The role of AI in email security

Barracuda

The evolution of email fraud

Email remains the most common initial attack vector for cybercriminals. Infiltrating an organisation via an email-based attack can happen at any level — phishing is not only targeted at the C-suite. Once attackers have got an individual's credentials then they can gain access. Once inside the network with one set of credentials, attackers can more easily move laterally and gain more permissions and fuller access. Even access to an employee's mobile can be escalated into wider network access.

Early email fraud messages were often badly written and frankly unbelievable. Criminals relied on a 'spray and pray' approach — sending out thousands of messages in the hope that a few would stick. Traditional gateway defences are quite adept at dealing with these high-volume attacks. Barracuda's own data shows that 16% of all email traffic is this sort of high-volume attack such as spam, malware, and other emails with a malicious payload. You still need gateway defences to stop these attacks as they remain a real danger.

But phishing is different. Barracuda sees only 0.1% of messages as being personalised phishing attacks. But while the numbers are not high, the potential danger is very real. Behind this small number of messages there are very determined and focused criminals.

Today's phishing and impersonation emails appear to come from someone you know and they ask you to act in a way that seems logical, and sensible. Finance departments get payment requests from CEOs and CFOs. Messages come from what looks like a genuine address. There is an explanation for why payment is needed in a different way from normal — an urgent opportunity for the business, or the need to pay a named, and correct, supplier to take advantage of a special offer. Emails are timed for month end when finance departments are busy and possibly paying less attention.

Criminals are quick to mimic new messaging formats. Account lock-out warnings are an increasingly common way to force a user into taking urgent action. But they also set up pages on third-party business services like Dropbox, OneDrive, or Google Drive to harvest credentials. These are hard for users to spot because businesses and their clients rely on an increasing variety of cloud services for collaboration and file sharing. These messages are not typically picked up by gateway defences because the emails themselves contain no malicious payload.

Why can't traditional gateway defences cope?

The problem with email defence is a problem of scale and flexibility. The old ways of blocking known domains do not work anymore because compromised domains change so quickly. Because attacks do not contain an easily detected payload, they are very hard to block at the gateway.

Setting rules to flag messages does not work when attacks change so fast.

The cost of defending a gateway like this is almost constant hands-on management and a high risk of false positives and false negatives. Such a system also comes with an infrastructure and compute cost – every rule added means more time spent processing.

And as the volume of attacks grows, existing systems — and staff — become overwhelmed.

Any system that relies on rules is at risk from attackers with automated systems that can learn your rules almost as fast as you deploy them. That does not mean you do not need gateway protection. Such defences remain excellent at blocking malicious payloads and spam which makes up the majority of bad email.

Good AI-based email defence can block the majority of attacks and dramatically reduce the number of alerts that require human intervention.

How can AI help keep you safe from phishing attacks?

AI uses data science and machine learning to examine metadata, content, context, and typical user behaviour.

AI can do what humans are meant to do. It can check domain spelling and email headers, and it can filter out suspicious emails better than non-smart or list-based systems.

But AI can also go a step beyond normal defences. AI uses natural language processing to look at the context and meaning of the whole message.

Good AI will learn about your organisation and environment in order to provide the best defence by spotting anomalies and unusual communications. By building an understanding of your users it will be more capable of blocking phishing attempts and less likely to flag false positives.

If someone makes an unusual request, uses an unusual email address, or asks a favour of someone they never spoke to before, AI can quickly flag this abnormal behaviour. It can even spot a change in a tone within a message — if a user becomes more polite or more demanding.

Phishing emails do have some traits in common. They often ask for fast responses, so people don't have time to think. They often demand secrecy, so people are discouraged from checking with others.

AI systems can not only process vast amounts of data quickly, but actually get better as a result. They are able to spot socially engineered attacks while standard email gateway defences would let them through. Properly set up AI systems should be cheaper to run, with less need for human oversight or management than traditional email defences. And cloud-based AI systems can scale fast when required.

AI best practises: How to choose the right provider

The difficulty with choosing an AI security provider is that you are dealing with something of a ‘black box’. So it is important to focus on real-world results rather than listening to lists of apparent capabilities the system offers.

That means looking at detection efficacy — how the system performs for your organisation. Barracuda and some other vendors offer ways to test the efficacy of their systems. There is no charge for running Barracuda’s Email Threat Scanner against users’ inboxes, to find the malicious emails your current defences have missed. Some 16,000 organisations have used the free scanner and found 12 million threats in their inboxes.

You also need to ask about the false positives, false negatives rate and how these numbers change over time as systems get smarter.

Good systems integrate easily into your existing security infrastructure and do not require much, or any, infrastructure investment. They should also provide flexibility in how they remediate against attacks and how they provide data for reporting and other analysis tools. And of course, AI should make life easier for security teams, not add more noise and unnecessary alarms and alerts.

Visit our website for more information on Barracuda’s AI-enabled Email Protection.

Barracuda

About Barracuda

At Barracuda we strive to make the world a safer place. We believe every business deserves access to cloud-first, enterprise-grade security solutions that are easy to buy, deploy, and use. We protect email, networks, data, and applications with innovative solutions that grow and adapt with our customers' journey. More than 200,000 organisations worldwide trust Barracuda to protect them — in ways they may not even know they are at risk — so they can focus on taking their business to the next level. For more information, visit barracuda.com.