VECTRA
SECURITY THAT THINKS

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

目次

「通常と異なる挙動」を検知 3

脅威検知でわかること 3

検知された脅威項目トップ10 4

ビジョンと可視性 5

企業規模別のトップ10分析 9

攻撃対象領域をサプライチェーン攻撃に照らし合わせて検証 12

違いを見極める：正規アカウントによる振る舞いの徹底理解 15

Vectra® AI社は、サイバー攻撃をいち早く検知して阻止することで、ビジネスの安全性を担保します。

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。

71%

昨年1年間で、Microsoft Office 365ユーザーの71%が平均7件のアカウント乗っ取り被害にあっています*。

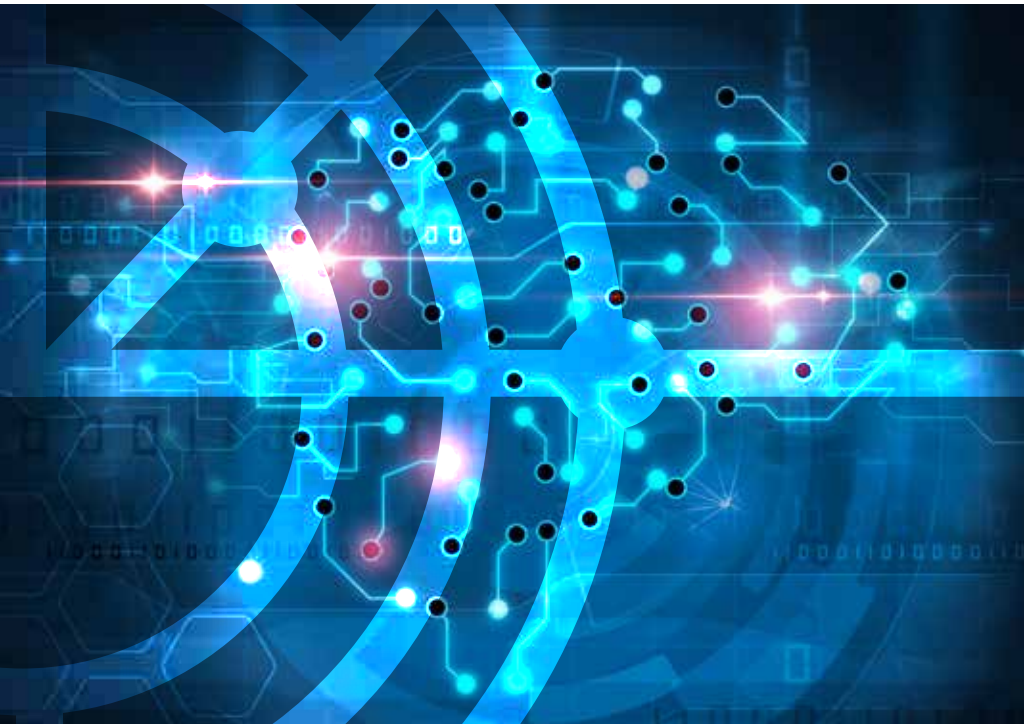
ハイライト

- 実用的なAIを駆使することで、ユーザーのクラウドアプリへのアクセス、使用および設定状況をコンスタントに分析できるだけでなく、アカウント乗っ取りなどの脅威を検知して阻止することができます。
- 普段発生しない異常または安全でない振る舞いの特定に役立つ「Microsoft Azure ADおよびOffice 365環境における脅威検知トップ10」をご紹介します。
- 企業の規模を問わず、当社のお客様全般で「Office 365 Exchangeの高リスク操作」がランキングのトップを占めました。
- 最近のサプライチェーン攻撃で確認されたAzure AD環境共通の攻撃活動を、当社独自の検知項目に照らし合わせて解説します。重点警戒領域としてご参照ください。

