Proofpoint TAP (Targeted Attack Protection)

未知の標的型攻撃に対抗するクラウド型サンドボックス

主なメリット

- 受信箱に届く前に、高度な脅威を検出、分析、ブロック
- 組織の中で注意すべき人物 Very Attacked People™ (VAP) を特定し、組織全体のセキュリティリスクを把握するための、独自の知見を提供
- プルーフポイントの脅威インテリジェンスを活用して脅威に対応し、詳細な攻撃のフォレンジック情報を提供
- Web 分離やセキュリティ意識向上トレーニングを通じて、それぞれの人に適切なセキュリティを提供するアダプティブ コントロールを実施
- URL ベース攻撃や Web ベース攻撃から VAP™ を保護し、未知の Web サイトでも企業メールから安心して閲覧できる環境を提供（プルーフポイントのソリューションバンドルの一部として提供）

90% 以上の攻撃は、メールから始まりますが、[1] メールからの脅威は常に変化しています。Proofpoint TAP (Targeted Attack Protection) は、ユーザーを狙う高度な脅威を検知して、分析し、ブロックするための革新的なアプローチです。脅威が可視化されるため、対応を最適化することができます。

Proofpoint TAP は、既知および未知のメール攻撃を阻止し、また、ポリモーフィック型マルウェア、武器化された文書、認証情報のフィッシングその他の高度な脅威も検知してブロックすることができます。疑わしいログイン、広範なファイル共有、高リスクのサードパーティ アプリケーションなど、クラウド アプリの監視を行い、攻撃されやすいユーザーを特定して保護するための情報を提供します。

BEC、URL、添付ファイル、クラウドベースの脅威からの防御

Proofpoint TAP では、静的手法と動的手法を組み合わせて、常に新しい攻撃パターンを検出し、対応しています。潜在的な脅威の分析は、振る舞い、コード、プロトコルを検証する複数のアプローチで行われ、これにより、一連の攻撃の初期の段階で、かつ可能な限り被害が及ぶ前に、脅威を検出します。

また、Proofpoint TAP は、ビジネスメール詐欺 (BEC) やサプライヤーのアカウント侵害などの脅威から組織を守ります。こういった脅威の多くには悪意あるペイロードが含まれていないことから、検知にはサンドボックス以上の高度な技術が必要です。Proofpoint TAP はプルーフポイントのインテリジェンスである Proofpoint Nexus Threat Graph によって強化されています。この Proofpoint Nexus Threat Graph は、1 兆ものデータポイントから E メール、クラウド、ネットワーク、ソーシャルメディアの情報を収集し、相関分析を行います。Proofpoint Advanced BEC Defense のエンジンは豊富な脅威データをもとに構築され、情報を蓄積しているほか、リアルタイムによる情報収集もおこない、脅威状況の変化にすばやく対応することができます。

さまざまな攻撃の分析には、サンドボックスが用いられます。攻撃の中には、マルウェアのインストールや、ユーザーをだまして機密情報を共有させようとすることをもくろむ、悪意のある添付ファイルや URL を含むものが少なくありません。このため、アナリストを支援する分析を活用して、検知機能とインテリジェンス抽出を強化しています。

1 Verizon「Data Breach Investigations Report (データ漏えい調査レポート)」2019 年 7 月

さらに、Proofpoint TAP では、クラウド アプリ内の脅威やリスクを検知し、これを認証情報の窃取やメール攻撃と関連付けています。プルーフポイントの技術は脅威を検出するだけではありません。機械学習を応用して各脅威のパターン、振る舞い、テクニックも観察します。これらの観察結果を用いることで、将来の攻撃をさらに迅速に捉えることができます。

Advanced BEC Defense

Advanced BEC Defense は、BEC やサプライヤーのアカウント侵害といった脅威から組織を防御するため、以下を含むメッセージの詳細かつ総合的な分析を行います。

- ヘッダーのフォレンジック
- 送信元 IP アドレス
- 送受信者の関係
- レピュテーション分析
- 詳細なコンテンツ分析

また、攻撃者の用いたテクニック、脅威の観測情報、メッセージのサンプルも可視化します。これによりユーザーがどのように攻撃を受けているのか理解することができます。

TAP URL Defense

TAP URL Defense は、マルウェアや認証情報のフィッシングを含む URL ベースのメール脅威を対象としています。独自の予測分析で、メール トラフィックのパターンに基づいて不審な URL を識別し、サンドボックスでの処理をおこないます。受信箱に届いた URL は、ユーザーに意識させることなく書き換えられ、ユーザーはどのデバイスを使っていてもどのネットワークを使っていても、保護されます。また、URL をクリックすると、その都度リアルタイムでサンドボックス解析も実施されます。

TAP Attachment Defense

TAP Attachment Defense は、添付ファイルによって行われる既知のまたは未知の脅威に対する防御です。さまざまなタイプのファイル、パスワードで保護された文書、URL が埋め込まれた添付ファイルや Zip ファイルなどの中に隠された脅威に対応します。

TAP SaaS Defense

Microsoft 365 や Google Workspace (旧 G Suite) に対応した TAP SaaS Defense は、疑わしいログイン アクティビティを発見します。対象となるのは、通常とは異なる場所からのログインや過剰なログインの試行、失敗などです。さらに、既知の悪意ある IP アドレスからの接続が複数回確認された場合にもフラグが立ちます。また内外のファイル共有のリスクも可視化されます。ユーザーは、過去 30 日間に、機密情報を漏洩する可能性があった時期を確認することができます。さらに、重大かつ危険度の高いサードパーティ アプリケーションが使用されている場合も検出します。

