クラウドアカウント乗っ取り対策

壊滅的な被害をもたらすクラウドアカウントの乗っ取りを未然に防ぐ

製品

- Proofpoint CASB (Cloud App Security Broker)
- Proofpoint ZTNA (Zero Trust Network Access)
- Proofpoint Browser Isolation
- Proofpoint Email Isolation
- Proofpoint 脅威プロテクションプラットフォーム
- Proofpoint TAP (Targeted Attack Protection)

主なメリット

- 認証情報の盗難やマルウェアの起動を目的としたフィッシング攻撃をブロックすることで、アカウントの乗っ取りを防止する
- 乗っ取られたクラウドアカウントのすべてのインスタンスを検知および修復する
- 貴重な資産の周りに強固なバリアを作り、脅威から防御する
- 従業員が意図せずに脅威を環境に持ち込むのを防ぐ
- 潜在的な新たな脅威に備えるための貴重な情報を得る

企業がクラウドに移行する中、サイバー犯罪者も追随し、クラウドまで侵入しています。ホスト型メールや Web メール、Microsoft 365 や Google Workspace などのクラウド生産性アプリケーション、AWS や Azure などのクラウド開発環境を採用する企業が増えるにつれて、サイバー犯罪者は、企業アカウント認証情報を用いれば、容易に金銭や権限を得ることができることに気付きました。そのため、現在、認証情報を標的とした攻撃キャンペーンが増えています。サイバー犯罪者の絶え間ない活動は、送金詐欺、産業スパイ、PII(個人識別情報)データの窃取などを目的とする活動の最初の一撃に過ぎません。

クラウドアカウントの乗っ取りは、攻撃者がユーザーの認証情報を侵害し、それを用いてユーザーのシステムに侵入することから始まります。多くの場合、これらの攻撃は、マルウェアが埋め込まれたメールや、ユーザーを騙して認証情報を提供させるフィッシングメールから発生します。アカウントを乗っ取ると、ユーザー組織内にいる実際の人物や信頼できる人物を装うことができてしまいます。潜入者は組織内をラテラルムーブメントして、広範囲にダメージを与えていきます。重要なデータを盗んだり、暗号化したりするだけではなく、マルウェアをアップロードして、エンドポイントやMicrosoft 365、その他のクラウドリポジトリ間の同期・共有機能を悪用することもあります。そして、そこから組織内に素早く拡散し、機密ファイルをダウンロードして脅迫に利用するなどの攻撃につなげていくのです。

また、シングル サインオン システムの利用拡大に伴い、1 つの認証情報が漏洩するだけで、攻撃者は社内の様々なシステムにアクセスできるようになります。

クラウドアカウントの乗っ取りの中でも最も脅威的で破壊的な形態の 1 つがランサムウェアです。この種のサイバー攻撃は、時には企業を倒産に追い込み、病院の機能を停止させ、行政業務がおこなえなくなるなど大きな問題を引き起こしています。昨年だけでも、米国では 65,000 件以上のランサムウェア攻撃を受けました。Palo Alto Networks の Unit 42 によると、メールがランサムウェア攻撃の起点の 4 分の 3 を占めています。[1] これは CISO にとって最大の懸念となっています。そして、国家安全保障上の問題にまで発展しています。

1 Unit 42, Palo Alto Networks (https://unit42.paloaltonetworks.com/ransomware-families/). “Ransomware Families: 2021 Data to Supplement the Unit 42 Ransomware Threat Report (ランサムウェア区分：Unit 42 ランサムウェア脅威レポートに関する 2021 年追加データ)” 2021 年 7 月

プルーフポイントのソリューション

サイバー犯罪者は、複数の戦略と脅威経路を利用して、ネットワークへの侵入の足掛かりを築きます。多くの場合、必要な情報を得るために、ハイブリッドなアプローチで攻撃を仕掛けています。その手段となるのは、総当たり攻撃、ソーシャルエンジニアリング、マルウェアなどです。その企てから身を守るためには、包括的で多層的な防御が必要です。プルーフポイントは、このような防御をサポートする多くの製品やサービスを提供しています。

