How AI is Becoming a Tool for Crooks, Terrorists

These days, just about anybody can have the digital equivalent of nukes.

Kevin McCaney

Fri, 05/11/2018 - 11:21

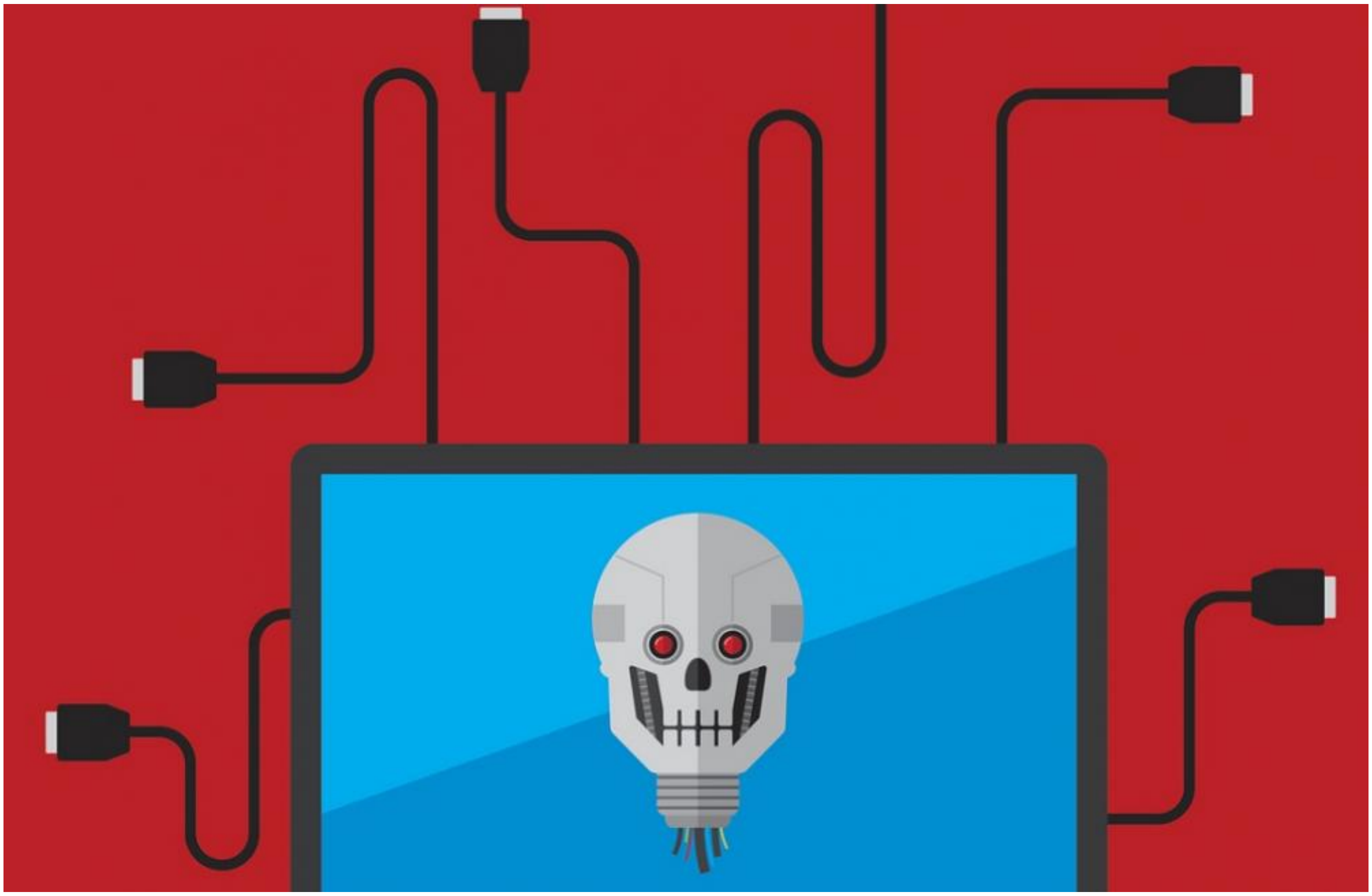

Illustration: JakeOlimb/iStock

Artificial intelligence is at the core of what's being called both the new space race and the new arms race, pitting global powers (i.e., the U.S., Russia, China) against each other to determine the "ruler of the world." But unlike those other races of days gone by, which tended to involve air forces, spacecraft, Manhattan projects and intercontinental ballistic missiles, AI isn't limited to the big cheeses on the U.S. Security Council. Because it's software, it can be employed by groups and individuals much further down the chain of aggression. These days, just about anybody can have the digital equivalent of nukes.

