BAE SYSTEMS

INSPIRED WORK

Defending against Business Email Compromise with Social Engineering Protection

Why Choose BAE Systems?

- **Strong heritage** with significant experience in deploying secure email systems, compliance and behavioural analytics
- **Machine learning** expertise enabling Social Engineering Protection to automatically update its model representing email communication patterns to maximise the protection of email infrastructures while minimising false positives
- **Advanced technology** research including Application Instrumentation to identify sandbox-aware malware, credential phishing prevention, and ClickTime analysis to ensure that links verified as malware-free by the email gateway are still safe when accessed by the end user

Block malicious, socially engineered emails as attackers move to exploiting human weaknesses.

The challenges

Companies lost over $5 billion due to business email compromise attacks between October 2013 and December 2016, according to the FBI[1].

These types of social engineering attacks, sometimes referred to as Business Email Compromise or Whaling, include:

- **Pretexting –** misrepresentation to gain access to privileged information
- **Phishing or spear-phishing –** attempts to obtain private or proprietary information either by sending a generic email to many, or a specifically crafted email to an individual
- **CEO fraud –** spoofs executive email address and sends to an employee asking them to urgently and secretly perform a wire transfer
- **Bogus invoice –** attacker contacts finance asking to change payment details for a particular supplier
- **Data theft –** request for sensitive data such as tax documents, which are then used by the attacker to initiate other criminal activities

Our approach

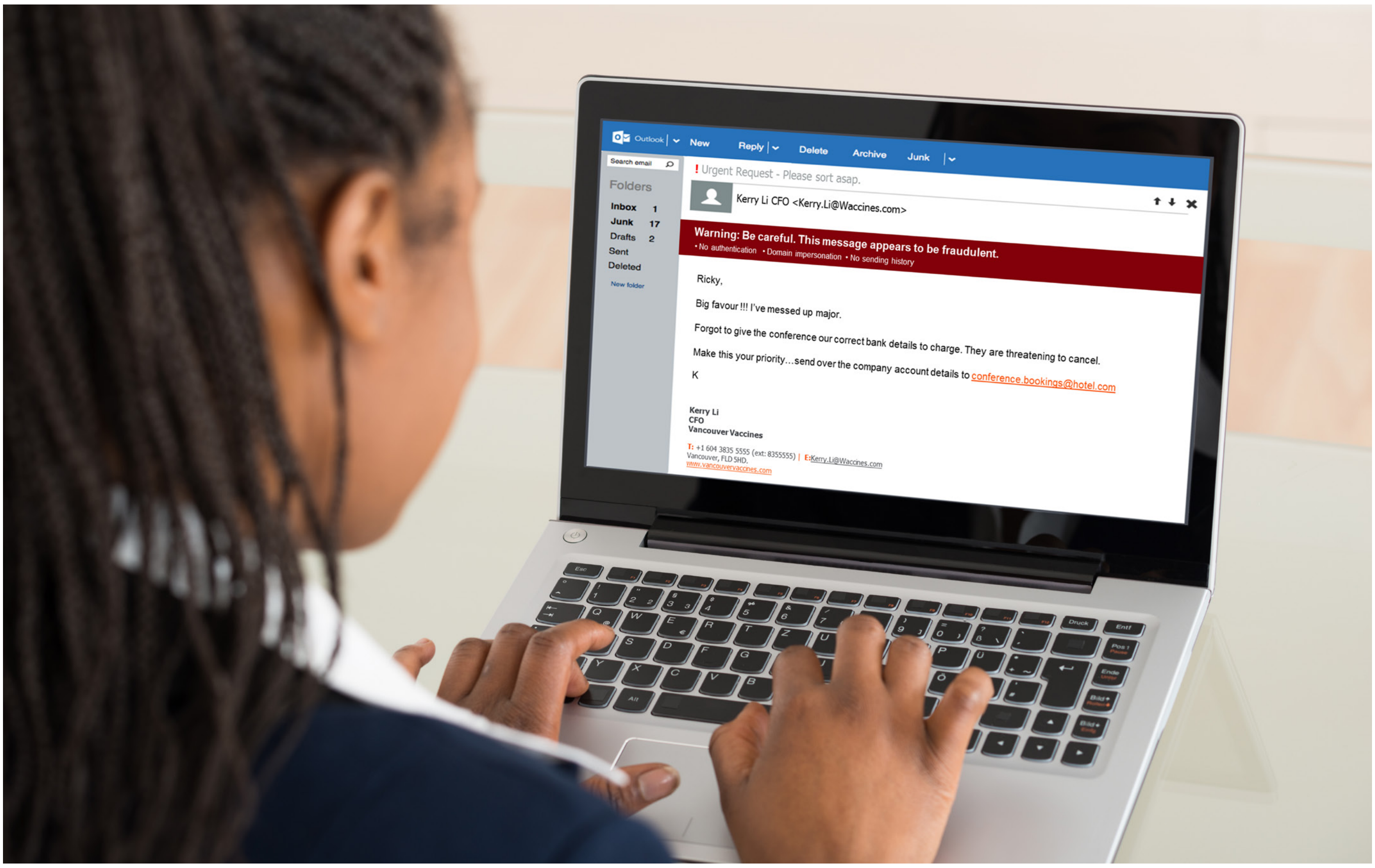
Unlike traditional security products that detect malware propagated by malicious attachments or links, Social Engineering Protection analyses parameters relating to authentication, domain reputation, message headers, and contextual indicators. This analysis determines factors such as:

