VECTRA
SECURITY THAT THINKS®

業界洞察

金融サービス機関における脅威検知

拡大する金融サービスのクラウド化に明確さを

この一年、多くの業界において導入が加速した新技術は、人々の安全、つながり、そして生産性を維持するためのものでした。規制の厳しい金融サービス業界でさえも、顧客に新しいサービスを迅速かつ経済的に提供するために、多くの機関がクラウドへと移行しています。さらに、柔軟性とアクセスの向上を実現するために、Azure Active Directory（AD）やOffice 365を利用したシングルサインオン（SSO）の使用が加速していますが、この流れは金融サービス機関においても浸透しつつあります。そのような中、攻撃対象領域はどのような状況なのでしょうか？サイバー犯罪者の多くは研究熱心で、新たなクラウドサービスへの攻撃を試そうと常に手ぐすね引いて待っています。

金融サービス機関にとってサイバーリスクはつきものです。そして、新しいテクノロジーの登場でそのリスクが完全に解消されるわけではありません。しかし、クラウドに対する適切なビジョンと可視性があれば、事業を順調に進めることができます。許可されたユーザーの利用方法をビジョンとして明確に理解し、それ以外の行動を監視・測定することで、攻撃者の振る舞いを特定し、見えるようにするという可視性が必要です。クラウドがセキュリティに関する私たちの常識を変え続ける中、適切なデータと実用的なAIがクラウドに明確さをもたらすのです。

クラウドがセキュリティに関する私たちの常識を変え続ける中、適切なデータと実用的なAIがクラウドに明確さをもたらすのです。

*本レポートは、Vectra AI社の2021年第2四半期 スポットライトレポート「ビジョンと可視性：Microsoft Azure ADとOffice 365の脅威検知トップ10」において収集した調査に基づく洞察となります。

ハイライト

- **脅威検知のトップ10**：金融サービス機関におけるMicrosoft Azure ADおよびOffice 365での異常、または安全でない活動は何か？
- **不審かつ高リスクな活動**：不審なダウンロードやOffice 365の高リスク操作が多く見られており、このような場合、攻撃者が機密情報にアクセスしている可能性があります。
- **ギャップ（死角）の解消**：人工知能（AI）は、クラウド環境で真に何が起こっているかを知るために必要なビジョンと可視性を提供できます。

金融サービス機関におけるCognito NetworkとCloud Detection Platformから得られた観察結果に基づき行った分析によって、Microsoft Azure ADとOffice 365で見られる脅威が明らかになりました。この情報の詳細は、Vectra AI社の2021年第2四半期 スポットライトレポート「ビジョンと可視性：Microsoft Azure ADとOffice 365の脅威検知トップ10」で紹介しています。