AI — in the form of machine learning, neural networks, cognitive computing and other approaches — has shown its power for good in fields as varied as medicine, business, transportation, cybersecurity and many others. But that power can also be put to nefarious uses beyond the tradecraft of world powers. Smaller nations, terrorist groups and straight-up criminals can now add AI to their arsenals.

A recent survey by the cybersecurity company Webroot found 91 percent of security professionals worry about hackers using AI in their attacks. How can AI ramp up attacks?

More Spears for Phishing

Phishing and the more precise spear-phishing, which can target individuals instead of broad swaths of people, has been the foot in the door for many of the most high-profile cyberattacks of recent years, like the 2014 hack of Sony.

Phishing, like spam and other email scams, is a popular tool among cybercriminals because it’s cheap —sending a million emails doesn’t cost much — and it often eventually works. Sooner or later, someone will click a spoofed link and/or give up their password. Spear-phishing, which might target an executive or manager, can be even more effective, but also requires more work. For that, attackers need to create a profile of someone, perhaps gleaned from their interactions on social media and other publicly reported work.

AI’s data collection and analytics tools can do those labor-intensive jobs for malicious actors, giving them more spears to work with. Thus, the more advanced, targeted attacks will likely become easier, cheaper and, as a result, more prevalent.

If it Looks Like a Duck and Quacks Like a Duck, it’s a Piranha

AI is getting awfully good at impersonations, especially recently. It took 64 years until a program in 2014 passed the “Turing Test,” designed to see if a computer program could convince someone it was human. Suddenly, the test seems to have become a very small hurdle.

AI systems now are capable of learning and mimicking writing styles. If a malicious program gains access to your email or personal assistant, it could learn how to impersonate you or someone else you regularly correspond with and trust. An apparently legitimate message from someone you trust could actually be from an AI bot.

AI is also making strides in speech synthesis and bringing Photoshop-like manipulation to videos, tactics that could be employed for propaganda and other misinformation as well as for more targeted uses. A report earlier this year by Oxford and Cambridge universities said “AI systems can now produce synthetic images that are nearly indistinguishable from photographs,” along with audio recordings and video, opening the possibility for entirely artificial creations people could mistake for the real thing.

Google demonstrated what’s possible this month at I/O 2018, playing a recording of Google Duplex making an actual call to book an appointment at a hair salon. In this case, Duplex’s voice was that of a young woman and was complete with verbal ticks like “um” and “ahh” and the habit of going up in register at the end of each sentence, you know, like everything’s a question. Anyway, the call worked, and the appointment was made.

While it would be handy to have your digital assistant make appointments for you — though Google says Duplex is still under development and has a long way to go — it isn’t hard to imagine something like that used for less than honest uses.

Barbarians Inside the Gates

Hackers get around most anti-malware protections using polymorphism, which uses algorithms to constantly change the identifiers — such as names, signatures or encryption keys — that security solutions use to recognize users and flag malware. It’s already in wide use — Webroot says in its 2018 Threat Report 94 percent of all the malicious executables it sees are polymorphic.

The next wave of polymorphic malware, turbocharged by AI, will be able to create entirely new, customized attacks that won’t rely on a single algorithm, as CSO Online points out. AI can also enhance other types of online attacks, getting around Captcha and other protections.

With the help of AI, criminals and other online actors will probably come up with types of attacks that haven’t been thought up yet. The key to defending against them, security experts say, is to expect them, and follow up with a defense-in-depth approach that includes user education, layered protections and, not least of all, AI-powered tools that can detect and mitigate AI-powered attacks.

View printer friendly version

Artificial Intelligence
Eye on AI
Federal Cybersecurity
phishing
cyberattacks
Google Duplex
Data Analytics
polymorphism