proofpoint.

ソリューション概要

Proofpoint Collab Protection

チャットツールやコラボアプリケーションより
侵入する脅威から人を守る

主なメリット

- メールの枠を超えて**フィッシング保護を提供**
- リアルタイムで**悪意のあるURLをブロック**
- すべてのデジタルチャネルにおいてフィッシング脅威を**可視化**
- 広範なフィッシング保護によりデータ侵害の**リスクを低減**

今日のダイナミックな業務環境において、コミュニケーションや共同作業に用いられているものはメールだけでなく、チャットツール、コラボレーション アプリ、ソーシャル メディア プラットフォームなど、その他の多くのデジタルチャネルも利用されています。攻撃者はこのように移行している状況を把握しており、こうしたチャネルを悪用して攻撃を仕掛けるようになっています。

包囲されるチャットツールおよびコラボレーション プラットフォーム

攻撃者は、チャットツールやコラボレーションのプラットフォームを、フィッシング攻撃の新たな起点としています。この目的のために、ソーシャル エンジニアリング戦術や悪意のあるURLを使用しています。悪意のあるURLは、攻撃者がペイロードを配布するために最も用いられている方法となっています。Proofpoint Threat Research チームによると、ここ3年で、SMSベースのフィッシング（スミッシング）によって配信されたURL脅威は2,524%もの上昇が確認されています。攻撃者は、チャットツールやコラボレーション アプリを使用して、偽のアカウントをセットアップし、見せかけの関係を築き、相手を偽のログインページに誘導します。こうしたページは、個人情報を取得したり、ユーザーを騙して送金させたり、企業の機密情報を提供させたりすることを目的としています。

チャットツールおよびコラボレーション アプリにおいて攻撃が発生する仕組み

Microsoft Teams、Slack、Zoomなど、チャットツールおよびコラボレーション アプリを標的にしたフィッシング攻撃は、以下の手順で行われます。

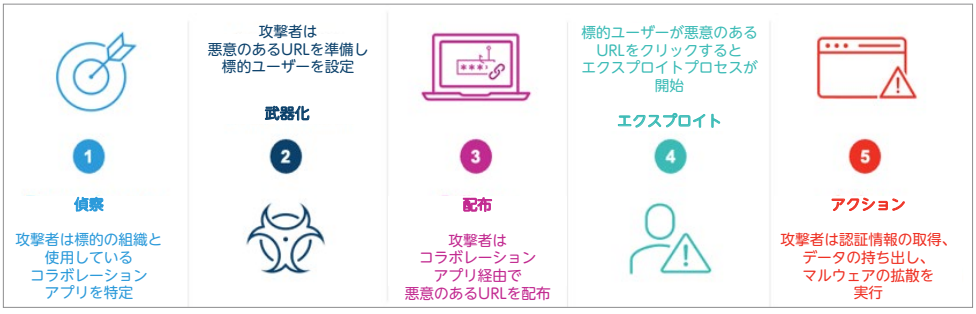

図1：チャットツールやコラボレーション アプリへの攻撃は一般的に複数の段階に分けて行われる

このソリューションは、人に起因する4つの主要リスクを低減する、プルーフポイントのHuman-Centric Security統合型プラットフォームの一機能です。

チャットツールおよびコラボレーション アプリのセキュリティを強化する

チャットツールおよびコラボレーション アプリは、人と組織をフィッシング攻撃から保護するためのネイティブセキュリティ機能を備えていません。そこでプルーフポイントが役立ちます。

Proofpoint Collab Protectionは、チャットツール、コラボレーション アプリ、ソーシャルメディアのアプリケーションで配布された悪意のあるURLから保護します。URLのレピュテーション調査と分析をリアルタイムで実行し、悪意のあるURLにユーザーがアクセスしようとすればブロックします。Proofpoint Collab Protectionにより、プルーフポイントは、ユーザーを高度なフィッシング攻撃からいつでもどこでも保護します。

従業員を悪意のあるメッセージから保護

Proofpoint Collab Protection は 、プルーフポイントの業界有数の脅威インテリジェンスを活用しています。従業員がデスクトップPCまたはモバイルデバイスから、チャットツールおよびコラボレーションアプリ内の不審なリンクにアクセスしようとすれば、Proofpoint Collab ProtectionはURLをリアルタイムで分析します。URLのレピュテーション チェックを行い、ブラウザで入力されたURLを分析します。Proofpoint Collab Protection が悪意のあるURLを検知した場合、これをブロックします。このようにしてユーザーは、悪意のあるWebサイトやコンテンツから保護されます。

