proofpoint

顧客事例

米国大手金融機関 事例

自社を狙う標的型攻撃から自社になりすまして顧客を狙う攻撃への対応も実現

プルーフポイントの People-Centric メール セキュリティ ソリューションで攻撃を阻止

課題

- 詐欺メールや標的型フィッシング攻撃によるサイバーセキュリティ リスクを低減
- 会社のドメイン名を悪用する、なりすまし詐欺を防止
- 顧客やパートナーからの信頼を維持し、財務リスクを低減

ソリューション

- Proofpoint Email Protection および Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Email Fraud Defense (EFD)
- Proofpoint Cloud App Security Broker (CASB)

導入効果

- わずか30日で660万通以上の迷惑メールをブロックまたは隔離
- 詐欺メールを100%阻止してリスクを低減
- ビジネスメール詐欺（BEC）およびメールアカウント侵害（EAC）攻撃から従業員のメールアカウントやクラウドアカウントを保護
- ドメインを悪用したなりすましを阻止し、会社のブランドを保護

会社概要

150年の歴史を持つこの米国大手金融サービス機関には6,500名以上のファイナンシャル アドバイザーが在籍し、約500万人のクライアントに様々な金融サービスを提供しています。サービス内容には、財産および資産所得の保護、教育資金計画および退職後の資産計画、投資に関するコンサルテーションなどがあります。同社はこれまでの業績や高い評判をもとに確実に成長をし、この業界で最も評価の高い企業のひとつになっています。

課題

コミュニケーションの保護

この会社は、企業の社会的信頼を表すインテグリティと安全性に定評があり、これら顧客からの信頼はこの会社が生み出す利益や運用している資産と同じくらい重要です。同社はデジタル化の推進に伴い多額の技術投資をしており、特にセキュリティに力を注いできました。そしてその経験を活かして、クライアント、従業員、パートナーを騙そうとする攻撃者との戦いに常に新しい技術を活用しています。攻撃者によく狙われるのは個人的なコミュニケーションで、特にビジネスメール詐欺（BEC）とメールアカウント侵害（EAC）は頻繁に発生します。

同社でメールセキュリティを担当するシニアエンジニアは次のように話しています。「サイバーセキュリティで最も問題になるのはなりすましメールやハッキングしたアカウントを悪用した攻撃です。またドメインのなりすましも問題となっており、私たちのドメインを利用して詐欺メールを送る攻撃が増えています。クラウドへの移行が増えると、クラウドメールアカウントへの攻撃も増えます。」

セキュリティチームはメールのトラフィックや内容を十分に可視化できていませんでした。そこで、以前使用していたメール ゲートウェイでルールを導入し、なりすましメールをブロックするフィルターも導入しました。しかし、送受信されるすべてのメールを可視化することは不可能で、そのためすべての不審メールの阻止はできていませんでした。

「プルーフポイントのマルチレイヤーのアプローチで、メールを使った攻撃の阻止やメールの信頼性を確保できるようになりました。これにより従業員、お客様、そしてパートナーは安心してコミュニケーションできるようになり、また私たちが管理する資産も安全だと確信していただいています。」

メールセキュリティ部門シニア サイバーセキュリティ エンジニア

ソリューション

インテリジェントな多層プロテクションで100%の保護を実現

この会社はこれらの問題の解決のためプルーフポイントのソリューションを検討し、Proofpoint Email Protection と Proofpoint Email Fraud Defense を採用しました。また Proofpoint Targeted Attack Protection (TAP) と Proofpoint Threat Response Auto Pull (TRAP) も導入することで高度なマルウェア、ランサムウェア、危険なリンクを含むメールを阻止できるようになりました。これらのインテリジェント ツールは既知の悪意ある送信者やその疑いのある送信者を識別します。そして疑わしいメールは、たとえ受信後でもブロックまたは隔離して分析します。分析の結果、悪意あるメールであることが判明した場合、Proofpoint TRAP はそのメールが転送された先や配信リストを追跡し、危険なコンテンツをシステムから除去します。これらの機能により高度なマルウェア、ランサムウェア、そして危険な URL リンクから会社を守ることができるようになりました。

プルーフポイントはまたビジネスメール詐欺（BEC）およびメールアカウント侵害（EAC）攻撃の対処もサポートしました。BEC は最近特に急増しています。攻撃者は表示名のなりすまし、ドメインのなりすまし、そしてよく似たドメインを使って、そのメールがよく知っている信頼できる人から送られてきたと受信者に信じ込ませます。例えばこの会社では、なりすましドメインから16日間に50万通のメールが送られてきたことがありました。

しかしメールセキュリティチームは無事この大規模攻撃をブロックし、またもう少し規模の小さい攻撃を無数にブロックしてきました。これが実現できたのは、セキュリティチームが Proofpoint Email Fraud Defense を使って DMARC (Domain-based Message Authentication Reporting and Conformance) を導入したためです。

