DARKTRACE

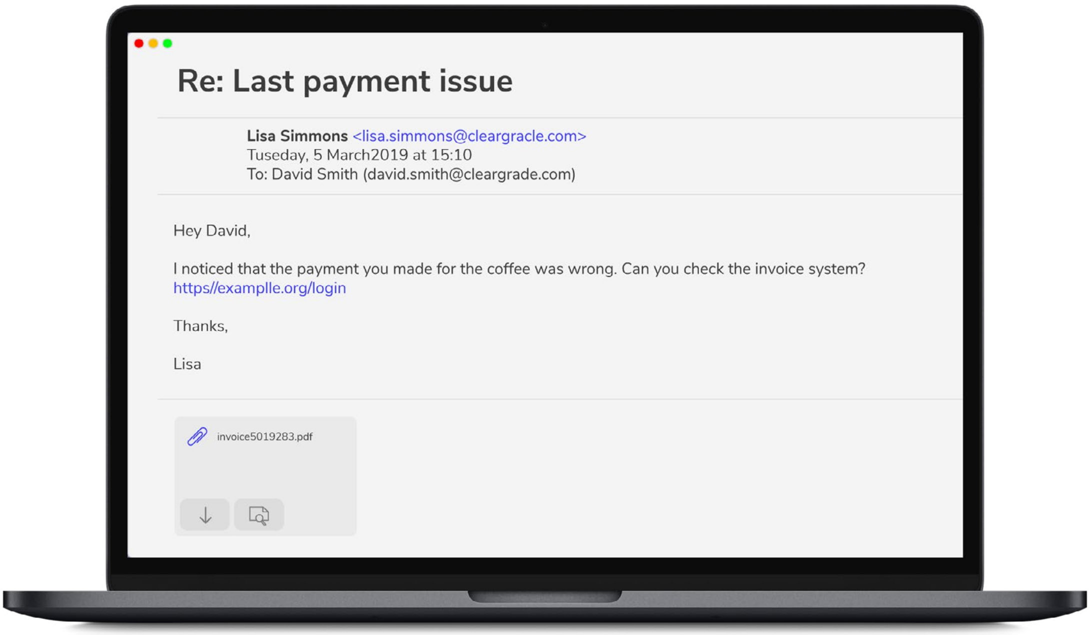
TECHNICAL BRIEF

Link Spoofing Attack

Darktrace detected a link spoofing attack targeting a financial institution in Atlanta, carefully constructed to trick them into clicking a malicious link.

A threat actor had registered a domain similar to that of the target company, but not an exact match. This can be done by making slight alterations to the company name but still have the domain look like the original one: for instance a single letter in the name or adding a hyphen into the domain.

The threat actor was able to enter into the flow of email exchanges. Once a series of back and forth correspondence is in place, the attacker leverages the trust that was built to send an email containing a malicious link.



Re: Last payment issue

Lisa Simmons <lisa.simmons@cleargracle.com>
Tuseday, 5 March2019 at 15:10
To: David Smith (david.smith@cleargrade.com)

Hey David,

I noticed that the payment you made for the coffee was wrong. Can you check the invoice system?
https//examplle.org/login

Thanks,

Lisa

invoice5019283.pdf

Figure 1: An incoming email containing a link to a spoofed domain.

Notice in the image of a spoofed email above, the incorrect spelling of the word ‘example.’ This is a subtle change that the recipient fails to notice and clicks on the link. This directs the user to a well crafted website that perfectly replicates the login page for Example.org, leading the user to input their credentials, which are now harvested by the threat actor, who is now able to use the victims credentials in the legitimate payment system.

Stopping Link Spoofing Attacks

Unlike any other solution, Antigena Email and the Immune System can correlate network, cloud, and email data to identify whether domains associated with a link and sender are abnormal, the location of a link in an email is strange, the topics of discussion and content are unusual, and even whether patterns in the URL pathway are suspicious.

This fundamentally unique approach means that Darktrace’s decision-making is drastically more accurate than that of other tools, such that it can take highly proportionate and targeted actions to neutralize phishing attacks at scale.

Darktrace not only identified the impersonation attempt by recognizing the look-alike domain name, but also that the emails had breached the ‘No Association’ model, indicating that across its entire understanding of the company’s email and network environment, it had seen no evidence of a relationship between this sender and the organization.

Antigena Email responded autonomously to neutralize the threat by forbidding access to the link. Additionally a warning banner was added to inform the user of and security team of the potential threat. Darktrace's Immune System was ready to take further action should this link have been sent to other users within the business, further preventing the attack to spread.

