Antigena Email: Supply Chain Account Takeover

By hijacking the account details of a trusted contact in your supply chain, sophisticated threat actors can gain the trust of a recipient and coax them into clicking a malicious link or transferring millions out of the business. Legacy email defenses assume trust, which means that sophisticated account takeovers often go completely unnoticed.

Cyber-criminals are increasingly leveraging supply chains – comprised of vendors, partners, and contractors – to infiltrate organizations. Earlier this year, a report on so-called 'island hopping' — where attackers try to expand on a breach through supply chains – found that this method accounts for half of today's attacks.

Attackers who have total access to a supplier's email account are able to study previous email interactions and produce a targeted response to the latest correspondence. The language they use will often appear benign, so legacy email security tools searching key words or phrases for spoofing will fail to pick up on these attacks.

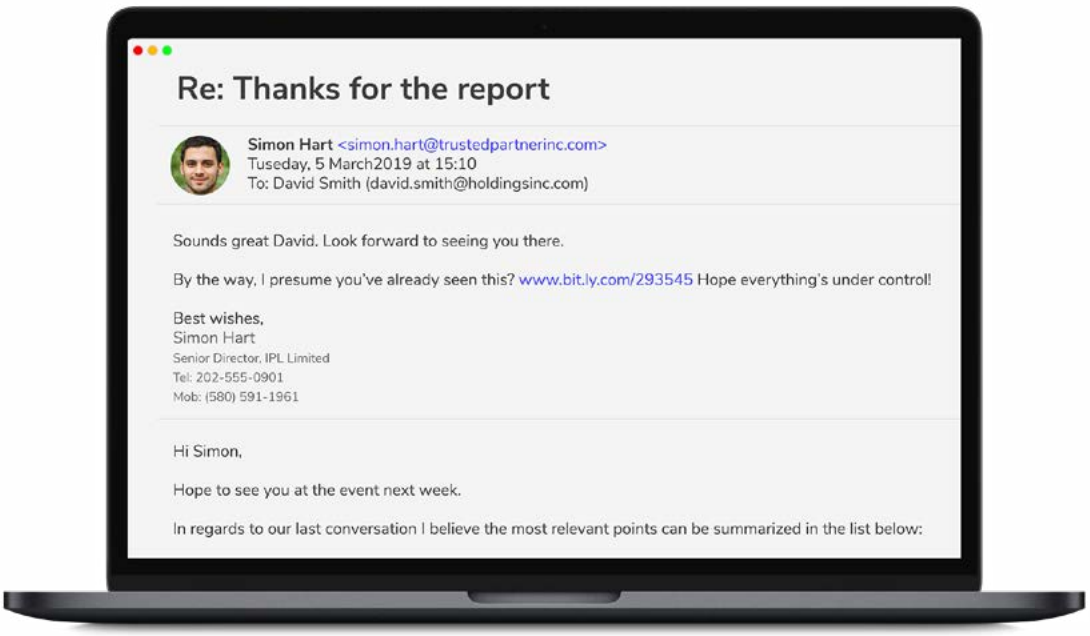

Figure 1: A plausible reply sent from a trusted supplier's compromised account. The link contained a malicious payload.

Antigena Email: Determining Friend from Foe

Analyzing patterns of communication across inbound, outbound, and lateral mail, Darktrace's Antigena Email uses a wide range of metrics to confidently identify cases of account takeover, something that is impossible to detect without a detailed understanding of 'normal' for the unique humans and relationships behind email addresses.

Antigena is able to analyze over 1,000 metrics for each email, including topic and content, consistency of the login location and the associated recipients, in conjunction with the learned 'pattern of life' for the sender. Antigena Email uses this deep knowledge of what's normal for your business to estimate the likelihood that contact from supply chains is in fact legitimate.

When it identifies an anomaly, Antigena will then action an autonomous response, which according to the severity of the threat can range from locking suspicious links and attachments to withdrawing an email from an employee's inbox entirely. Antigena Email continuously updates itself in light of new evidence, learning on the job to ensure your email platform is always protected.

Case Study: Antigena Email Identifies Supplier Account Hijacking

A customer trialing Antigena Email experienced a serious security incident when the account of a trusted supplier became the source of a malicious email campaign. The technology recognized that the sender was well known to the company, with a number of internal users having corresponded directly with them previously. In fact, earlier that day one of these users was engaged in normal correspondence with the soon-to-be hijacked supplier account.