Proofpoint Email Fraud Defense では、ドメインを使って従業員、顧客、ビジネス パートナーを狙う攻撃の詳細を可視化します。また不審なドメインからのメールを隔離またはブロックします。このソリューションを導入したことによって、メールセキュリティチームは数千通規模のメールが短期間に、複数のなりすましドメインから送られてきていたことを発見できました。詳細な可視化によって、セキュリティチームはドメインを悪用した詐欺メールを識別、隔離、ブロックするルールを作成できるようになりました。

同社のメールセキュリティのシニアエンジニアは次のように述べています。「メールセキュリティチームは従業員やファイナンシャル担当者の安全を確保する責任があります。詐欺師や攻撃者は、CEO から送られてきたようにみせかけた偽のメールで人を騙して、銀行送金させたりギフトカードを送付させようとします。こういった攻撃はますます高度化してきています。メールのうちの50%が偽のメールである場合もあるのです。」

その後、セキュリティチームはクラウドを使ったコミュニケーションに目を向けました。クラウドメールサービスの利用が増えるにつれ、クラウド アカウントへの攻撃が急増しています。リモートアカウントは一度ハッキングされると、ハッカーに完全にコントロールされてしまいます。こういったアカウントからメールを受け取った人は、それが信頼できる本物のメールだと思ってしまうため、甚大な被害が起こる可能性があります。そこで同社ではクラウド上のコミュニケーションを保護するために Proofpoint Cloud App Security Broker (CASB) を導入しました。CASB はクラウドでの高度な脅威保護を実現し、機密データやアカウントにアクセスしようとする悪意のある攻撃者を検出、調査、阻止します。例えばクラウド上のコラボレーションアプリに不審なファイルがアップロードされた場合、直ちに隔離してリスクを分析します。CASB はプルーフポイントの保護ツールとシームレスに連携してデータを共有し、クラウド全体まで保護範囲を効果的に拡大します。

結果

People-Centric な多層アプローチで安全なコミュニケーションを実現

プルーフポイントの自動脅威検出と修復ですぐに効果が出ました。例えばこの会社では直近30日間に1,800万通以上のメールを受信しましたが、そのうち37%（約660万通）がブロックまたは隔離されました。同社のメールセキュリティチームは Proofpoint Email Protection と Email Fraud Defense（特に TAP および TRAP）のおかげで従業員に送られたマルウェアの大半を阻止できたと感じています。

メールセキュリティチームのシニアエンジニアは以下のように説明しています。「一目見ただけでは正規のメールかどうかわからないメールも多くあります。しかし TAP はすべてのメールを分析し、不審なメールをブロックまたは隔離して通知してくれるので、私たちはその通知を基に詳細調査を始めることができます。悪意のあるメールが届いてしまった後でも、TRAP はそれを自動的に受信箱から抜き出します。このおかげで私たちのチームはマニュアル作業の多くから解放されました。」

DMARC によりコミュニケーション システムに保護レイヤーを追加できます。同社では DMARC を導入したことによって、ドメインを悪用した攻撃が定期的に大量に来ていたことを発見できました。数千通規模のなりすましメールが短期間に、複数のなりすましドメインから送られてきていたのです。また DMARC を用いたことによって、同社のドメイン名が第三者への攻撃に悪用されることも防止できるようになり、ブランドを保護できるようになりました。

そしてメールセキュリティチームは最後にクラウドベースのツールの使用の増加への対策に注意を向けました。EAC攻撃は特に、コラボレーションやコミュニケーション用にクラウドアプリの使用が増えるにつれて増加しています。そこでメールセキュリティチームは従業員のクラウド上でのアクティビティを保護するために CASB を導入しました。メールセキュリティチームのリーダーによると、CASB でクラウドユーザーの監視と保護を開始して以降、クラウドアカウント侵害は1件も発生していません。

シニア メールセキュリティ エンジニアは以下のように話しています。「リモートアカウントは一度ハッキングされると、ハッカーに完全にコントロールされてしまいます。こういったアカウントからメールを受け取った人は、それが信頼できる本物のメールだと思ってしまうため、甚大な被害が起こる可能性があります。」

プルーフポイントはすべての攻撃対象への保護をシームレスに統合して、コミュニケーション セキュリティ システム全体を一元的に可視化します。新しい脅威が発生したときは、システムの変更や、新しいルールおよび機能の追加も可能です。

「Email Protection、Email Fraud Defense、そしてそれに DMARC や CASB を組み合わせることで、プルーフポイントはメール詐欺への『特効薬』に限りなく近いものを提供してくれました」と同社のメールセキュリティチームのリーダーは締めくくっています。

詳細

詳細は proofpoint.com/jpでご確認ください。