金融サービス機関全般で検知された脅威

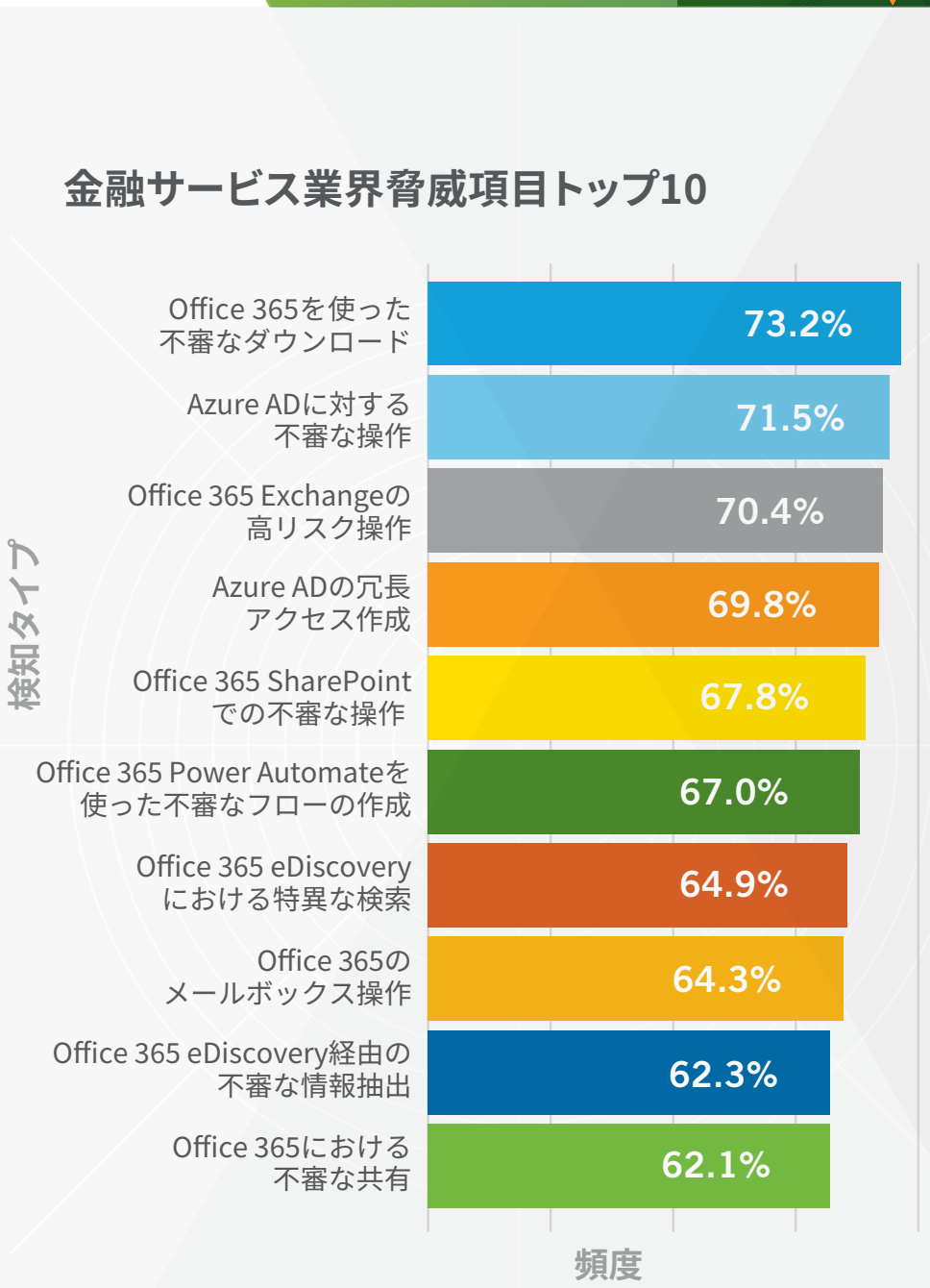
ここでは、金融サービス機関のお客様を対象とした上位の検知結果に焦点を当てていますが、明らかに悪質な攻撃行動は簡単に検知できるということが大前提です。そのため、現代のネットワーク防衛においてきわめて重要なのは、攻撃者がその目的を遂行するために取っている行動と、許可されたユーザーによる日常的な振る舞いを正しく区別することです。このレポートで取り上げられている検知の多くは、異常な動作を示しているものの、すべてが悪意のある活動によるものではありません。頻繁に検知されている内容の詳細を見てみましょう。

どんなリスクがあるのか？

結果：金融サービス機関では、「Office 365 Exchangeの高リスク操作」と「Azure ADの冗長アクセス作成」が多く検知されています。

分析: 「Office 365 Exchangeの高リスク操作」が検知されているという結果は、電子メールを介して機密情報へアクセスが行われていることを示しています。これは、攻撃者がExchangeを操作してデータにアクセスし、さらに攻撃を進めようとしていることも考えられます。この場合のリスクは、攻撃者がバックドアを作成したり、永続的にアクセスできる方法を確立できることです。一方、「Azure ADの冗長アクセス作成」は、アカウントの乗っ取り後に攻撃者が特権を拡大し、管理者レベルの操作を行っている可能性があります。

