データシート

proofpoint.

PROOFPOINT THREAT RESPONSE AUTO-PULL

配信された悪意のある電子メールを自動的に抽出して隔離 (AUTOMATICALLY PULL DELIVERED MALICIOUS EMAIL INTO QUARANTINE)

主なメリット

- 隔離にかかる時間を短縮し、電子メールの脅威を抑える
- 悪意のある電子メールの露出時間を短縮
- 配布リストまたは個人に転送されたメッセージの隔離
- 既存のインフラストラクチャの投資収益率 (ROI) を向上させるための監査アクションの履歴
- カスタムコード化されたソフトウェアへの依存を減らす
- インシデントの変更または隔離確認の電子メール通知の受信
- 発券システムへの容易な統合のための柔軟な通知
- コンテンツの設定脅威の悪用メールボックスメッセージを自動的に監視して確認
- 隔離されたメッセージを「元に戻す」機能
- CSV ファイルまたは SmartSearch の結果を使用したメッセージのグループのクリーンアップ

Proofpoint Threat Response™は、初の脅威管理プラットフォームです。オーケストレーションと自動化の拡張により、受信トレイに配信された悪意のある電子メールのリトラクト機能を含めることができました。Threat Response Auto-Pull は、悪意のある電子メールの管理をユーザーの手から離れさせ、追加のビジネスロジックを実装して、転送されたメッセージの内部コピーを見つけて削除する、プラットフォームのエントリーレベルのバージョンです。

ほとんどの組織で、セキュリティインシデントの対応は遅く、人手の要るプロセスとなっています。電子メールセキュリティインシデントに対処するには、手作業による電子メールのクリーンアップは面倒な作業になる可能性があるため、数時間から数日かかることがあります。マルウェア、不正な URL、または認証情報のフィッシングで配信された電子メールを処理するには、次のような多くのステップが必要になります：

- 内部 ID に電子メールアドレスを接続
- 選択された悪意のあるメッセージをサーバー上で検索して見つける
- ユーザーの受信トレイやその他のフォルダから悪質なメッセージを削除する
- 転送された悪意のあるメッセージを特定し、それらを隔離する

すべての電子メールインシデントに対してこれらのタスクを繰り返し実行すると、1 日に数時間かかることがあり、すでに多くの負担を抱えるセキュリティとメッセージングのチームの仕事量が限界を超えてしまう可能性があります。

電子メールクリーニングの「落とし穴」(EMAIL CLEANING "GOTCHAS")

悪意のあるメッセージの電子メールクリーンアップは、悪意のある電子メールが通過したという警告または申し立てから始まる手動のプロセスです。

表面上、電子メールインシデントを解決することは、受信ボックスを見ることと同じくらい簡単です。メッセージを削除することもできますが、これはコストのかかる前提となるでしょう。クリーンアップの一般的なミスステップは、プロセスの過度の単純化が原因であり、メッセージの量や基本的なケースを超えたものは無視することにあります。この他に考慮すべき重要な事項は次の通りです：

- メールは受信トレイにあるのか、それとも別のフォルダに移動されたのか？
- 他のフォルダでそのメッセージのコピーを確認する必要があるのか？
- メッセージは内部で送信されたのか？もしそうであれば、誰にどのくらいの数のコピーがあるのか？
- 取られたすべての措置の監査記録または記録があるのか？

DIY や自宅の電子メールクリーンアップスクリプトにつながった電子メールのクリーンアップがどれほど成功するかに影響する他の変数があります。これらはまたそれ自身にもリスクをもたらします。

DIY とカスタムコードの危険 (PERILS OF DIY AND CUSTOM CODE)

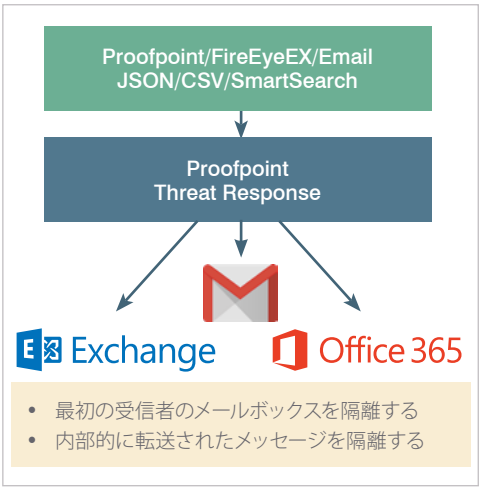
電子メールをクリーンアップするためのカスタムコードを作成して実行することは、配信された悪意のある電子メールに対する最善の解決策でした。

