ビジネス メール詐欺や メール アカウント侵害から 組織を守る 7 つの方法

主なメリット

- あらゆる攻撃手法に対処して、BEC/EAC 攻撃を検知、阻止する
- 検知機能と修復機能を自動化して、脅威に迅速に対応し、対応時間を短縮する
- 詐欺の手口を認識できるようにエンドユーザーをトレーニングしてリスクを低減する
- 統合型のエンドツーエンド ソリューションで、セキュリティやオペレーションの効果を最大化する
- 攻撃対象となる人を可視化して、分離機能やセキュリティ意識向上トレーニングを割り当てるなど、それぞれの人に応じたアダプティブ コントロール(適応型制御)を実現する

概要

メール詐欺とは、主に次の 2 つに分類できます。

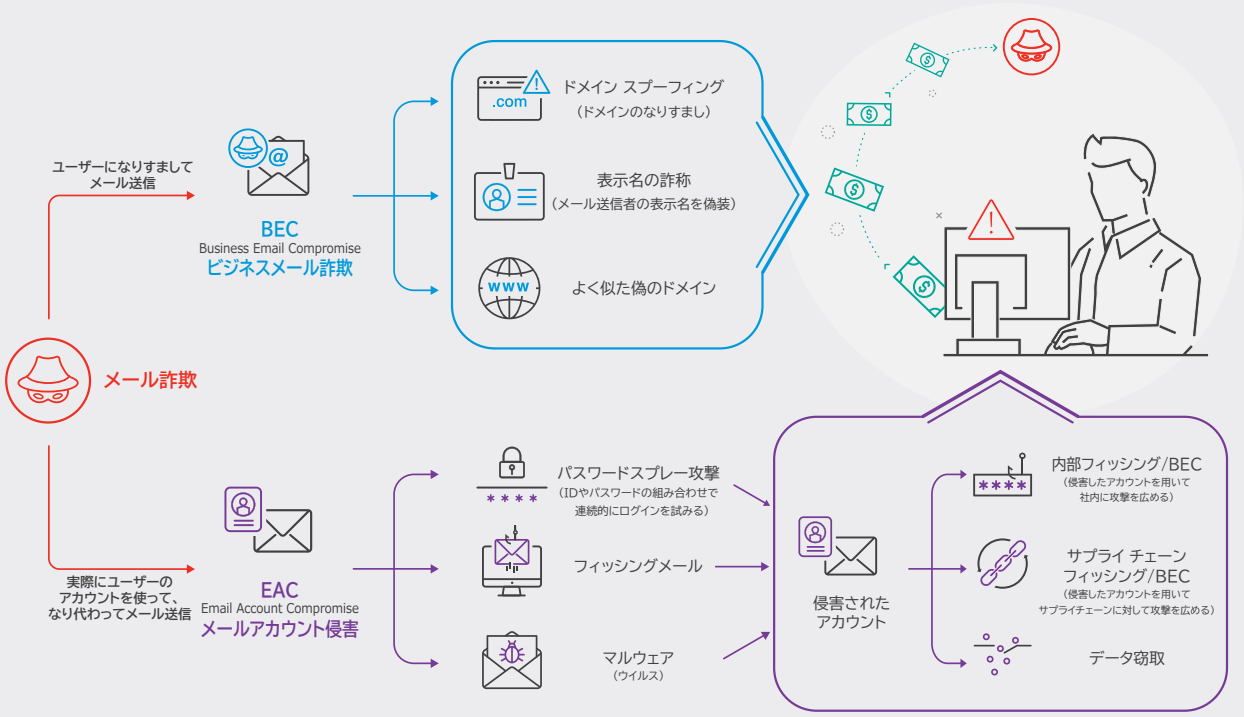
- 攻撃者がユーザーに**なりすます**ビジネス メール詐欺 (BEC / Business Email Comromise)
- 攻撃者がユーザーに **なり代わる** メール アカウント侵害 (EAC / Email Account Compromise)

BEC や EAC は、様々な要素を含む複雑な問題で、攻撃者は、多様な手口やチャネルを使って、ユーザーのコーポレートメール、個人メール、クラウドアプリ、さらにサプライチェーンすら標的にして攻撃を仕掛けます。

