Antigena Email: Spear Phishing & Payload Delivery

Phishing attacks typically aim to deceive employees into clicking malicious links or attachments in an email, with the ultimate aim of harvesting credentials or deploying malware into an organization. These emails can be launched either as indiscriminate 'drive by' campaigns aimed at thousands of organizations, or carefully crafted 'spear phishing' attacks that are targeted towards the recipient.

Most email security tools rely on knowledge of previously identified threats, measuring inbound emails against a pre-defined blacklist to determine whether they are malicious. These solutions are confined to the border and only look at emails in isolation. In addition, payloads containing novel strains of malware easily bypass this legacy approach, leaving business vulnerable to these advanced attacks.

As email-borne attacks begin to utilize artificial intelligence, phishing emails are becoming increasingly well-crafted and customized to the recipient, with malicious payloads often concealed behind plausible links and disguised buttons.

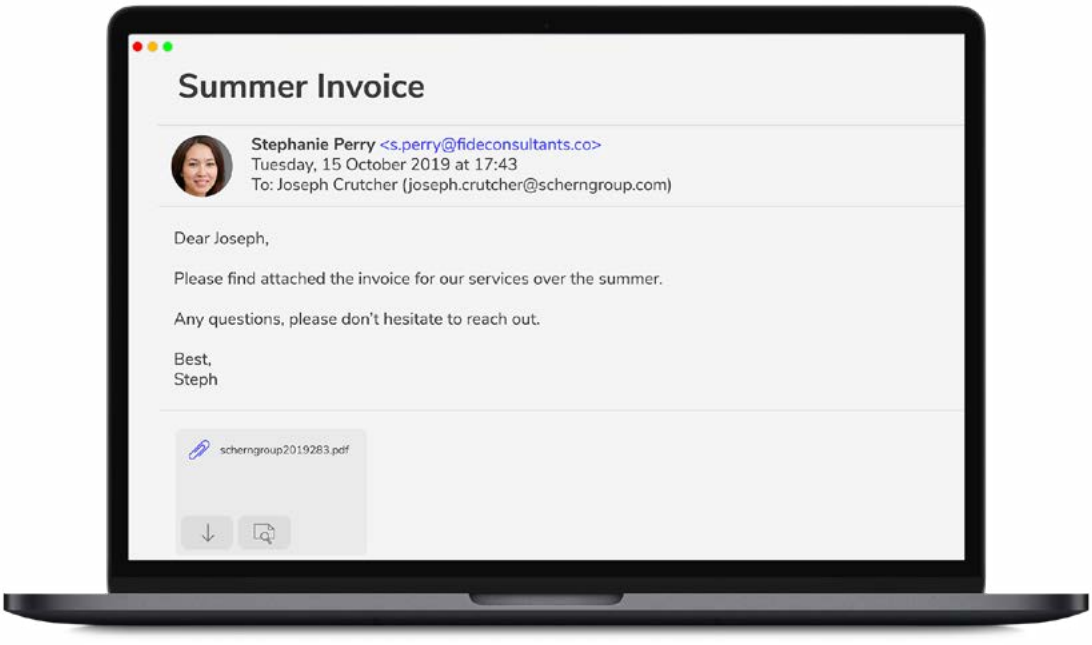

Figure 1: An email coaxing an employee into clicking on an attachment containing a malicious payload

Antigena Email: Learning Patterns of Life

Antigena Email is able to analyze hidden links and attachments in connection with all inbound, outbound, and lateral communication, and with the rich context of what normal 'patterns of life' look like for the dynamic humans behind every email. In instances of phishing attacks, Antigena will recognize that neither the recipient nor anyone in their peer group has visited the suspect domain before, raising a high-confidence alert. It also analyzes where the potentially malicious payload is located within an email, noting, for instance, if it is disguised behind various buttons designed to look like trusted sites.

By learning the digital DNA of your organization's email platform, Antigena Email can make intelligent decisions autonomously, initiating a targeted response in real time. Depending on the perceived nature of the threat, possible actions include flattening attachments, locking malicious links as they enter the network, and even retrospectively pulling emails from inboxes in light of emerging evidence.

Case Study: Antigena Email Stops 'WeTransfer' Phishing Attack

Antigena Email had been deployed for only a week at an academic institution when it detected a sophisticated email attack targeting five high-profile users. The emails were well-written and highly plausible, attempting to coax the recipients into clicking on a malicious link. This attack could easily have succeeded had Antigena not been analyzing every incoming email against the 'pattern of life' of the organization.

The emails, supposedly coming from WeTransfer, were given a 100% anomaly score and Antigena Email suggested holding them back from the end user. Darktrace recognized a disguised malicious link and also identified the signs of spoofing, despite the organization having a known relationship with this sender.

From the connection data, we can see that there were no clear signs in the headers that this email was not in fact coming from WeTransfer. However, there were some subtle anomalies that Antigena Email was able to pick up on. Firstly, the 'Address IP Anomaly Score' was high (63%). This metric indicates how unusual it is for this email address to send from this IP based on historical sending patterns, and is also an indicator of spoofing or account hijack.

In addition, as Antigena Email is constantly modeling the 'normal' behavior of every trusted external sender, it was able to pick up on a key anomaly in the body of the email: an inconsistent link, which was totally irregular compared to what Darktrace had seen from WeTransfer previously. This context allowed Antigena Email to identify the link as the malicious payload in the email.

The link in question was hidden under buttons in multiple places within the email, including a fake 'https://wetransfer.com/...' link and the text 'Inquiry Sheet.xls'. Antigena gave the link a 96% anomaly score.

This incident demonstrates Antigena Email's application of anomaly detection to identify advanced phishing attacks that leverage the familiarity of a trusted website in order to deliver a harmful link and gain multiple footholds in the organization.

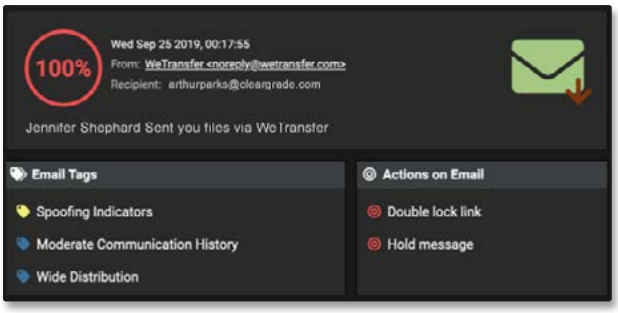

Figure 2: The user interface showing the model breaches and actions

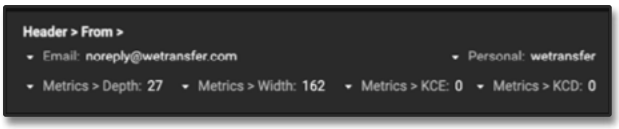

Figure 3: The connection data of the relevant emails

Figure 4: A breakdown of the links shown in the emails