SOPHOS
Cybersecurity evolved.

ビジネスメール詐欺 (BEC)の検出

問題点

ビジネスメール詐欺(BEC)の攻撃は増加傾向にあり、さらに高度化が進んでいます。2020年、FBIは、BECが18億ドルを超える損失を引き起こしたと報告しました。[1]

他のフィッシング攻撃とは異なり、悪意のある攻撃者による多大な労力が複数のメールの作成に費やされ、訓練を受けた作業者が犯罪者の望むことを確実に実行できるようになります。 カスタムメッセージの性質は、通常、受信者のビジネスに関する高度な知識を持つ信頼できるソースから発信されているように見えますが、従来の手法では検出が困難です。 また、これらの攻撃にはURLや添付ファイルが含まれていないことがよくあります。つまり、攻撃を示すアーティファクトが少なくなります。

ソフォスのAIソリューション

ソフォスAIによるBECモデルは、ニューラルネットワークによって標的型フィッシングおよびBECスタイルの攻撃を正確かつ迅速に識別します。

モデルは、自然言語処理(NLP)を使用して、メッセージの意図、トーン、言い回し、概念的な参照に関連する機能など、構文的および文脈的な意味を分析することにより、メールのテキストの背後にある意図を確定します。

このモデルは、自然言語処理における最新の革新的技術であるトランスフォーマーニューラルネットワークブロックに基づいています。 2017年に導入されたトランスフォーマーは、ドキュメント内のトークン間の関係だけでなく、使用されているコンテキストで言語トークンを見出す機能により、現在の自然言語処理を根本的に変更しました。

ソフォスは、通常はメールセキュリティ以外で使用されるトランスフォーマーの概念を採用し、メールが疑わしいかどうかについて最終決定を下すための情報源として、トランスフォーマーブロックを使用してメールテキストを分析し、フィードフォワードネットワークブロックを使用してメールヘッダーを分析する特別なニューラルネットワークアーキテクチャを設計することにより、フィッシングメールの検出の問題に適応させました。

これらの情報ソースを組み合わせることで、悪質性に対して正確な予測を提供できます。

実稼働環境では、ソフォスのAI BECモデルは90%を超える検出率を示しています。

インテグレーション・ガイドライン

ソフォスのBEC検出モデルはDockerコンテナ上で利用することができます。そのため既存のクラウドベースのセキュリティ・インフラストラクチャーに容易にBECテクノロジーを追加することができます。Docker / Kubernetes環境内で実行されると、コンテナーはRESTAPIを介して送信を受け入れます。

主な特徴

- ニューラルネットワーク・モデル
- BEC /標的型フィッシング攻撃の可能性に基づいてメールをスコアリング
- BERTフレームワークを介した検出とNLPを活用

NLPを使用して以下を検出:

- 切迫感
- 支払い請求

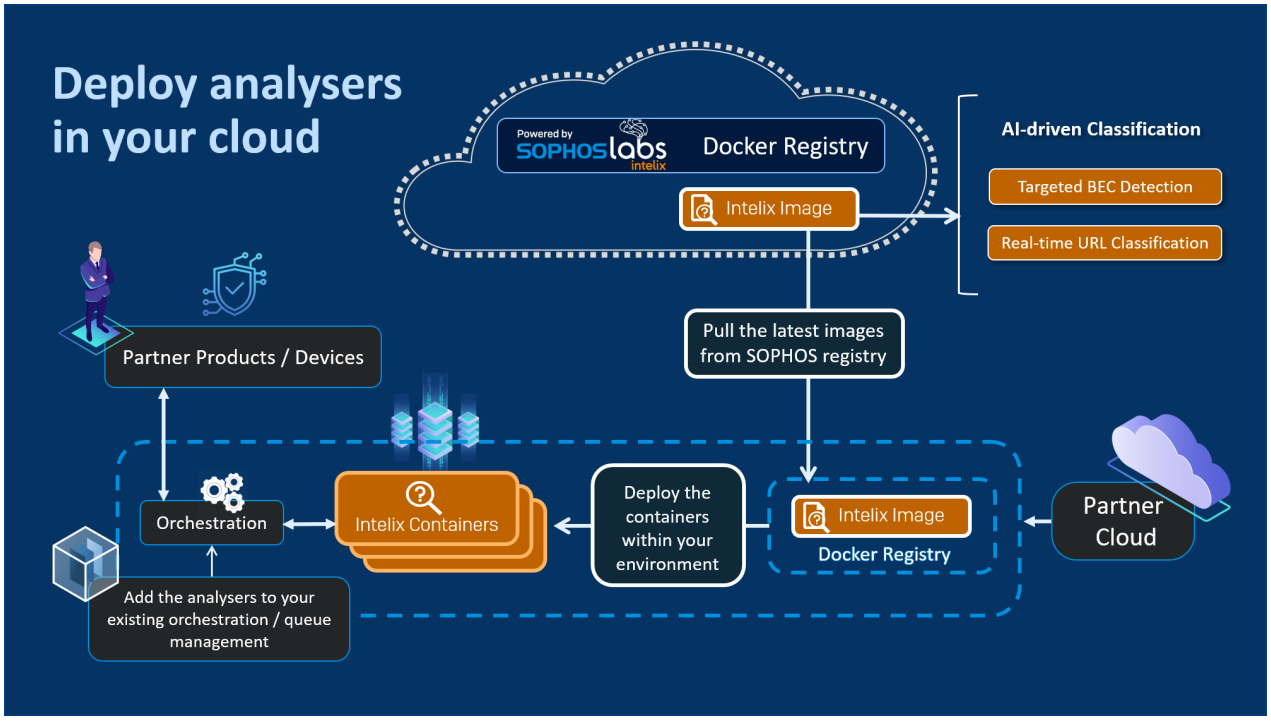
指標

BECサンプルにてFPが1%以下で90%以上の検出

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*

一般的な既存のクラウド・インフラストラクチャーへの適用例:



提供するオーケストレーションレイヤーにより、キューの管理、モデルの結果を他のテクノロジーと統合、クラウドにある制御の補正を行うことがきます。スパム対策エンジンやマルウェア対策エンジンなど、他のメールフィルタリングソリューションの後にBECモデルを使用することをお勧めします。

BEC検出モデルは、RFC822のメール形式を受け入れます。利用者はこのソリューションをRESTAPIを介して送信します。モデルは、メールの悪意の可能性を示すスコア(0から100の間)を返します。スコアが高いほど、メールの悪意がある可能性が高くなります。

ソフォス製品内では、スコアが特定のしきい値を超えている場合、メールがフィッシングの可能性があることをバナーを介してユーザーに警告します。他のAIベースのテクノロジーと同様に、利用者はリスクに対する対処と誤検知(FP/FN)の間の調整に基づいて、このしきい値を設定することができます。利用者と協力して、利用環境に合わせてしきい値を正しく設定することをお勧めします。

ソフォスOEM製品のお問い合わせは
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

21-10-22 TP-JP (MP)

SOPHOS