ビジネスメール詐欺（BEC）を防ぐ5つのステップ

- 複数の攻撃手法に対処し、様々なBEC攻撃を検知、阻止する
- 最も攻撃されているユーザーと最も危険なサプライヤーを可視化する
- メール詐欺を識別して報告できるようにユーザーをトレーニングする
- 脅威に対する対処機能を自動化し、対処時間を最小化する
- 統合型のエンドツーエンド ソリューションで、セキュリティとオペレーションの効率を向上させる

FBIによると、2020年に発生した経済的損失の中で最も大きかったサイバー攻撃はメール詐欺で[1]、その損失額は約20億ドルに上ります。これは、報告された損害額の44%を占めています。Gartnerによると、2023年までビジネスメール詐欺（BEC）は毎年倍増していき、損失額は50億ドルを超えると予測されています。これは大企業にとって大きな打撃となります[2]。

BECは、信頼できる相手から送られたように見えるメールから始まります。攻撃者がその相手になりすましている場合もあれば、本人のアカウントを乗っ取り、悪用する場合もあります。攻撃者は、ソーシャル エンジニアリングでユーザーを騙したり脅迫したりして、電信送金させたり、機密情報を開示させたりします。BECには不正なペイロードがないため、レピュテーションやサンドボックスに頼る従来のゲートウェイでは、こうした攻撃に対応することはできません。

詐欺の手口も巧妙化が進み、様々なBECが確認されています。たとえば、偽のギフトカードや給与明細を使用する詐欺や、サプライヤーからの偽の請求書を使用する詐欺が発生しています。変化の激しいメール詐欺の脅威を阻止するには、BEC攻撃のあらゆる手口を網羅した包括的なソリューションを利用し、複数のセキュリティ対策を統合して、ユーザーの意識を高めていく必要があります。

プルーフポイントのBEC対策

プルーフポイントは、業界で初めて包括的な統合型脅威対策プラットフォームを開発し、提供している唯一のベンダーです。このプラットフォームにより、次のことが可能になります。

- BECを早期に検知し、組織への侵入を防ぐ
- BECのリスクを可視化する
- ユーザーがBECを特定し、報告できるようにする
- 脅威の検知から対応までを自動化する
- メール詐欺攻撃から組織のブランドを守る

このソリューション概要では、一般的なBEC攻撃を阻止する方法について説明します。

1 FBI: Internet Crime Report（インターネット犯罪レポート）- 2021年
2 Gartner: Protecting Against Business Email Compromise Phishing（ビジネスメール詐欺からの保護）- 2020年

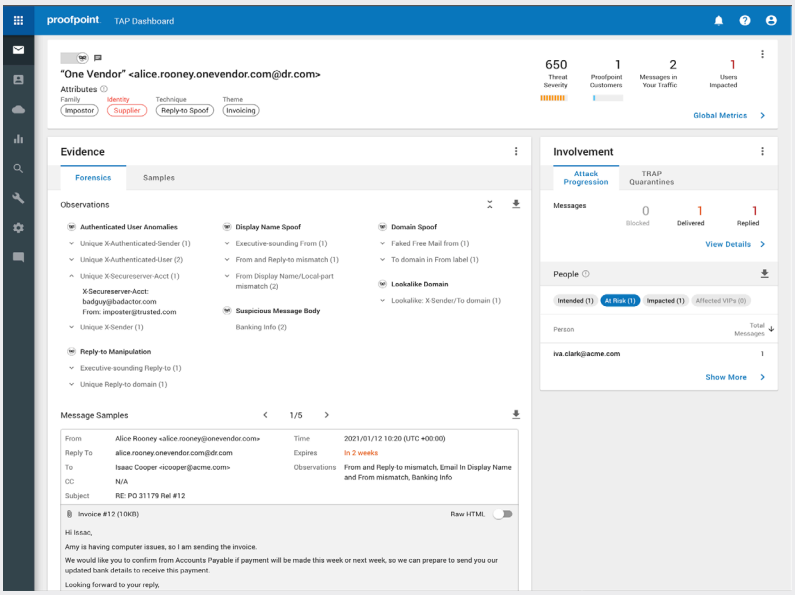

図1: なりすましの脅威に最も影響を受けているユーザーを特定し、BEC脅威の詳細を可視化する

1. なりすましの脅威を早期に検知し、侵入を防ぐ

プルーフポイントの統合型の脅威対策プラットフォームでは、Advanced BEC Defenseを使用しています。これはAIの機械学習を利用したBEC検知エンジンで、様々なメール詐欺攻撃を動的に検知します。また、次のような複数のメッセージ属性を分析します。

