Architecting the Developer Experience (Nov 12th): Register Free with promo code DEVEXNOV25

Has an AI Cyber Attack Happened Yet?

Key Takeaways

- AI cyberattacks are becoming a rising security threat both for everyday people and large government agencies.
- It is now becoming easier for hackers to develop machine algorithm hacking methods or use botnets to their full capabilities as those methods spread across the web
- Overall, machine learning algorithms are becoming more complex and accurate. Every time a bot system makes a spam attack, it becomes better when it tries again.
- Cybersecurity agencies and website developers will need to respond with far more innovative solutions to effectively protect their users' data.

It is a truth in the IT sector that digital developments are rarely as impressive or dramatic as what sci-fi movies and books imagine them to be.

Take AI cyber attacks as an example. There haven't been any robot or AI uprisings, obviously (at least not yet). But if you were to ask a random person if an AI cyber attack has happened yet, odds are good they will respond in the negative.

But the reality is that AI cyber attacks have happened and are happening, with increasing regularity to boot. We are now living in a vastly more sophisticated digital landscape, even if it isn't quite as flashy as many people predicted. Even though the AI algorithms running around online aren't as noticeable as you might think, they exist, and they're affecting the cybersecurity industry dramatically.

As a result, AI cyber attacks are becoming a rising security threat not just for big government agencies but for everyday people, too. While hackers have been a problem for as long as the Internet has existed, their reach and ability to steal vast amounts of data have become more powerful.

Recent Attacks

One of the most recent AI-assisted cyber attacks came when TaskRabbit, an online marketplace for freelance laborers and their clients, was attacked by hackers. 3.75 million users of the website were affected in April 2018 when their Social Security numbers and bank account details were scooped from their user data. The attack was performed by hackers using a huge botnet controlled by an AI, which used slaved machines to perform a huge DDoS attack on TaskRabbit's servers. The attack was so drastic that the entire site had to be disabled until security could be restored. In the interim, unfortunately, an additional 141 million users were affected.

Let's also not forget that WordPress has recently revealed that its websites have come under massive botnet assaults. Over 20,000 WordPress sites have so far been infected with a botnet-style cyber attack, which may eventually grant hackers access to users' personal information and credit card numbers. This attack shook faith in WordPress for many users, even those with great hosting services.

More recently, the social media giant Instagram suffered two cyber attacks in 2019 alone. Starting in August, many Instagram users found that their account information had been changed by hackers, locking them out of their social profiles. In November, a bug in Instagram's code led to a data breach that showed users' passwords in the URL of their browsers – a massive security issue, to be sure. Though Instagram have so far failed to release detailed information on the hack, many have speculated that hackers are using AI systems to scan Instagram user data for potential vulnerabilities.

Overall, it's clear that AI-assisted attacks are only going to get worse, both from botnet attacks and from general malware spreading.

In a nutshell, a single minor security breach now has the potential to lead to more dramatic breaches. Even if you've ticked the boxes of basic internet security - setting up a firewall, regularly scanning for malware, using a secure CMS like WordPress, and an experienced cyber security team - hackers who have the technology and know-how necessary to make the most of security vulnerabilities will do so.

The Rise of Bots

One of the biggest ways in which we can see AI-assisted cyber attacks affecting our daily lives is through Twitter. We've all heard one political party or another accusing the other of using "bots" to misrepresent arguments or make it seem like certain factions had more followers than they actually did.

Bots by themselves aren't a huge deal, and lots of companies and services use bots to drive customer engagement and funnel people through different areas of the website. We've all seen the bot-powered chat boxes on sites where you might have a question, like the homepage of a college.

But the real issue with bots is that they are becoming more sophisticated. In an ironic twist to the Turing test, it's becoming increasingly difficult for people to tell bots apart from real people, even though machines once almost universally failed the exam. Google has recently provided higher metrics for AI-generated audio and video, demonstrating this trend.

These bots can pretty easily be used for misinformation, like when users marshal them to flood a Twitter thread with false posters to influence an argument. But

they can also be used to DDoS the computers and networks of an enemy. Granted, this kind of attack has been in the toolkit of hackers and teenagers with too much time on their hands for decades now. But infamous moments like the time a group of hackers took down the PS4 network using a variety of DDoS attack demonstrates the issue.

Not to mention the bots who do only spam on Facebook and Twitter are often better at it than their human counterparts. While it is somewhat humorous that machines are better than people are spam, it's still a real problem to be solved before online discussion forums can ever be taken seriously. Many might even say that misinformation on this scale is a kind of cyber attack even if the threat is not what you would expect.

Overall, machine learning algorithms are becoming more complex and accurate. As reported by the World Economic Forum, AI tools could "supercharge" traditional cyberattacks by gradually learning what kind of approach works best. They highlight a notorious phishing Trojan – Emotet – as one potential piece of malware that could be "improved" in this way. Currently, the message on the phishing email sent by Emotet is highly generic – "Please see attached", for instance – and this may sometimes arouse suspicion. By leveraging an AI's ability to learn and replicate natural language, though, these phishing emails could become highly tailored to individuals.

