AI in cybersecurity - friend or foe?

By Simon McCullough

13 Jun 2019

It's no news that advances in AI and machine learning have enormous transformative potential for cybersecurity defences.

Simon McCullough, Major Channel Account Manager, F5 Networks

However, rapid advances in technology also result in big opportunities for hackers to get smarter and faster. So, when it comes to cybersecurity, is AI a friend or foe?

Although the AI arms race is just beginning, the ultimate potential for automated threats is vast and unknown. AI-based malware alone will soon become a widespread plague, so businesses need to pay attention or risk getting caught out.

Automated threats on the rise

We've already started to see how AI-based malware can be used to scale up attacks. Polymorphic malware, for instance, can constantly adapt so its code can't be identified. TrickBot is another example of a stealthy threat that has evolved and expanded its capabilities from a banking trojan to target credit card companies and wealth management services.

With TrickBot, the threat's code enters a network and infects systems automatically, making it difficult to detect and mitigate as it changes to avoid detection. TrickBot is also known for its resilient infrastructure, including command and control (C&C) servers set up on hacked routers, many unique C&C IP addresses, as well as regular updates to make it harder to take down.

Where next?

It is conceivable that we'll soon see a rise in AI-powered phishing emails, high-quality spam and a vast proliferation of false flags. We're already noticing this with threats like TrickBot, which consistently use email spam and phishing campaigns as its initial attack pattern. As a result, it is imperative that businesses train their employees to spot potentially fake emails, not to open suspicious file attachments or click on questionable embedded links. Currently web application firewalls can help

detect and mitigate banking trojans, but businesses need to ensure they are updated regularly to keep pace with AI-powered threats.

Intriguingly, AI could soon be used to conceal malware presence in a victim's network and combine various attack techniques to identify the most effective disruptive option. In time, hackers will be able to use AI to bypass security algorithms. It is critical that all likely targets – and few are immune – start to harness AI to fight back.

The business battle

AI's widespread adoption across different areas of a business can make it difficult to understand where to best deploy security systems, and where to focus cybersecurity teams' efforts.

Organisations need to ask themselves a series of questions. What are the strengths and weaknesses of the IT infrastructures? Who in the cybersecurity team is fighting the attacks? Where are resources required to better cope with AI-based threats? What employee and industry behaviours influence security defences? Answering these kind of questions makes it easier to determine the best use of AI.

The key is to adopt a prevent, detect and response strategy. If deployed correctly, AI can be used to collect intelligence about new threats, attempted attacks and successful breaches. It can detect abnormalities within an organisation's network and flag them more quickly than a human ever could.

Businesses can also make life difficult for hackers by isolating vulnerable applications. This is a useful method to reduce threat risk and render malware harmless by allowing it to fully execute in a completely isolated, contained environment. Crucially, it helps protect against the most common attack vectors, such as malicious downloads, plug-ins and email attachments.

As the use of apps across organisations continues to soar, these are the areas hackers will target with AI-powered attacks. Securing applications must always be a key concern for business leaders looking to ensure IT infrastructures are continually protected, despite new technologies entering the market.

AI versus AI

The business case for AI in cybersecurity is strong, and the operational efficiencies of automation are becoming clearer with each passing day. Even so, it is important to not entirely rely on automation. It is not a silver bullet, and security teams should still be present in frontline roles. For example, there will always be a need for specific human knowledge and interaction with application services.

Cybersecurity as a discipline currently boasts one of the widest uses of AI in the enterprise space, and it's clear that adoption isn't slowing any time soon. Everyone needs to remember that AI can be both a weapon of mass destruction and a vital part of the solution.

ABOUT SIMON MCCULLOUGH

Major Channel Account Manager at F5 Networks

- Try to tackle cybersecurity during #RWC2019 - 20 Sep 2019
- Stay safe from cybercrime with what's left of 2019 - 30 Aug 2019
- Multi-cloud's new multiculturism - 21 Aug 2019
- A new phase of cyber warfare has begun - 7 Aug 2019
- The ABC of DevOps - 27 Jun 2019

View my profile and articles...