proofpoint.

Proofpoint STP (Supplier Threat Protection)

侵害されたサプライヤーやサードパーティのメールアカウントを識別しこれがもたらすなりすましリスクに関する知見を得る

主なメリット

- 金銭的損失やデータ脅迫を招くなりすまし脅威から保護
- 侵害されたと思われるサプライヤーやサードパーティのアカウントをプロアクティブに検知することで可視性を向上
- 悪意のあるメッセージを組織に送信している、侵害されたと思われるアカウントの自動通知を提供
- 侵害されたと思われるアカウントとのユーザーのやり取りを制限することで防護レイヤーを追加
- 調査や修復において、侵害されたと思われる高リスクアカウントの優先順位付けを行うことで、チームリソースを効果的に管理
- 侵害されたと思われるアカウントと最近やり取りした従業員を識別

Proofpoint STP (Supplier Threat Protection) は、高度なフィッシング、マルウェア、ビジネスメール詐欺（BEC: Business Email Compromise）攻撃を招くなりすまし脅威からサプライチェーンを保護します。侵害が疑われる兆候がないか、サプライヤーアカウントや既知のサードパーティ アカウントをチェックします。脅威インテリジェンスや振る舞いAIを用いて、侵害されたアカウントから送信された、なりすまし脅威が含まれる不審なメールがあれば特定し、アダプティブ セキュリティ コントロールにより、こうしたやり取りを制限します。しかし、Proofpoint STPは組織のコミュニケーションのみを可視化するわけではありません。不審なアカウントと貴社以外のプルーフポイント顧客との間のパターンも観察し、アカウントが攻撃を仕掛ける前に通知することができます。

Proofpoint STPは、メール脅威を未然に防ぐ、サプライチェーン向けの、他にはないなりすましリスク保護ソリューションです。ブラウザ分離やメール警告タグといったアダプティブ コントロールを用いて、侵害されたと思われるアカウントがユーザーにアクセスするのを制限します。メールアクティビティの記録や豊富なコンテキストデータを提供し、ダッシュボードではどのサードパーティ アカウントが最も大きなリスクをもたらしているか確認することができます。これらにより、リスク処理の優先順位付け、調査の効率化、迅速な対応が可能となります。

図1: Proofpoint Supplier Threat Protection は、不正アクセスを受けたと思われるアカウントを検知し、関連するコンテキスト情報を提供

このソリューションは、人に起因するリスクの4つの主要エリアを低減する、プルーフポイントの「人」を中心とした統合型セキュリティ プラットフォームの一機能です。

比類なき可視性

Proofpoint STPは、侵害されたと思われるアカウントが従業員にメッセージを送信するような、なりすましリスクを詳細に可視化します。プルーフポイントは全体を見渡すことができるため、侵害されてはいるが、まだユーザーに攻撃を仕掛けていない、そういうアカウントも明らかにすることができます。このような知見により、特定のユーザーに優れたセキュリティ対策を適用できるだけでなく、予防策を講じることもできます。

Proofpoint STPは、組織とやり取りをしているサードパーティアカウントを識別します。また、従業員とサプライヤーのメールアクティビティのベースラインを確立し、続いて脅威インテリジェンスとAI/ML（機械学習）を使用して不審な行動を検知します。このソリューションは、侵害されたと思われるアカウントを表示し、高リスクパートナーのランク付けを行います。ランキングは、やり取りの頻度や不正な行動パターンなどの要素に基づいて作成されます。これにより、最もリスクのあるパターンにフォーカスすることができます。

プロアクティブな保護

Proofpoint STPにより、組織はセキュリティに対しプロアクティブなスタンスを取ることができます。Proofpoint STPが、プルーフポイントのエコシステムにおいて、侵害されたパートナーアカウントによる活動を確認すると、ダッシュボードにクイックアラートを提供します。また、アダプティブ コントロールを適用し、ユーザーを保護します。こうしたコントロールにはProofpoint Isolationが含まれています。これは、不審なアカウントからのリンクを、分離された安全なブラウザで開きます。侵害されたと思われるアカウントについてユーザーに通知する、カスタマイズ可能なメール警告タグも備わっています。これにより、ユーザーが機密情報を転送する、悪意のあるファイルをダウンロードする、認証情報をアップロードする、といったことを防ぐことができます。

アラートを受け取ると、送信者ベースまたはドメインベースのセキュリティポリシーを作成できます。これらのアカウントのいずれかからトラフィックを受信した場合にメールアラートを送信するようProofpoint STPを設定するか、APIによりSIEM (Security Information and Event Management)システムに通知を送信するよう設定できます。

シンプルな調査

Proofpoint STPはセキュリティ アナリストを支援します。何が起こっているのか、どのような行動が取られたか、次に何をすべきかを迅速に判断することができます。調査を効率化し、時間を節約し、チームの業務効率を改善します。

このソリューションは、侵害されたと思われるサプライヤー アカウントに関する知見を提供します。これらの知見には、プルーフポイントの分析、送信者と受信者の関係に関するコンテキスト、そしてメッセージ アクティビティのタイムライン ビューが含まれます。また、どのコントロールが発動されたかを提示し、調査プロセスにおいて次にとるべき実用的なステップを提案します。

Smart Searchとの統合により、アナリストは、どの受信者がどのような方法で標的にされたかを特定することができます。不審なサプライヤーアカウントとの間で交わされた、その他のメッセージも見つけることができます。また、流出した財務データや機密データだけでなく、そのアカウントとやり取りした可能性のある他の従業員も確認することができます。これらはすべてProofpoint STPダッシュボードから可能です。

プルーフポイントのエコシステムがもたらすメリット

Proofpoint STPは、プルーフポイントのエコシステム全体でデータを監視します。世界中のメールトラフィックの大部分（1日あたり31億件以上のメッセージ）を確認できるプルーフポイントの能力を活用し、侵害された可能性のあるアカウントや、なりすまし攻撃を仕掛けているアカウントを特定することができます。

Proofpoint STPは、組織がやり取りをしているサードパーティやサプライヤーを確認すると、その組織だけでなく、他のプルーフポイント顧客とサードパーティやサプライヤーのコミュニケーションを追跡します。これにより、不審なサプライヤーがあれば攻撃される前に通知することができます。あなたの組織が今後、そのサプライヤーのアカウントを通して攻撃される可能性もあるため、この機能は重要です。

詳細はこちら

詳細は、proofpoint.com/jpでご確認ください。

0103-009-08-03 7/24

proofpoint.