近年、こうした攻撃は、企業の規模を問わず、あらゆる組織にとっての最大の懸念となっています。2019 年には、およそ 90% の組織が、BECや、アカウント侵害につながるスピアフィッシング攻撃に直面しました。[1]FBI の報告によれば、BEC や EAC 詐欺のため、企業各社は2016年より累計で 260 億ドル以上の被害を受けています。[2]そして、こうした詐欺に伴う経済的な損失は、拡大するばかりです。ガートナー社は、2023年までに、毎年 BEC 攻撃は倍増し続けて被害額は 50 億ドルを超え、企業にとって大きな損失になるだろうと予測しています。[3]

BEC と EAC は互いに結びついていることから、両者に同時に対処する必要があります。こうした脅威については、あらゆる攻撃手法を対象として、検知と修復を自動化し、組織の BEC/EAC リスクを可視化することのできる、総合的なソリューションこそが唯一の解決策となります。以下では、新しい形態によるメール脅威から組織を守るため、プルーフポイントがお手伝いできる 7 つの方法をご紹介します。

1 プルーフポイント 「State of the Phish レポート」2019年
2 FBI 「Business Email Compromise: the $26 billion scam (ビジネス メール詐欺 : 被害額 260億ドル)」2019年 9月
3 Gartner 「Protecting Against Business Email Compromise Phishing (ビジネスメール詐欺のフィッシングから保護する)」2020年



1. なりすましやフィッシングの脅威を侵入前にブロックする

多くの場合、BEC は、攻撃者がユーザーの信頼する誰かになりすまして電子メールを送信することから始まります。ソーシャル エンジニアリングを使ってユーザーを騙したり脅迫したりして、電信送金させ、機密情報を開示させます。悪意のあるペイロードが含まれる訳ではないため、こうしたなりすましの脅威を検知することは困難です。攻撃者は、マルウェアを使わない方法を好み、マルウェアや悪意のある URL を使用しないことがありますが、マルウェアが含まれていないとはいえ、お金や情報を盗もうという意図は、当然ながら犯罪です。よく使われる BEC 攻撃としては、ドメインのなりすましや、偽の表示名、よく似た偽のドメインの使用などがあります。

こうした新しいメール脅威を阻止するには、新しいアプローチが不可欠です。プルーフポイントの強固なメールゲートウェイでは、こうしたなりすましメールがユーザーに届く前に、これを検知して、ブロックします。

電子メール セキュリティ ソリューションは、企業を守るために、独自の機械学習テクノロジーである「なりすまし分類機能」を使って、悪意のペイロードの有無にかかわらず、フィッシング攻撃やなりすましなどの様々な電子メールを動的に分類し、脅威を検知しています。さらに、次のものを含む数十億通のメールの属性の分析結果を用いて送信者のレピュテーションを判断します。

- ヘッダー
- コンテンツ
- IP アドレス

この情報に加えて、組織内の通常フローを学習し、また他のプルーフポイント製品の利用内容を集めてベースラインを形成します。このベースラインを基にすれば基準から外れたメールを迅速に識別できるため全体的な有効性が上がります。

この「なりすまし分類機能」は、他の静的ルールマッチングや手動チューニングに依存する電子メール セキュリティ ツールとは異なり、リアルタイムで学習します。学習機能により、「良い」メールと「悪い」メールを動的に分類したり、攻撃手法の変化に反応して、マルウェアを用いない脅威を効果的に阻止します。また、プルーフポイントのメール セキュリティ ソリューションでは、受信メールに関する SPF、DKIM、DMARC などのメール認証ポリシーを、入口段階で実施することができます。このようなテクノロジーを用いて、ドメインのなりすましメールが組織に侵入することを防いでいます。

さらに、プルーフポイントのソリューションは、EAC につながりかねない認証情報のフィッシングや悪意あるメールをブロックすることもできます。サンドボックスを用いて、数分で添付ファイルベースの脅威を分析してリアルタイムで検知します。またURL をあらかじめ検証するだけでなく、クリックした際にも再びサンドボックスで検証することで悪意あるURLを検知してブロックします。

攻撃に関する詳細な脅威フォレンジックから、組織で何が起きているのかを正確に把握することができるでしょう。攻撃の対象となっているユーザー、攻撃の発信源、攻撃の様相（実際のスクリーンショットを含む）まで、詳細に確認することができます。

2. DMARC でメールを認証する

Domain-based Message Authentication, Reporting and Conformance（DMARC）は、メール認証プロトコルです。DMARCは、Sender Policy Framework (SPF) および Domain Keys Identified Mail (DKIM) という 2 つの重要なメール認証基準を基盤として構築されました。DMARC は、正当な送信者を検証して、詐欺メールや未検証のメールがユーザーの受信箱に届かないようにします。ドメインのなりすましや組織のドメインを不正に使ってEメールを送信するメール詐欺を防ぐための最も効果的な方法であることが証明されています。