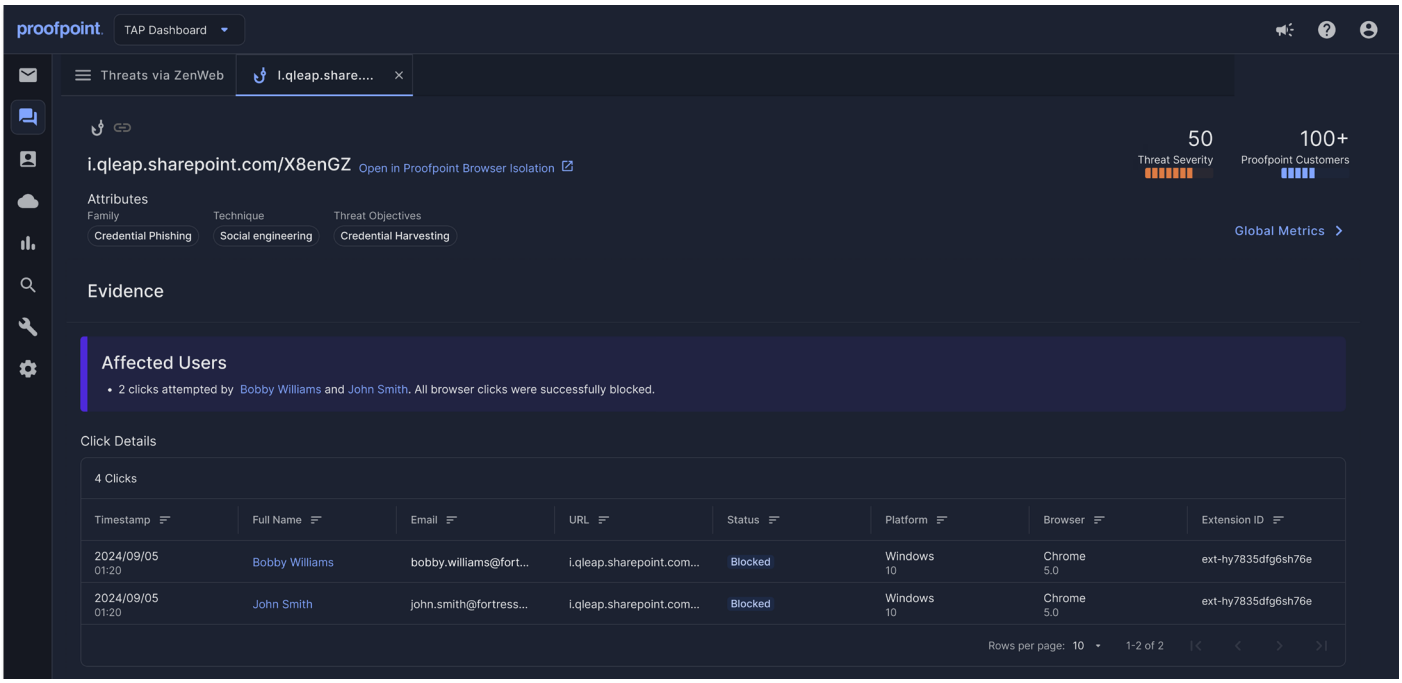

図2：Proofpoint Collab Protectionはユーザーがアクセスしたリンクをリアルタイムで分析

マルチチャネルのフィッシング脅威の可視化

攻撃者は、さまざまなデジタルチャネルで従業員を標的にするようになっています。これらのチャネルには、メール、コラボレーション プラットフォーム（Microsoft Teams、Slack、Zoom）、そしてテキストメッセージさえも含まれます。セキュリティチームやITチームは、これらすべてのチャネルにおいて脅威を監視しなければなりません。Proofpoint Collab Protectionはこのようなマルチチャネルの可視性を提供します。従業員がチャットツールまたはコラボレーション アプリ内の不審なリンクにアクセスした場合、Proofpoint Collab Protectionはリンクにアクセスしたユーザーと、リンクを送信したデバイス（デスクトップPCまたはモバイルデバイス）を表示します。また、該当するURLがブロックされたかどうかも示します。Proofpoint Collab Protectionは、すべてのチャネルにおける脅威に関する統一されたビューを提供するため、フィッシング脅威を迅速に追跡し、軽減できます。セキュリティチームやITチームは、組織に害を及ぼす前に攻撃を検知し、阻止できます。