プルーフポイントのソリューションを併用して以下を可能にすることで、クラウドアカウントの乗っ取りの脅威から防御することができます。

- 初期のクラウドアカウントの乗っ取りを防止する
- クラウドアカウントの乗っ取りを検知および修復する
- 貴重な資産（人とシステムの両方）の周りに強固なバリアを作り、外部の脅威からの攻撃を防ぐ
- 従業員が意図せずに脅威を環境に持ち込むのを防ぐ
- 潜在的な来たるべき脅威に備えるための貴重な情報を得る

防御、検知、対処

プルーフポイントの脅威プロテクション プラットフォームは、クラウドアカウントの乗っ取りリスクを低減する、統合されたマルチレイヤーのソリューションです。業界最先端の脅威検知機能により、マルウェアや認証情報のフィッシングなどのメールベースの攻撃を防ぎます。また、侵害されたアカウントを修復するためにセキュリティ制御を調整します。これにより、インシデント レスポンス時間が短縮され、IT 部門の負荷を低減できます。標的となったユーザーや実際に認証情報の脅威に関わったユーザーは、セキュリティ意識向上トレーニングを通じて、短期間のタイムリーなレッスンを受けることができます。また、カスタマイズ可能な HTML バナーを利用すれば、ユーザーに情報が伝わりやすく、危険となり得るメッセージに注意を促すことができます。このソリューションでは、DMARC を介してインバウンド メッセージとアウトバウンド メッセージを認証することができます。乗っ取られたサプライヤーのアカウントを特定することも可能です。こういった多層アプローチを擁するプルーフポイントは、Fortune 1000 の 60% 以上の企業から、クラウドアカウントの乗っ取りのリスクを軽減するための脅威対策として信頼を寄せられています。