These systems also have a huge amount of data from which they can learn and refine their techniques. At the same time, it's getting easier for many to build AI

bots, which just makes it even easier for novice hackers to cut their teeth on simple hacking jobs and find relative success.

In a very real way, the bar has never been lower for the skills and tech you need to successfully pull off some kind of AI-assisted cyber attack.

Why Are AI Attacks on the Rise?

AI cyber attacks have been on the rise in recent years. Even as many companies transition to more secure data protection solutions such as cloud storage services, their data remains very vulnerable to hackers. At the same time, everyday people are giving more data to companies than ever before, particularly through device or app usage or through subscription services.

It's just a matter of machine efficiency versus human effort. An AI botnet that can harness a multitude of computers far beyond what a human could enlist and make an attack faster and more unpredictable than even the best cybersecurity team can react to.

Machine learning allows every algorithm to adapt and become more efficient at attacking processes, whether they're successful or not.

Think about it. Compared to humans, AI:

- Is faster
- Is more adaptable (in some ways)
- Doesn't get tired
- Doesn't need to get paid

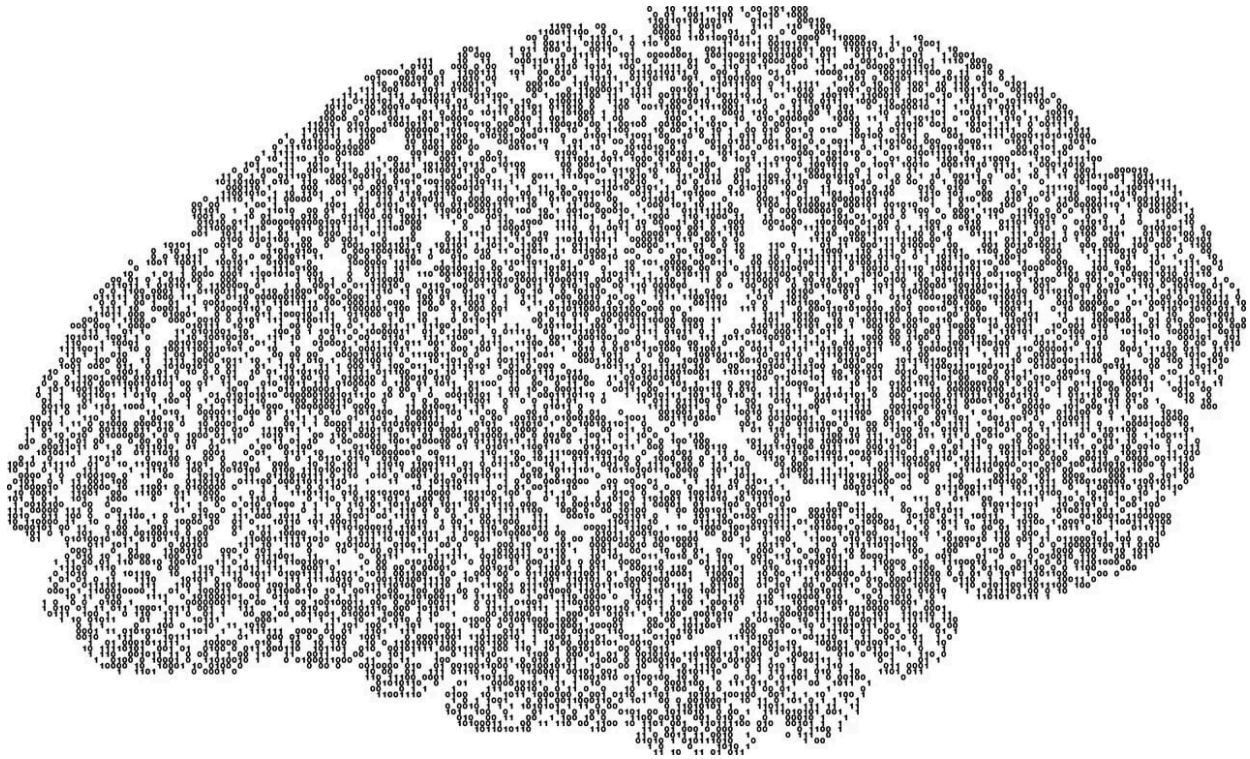
To make things even worse, it's becoming easier for hackers to develop machine algorithm hacking methods or use botnets to their full capabilities as those methods spread across the web. AI-assisted attacks and algorithms were once relatively obscure or rare, but now they're easy enough to create than even *Twitter* is inundated with them.