TAP URL Isolation for VAP*

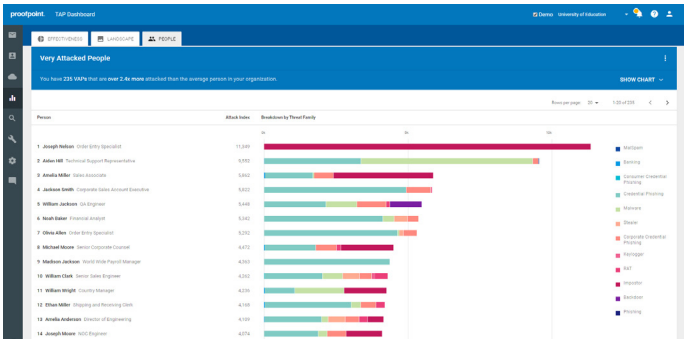
TAP URL Isolation for VAP は、URL ベース攻撃や Web ベース攻撃から組織の中の要注意人物である Very Attacked People™ (VAP) を保護するために設計されています。フィッシング攻撃をリアルタイムで検知するほか、未知の URL やリスクの高い URL をクリックしてしまった場合でも保護できるようにサポートしています。プルーフポイントの Web 分離ソリューションがあれば、組織の安全性が確保されることから、VAP™ に該当する従業員も安心して企業メールから Web サイトにアクセスできます。

* P ソリューション提供モデルを契約いただいているお客様向け機能です。

脅威や標的に関する詳細な分析と可視化

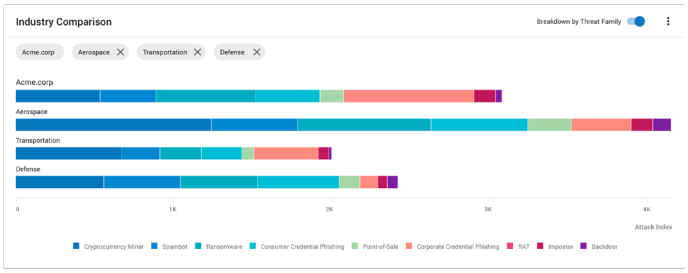
プルーフポイントでは、E メール、クラウド、ネットワーク、ソーシャルメディアといった複数の脅威経路を可視化して把握しています。これはプルーフポイントのグローバルな11万5000以上の顧客ベースから得られる情報をもとにしています。収集されたデータは、Proofpoint Nexus Threat Graph に送られ、互いに関係付けられます。これにより、脅威状況を把握するための可視性が高まります。Proofpoint TAP の Threat Insight ダッシュボードから、脅威やキャンペーンに関するリアルタイムの詳細情報を提供しています。ここからグラフを確認したり重要な知見を得たりすることができます。こうしたデータから、ばらまき型攻撃と標的型攻撃の両方を把握することが可能です。影響を受けるユーザー、攻撃に使われたメール文面やおとり文書などのスクリーンショット、そして詳細なフォレンジックなどの脅威に関する情報も提供されます。

Very Attacked People™ (VAP)



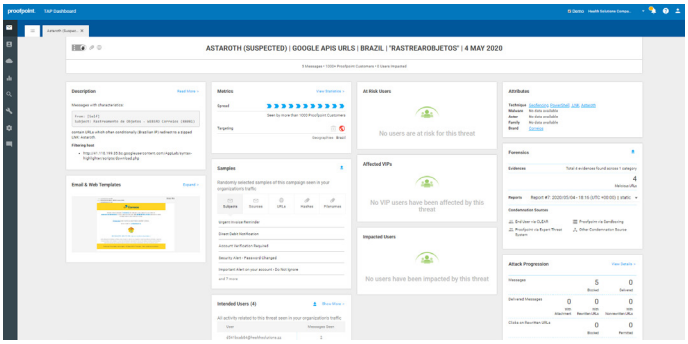
Attack Index を使えば、組織の中でもっとも注意しなければならない人物であるVAP™ を見つけ出し、組織内の標的になりやすいユーザーを特定することができます。このインデックスは組織内のユーザーに送付されたすべての脅威に関する加重複合スコアで、脅威の洗練度、拡散と集中の度合い、攻撃タイプ、全体的な攻撃ボリュームに基づいて、0 から 1000 の範囲で脅威を採点します。VAP™ を把握すれば、より効果的な対策を優先して、脅威を阻止することが可能になります。

企業レベルでの Attack Index



Attack Index を企業レベルに適用して、組織の全体的なリスク状況を把握することもできます。情報セキュリティ最高責任者 (CISO) やセキュリティ チームは、同じ業界の他社と自社を比較させることにより、自社の攻撃状況を理解することができます。レポートには、攻撃の頻度や脅威のタイプも含まれており、各社固有の状況に応じたセキュリティ コントロールの実施が可能になります。

攻撃者に関する知見



引き続き人が標的になることから、これまで以上に、攻撃を実行する犯罪者の全体像を把握することが重要です。プルーフポイントの脅威リサーチャーは、長年にわたり攻撃者に関するデータを収集・整理しており、このインテリジェンス情報は、TAP ダッシュボードで表示されます。お客様は、自社を標的とする攻撃者、標的となっている対象者、使われている手口やテクニック、攻撃者の一定の傾向といった情報を直接見ることができます。これにより、ユーザーの保護を強化するための追加的なセキュリティコントロールや対応に、優先順位をつけることができるようになります。

詳細

詳細は **proofpoint.com/jp** でご確認ください。