*出典：Securing Microsoft Office 365 in the new normal

「通常と異なる挙動」を検知

クラウドの普及によってセキュリティの常識が一変し、資産保護に関する従来型アプローチは時代遅れになっています。しかし、実用的な人工知能(AI)を使って適切なデータを収集することで、ネットワークに出入りする攻撃者の状況をピンポイントで把握できるため、セキュリティ担当チームは無害なアラートに貴重な業務時間を取られることなく、注意を要する脅威の対応に集中できます。このレポートでは、攻撃の実態把握にお役立ていただけるよう、当社のお客様全般で検知されたMicrosoft Azure ADおよびOffice 365に関する脅威のトップ10項目について解説します。ご紹介するデータはすべて、通常とは異なる挙動を検知した際にお客様のセキュリティ部門に通知する脅威の実例です。



脅威検知でわかること

このレポートでは、当社のお客様全般で見られるOffice 365とAzure ADの脅威検知項目トップ10を相対頻度にもとづいてご紹介しますが、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。しかし企業側のサービスやアクセス先に紛れ込み、不正使用や悪用できることに目を付けた攻撃者は、あからさまな行動を取らなくなっています。これが現代のネットワーク防御における残念な現実です。

したがって、エンタープライズ環境全体に存在し得る数々の類似行動パターン（共通点）の中から、攻撃者がその目的を遂行するために取っている行動と、正規の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がきわめて重要になります。判断に迷う場合は、「意図、コンテキスト、権限」の3要素をもとに無害なユーザーによる内部脅威と攻撃者による脅威を識別します。クラウドアプリのアクセス、使用および設定に関するユーザーの状況を、実用的なAI機能でコンスタントに分析して洞察とナレッジを取得すると同時に、自社ホスト、アカウント、ワークロードへのアクセス状況を把握することで、圧倒的に優れた防御対策を実現できます。

攻撃者による脅威と無害なユーザーによる内部脅威を識別するために重要な要素は「意図、コンテキスト、権限」です。

両者を識別できれば、「Office 365の不審なメール転送」の検出通知のような深刻な事象と、脅威に該当しない大量の通知、または、通知が1件もない状態との明確な違いを見極めることができます。アカウント乗っ取りなどの脅威により、企業が年間何十億ドルもの損失を被る今、セキュリティのリスクはこれまで以上に高まっています。しかし、攻撃戦術として用いられる振る舞いはすべて、AIを使ってあぶり出すことができます。では、検知された脅威項目トップ10を詳しく見ていきましょう。

検知された脅威項目トップ10

ご紹介する検知内容の多くはあくまでも異常な振る舞いであり、すべてが悪質な活動に起因するものではありません。また、対象環境では通常発生しない異常な振る舞い、ポリシー違反と見なされる振る舞いなどが混在しています。様々な活動にまたがる検知内容を見ると、企業がカバーすべき攻撃対象領域は広範囲に及ぶことがわかります。調査結果の科学的根拠については、ホワイトペーパー「The Data Science Behind Vectra AI Threat Detection Models」をご参照ください。

様々な活動にまたがる検知内容を見ると、企業がカバーすべき攻撃対象領域は広範囲に及ぶことがわかります。

ビジョンと可視性：攻撃側と防御側に共通する振る舞い

ビジョン：

規範となるポリシーなどをもとに「何が許可されているのか」を明文化しておかないと、表面上の脅威以外にまで目を配ることは困難です。そのため、自社のクラウドサービスにおいてどのような使用形態が許可されているのかを、**ビジョン**として（通常は、ポリシー形式で）明文化する必要があります。

その際、以下を考慮する必要があります。

- 許可されるサービスと振る舞いの種類
- 許可の対象となるコンテキストの種類
- ユーザーによるクラウドストレージの使用可否および、外部エンティティとの通信方法
- クラウドサービス上での振る舞いに対して適用すべき監視パラメータと保護策の種類