In addition, the exposure score of the impersonated users was high, indicating they were high-profile targets, and hence breaching the 'Whale Spoof' model. Understanding that key internal users had been targeted allowed Darktrace's AI to prioritize this attack, initiating a proportionate response in real time.

Antigena Email: Social Engineering and Solicitation

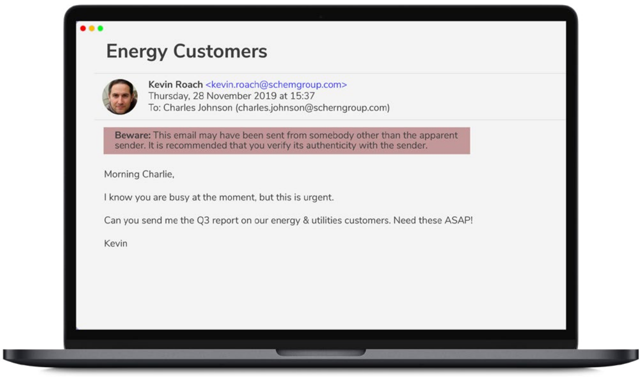
Social engineering and solicitation attacks typically involve a sophisticated attempt at impersonation, where disguised attackers urgently prompt a recipient to reply, take communications offline, or perform an offline transaction. Their goals range from wire fraud to corporate espionage and even IP theft. While organizations should of course invest in security training and educate their employees to look out for warning signs, no amount of guidance can guarantee complete immunity from these increasingly sophisticated attacks.

While traditional phishing campaigns generally include a malicious payload hidden behind a link or attachment, social engineering attempts often involve sending 'clean emails' that contain only text. These attacks easily bypass legacy security tools that rely on correlating links and attachments with blacklists and signatures. Moreover, this vector of attack generally involves registering new 'look-alike' domains, which not only trick the recipient but also bypass traditional defenses.

Antigena Email has a unified understanding of 'normal' across all email and network traffic that evolves with the business, allowing it to detect subtle cases of solicitation. Clean emails that bypass traditional defenses can be identified in seconds given a vast range of metrics, including suspicious similarities to known users, abnormal associations among internal recipients, and even anomalies in email content and subject matter.

More often than not, social engineering attacks aim to immediately take the conversation offline, which means that slow and reactive security measures tend to only intervene after the damage is done. Its powerful understanding of every user, device, and relationship in the organization allows Antigena Email to respond proactively and with high confidence the first time around, intervening at this crucial early stage.

Antigena Email can respond in a number of ways, including but not limited to: notifying the security team, issuing a warning to the email recipients by appending a warning banner to the content of email, rewriting and locking links, and completely holding back emails. Antigena is unique in its ability to intelligently and autonomously tailor these responses to specific threat types.



Energy Customers

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

Beware: This email may have been sent from somebody other than the apparent sender. It is recommended that you verify its authenticity with the sender.

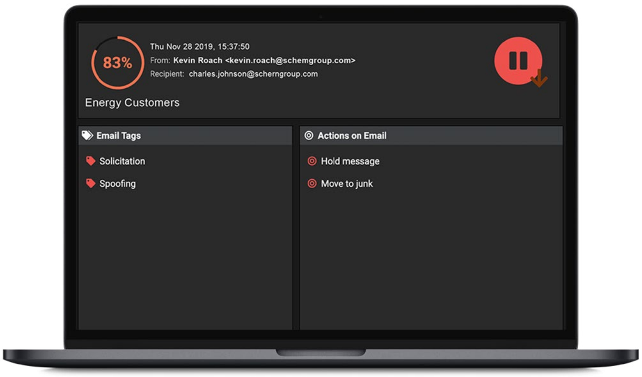
Morning Charlie,

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 2: A warning banner was appended to a spoofed incoming email requesting sensitive corporate documents.



83%

Thu Nov 28 2019, 15:37:50
From: Kevin Roach <kevin.roach@schemgroup.com>
Recipient: charles.johnson@scherngroup.com

Energy Customers

Email Tags
- Solicitation
- Spoofing

Actions on Email
- Hold message
- Move to junk

Figure 3: Antigena Email identified the above email as 83% anomalous due to indications of solicitation and spoofing.

Enterprise-Wide Context

Darktrace Antigena Email is able to analyze hidden links and attachments in connection with all email traffic, as well as the conventional 'pattern of life' of the digital environment. In instances of phishing attacks, Darktrace will recognize that neither the recipient nor anyone in the peer group has visited the suspect domain before, raising a high-confidence alert, and autonomously initiating a targeted response.

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. In addition, it looks at patterns within the URL address, comparing it to previously thwarted attacks in order to spot suspicious links. Applying this wealth of context to every inbound and outbound email within your organization allows Antigena Email to 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.