Digital Security
Progress. Protected.

THE ROLE OF AI:
can hacking become easier?

Should the cybersecurity world prepare for AI-based critical infrastructure attacks?

Imagining a future, in which anyone could be attacked by an intelligence beyond the means of humans is rather scary. Perhaps that's why AI is better imagined as another tool to support people's work. Again, however, the combined capability of such a human actor is also of concern, especially if said actor does not have their community's best interests in mind.

With AI becoming increasingly important, just like companies, people race to figure out how it could be used to serve their own purposes, supporting their endeavors. Specifically in the field of cybersecurity, AI can serve both a constructive, but also a destructive role, with the former meaning the support of better cyber defense, and the latter attempting to cripple said cyber defenses.

June 2023

Of specific concern is the potential for cyberattacks on critical infrastructure to become more widespread.

Critical infrastructure, usually considered to include power generation and electrical grid, hospitals and healthcare systems, and the global supply chain, could also include digital supply chains and the internet itself. Depending on the specific needs, resources, and development level of a nation, critical infrastructure represents all the systems, networks, and assets that are essential, with their continued operation required to ensure the security of a given state, its economy, and the public's health or safety. As the idea behind the attacks is to weaken adversaries by crippling their day-to-day business, an effective AI tool could, hypothetically, help bad actors commit attacks, or even increase the pool of potential attackers, by making malware coding easier. However, not everyone shares the same opinion.

www.eset.com

The role of AI
CAN HACKING BECOME EASIER?

According to an interview with ESET security researcher Cameron Camp, we are not really close to "full AI-generated malware," though ChatGPT is quite good at code suggestion, he says, generating code examples and snippets, debugging, and optimizing code, and even automating documentation.

He agreed that ChatGPT could be used as a handy tool to assist programmers, one that could serve as a first step toward building malware, but not yet, as it is currently rather shallow, makes errors, creates bogus answers and is not very reliable for anything serious.

Nonetheless, Mr. Camp highlighted three areas, which might be interesting from the perspective of language models:

More convincing phishing

From probing more data sources and combining them seamlessly to create specifically crafted emails where clues to their malicious intentions would be very difficult to detect, readers will be hard-pressed not to fall for social engineering.

> *we are not really close to "full AI-generated malware," though ChatGPT is quite good at code suggestion, generating code examples and snippets, debugging, and optimizing code, and even automating documentation.*

Nor will people be able to spot phishing attempts simply due to sloppy language mistakes, as they could have convincing grammar.

More specifically, spear-phishing could become even more convincing, as tailor-made emails or messages, even including personalized emotional triggers, could become easier to construct thanks to AI help. These abilities will be further supported by with multilingual text-generating options, such methods might work on a wider, global scale, which in case the targeting of critical infrastructure of several states at once would serve a useful purpose.

Ransom negotiation automation

Smooth-talking ransomware operators are rare, but adding a little ChatGPT shine to the communications could lower the workload of attackers seeming legit during negotiations. This will also mean fewer mistakes that might enable defenders to home in on the true identities and locations of the operators.

Better phone scams - With natural language generation getting more natural

Furthermore, thanks to easier video and voice generation with AI (see example here), malicious actors could become anyone, hiding their identities more efficiently. In fact, concerns about AI have become so widespread in this area that many professionals want to stipulate in their contracts a ban on the use of their work for AI purposes. And if you don't believe this, check out this video of President Biden, Trump and Obama discussing a video game, all AI-generated, of course. Imagine how, during a ransomware attack, an online intruder could imitate a highly placed official to ask for access to a network or a system remotely...

Better phone scams

With natural language generation getting more natural, scammers will sound like they are from your area and have your best interests in mind. This is one of the first onboarding steps in a confidence scam: sounding more confident by sounding like they're one of your people.

As long as scammers generate the right natural cadence to a person's voice, they can easily fool their victims, but the problem with any AI-generated content today is that there is an inherent, let's say, 'artificiality' to it, meaning that despite these voices, videos or text looking legit, they still harbor some specific mistakes or issues that are easy to spot, like how ChatGPT makes false statements or how its responses might seem like it is just regurgitating a Wikipedia page.

However, all of this does not mean that generative AI cannot be used for brainstorming, to create a base for some work, however, the correctness of the information one is provided should still be checked. The legal ramifications of using AI-generated content (sourced from the net) might also be something to consider.

ESET® Digital Security
Progress. Protected.

Critical Infrastructure vs. AI – emerging legislation

As AI starts to play an increasingly important role in cybersecurity, businesses and governments will need to accommodate and use AI to their own advantage – as crooks will definitely try to do the same. From a July 2022 report by Acumen Research and Consulting, the global AI market was $14.9 billion in 2021 and is estimated to reach $133.8 billion by 2030.

Thanks to the growing use of the Internet of Things and other connected devices, cloud-based security services could provide new opportunities for the use of AI. Antivirus, data loss prevention, fraud detection, identity and access management, intrusion detection/prevention systems, and risk and compliance management services already use tools like Machine learning to create more resilient protection.

On the flip side, bad actors could also use AI to their advantage. With a large enough market of smart AI, crooks could easily use it to identify patterns in computer systems to reveal weaknesses in software or security programs, enabling them to exploit those newly discovered weaknesses.

So, critical infrastructure could become one of the targets. With AI attacking and defending it, going for a tit-for-tat, security actors and governments will have to remain smart. The European Union is already trying to assess the risks by proposing the EU AI Act, to govern its use in Europe, classifying different AI tools according to their perceived level of risk, from low to unacceptable. Governments and companies using these tools will have different obligations, depending on the risk level.

Some of these AI tools may be considered high risk, such as those used in critical infrastructure. Those using high-risk AIs will likely be obliged to complete rigorous risk assessments, log their activities, and make data available to authorities to scrutinize to increase compliance costs for companies. In case a company breaks the rules, the fine would likely be around 30 million euros or up to 6% of their global profits.

Similar rules and ideas are included within the recently proposed EU Cyber Solidarity Act, as government officials try to stay ahead of critical infrastructure attacks.

Further reading:

- Cybersecurity threats to critical infrastructure - Video
- Critical infrastructure: Under cyberattack for longer than you might think
- Critical infrastructure attacks on the rise

Author

Márk Szabó
PR and Security Writer,
ESET