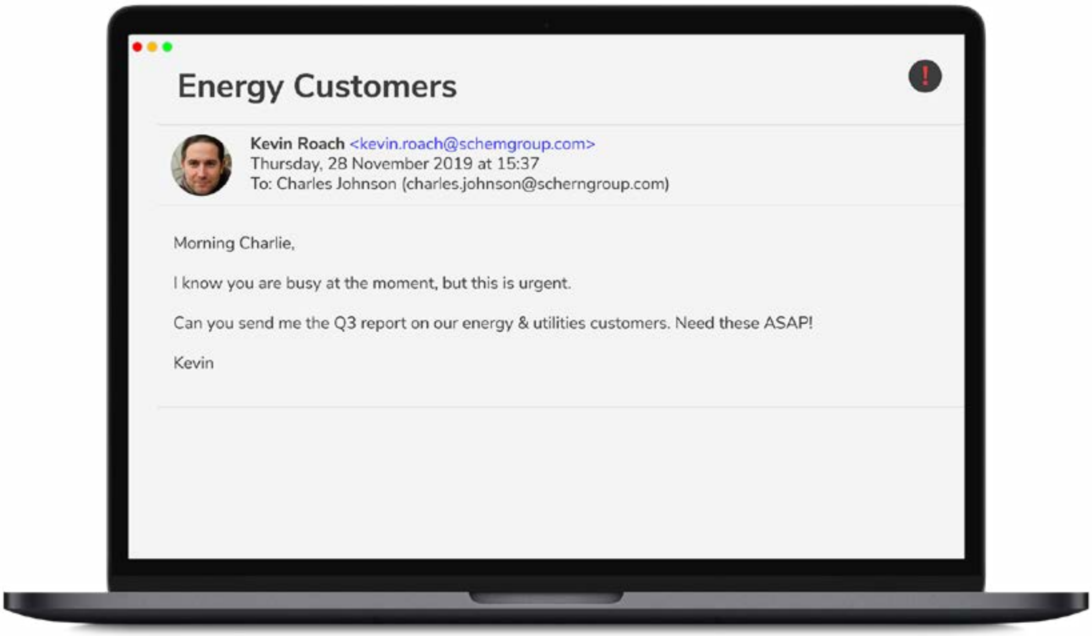
Antigena Email: Social Engineering & Solicitation

Social engineering attacks are characterized in every case by an attempt to leverage the pervasive assumption of trust in an enterprise. By posing as a trusted colleague, contact, or executive, attackers can tailor their communications accordingly and quickly gain a foothold in an organization – whether to wire a fraudulent payment or coax an employee into sharing sensitive documents and company information. These attacks typically come in the form of 'clean' emails, with no malicious links or payloads, which makes them even harder to detect.

As attackers continue to develop their tactics and techniques, social engineering and solicitation attacks are becoming even more effective. Machine learning software is available today that can learn the style in which two users interact and replicate these communication patterns. This can be leveraged by attackers to convincingly impersonate a trusted contact, such that the task of differentiating between a legitimate email and an AI-powered social engineering attack becomes nearly impossible.



Energy Customers

Kevin Roach <kevin.roach@schemgroup.com>
Thursday, 28 November 2019 at 15:37
To: Charles Johnson (charles.johnson@scherngroup.com)

Morning Charlie,

I know you are busy at the moment, but this is urgent.

Can you send me the Q3 report on our energy & utilities customers. Need these ASAP!

Kevin

Figure 1: An attacker posing as an executive, seeking to leverage sensitive documents. Note the spoofed email address.

Antigena Email: An Immune System Approach

Delivering a fundamentally unique approach in this area, Antigena Email uses self-learning AI to help organizations finally regain the advantage. The technology leverages Cyber AI to analyze all inbound, outbound, and lateral email traffic, allowing it to understand the dynamic humans and relationships behind emails. This deep insight lets lets Antigena recognize threats immediately, which is crucial in the case of solicitation attacks, where the goal is often to take the conversation offline and bypass security measures.

Unlike legacy defenses at the border, which rely on retrospective information, Darktrace's bespoke and continuously evolving understanding of 'normal' allows Antigena Email to autonomously respond to subtle impersonation attacks that evade email gateways by design. Antigena Email's decision-making is also operative throughout the entire lifespan of an email, enabling the system to update its analysis in light of new evidence even after the email has been delivered. With Antigena's ability to continue monitoring after delivery comes the ability to retroactively retrieve sent emails, should they later be revealed to be malicious.