自社のクラウドサービスにおいてどのような使用形態が許可されているのかを、**ビジョン**として明文化する必要があります。

可視性：

組織として明確なビジョンがあっても、**可視性**が確保できなければビジョンの順守状況を監視したり逸脱度合いを測定できないため、たちまち問題が生じます。この課題を解決するには、攻撃者が取りそうな振る舞いを理解し、それらを集中的にあぶり出すためのデータをセキュリティ対応業務に役立つ形で収集し、蓄積する必要があります。

明確なビジョンがあっても**可視性**が確保できなければ、たちまち問題が生じます。

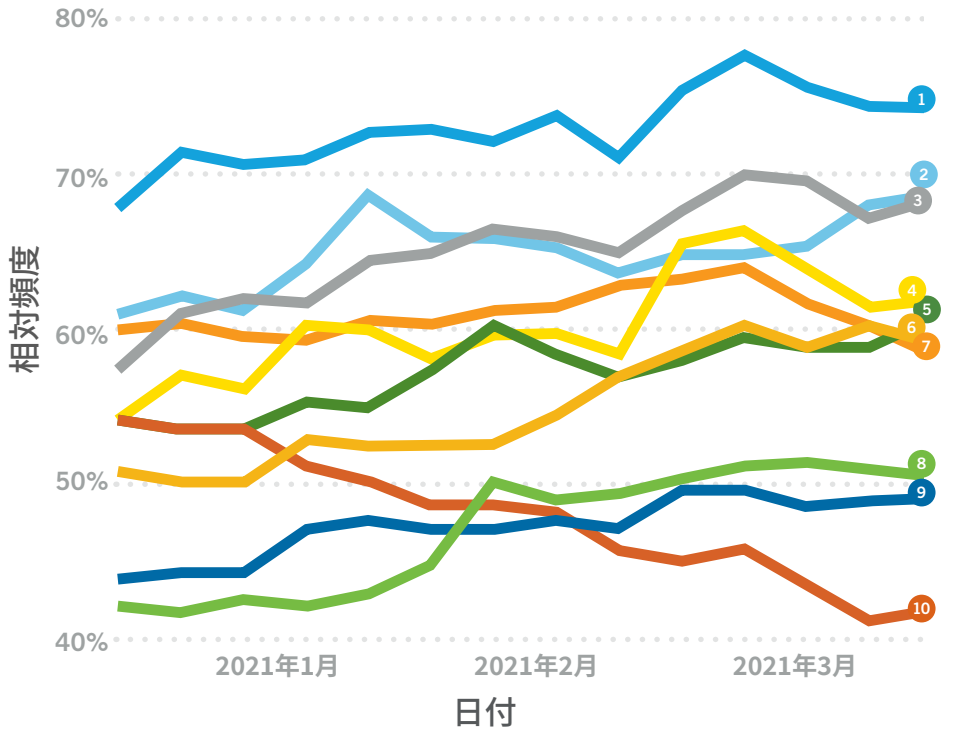
可視性をさらに高める

- **サービス：**保護機能が搭載されているPower Automateなどであっても、C&C（コマンド&コントロール）への経路として悪用される恐れがあります。セキュリティ担当者は、企業のクラウドサービスで実行されるこうした悪質攻撃を検知できますか？
- **管理：**管理者機能や管理機能が不正使用、悪用されると、攻撃者や内部ユーザーによる権限昇格や機密情報の収集・窃取につながる恐れがあります。セキュリティ担当者はこうした状況（Exchangeの高リスク操作など）を特定できますか？
- **サプライチェーン：**信頼できるサプライヤーおよびサービスプロバイダーの環境が侵害を受け、攻撃者が当該企業のセキュリティ統制（保護/防御策）を迂回して足場を固めている可能性もあります。セキュリティ担当者は、こうした状況を発見できますか？