Less than two hours after this legitimate, routine exchange, emails were sent from the supplier to 39 users, each containing a malicious link. There was variation in the subject lines and links contained in the emails, suggesting highly targeted emails from a well-prepared attacker. The purpose of the links could have been to solicit payments, harvest passwords, or deploy malware. Antigena Email identified the full range of red flags that are typically associated with supply chain account takeovers, and recommended holding all 39 emails back based on:

1. Unusual Login Location: Antigena Email determined that the emails had been sent from an authentic Outlook web server. This itself was not unusual for the supplier, but within this connection data it was also possible to extract the geo-locatable IP address. This revealed that the attacker initiated their login from an IP in the US, as opposed to their usual login location in the UK.

2. Link Inconsistency: The malicious links contained in the emails were all hosted on the Microsoft Azure developer platform – likely to skirt reputation checks on the host domain. Despite the widely assumed legitimacy of azurewebsites.net across the web, Antigena Email was able to detect that this domain was highly inconsistent for the sender based on previous correspondence history.

3. Unusual Recipients: A recipient's 'Association Anomaly' score is assigned to estimate the likelihood that this particular group of recipients would be receiving an email from the same source. Adding context to its investigation over time, Antigena Email deduced that this recipient group was 100% anomalous by just the third email.

4. Topic Anomaly: The subject lines for these emails suggest an attempt to appear low-key and professional. Consequently, any signature-based attempts to look for keywords associated with phishing would have failed. However, Antigena Email recognized that these recipients do not typically receive emails about business proposals using this style of phrasing.

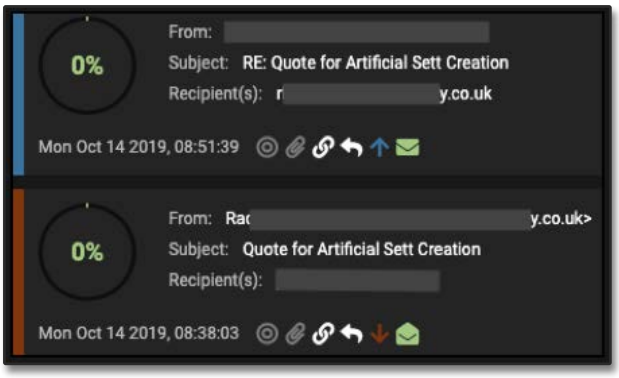

Figure 2: Earlier 'normal' correspondence with the sender – with a 0% anomaly score

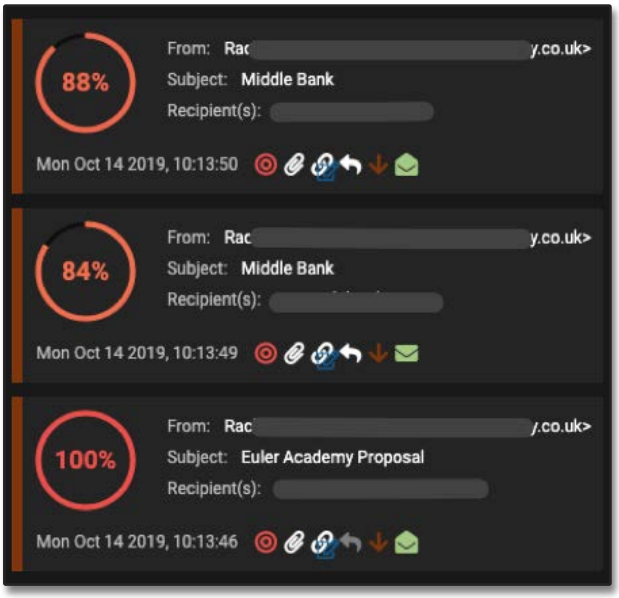

Figure 3: Emails sent later the same day containing malicious attachments

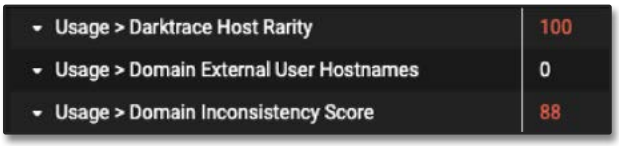

Figure 4: Models triggered by the rarity and inconsistency of the link

Figure 5: Antigena Email rapidly detected that this group of recipients was not closely related