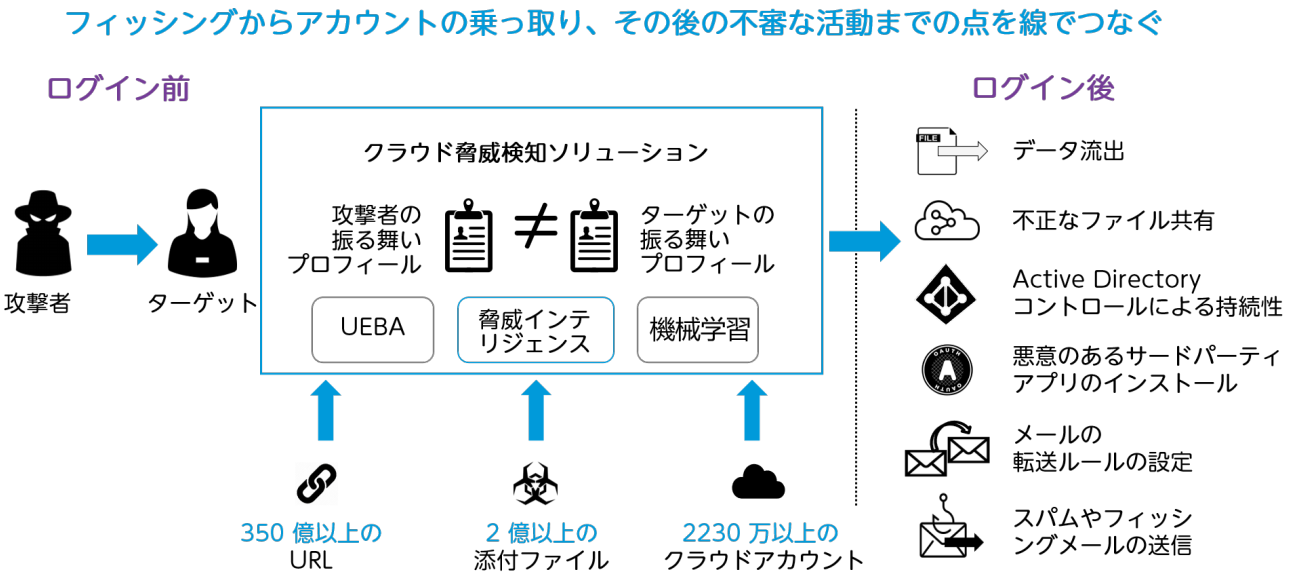

図 1:CASB による侵害されたアカウントの検知

Proofpoint CASB (Cloud App Security Broker) は、クラウドアカウントの乗っ取りに対する防御の要です。クラウドの脅威からユーザーを守り、機密データを保護するために、人を中心としたアプローチをとります。その防御は、可視性とアクセス コントロールから始まります。なぜなら、見えないことを見えるようにするまでは、クラウドアカウントの乗っ取りに対して効果的な防御を行うことができないからです。Proofpoint CASB は、ステップアップ認証を含む、アダプティブ アクセス コントロールなどの予防的セキュリティ対策の導入をサポートします。乗っ取りの試みをすべて検知し、攻撃者がアカウントにアクセスした後の行動を知らせます。Proofpoint CASB は、侵害されたアカウントを停止し、乗っ取り後のすべての脅威を修復します。たとえ攻撃者がお客様のアカウントにアクセスしたとしても、Proofpoint CASB は、メールの転送や委任、データの流出、フィッシング メールやスパムメールの送信などに利用しようとする試みを阻止することができます。

VPN からゼロトラストへの移行

リモートワーカーやモバイルワーカーは世界中で増加しています。それに伴い、クラウドに移行するアプリケーションが増えることで、ネットワークの境界線が消えつつあります。多くの企業は、この新しいパラダイムに伴う新しいセキュリティの課題に取り組み始めたばかりです。そのため、サイト中心の接続やセキュリティ スタックに基づいて構築された従来のセキュリティ システムでは、ますます革新的になっていくクラウドベースの脅威から保護する役割は果たせないということに、気付いたばかりなのです。

Proofpoint ZTNA (Zero Trust Network Access) は、データセンターとクラウドの両方でユーザーをアプリケーションに安全に接続できるように手助けします。VPN に代わる、「人」を中心にセキュリティを構築するPeople-Centricの手法は、アクセス許可の対象を細かくセグメント化し、必要な人に必要なレベルの許可を与えることで、ネットワークの攻撃対象領域を大幅に減らします。これにより、SDP(Software-Defined Perimeter: ソフトウェアで定義された境界) を提供し、ゼロトラストのネットワークアクセスを実現します。

Proofpoint Browser Isolation と Proofpoint Email Isolation

IT チームとセキュリティチームは、ユーザーのためにセキュアな環境を確保する必要があります。しかし、ユーザーがWebで何かを調査したりチームメンバーとのコラボレーションしたりするのを、業務効率を落とさずに行えるようにする必要もあります。クラウドアカウントの乗っ取りの主要な経路が、調査やコミュニケーションに使用されるツールと同じ場合、つまりWeb とメールの 2 つである場合、複雑性が増します。プルーフポイントでは、お客様のチームにそれぞれの長所をもたらす 2 つのソリューションを提供しています。これらは、シームレスなブラウジングとコミュニケーションの体験を提供しますが、クラウドアカウントの侵害からもユーザーを保護します。

Proofpoint Browser Isolation は、ユーザーが誤ってフィッシング リンクをクリックしたり、悪意のあるファイルを企業のデバイスにダウンロードしたりしないように保護しながらWeb を閲覧できるようにして、クラウドアカウントの侵害から防御します。

Proofpoint Email Isolation は Proofpoint TAP (Targeted Attack Protection) の機能を拡張したものです。コーポレートメール内の URL をユーザーがクリックした場合に、そのリスクに基づいて処理を分離します。また、最もよく狙われるユーザーに注目し、該当のアドレス宛てのメールに含まれている URL の中で最もリスクの高いものを識別します。

最新のインテリジェンス

脅威の状況を深く、広く知ることで、次の大きな脅威に備えることができます。Proofpoint Nexus Threat Graph は、今日の最大のサイバー脅威を常に把握するために必要な包括的な脅威インテリジェンスを提供します。世界中の複数の脅威経路にまたがる何兆ものリアルタイムのデータポイント、高度な AI と機械学習、そしてサイバーセキュリティ調査エキスパートから成るグローバルチームを組み合わせています。

詳細

詳細は **proofpoint.com/jp** でご確認ください。