- メッセージヘッダーのデータ
- 送信者のIPアドレス
- 送受信者の関係
- 送信者のレピュテーション

また、メッセージの本文を使用して感情や文言などの言語解析をおこない、メッセージにビジネスメール詐欺（BEC）の脅威が含まれるかどうか判定します。

Advanced BEC Defenseを使用すると、BEC攻撃で使われている様々な手口を検知できます。これには、表示名のなりすまし、一見して見分けのつかないドメインなどが含まれます。さらに、次のようなサプライヤーの偽請求に関連する様々な兆候を動的に分析し、巧妙ななりすまし詐欺を検知、ブロックします。

- Reply-toピボット（返信先に他のメールアドレスを設定する手法）
- 悪意のあるIPアドレスの使用
- なりすましで利用されたサプライヤー ドメイン
- サプライヤー詐欺攻撃でよく使われる語句やフレーズ

大半のメールセキュリティ製品は、静的なルール照合のみを使用していたり、コンテキストデータが制限されているため、手動での調整が必要になります。プルーフポイントのAdvanced BEC Defenseは違います。この検知エンジンは、**NexusAI**を使用し、リアルタイムでの学習が可能です。これは、規模の大小を問わず、様々な企業で利用できます。また、メール、クラウド、ネットワークなど、デジタル環境全体を可視化できます。

プルーフポイントは、様々な脅威状況に対応できる真の機械学習を提供しています。この学習機能では、誤検知を最小にしながら「良性」メールと「悪性」メールを動的に分類できます。攻撃者の手口に合わせて変更を行い、「悪性」メールをブロックして「良性」メールのみを配信します。

2. 組織のBECリスクを可視化する

プルーフポイントを使用すると、マネージメント チームに以下の情報を提供できます。これにより、BECのリスクをより正確に把握し、リスクを回避できます。

- どのようなBECリスクにさらされているか
- 最も脆弱なユーザーは誰か
- 自社にとってリスクのあるサンプライヤーはどこか
- リスクを低減するために何をすべきか

プルーフポイントを使用すると、現在なりすましの被害を最も多く受けているユーザーや、このような脅威の影響を最も受けやすいユーザーを特定できます。また、BEC脅威の詳細をビジュアルに確認できます。たとえば、ギフトカード、おとり、サプライヤーからの偽の請求、偽の給与明細などのテーマが表示されます（図1を参照）。これにより、セキュリティチームは攻撃をより正確に把握し、情報を交換することができます。

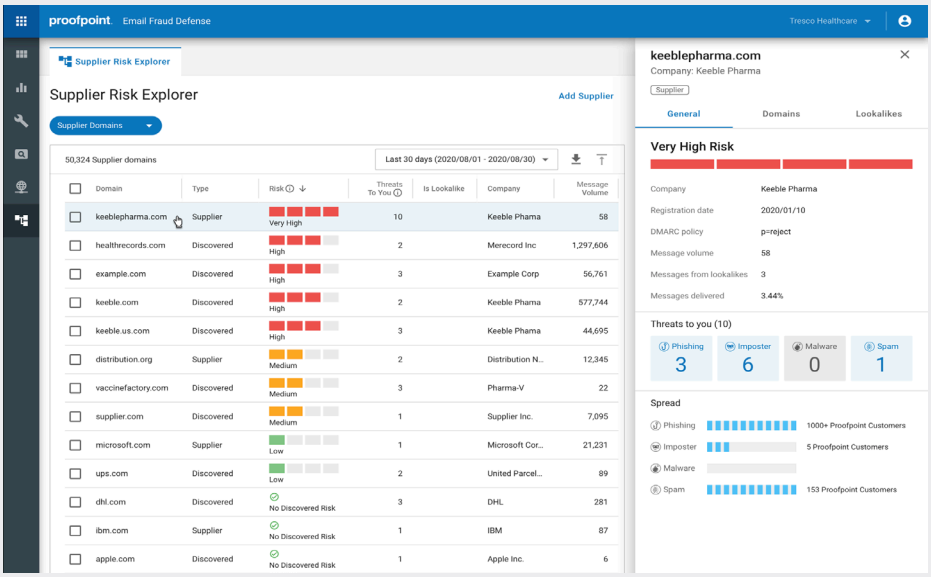

図2: Supplier Risk Explorerにより、組織にリスクをもたらすサプライヤーのドメインを特定し、可視化する

また、サプライヤーが組織にもたらすリスクも可視化されます。**Nexus Supplier Risk Explorer**（図2）を使用すると、次のことが可能になります。