業界のアナリストたちは DMARC 認証を強く推奨していますが、DMARC の実施プロセスは、時間を要し、かつ複雑なものになりかねません。自社とともに第三者である Salesforce、Marketo、 Workday などの送信者がメール ドメインを使用する場合を含めて、使用方法のすべてを把握する必要があるからです。また、過去に乗っ取られたドメインがあるかについても見極める必要があります。

このように、DMARC の導入には時間と手間を要する場合があることから、弊社では、可視性、ツール、サービスを用いて、正当なメールの承認や、詐欺メールのブロックを簡単に行えるようにしました。信頼されたドメインのなりすましメールをプルーフポイントのゲートウェイでブロックできるように、DMARC 認証を迅速かつ確実に実施しています。

さらに、組織のすべてのEメールを可視化して十分な分析も行います。この中には、組織から送信および受信される B2B メール トラフィックが含まれます。このレベルの詳細なデータは、一般のデータソースや他のセキュリティ ツールからは得られないものです。どのような手法が使われていても、また誰を標的にしたものであっても、あらゆるなりすまし脅威を単一のポータルから確認できます。

また、外部者が登録した類似の偽ドメインも自動的に識別してフラグを立てます。この機能により詐欺的なよく似た偽のドメインを使用したメール攻撃を、攻撃が行われる前に阻止することができます。プルーフポイントの管理サービスには、お客様の導入プロセスをサポートする経験豊かなコンサルタントによるサポートが含まれています。第三者を含むすべての正当な送信者が適切に認証されるように、送信者の識別をサポートします。

確かな実行プランと世界レベルのサポートがあれば、有効な電子メールを誤ってブロックすることなく、認証プロセスの迅速化を図ることができます。

3. クラウド アプリケーションを保護する

サイバー犯罪では、ユーザーを狙おうとする様々な手口が使われます。EAC を狙う攻撃者は、ありとあらゆる手法を用いて正当なメール アカウントへのアクセスを試みます。

最もよく使われる手口は、ブルートフォース（総当たり）攻撃です。ブルートフォース攻撃では、アカウント侵入が成功するまで様々なユーザーネームとパスワードを繰り返し試行する自動化されたツールが使われます。アクセスに成功すれば、組織内外の攻撃開始は簡単です。BEC 攻撃でよく使われる支払い先の変更を仕掛けることもよく見られます。このため、組織のクラウド ベース アプリケーションを保護することが重要なのです。

プルーフポイントでは、Microsoft 365 (Office 365) などのプラットフォーム上で行われるアカウント侵害から組織を保護しています。アカウント不正アクセスの兆候と考えられる、ログインの失敗、過剰なログイン、または通常とは異なるログインなどのクラウド上の不審なアカウント アクティビティを識別することで、アカウント侵害から組織を保護しています。

同時に、企業の機密情報や信頼されるアカウントにアクセスしようとするサイバー犯罪者を検知し、調査して、防御することもできます。弊社では、高度な機械学習機能により、次のようなデータを分析して、ユーザー行動のベースラインを作成します。

- ユーザーアクティビティ
- メールによる脅威に関するデータ
- ユーザーの位置、デバイス、ネットワーク、ログイン時間などの状況に関するデータ

その後、異常行動や外部脅威、内部脅威を検知します。さらに、ユーザー毎のリスクインジケーターと豊富な脅威インテリジェンスを組み合わせ、プルーフポイントのグローバル脅威インテリジェンスを用いて IP レピュテーション チェックを行い、不審なログインを検知します。

重要なことは、Eメールとクラウド全体の脅威アクティビティを相互に関連付けることです。プルーフポイントでは、認証情報のフィッシングを狙う電子メール攻撃と不審なログインとを結びつけ、また、アラートの優先順位付けをして、優先度の低いものに高いものが埋もれてしまわないようにしています。

攻撃者は、アカウントに不正にアクセスしようとしてフィッシング攻撃に出ることもあれば、逆に、不正アクセスしたアカウントを利用して組織内でフィッシング攻撃を開始することもあります。弊社ではこうした攻撃の経路を示すことで、攻撃に対して総合的に対応できるようにしています。不審なクラウド アクティビティに迅速に対応するために、必要な措置を自動的に講じるポリシーを策定することもできます。例えば、問題が発生した場合に、ユーザーセッションを遮断したり、パスワードの再設定を強制したり、ユーザーの利用を停止したりすることができます。