With the proliferation of machine learning and AI-assisted hacking techniques, cybersecurity is also becoming less reliable. It's now less about stopping threats and more about patching holes in a leaky ship. There's simply too much rapid development on the side of hackers that it's impossible to keep up.

This doesn't even get into the added complexity from the Internet of Things. As devices become more interconnected than ever before, new doorways that hackers can use to get access to networks and sensitive information multiply. In prior decades, hackers were relatively limited to terminals if they wanted to crack a network.

Now, the Internet of Things can be hacked and provide security breaches into networks like those of a smart home or small business. Imagine your smart home security system being breached and giving a hacker your account information for your streaming services. These, then, allow access to your credit cards, which then lead to your social security number, which can lead to account creation fraud, and so on.

It isn't just about data, of course. Many aren't yet aware of the ways that hackers can gain access to networks, especially as potential vulnerabilities keep multiplying faster than anyone can keep up with. For instance, new small businesses that don't use secure payment processing might be especially vulnerable to financial breaches through something as simple as an issue with their site's payment page.



Defense Strategies

Part of the difficulty of adjusting to these threats is that they evolve rapidly and

they allow hackers to remain hidden much more easily than before. It's much more difficult to find out who's behind a big botnet attack, obviously, than an isolated actor.

Things are tricky as well because defending against AI cyber attacks isn't as simple as securing your website's http tag with httpS. Oftentimes, your information is vulnerable because it's in the hands of other companies who may not be so secure, or your password might have been leaked. Data that is leaked in this way is worth its weight in gold for hackers running AI-assisted attacks, because it can be used to "feed" the AI engines that are looking for patterns in user data, and vulnerabilities in corporate systems.

Some have therefore wondered if we might be able to use AI to turn the tide. After all, fighting artificial intelligence with more AI does sound like an efficient way forward.

One of the best ways in which bots spamming on political or social media channels can be countered is through the use of machine learning bot detection programs. Several companies and organizations have developed these. Botometer is a bot-detection app developed by the Indiana University Network Science Institute (IUNI) and the Center for Complex Networks and Systems Research (CNetS). Similarly, for developers there is Tweetbotornot, an open-source package for developers created by Michael Kearney, a professor at the Informatics Institute in the University of Missouri.

These programs use the same algorithmic methods that bots do to become more effective at their disruption to tell when a bot is behind all the ruckus. The ways in which this can work are varied: sometimes it's biometric, or sometimes it's based on prior user data (in the event of a hacked account).

Another potential solution is to use AI-enhanced fact-checking. Machine learning and algorithms that benefit from this are much more efficient than if you were to hire many humans to check the millions of tweets and social media posts that are generated each day. It may be that the same kinds of artificial intelligence systems that create the problem misinformation may be responsible for fixing it in the future.

AI isn't the only way forward, either. Preventative or proactive security methods from cybersecurity teams may yield greater security results than typical antivirus

measures. Focusing on shoring up basic cybersecurity defenses is one way in which they can make the job of a would-be hacker more difficult.

Plus, AI can't help with strong password security and generation. Basic digital hygiene practices, like relying on strong passwords that you alternate between every so often, can do a lot for general security for your home network or your company. Many companies are investing in regular meetings in educational seminars for their employees so that basic computer security can be shared and understood by all.

This is more important now that the Internet of Things is in play. If letting hackers into your Netflix account is enough to eventually giving them access to everything else, there's really nowhere in your network where subpar security is allowed. It all sounds a little over-the-top, but it's the reality when AI has become such a big player in the cybersecurity game.

Conclusion

Ultimately, the future of digital security is unclear now that AI has become a major tool in the hands of hackers. While AI may be an effective shield against these kinds of cyber attacks and misinformation campaigns, cybersecurity agencies and website developers will need to respond with far more innovative solutions to effectively protect their users' data.

Still, the rise of AI cyber attacks may yet yield some interesting developments. We've long gotten used to an Internet where total, perfect security was not fully necessary for many of the general population. If that laziness is no longer rewarded, the eventual result may be an Internet that is safer and more mature than before.

About the Author

Sam Bocetta is a former security analyst, having spent the bulk of his as a network engineer for the Navy. He is now semi-retired, and educates the public about security and privacy technology. Much of Sam's work involved penetration testing ballistic systems. He analyzed our networks looking for entry points, then created security-vulnerability assessments based on my findings. Further, he helped plan, manage, and execute

sophisticated "ethical" hacking exercises to identify vulnerabilities and reduce the risk posture of enterprise systems used by the Navy (both on land and at sea). The bulk of his work focused on identifying and preventing application and network threats, lowering attack vector areas, removing vulnerabilities and general reporting. He was able to identify weak points and create new strategies which bolstered our networks against a range of cyber threats. Sam worked in close partnership with architects and developers to identify mitigating controls for vulnerabilities identified across applications and performed security assessments to emulate the tactics, techniques, and procedures of a variety of threats.

Please see https://www.infoq.com for the latest version of this information.