- なりすまし攻撃や侵害を受けてユーザーにメールを送信している可能性のあるサプライヤーとドメインを自動的に特定します。
- BEC脅威について、サプライヤーを中心としたビューを提供します。
- メッセージの量を確認できます。
- サプライヤー ドメインから検出された脅威の情報を提供できます。
- サプライヤー ドメインの不正な類似性によりブロックされたメッセージを提供します。

これらのサプライヤー ドメインのリスクレベルを診断して、優先度を設定することで、セキュリティ チームは、組織にとって最も危険なサプライヤーにフォーカスできます。

3.BECに対するユーザーの耐性を強化する

BECは「人」をターゲットにしています。人は、知らないうちに攻撃に加担してしまうことがあります。なりすまし攻撃はソーシャル エンジニアリングやアイデンティティ詐称に依存するため、ユーザーが防御の最後の砦となることもあります。BECのリスクを低減するには、**技術**だけでなく、ユーザーへの**トレーニング**も必要になります。

プルーフポイントは、不審な詐欺メールを識別し、報告できるようにユーザー教育をサポートします。人のアクションから引き起こされる脅威から組織を守るため、必要な知識とスキルがユーザーに提供されます。統合型プラットフォームから提供された分析情報に基づいて、組織で最も注意しなければならない人物である Very Attacked People™や、既知の悪質なコンテンツの影響を受けるユーザーに対する研修プログラムを作成できます。

トレーニングでは、まず、BECの脅威に脆弱なユーザーを特定します。次に、安全な環境でBEC攻撃を体験してもらい、日々の環境の中でなりすまし攻撃がどのように行われるのかを評価します。シミュレーションで騙されてしまったユーザーには、自動的にその時に学ぶことができるジャストインタイムのガイダンスが提供され、誤った対応に関する情報が送信されます。これらのユーザーを特定のトレーニング モジュールに自動的に登録することもできます。

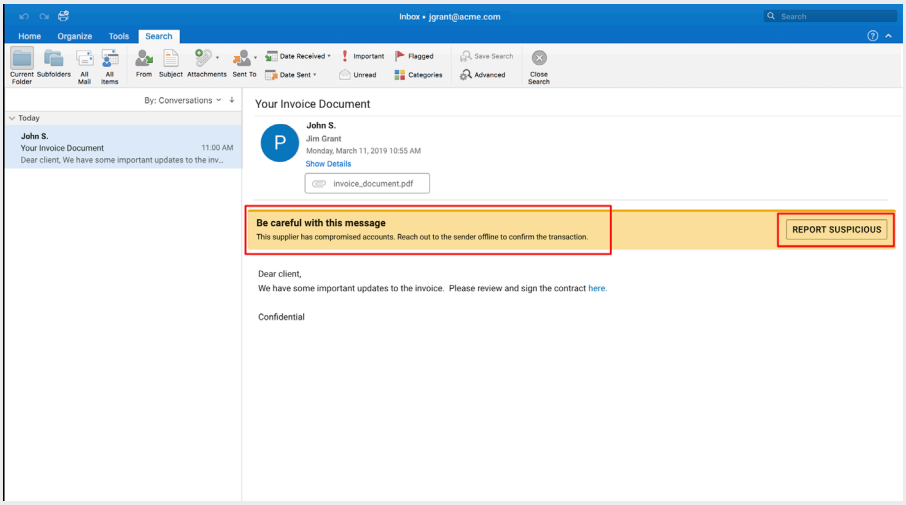

図3: メール警告タグでアラートを通知
ユーザーは的確な情報に基づいて、怪しいメールに対する意思決定を行うことができる

トレーニング マテリアルは、関連する社内プロセスを改善するために、カスタマイズ可能な形式で提供されます。たとえば、なりすまし脅威の可能性を不正メールのボックスに報告するように教育できます。組織の特定のプロセスに従って金銭に関係するリクエストを検証することもできます。

また、メールの警告タグで、特定のメールに関するリスクを簡単に伝えることができます。たとえば、外部の送信者や新規に登録したドメインからメッセージを受信したとき、ユーザーに警告を表示します。これにより、ユーザーは的確な情報に基づいて、怪しいメールに対する意思決定を行うことができます。また、侵害を受ける潜在的なリスクも軽減されます。