セキュリティ責任者としてこれらの質問に自信をもって「YES」と答えるためには、単なるコンプライアンスチェックやベンチマーク以上の対策が必要です。積極的な調査、脅威ハンティング、セキュリティテストの演習を通じてセキュリティ部門の実践力を高めていくことが理想的です。

検知された脅威の相対頻度別トップ10

このグラフは、当社のお客様全般で検知された脅威の上位10項目を、相対的な発生頻度別に時系列で表したものです（検知がトリガーされたお客様の割合を1週間単位で算出）。



検知項目

- 1 Office 365 Exchangeの高リスク操作
- 2 Azure ADに対する不審な操作
- 3 Office 365を使った不審なダウンロード
- 4 Office 365における不審な共有
- 5 Azure ADの冗長アクセス作成
- 6 Office 365 Teamsへの外部アクセス
- 7 Office 365 Power Automateを使った不審なフローの作成
- 8 Office 365における不審なメール転送
- 9 Office 365 eDiscoveryにおける特異な検索
- 10 Office 365 SharePointでの不審な操作

検知された脅威項目トップ10

1. **Office 365 Exchangeの高リスク操作**
   Exchangeの異常な操作を検知。攻撃者がExchangeを操作し、特定のデータへのアクセスを試みている、または攻撃をさらに進めている疑いがある。
2. **Azure ADに対する不審な操作**
   Azure ADの異常な操作を検知。通常のアカウント乗っ取りに成功した攻撃者が権限を昇格させ、管理者レベルの操作を実行している疑いがある。
3. **Office 365を使った不審なダウンロード**
   異常な数のオブジェクトをダウンロードしているアカウントを確認。攻撃者がSharePointやOneDriveのダウンロード機能を使ってデータを窃取している疑いがある。
4. **Office 365における不審な共有**
   通常より多くのファイルやフォルダを共有しているアカウントを確認。初期アクセスを確立した攻撃者がSharePointを使ってデータを窃取している、またはアクセス状態を維持している疑いがある。
5. **Azure ADの冗長アクセス作成**
   管理者特権が付与されたエンティティを確認。攻撃者が修復措置を迂回するために、冗長アクセスを作成している疑いがある。
6. **Office 365 Teamsへの外部アクセス**
   Teamsのチームに外部アカウントが追加されている。攻撃者が所有するアカウントが追加された疑いがある。
7. **Office 365 Power Automateを使った不審なフローの作成**
   通常では考えられないPower Automateフローが作成されている。攻撃者が永続的アクセスを確立している疑いがある。
8. **Office 365における不審なメール転送**
   永続的アクセス不要の情報収集や窃取経路としてメール転送が使用されている疑いがある。
9. **Office 365 eDiscoveryにおける特異な検索**
   eDiscoveryの検索内容を作成、更新しているユーザーを確認。攻撃者がeDiscovery機能にアクセスし、偵察活動を行っている疑いがある。
10. **Office 365 SharePointでの不審な操作**
    通常では考えられないSharePoint管理者ユーザーの操作を検知。悪質な活動の疑いがある。

便利なコラボレーション機能の裏側

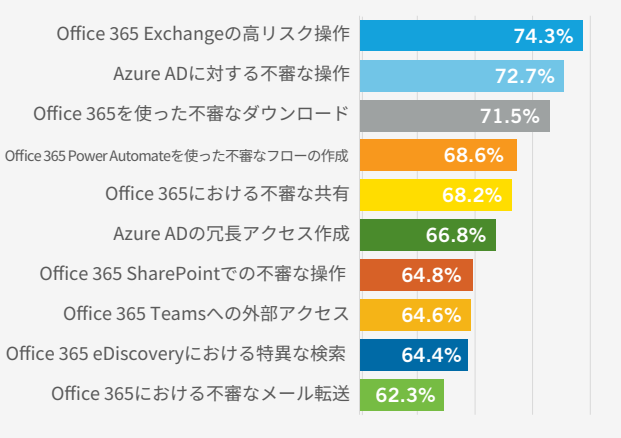
このようにMicrosoft環境で検知された脅威の多くは、使いやすさや外部連携機能、Azure AD環境への管理者アクセス権付与などに関する内容です。ドキュメントを簡単に共有できるOneDriveやSharePointは外部関係者との情報共有に便利なサービスですが、保存中および転送中の情報は攻撃者からもアクセスされる恐れがあります。こうした状況で検知される脅威のほとんどが「Office 365を使った不審なダウンロード」、「Office 365 SharePointでの不審な操作」、「Office 365における不審な共有」です。

