Proofpoint TAP Account Takeover

メールやクラウド環境で侵害されたアカウントを検知し修復

主なメリット

- 脅威インテリジェンスと振る舞い分析を使用して侵害されたメールアカウントを検知
- 多要素認証の回避から保護
- アカウント乗っ取り攻撃や侵害後のクラウドのアクティビティのメール脅威調査を加速して統合
- メールやクラウド環境において、アカウント、悪意のあるメールボックスルール変更、悪用されたサードパーティアプリ、データの抜き出しを修復

Proofpoint TAP Account Takeoverは、侵害されたアカウントを検知し、メールやクラウド環境を保護することにより、Proofpoint TAP (Targeted Attack Protection)のパワーを拡大します。フィッシング、総当たり攻撃、ビジネスメール詐欺(BEC)、マルウェア、データ抜き出し、攻撃者の継続的なアクセスから保護します。

Proofpoint TAP Account Takeoverは、人工知能（AI）に加え、相関する脅威インテリジェンスや振る舞い分析を用いてメールアカウントへの攻撃チェーンにおける不審なアクティビティを検知します。これにより、アカウントを標的にしているメール脅威の種類が確認できます。攻撃者がアカウントを侵害した際に、これを保護するためのアクションを取ることができます。また、悪意のあるメールボックス ルール変更、悪用されたサードパーティ アプリ、機密ファイルの過度の共有を自動的に修復します。Proofpoint TAP Account Takeoverは、不審なログイン、アカウント乗っ取り、影響を受けたユーザー、脅威を修復するために取ったアクションに関する詳細なレポートを提供します。これらの知見により迅速に悪意のあるアクティビティを調査し、脅威に対応し、リスクを抑えることができます。

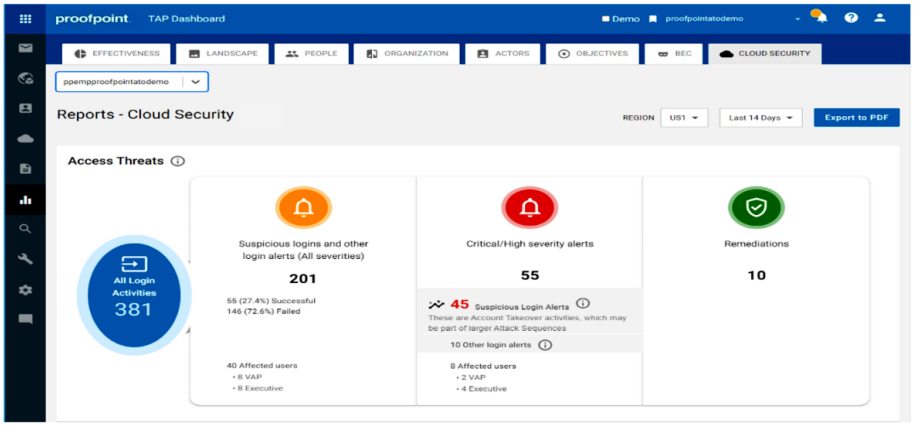

図1：プルーフポイントはすべてのログインアクティビティを監視
アクセス脅威レポートにより不審なログインを可視化し、自動で修復

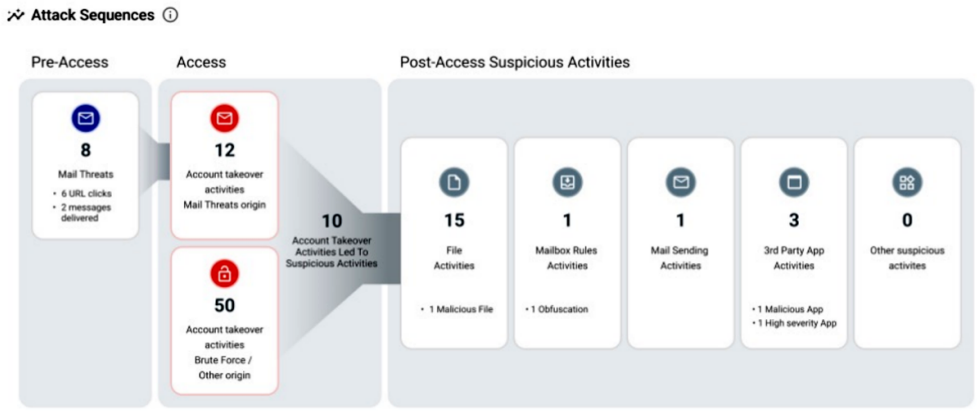

図2：攻撃シーケンスレポートから攻撃チェーン全体のアクセス脅威を確認可能

可視性

Proofpoint TAP Account Takeoverは、メールやクラウド環境における侵害されたアカウントやアクセス後の不審なアクティビティを可視化します。脅威インテリジェンスをAI/MLや振る舞い分析と関連付けて悪意のあるイベントを検知します。このアプローチは完全な可視性を提供するため、どのアカウントがどのように侵害されたか確認することができます。また誤検知アラートも削減するため、アカウント乗っ取りの判定により確信をもつことができます。

Proofpoint TAP Account Takeoverは、アカウントが侵害されるとTAPダッシュボードで自動アラートを提供し、アカウント侵害リスクの概要が攻撃シーケンスタイムラインで確認できます。影響を受けたアカウントや、アクセス前およびアクセス後の悪意のあるアクティビティも確認でき、攻撃者がどのようにアクセスし、ログイン後に、ファイルアクティビティなど、どのような行動を取ったかがわかります。また、メールボックスルールの変更も特定できます。これによって、攻撃者がシステムに潜んでいたり、メール送信アクティビティやサードパーティアプリの操作を隠そうとしていてもわかります。

迅速な調査

Proofpoint TAP Account Takeoverにより、セキュリティアナリストは、何が起こっているか、どのようにリスクを低減できるかを即座に知ることができます。アカウント侵害に関する情報は、Proofpoint TAP調査システムとプロセスに統合されています。Proofpoint TAPダッシュボードで同様の、相関的で「人」を中心としたPeople-Centricな知見と脅威インテリジェンスが利用できます。乗っ取られたアカウントに関する知見はアクティビティのタイムラインビューで確認できます。どのデータもクリック可能なため、アナリストは、アカウント侵害を受けた各インシデントを掘り下げて調査することができます。ユーザーがVery Attacked Person™ (VAP)であるか、アカウントがどのように侵害されたか、また攻撃者の場所を確認することもできます。また同様の脅威の被害を受けたユーザーについても知ることができます。

自動対応

攻撃者がメールボックスルールを変更すると、Proofpoint TAP Account Takeoverは自動的にこれを検知し、修復します。攻撃者はしばしばこれらのルールを変更し、自身が誰であるか隠したうえでBEC攻撃を仕掛けます。また、Proofpoint TAP Account Takeoverは、攻撃者が検知されずに制御できるようにする、サードパーティアプリの悪用を検知し、無効化することができます。これらのアクションにより、攻撃者のアカウント内の滞在時間を減らすことができます。また、組織への被害を抑え、チームの負荷を軽減することができます。他の悪意のあるアクティビティが調査によって明らかになれば、乗っ取られたアカウントを修復するためのアクションを取ることができます。情報漏えいを抑止したり、攻撃者が組織の環境内に忍び込ませた悪意のあるファイルを削除したりできます。

詳細はこちら

詳細は、**proofpoint.com/jp**でご確認ください。