- **Inconsistent sending history –** such as the first email sent from this sender
- **Display name abuse –** when an executive's name is used in a personal email address
- **Spoofed domain names –** which look similar to the company's actual domain

This analysis determines an **email trust score**, which is used to create an in-email 'traffic light' banner; alerting the recipient that it is potentially suspicious and should be treated with caution.

[1] https://www.ic3.gov/media/2017/170504.aspx

Feature	Benefit
BEC, CEO fraud and Whaling email detection	Detects potentially dangerous emails that, unlike traditional malware emails, do not contain attachments or links but instead use social engineering to exploit human weaknesses to persuade readers to compromise their organisation by, for example, paying fake invoices or divulging personal or company confidential information.
Machine learning	Reduces the need for ongoing fine-tuning of the social engineering detection engine, by automatically building an updated model of the unique email patterns within the organisation. This model is used to detect potential anomalies that could indicate a social engineering attack attempt.
In-email warning banner	Reinforces end-user security training by reminding email recipients to be aware of potentially suspicious emails, especially if they are tailored to look like they are specifically for them. In addition, the introduction of the banner increases the level of trust end users have of legitimate emails, which reduces the number of false positive emails that are reported to the IT security team to be investigated.
Email spoofing detection	Identifies attempts by hackers to impersonate company executives or legitimate suppliers by using similar domains or display names to ask for fraudulent payments to be made or sensitive information to be leaked.



! Urgent Request - Please sort asap.

Kerry Li CFO <Kerry.Li@Waccines.com>

Warning: Be careful. This message appears to be fraudulent.
• No authentication • Domain impersonation • No sending history

Ricky,

Big favour !!! I've messed up major.

Forgot to give the conference our correct bank details to charge. They are threatening to cancel.

Make this your priority…send over the company account details to conference.bookings@hotel.com

K

Kerry Li
CFO
Vancouver Vaccines

T: +1 604 3835 5555 (ext: 8355555) | E:Kerry.Li@Waccines.com
Vancouver, FLD 5HD.
www.vancouvervaccines.com

"Social Engineering Protection allows customers to keep one step ahead of the attackers by detecting non-traditional email threats using social engineering techniques to persuade end users to transfer funds or send confidential information."

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK
UK: +44 (0) 1483 816000
E: learn@baesystems.com | W: baesystems.com/businessdefence

linkedin.com/company/baesystemsai
twitter.com/baesystems_ai