なかには、Microsoft Teams経由での外部ユーザーとの通信やコラボレーションがきっかけで検知される脅威もあります。こちらも正規ユーザーにとっては便利な機能ですが、攻撃者が有益な情報を探したり、ドキュメントや情報を入手する際にも便利な手段となってしまいます。そのため、「Office 365 Teamsへの外部アクセス」の検出通知が配信されることは珍しくありません。

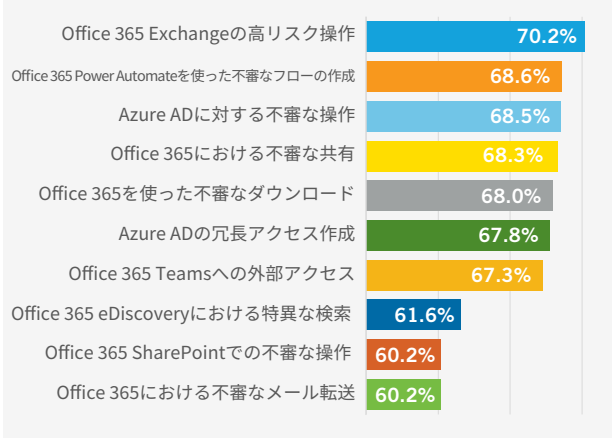
Microsoft環境で検知された脅威の多くは、使いやすさや外部連携機能、Azure AD環境への管理者アクセス権付与などに関する内容です。

企業規模別のトップ10分析

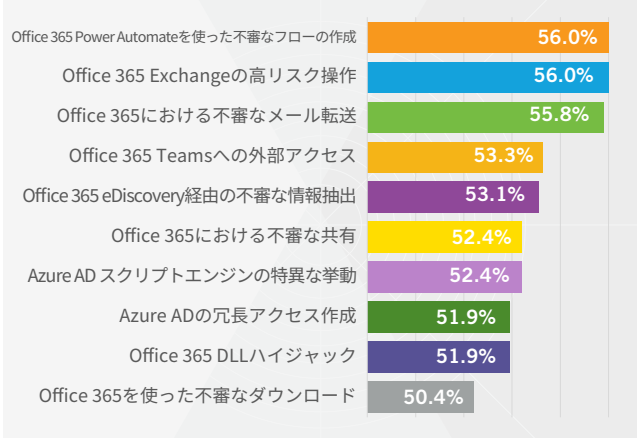
小規模企業における上位10項目



中規模企業における上位10項目



大企業における上位10項目



このグラフは、調査対象の3ヶ月間にトリガーされた脅威検知の相対頻度を、お客様の規模別に分類したものです。企業規模（大、中、小）別の上位10項目を見ると、企業規模が大きくなるにつれ、各項目で実際にトリガーされる脅威検知の割合が小さくなっています。つまり全般的な傾向として、大企業の社内ユーザーや管理者は、Office 365やAzure ADの操作を中小企業に比べて定常的に行っている、という可能性が示唆されます。当社による考察結果を次項で説明します。