4. 脅威への対処を自動化する

多くの企業はITセキュリティのスタッフ不足に悩んでいます。セキュリティ チームは、多くのセキュリティベンダーやセキュリティ製品を管理する必要がありますが、対応しきれなくなっています。その結果、組織全体でBECの脅威を迅速に見つけ出し、調査・対応することが難しくなっています。対応に時間がかかればかかるほど、組織がリスクにさらされる時間は長くなります。

プルーフポイントを使用すると、脅威の検知と対処を自動的に行うことができます。Proofpoint TRAP (Threat Response Auto-Pull) を使用すると、怪しいメールや不要なメールをワンクリックで隔離または削除できます。悪性メールが誤って他のユーザーに転送されてしまった場合でも、このプロセスを自動的に実行できます。さらに、Abuse(不正報告)メールボックスの効率化も可能です。アクティブな脅威を数分で自動的に無害化し、ITチームの作業負荷を軽減できます。

ユーザーは、特定のメッセージのリスクを説明する警告タグから直接、不審なメッセージの受信を簡単に報告できます。また、PhishAlarm® メール レポーティング アドインを使用することもできます。いずれの場合もワンクリックで報告できます。

報告されたメッセージは、複数の脅威インテリジェンスとレピュテーション システムによって自動的に分析されます。BEC脅威ハンティング機能を使用すると、メール環境を迅速に検索し、他のユーザーが同じメッセージを受信しているかどうか確認できます。

メールが悪意のあるものであると分かれば、報告のあったメールやその他のコピー(転送されたものも含む)は自動的に隔離されます。インシデントの管理や調査を手動で行う必要がないため、効率的に作業を行い、負荷を軽減できます。最後に、ユーザーにはカスタマイズされたメールが送信され、悪質なメールであったことが通知されます。この通知により、将来、類似するメールを見たときに報告できるように行動を強化します。

5. メール詐欺攻撃からブランドを守る

ブランドのなりすましの場合、攻撃者は社名やブランドを悪用してその企業の顧客やビジネスパートナーから金銭を盗み出そうとします。金銭的な被害が直接発生しなくても、会社の評判が傷つき、顧客からの信頼を失う結果になりかねません。長期的に見れば、ビジネスにマイナス要因となることは間違いないでしょう。

プルーフポイントは、組織の信頼されたドメインから詐欺メールが送信されないようにすることで、メール詐欺攻撃からブランドの価値と信頼性を守ります。また、組織間で送受信されるすべてのメールを認証します。ガイド付きのワークフローとマネージドサービスでDMARCを効率的に実装することで、DMARCのRejectポリシーを確実に公開できます。これにより、ドメインのなりすましを防ぎ、信頼するドメインから送信される未承認メールをすべてブロックします。

さらに、信頼できる第三者を含む組織のドメインを使用して送信されたすべてのメールを可視化し、類似ドメインを特定します。メール攻撃やフィッシング サイトで、ブランドを偽装した新規登録ドメインを動的に検知します。また、不審なドメインが活動を始めて武器化した場合、ただちにアラートで警告します。

メール、Webドメイン、ソーシャルメディア、ダークネットなどのデジタルチャネルで、ブランドのなりすましがどのように行われているかも通知します。こうした可視化とVirtual Takedownサービスにより、一見して見分けのつかないドメインから顧客とビジネスパートナーを守ることができます。

まとめ

メール詐欺は金銭的損失の大半を占めています。詐欺の手口はさらに巧妙化し、サプライヤーに対する複雑な詐欺行為が発生しています。プルーフポイントは、こうした脅威を効果的に阻止できる統合型のエンドツーエンド ソリューションを業界で初めて開発し、提供している唯一のベンダーです。

プルーフポイントのBECソリューションを使用すると、次のことが可能になります。

- 様々なタイプのBEC攻撃を検知し、阻止する
- 攻撃対象とBEC脅威の詳細を可視化する
- リスクのあるサプライヤーを特定する
- BEC対する耐性を高められるようにユーザーをトレーニングする
- インシデントの調査と対応を自動化する
- メール詐欺攻撃からブランドを守る

プルーフポイントとともに、迅速、簡単、効果的に、BECから組織を守りましょう。

詳細

詳細は**proofpoint.com/jp**でご確認ください。