4. アダプティブ コントロールを用いて Web アクセスを分離する

認証情報のフィッシングは、メールアカウントに不正にアクセスしようとして使われる、もうひとつのよくある手口です。攻撃者は URL を含んだ電子メールを送信します。この URL は、認証情報を盗むために設計された偽の Web サイトへのリンクになっています。こうした偽の Web サイトは非常に巧妙に作られていることから、慎重なユーザーでさえ、これを見極めることは困難です。メールアカウントの保護策として、個人の Web メールとリスクの高い URL を分離することが重要である理由はここにあります。

プルーフポイントの Web 分離機能では、ブラウザーセッションを安全なコンテナ内に分離するため、ユーザーは、Web サイトへのアクセスも、個人 Web メールの使用も、コーポレートメールの使用も、すべて安全に行うことができます。

ここでは安全な環境内での Web サイト上の操作は認められますが、アップロードやダウンロード機能は使うことはできず、さらに Web サイトの分析中はデータ入力も制限されます。(Web サイトの分析には、通常数分もかかりません。)プルーフポイント独自のリアルタイム フィッシング対策スキャンは、ページが開かれると即座に作動します。開かれたページが悪意のあるページであると特定されると、それ以上の操作は自動的にブロックされます。このテクノロジーにより認証情報の盗難が阻止され、マルウェアや悪意のあるコンテンツ、特に送付されればリスクを伴う URL を含むフィッシングメールからユーザーを守ります。

他のベンダーは、汎用的なアプローチで Web 分離を行っていますが、プルーフポイントのソリューションでは、それぞれのユーザーのリスク状況に基づいてユーザーを選択する、アダプティブ分離コントロールが可能です。それぞれの人に適切なセキュリティを施す People-Centric のアプローチにより、企業リスクを低減させながら、標的となるユーザーのためのカスタムメイドの分離ポリシーを定めることができます。

また、ブラウザー分離機能により、未知の URL、ソーシャル ネットワーク、オンライン上のクラウド アプリケーションを含む高リスク URL からユーザーを保護します。組織内の Very Attacked People™ (もっとも注意すべき人物) のための、リアルタイムのフィッシング検知や URL リライト機能も提供しています。これにより、人それぞれに適応するきめ細かいセキュリティ制御に加えて、組織のリスクをより望ましい形で管理することができます。

5. 組織の BEC や EAC のリスクを可視化する

BEC や EAC は、性質上、人をターゲットにしており、組織の重要インフラの脆弱性をターゲットにするわけではありません。したがって、組織の BEC や EAC のリスクを理解せずには、説得力をもって説明することも、またはそのリスクを低減することもできません。プルーフポイントでは、マネジメント チームに対して、次のような点を提示できるようにサポートを行っています。

- 自社の BEC や EAC のリスクは何か？
- 最も脆弱なのは誰か？
- リスクを低減するためになすべきことは何か？

人に焦点を当てて可視化することで、組織内のVery Attacked People™ (もっとも注意すべき人物) を特定できるようになります。また、フィッシングやなりすましメールの攻撃を受けているユーザー、こうした脅威の被害者となるおそれのあるユーザー、不正アクセスを受けたクラウド メールアカウントを有するユーザーがそれぞれ誰であるのかを伝えることができます。

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すべて可視化し、よく似た偽のドメインの登録状況についても情報を得ることができます。こうした様々な要素を横断的に確かめることで、BEC や EAC のリスクを把握し、これを自社のマネジメント部門に伝えるとともに、リスク低減のための優先順位をつけて、リスクの高いユーザーを対象に、適応型のセキュリティ制御を展開することができるのです。

6. 脅威の修復を自動化する

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、通常あまりやりとりのない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性にかられ、対応しきれなくなっています。その結果、組織全体で BEC および EAC 脅威を迅速に見つけ出し、調査して対応することが容易ではなくなっています。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。

アカウントの不正アクセスが検知された場合、被害が及ぶ前に行動を起こす必要があります。プルーフポイントのソリューションでは、素早く対応するためのポリシーを策定して、自動的にパスワードの再設定を強制したり、不正にアクセスされたアカウントを停止したり、ユーザー セッションを遮断したり、またはリスクベースの認証を実行したりすることができます。Proofpoint Threat Response Auto-Pull (TRAP) 機能により、送信後に害を及ぼすような URL を含むフィッシングメールや不正アクセスされた社内アカウントを使って送信された不正メールを除去することも可能です。こうしたタスクは、メールが転送された場合でも、他のエンドユーザーがメールを受信した場合でも、1 回のクリックで、または自動的に、対応できる仕組みになっています。