このことは、本質的に間違っていませんが、カスタムコードを作成し実行することは、標準的なソフトウェア開発の問題をもたらすため、責任をともなうことを意味します。

- 仕様があるか、あるいはカスタムコードが 1 つの機能しか実行しておらず、完全な仕様は必要がないのか？
- スクリプトがどのように維持されているのか？問題を解決するために対応できるオーナーがいるのか？開発者が離れるとどうなるのか？
- スクリプトがサードパーティ製品に対して動作する場合、サードパーティ製品の製品バージョン、テスト、インターフェイスまたは API の変更に対処する担当者が誰なのか？

これらの明らかな技術上の懸念事項の他にビジネス側では、カスタムコードがビジネスロジックと可視性の目標を達成する必要があります。それには次のような事項が含まれます：

- 進行中のコード操作の監視
- コードの有効性の測定または追跡
- すべての悪意のあるメッセージのバージョンが転送されたものであっても処理されたことを保証



THREAT RESPONSE AUTO-PULL を検討

Threat Response Auto-Pull は、Proofpoint Targeted Attack Protection (TAP) と O365 の電子メールやプレム上の Exchange のいずれかに接続されたときに電子メールの隔離機能を提供する Threat Response のエントリーレベルのバージョンです。
TR Auto-Pull は、FireEye EX CSV ファイル、SmartSearch、および JSON アラートの受け入れも可能です。

ユースケースはシンプル－悪意のある電子メールが検出されると、システムは、そのメッセージに関する情報を Threat Response にアラートを送信します。すると、Threat Response は Exchange、Office 365、および/または Gmail に入り、メッセージを隔離します。また、Auto-Pull は、同じサーバー上の他のメールボックスにあるメッセージおよび配布リストの受信者への配信済みコピーを探し、アクセス制限付きの隔離場所に移動します。

インテグレーションビルトイン (INTEGRATIONS BUILT-IN)

Threat Response Auto-Pull には、Exchange、Office 365、Gmail、CSV、SmartSearch、TAP、FireEye EX、および JSON ソースを数分で接続するアダプタが含まれているため、システムやコネクタを購入する必要はありません。管理者は必要なのは、Exchange の場合は適切な資格情報、電子メールのリトラクトの場合は O365 だけです。さらに、Threat Response Auto-Pull は悪用メールボックスを監視し、そこに送信されたメッセージをインテリジェンスと評判に照合するかどうかを自動的にチェックします。

AUTO-PULL OR FULL THREAT RESPONSE

Auto-Pull は電子メールのセキュリティインシデントに対処しますが、セキュリティ担当者は電子メール隔離を超える完全な脅威の対応も検討してください。検討に値する重要な機能：

- インシデント対応のセキュリティオーケストレーションと自動化
- ショートカットインシデントトリアージへのコンテキストとインテリジェンスの追加
- サンドボックスフォレンジックに対するエンドポイントフォレンジックの収集と検証
- すべてのインシデントに対して第三者情報を受け入れて適用するファイアウォール
- プロキシ、および AD による脅威の隔離と格納
- キャンペーン、ユーザー、インシデント、脅威、およびターゲットに対するリアルタイムのレポート

「...TAP と AD と統合されて配備され、数時間以内でメッセージを自動消去できるようになりました。」

匿名医療関連企業カスタマー

概要

Threat Response Auto-Pull は、内部で転送されたメッセージの削除など、受信トレイに配信された悪意のある電子メールを積極的かつ自動的に隔離および封じ込めることができます。セキュリティ担当者は、時間、効率性、および電子メールの問題処理を超える機能を得るために、Threat Response を検討すべきです。

PROOFPOINT について

Proofpoint Inc.(NASDAQ:PFPT) は次世代のサイバーセキュリティ企業です。組織が高度な脅威とコンプライアンスのリスクから今日の業務のあり方を保護できるようサポートしています。Proofpoint は、サイバーセキュリティに従事する人々が、そのユーザーを標的にした高度な攻撃（電子メール、モバイルアプリ、ソーシャルメディア経由）からユーザーを守り、社内の重要な文書や情報を保護し、万一の場合には社内のチームが、素早く対応するために必要な知識とツールを活用できるようにしておく支援をさせていただきます。現在のモバイルおよびソーシャルメディアに対応した IT 環境向けに構築され、クラウドの力とビッグデータを生かした分析プラットフォームを活用して、今日のより高度な脅威に対抗することができる Proofpoint ソリューションを、フォーチュン 100 企業の半数以上を含む様々な規模の一流企業にご利用いただいています。