Case Study: Antigena Email Pre-emptively Identifies C-level Impersonation

Darktrace recently detected a highly targeted social engineering attack attempting to impersonate C-level executives at a US technology company. The threat actor apparently sent a number of 'clean' emails in an effort to garner trust and establish offline communications, preemptive of a request for payment.

Extensive research was clearly carried out, as for each targeted user, the attacker knew who the relevant C-level executive at their office was and used them in the impersonation attempt. Antigena Email identified the social engineering attempts and as a result held back every email from the intended recipients, following this process:

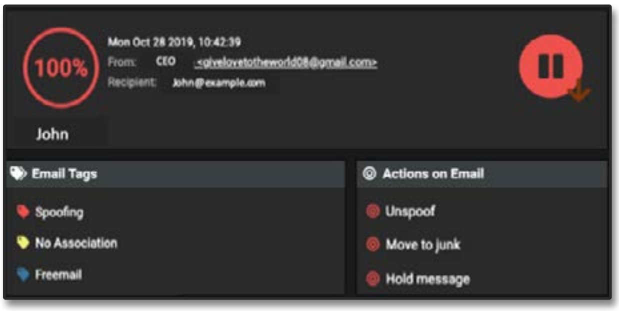
1. Recognizing Abnormal Subject and Sender. The emails had the first name of the targeted employee as the subject line, and further came from a seemingly unrelated Gmail address. Despite the lack of a malicious payload (such as links or attachments), Antigena Email was still able to identify the emails as malicious.

2. Seeing No Association. Antigena identified the impersonation attempts by recognizing not only the look-alike domain name, but also that the emails had breached the 'No Association' model. This indicates that across its entire understanding of the company's email environment, Antigena had seen no evidence of a relationship between this sender and the organization.

3. Preventing Offline Communication. Correlating these multiple weak indicators, Antigena recognized the emails as components of one systematic attack, causing it to hold them back in a buffer for the organization's security professionals to review. Antigena discerned that this was the most appropriate action in this case, preventing the targeted recipients from reading the contents of the email and establishing that offline communication.

4. Identifying Spoofing. Antigena Email not only identified the three C-level executives who were being impersonated, but also recognized that the attacker was using a spoof of their CEO's legitimate external personal address.

5. Exposing the Whale Spoof. In addition, the exposure score of the impersonated users was high, indicating that they were high-profile targets subject to a 'Whale Spoof' attack. While the legacy email defenses in place were unable to detect the attack given their static analysis and limited scope, Antigena Email used its deep understanding of the organization's digital users and their 'patterns of life' in the inbox to neutralize the threat.



Mon Oct 28 2019, 10:42:39

From: CEO <givelovetotheworld08@gmail.com>

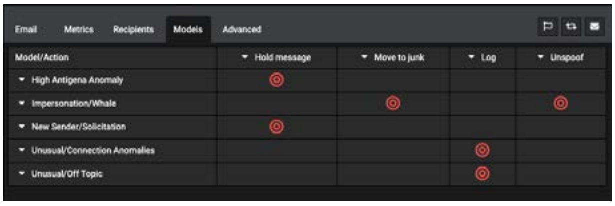
Recipient: John@example.com

John

Email Tags
- Spoofing
- No Association
- Freemail

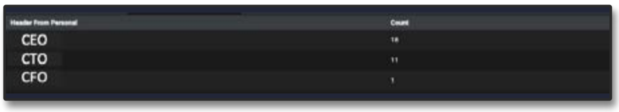
Actions on Email
- Unspoof
- Move to junk
- Hold message

Figure 2: One of 30 emails, with a 100% anomaly score



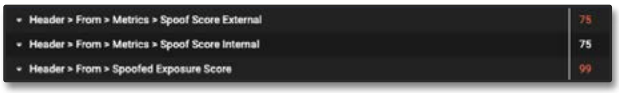
Model/Action	Hold message	Move to junk	Log	Unspoof
High Antigena Anomaly	◎			
Impersonation/Whale		◎		◎
New Sender/Solicitation	◎			
Unusual/Connection Anomalies			◎	
Unusual/Off Topic			◎	

Figure 3: The models that caused Antigena Email to respond



Header From Personal	Count
CEO	18
CTO	11
CFO	1

Figure 4: Three C-Level executives identified



Header > From > Metrics > Spoof Score External	75
Header > From > Metrics > Spoof Score Internal	75
Header > From > Spoofed Exposure Score	99

Figure 5: Antigena Email identifying the spoofing attempt