金融サービス業界のトップ10に含まれるその他の脅威結果は、「Office 365を使った不審なダウンロード」、「Office 365 Power Automateを使った不審なフローの作成」、「Office 365 eDiscovery経由の不審な情報抽出」となりました。これらの動きは、データが環境外に移動している可能を示しています。攻撃者が、SharePointやOneDriveを使ってデータをダウンロードして流出させていることも、Power Automateのフロー作成が示すような永続化な方法が構築されていることも考えられます。どちらにせよ、セキュリティチームは把握する必要があります。



金融サービス業界では、組織にスピードと効率をもたらす方法として、クラウド技術の導入が進んでいます。これにより、外部の組織とのデータの共有やコラボレーションがさらに進む可能性があります。今回検知された脅威は、現段階において、攻撃者がどのような方法で情報を見つけ抽出するのか、さらに、組織内に入り込んだ上でさらにどのような行動を起こすのかを示しています。すべてのお客様は、定期的にセキュリティ管理の見直しを行うべきです。そして、データの取得や損失につながる可能性のある異常な活動を検知できる調査プロセスが、自社のセキュリティプログラムに入っているかを確認する必要があります。

自社のアカウントにおける振る舞いを知る

新たな技術的ソリューションを取り入れているのは、金融サービス業界だけではありません。今後は、どのようなセキュリティツールを使い、攻撃者に対抗するのかというのが企業としての課題となります。厳格な規制と侵入テストの実施により、金融機関は一般的に攻撃から保護されていますが、だからといってサイバー攻撃者を過小評価してはいけません。攻撃者は狡猾で、ブロックされていない場所に隠れる方法を見つけ出すため、企業は通常とは異なる行動を検知することが、今まで以上に重要になります。攻撃者の振る舞いと許可されたアカウントの使用を区別するには、定義されたビジョンと可視性に沿った適切なデータ収集ができていなければ、曖昧な領域となってしまうのです。

実用的なAIは、Azure ADとOffice 365アカウントのギャップ（死角）を解消し、通常とは異なることが起こったときに検知するための適切なデータを提供できます。怪しい添付ファイルがダウンロードされたり、転送されてきたり、共有されたりしたとき、あなたは気づくことができますか？どんな攻撃があり得るのか知っておいて損はないでしょう。

Vectra AIについて

Vectra AI社は、クラウドやデータセンターのワークロードからユーザー、IoTデバイスに至るまで幅広い範囲で発生する脅威の検知および対応サービスにおける世界的リーダーです。当社のCognitoプラットフォームは、AIを活用して収集・保存したネットワークメタデータに、既知および未知の脅威をリアルタイムで検知、ハンティング、調査するためのコンテキストを追加してデータを強化することで、検知および調査のプロセスをスピードアップします。Cognitoプラットフォームでは、重要なユースケースに対応するために4種類のアプリケーションを提供しています。Cognito Stream™は、セキュリティ情報が強化されたメタデータをデータレイクやSIEMに転送します。Cognito Recall™は、強化版メタデータの脅威情報を保存・調査するためのクラウドベースのアプリケーションです。Cognito Detect™はAIを活用し、隠れた攻撃や未知の攻撃行動を素早く特定し、優先度を決めスピードと共に対応します。Cognito Detect for Office365 and Azure AD™は、エンタープライズSaaSアプリケーションおよびMicrosoft 365エコシステムにおいて発生する攻撃を検知し、阻止します。詳細は、vectra.aiをご覧ください。

レポートを入手する

Vectra®のCognito® Detect for Office 365は、隠れたサイバー攻撃者の振る舞いを自動的に検知して対応することでインシデント調査を迅速化し、一歩先を行く脅威ハンティングを可能にします。

お問い合わせ：info-japan@vectra.ai　vectra.ai/jp