"We have a lot of reason to believe this is the next big thing," said lead IBM researcher Marc Ph. Stoecklin. "This may have happened already, and we will see it two or three years from now."

Read full story here…