また、なりすまし攻撃やフィッシング攻撃についてのエンドユーザーからの報告やセキュリティ レスポンスを効率化することも可能です。これにより脅威を数分で自動的に無力化して、IT のオーバーヘッドを削減します。エンドユーザーは、PhishAlarm®メール レポーティングのアドインにより、1 回のクリックでフィッシングメールやなりすましメールを簡単に報告することができます。

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。手動でインシデントを管理したり調査したりする必要はありません。最後に、エンドユーザーには、カスタマイズされたメールが

送られ、メールが悪意のあるものであったことが通知されます。この通知により、将来、似たような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。こうした機能は自動化されているため、BEC や EAC の脅威を素早く封じ込めることができます。手動の作業が少なくなる一方で脅威レスポンスは迅速化されるのです。

7. なりすましを見抜くため エンドユーザーをトレーニングする

BEA も EAC も人を標的にして、送金や金融詐欺などの攻撃に無意識のうちに応えてもらうことを期待しています。こうしたなりすまし攻撃は伝統的なセキュリティを迂回するように設計されているため、ユーザーが防御の最後の砦となることもあります。このため、BEC や EAC のリスクを低減するには、技術のみならずトレーニングも求められます。企業はトレーニングを実施して、ユーザーがBEC や EAC 攻撃への耐性を高められるようにする必要があります。

プルーフポイントのセキュリティ認識トレーニングでは、ユーザーが認証情報のフィッシングやよくある ビジネスメール詐欺（BEC）の手法である偽の表示名やよく似た偽のドメインなどを見抜くことができるようにサポートしています。ユーザーには、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提供されます。

トレーニングでは、まず、BEC や EAC の脅威に脆弱なユーザーを特定します。そして、BEC やフィッシングの疑似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取り扱われるのかを、安全な形で評価します。

シミュレーション攻撃で騙されてしまったユーザーには、自動的にその瞬間に学ぶことができる「ジャスト イン タイム」のガイダンスが送られ、問題となる対応について情報が送られます。将来のなりすましやフィッシング脅威を回避するためのヒントも提供されます。さらに、ユーザーを自動的に登録して、後に行われるトレーニングの受講を義務付けることもできます。

トレーニングの資料は、関連性のある、社内プロセスを考慮した完全にカスタマイズされたものになっています。このため、例えばなりすましメールを不正メールボックスに報告する、または組織の既定のプロセスを使って金銭の要求を検証するなど、組織に合わせたトレーニングを行うことができます。

まとめ

BEC と EAC は互いに結びついていることから、両者に同時に対処する必要があります。プルーフポイントは、BEC や EAC 攻撃を効果的に阻止することのできる統合型のエンドツーエンドのソリューションを提供する唯一のベンダーです。

プルーフポイントの BEC および EAC 対策ソリューションでは、次の機能を提供しています。

- あらゆる攻撃手法に対処
- 検知と修復機能を自動化
- 攻撃対象がだれかを可視化
- エンドユーザーが BEC/EAC 攻撃に対する耐性を高められるようにトレーニングを提供

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

詳細

詳細は proofpoint.com でご確認ください。

プルーフポイントについて

Proofpoint, Inc.（NASDAQ:PFPT）は、サイバーセキュリティのグローバル リーディング カンパニーです。組織の最大の資産でもあり、同時に最大のリスクともなりえる「人」を守ることに焦点をあてています。Proofpointは、クラウドベースの統合ソリューションによって、世界中の企業が標的型攻撃などのサイバー攻撃からデータを守り、そしてそれぞれのユーザーがサイバー攻撃に対してさらに強力な対処能力を 持てるよう支援しています。また、Fortune 1000の過半数を超える企業などさまざまな規模の企業が、プルーフポイントのソリューションを利用しており、メールやクラウド、ソーシャルメディア、Web関連のセキュ リティのリスクおよびコンプライアンスのリスクを低減するよう支援しています。詳細は www.proofpoint.com/jp にてご確認ください。

©Proofpoint, Inc. Proofpointは、米国およびその他の国におけるProofpoint, Inc.の商標です。記載されているその他すべての商標は、それぞれの所有者に帰属します。