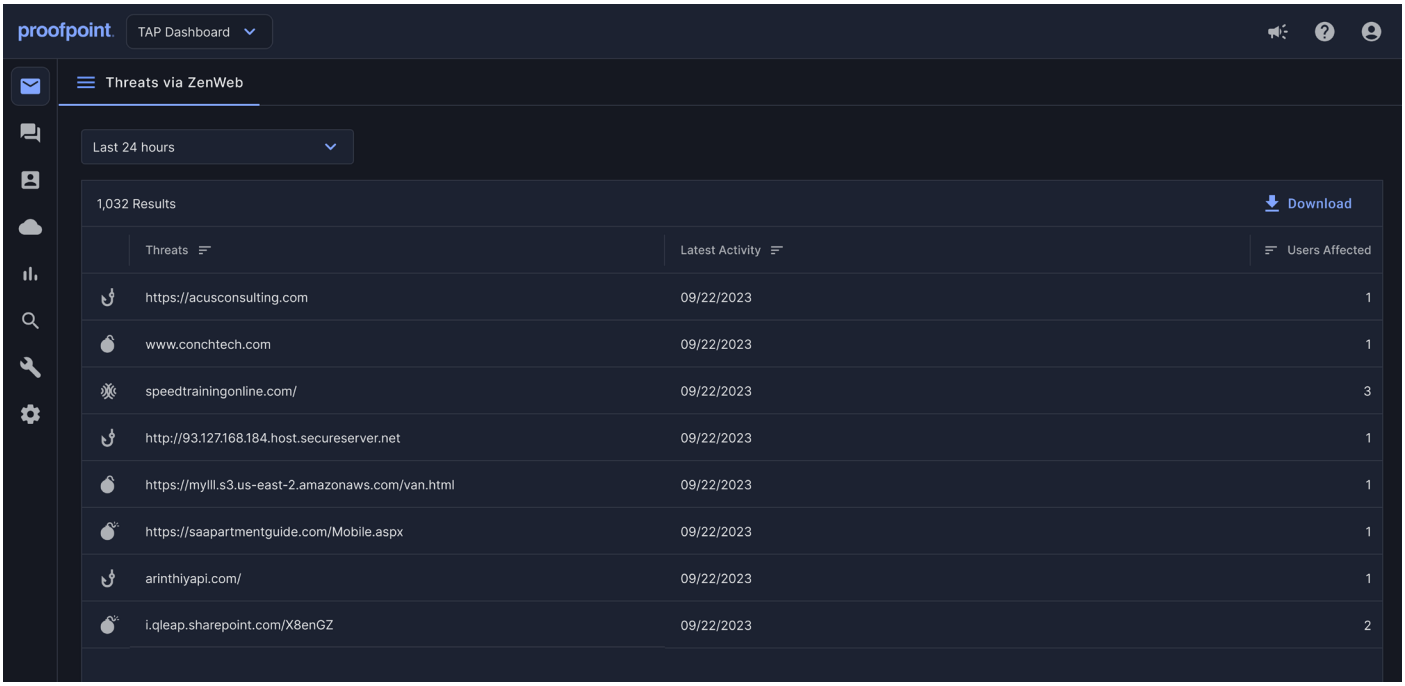

図3：Proofpoint Collab Protectionは複数チャネルでの脅威に関する統一されたビューを提供

次の進化：Human-Centric Security

近年、企業業務におけるコミュニケーションや共同作業に、ますますメール以外のチャネルが利用されるようになっています。攻撃者はこの変化に目を付け、サイバー攻撃のための新たな侵入経路を見出しています。そういった攻撃には、フィッシング、マルウェア、アカウント乗っ取りが含まれます。こうした新たな脅威に先手を打つためには、メール保護と同等の検知精度をチャットツールやコラボレーション アプリにも拡大するソリューションが必要です。

Proofpoint Collab Protectionなら、メールの枠を超えてフィッシング保護を拡大することができます。Proofpoint Collab Protectionは、チャットツールまたはコラボレーション アプリにおいて悪意のあるフィッシング メッセージを阻止できます。URLのレピュテーション調査と分析により、これらの脅威がリアルタイムで検知され、阻止されます。これにより、従業員を高度なフィッシング攻撃からいつでもどこでも保護できます。