SOPHOS
Cybersecurity evolved.

Business Email Compromise (BEC) Detection

The Problem

Business E-mail Compromise (BEC) attacks are on the rise, with ever increasing sophistication. In 2020, the FBI reported that BEC caused losses in excess of $1.8 billion[1].

Unlike other phishing attacks, significant effort by the bad actors is put into crafting multiple e-mails that will ensure a trained employee does what the criminal wants. The nature of the custom message, typically appearing to originate from a trusted source with high knowledge of the recipient's business, is hard to detect with traditional techniques. Also, these attacks often do not contain URLs or attachments, which means there are fewer artefacts to indicate an attack.

Sophos AI Solution

Sophos AI's BEC model is a neural network which accurately and quickly identifies targeted phishing and BEC style attacks.

Using Natural Language Processing, (NLP), the model determines the intent behind the text of the e-mail by analysing its syntactic and semantic meaning, including features related to the message's intent, tone, phrasing, and conceptual references.

The model is based on a recent innovation within natural language processing: the transformer neural network block. Introduced in 2017, transformers have fundamentally changed modern natural language processing, with their ability to represent language tokens in the context of their use, as well as relationships between tokens in a document.

Sophos has taken the transformer concept, normally used outside of email security, and adapted it to the problem of detecting phishing emails, by designing a bespoke neural network architecture that analyses email text with transformer blocks and email headers with feedforward network blocks, subsequently combining these information sources to make a final decision about whether an email is suspicious.

Combining these information sources can provide a highly accurate prediction of maliciousness.

In production environments, Sophos' AI BEC Model shows a detection rate of more than 90%.

Integration Guidelines

Sophos' BEC detection model is available in a Docker container. This allows you to build the technology into your existing cloud-based security infrastructure. Once running inside a Docker / Kubernetes environment the container will accept submissions via a REST API.

Key Features

- Neural network model
- Scores e-mails based on likelihood of being BEC / targeted phishing attack
- Leverages advances in NLP in sentiment detection via BERT framework

Uses NLP to detect:

- Sense of urgency
- Request for payment

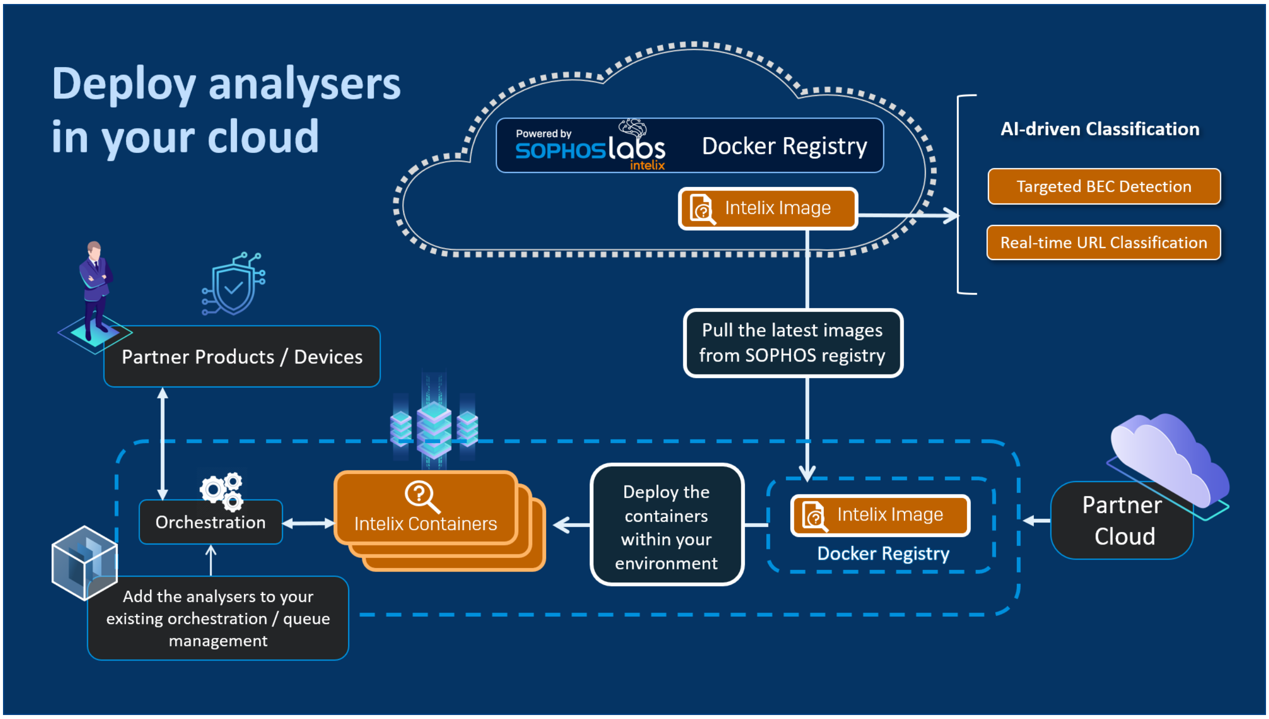
Metrics

Detects >90% of BEC samples with a FP rate <1%

True Positive Rate	False Positive Rate
95	1
87	0.1

[1] *Source: FBI Internet Crime Report 2020 - https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf*

Below is a diagram showing the typical deployment within an existing cloud infrastructure:


Deploy analysers in your cloud
Powered by SOPHOSlabs intelix
Docker Registry
Intelix Image
AI-driven Classification
Targeted BEC Detection
Real-time URL Classification
Partner Products / Devices
Pull the latest images from SOPHOS registry
Orchestration
Intelix Containers
Deploy the containers within your environment
Intelix Image
Docker Registry
Partner Cloud
Add the analysers to your existing orchestration / queue management

The orchestration layer you provide allows for queue management and integration of the results from our model alongside other technologies, or, compensating controls that you have in your cloud. We recommend that you use the BEC model after other e-mail filtering solutions e.g., anti-spam and anti-malware engines.

The BEC detection model accepts e-mail in the form of RFC 822. Your solution will submit this via a REST API. The model will process return a score (between 0 and 100) which gives the probability of the mail's maliciousness. The higher the score the higher the likelihood that the e-mail is malicious.

Within the Sophos products, a banner warns users that an e-mail is likely to be phishing if the score is above a specific threshold. As with any AI based technology, customers can configure this threshold based on their attitude towards risk and compromise between false positives (FPs) and false negatives (FNs). We will work with you to set the thresholds correctly for your environment.

To learn more,
speak with a Sophos OEM expert
oem.sales@sophos.com

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com