企業規模が大きいほど、社内ユーザーや管理者によるOffice 365やAzure ADの操作頻度が高くなる傾向があります。

中規模企業と小規模企業における検知項目の類似性

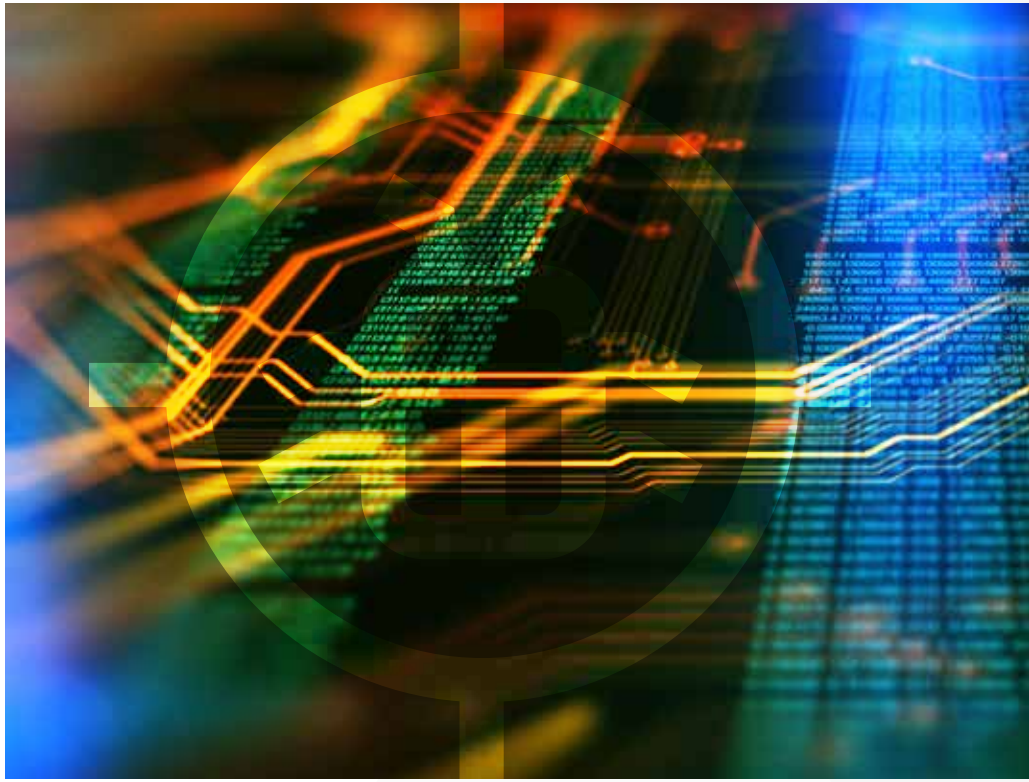
調査結果： 企業規模別トップ10の内訳を見ると、順位の入れ替わりはあるものの、中規模企業と小規模企業の検知項目は共通しています。大企業における上位10項目の内訳を見ると、中小企業のトップ10項目にはない「Office 365 DLLハイジャック」、「Office 365スクリプトエンジンの特異な挙動」、「Office 365 eDiscovery経由の不審な情報抽出」がランキングに入っています。中小企業では、大企業ではランク外だった「Office 365 SharePointの不審な操作」、「Office 365 eDiscoveryにおける特異な検索」、「Azure ADに対する不審な操作」がトップ10入りしています。

クラウド上にアプリケーションを保存していると、よく使う共有フォルダに悪質コードやDLLを挿入されたり改ざんされる恐れがあります。

考察結果： これを見ると、企業規模が大きいほどOneDriveやSharePointに保存されているアプリケーションにアクセスするユーザーが多くなることがわかります。クラウド上にアプリケーションを保存していると、よく使う共有フォルダに悪質コードやDLLを挿入されたり改ざんされる恐れがあります。クラウド上でよく使われるファイルタイプへのアクセス頻度が高まっても気づかれにくいため、攻撃者にとっては便利な手法となります。

侵害の検知

大企業では「Office 365 eDiscoveryでの不審な検索」ではなく「Office 365 eDiscovery経由の不審な情報抽出」がトップ10入りしています。このことから、大企業でeDiscoveryを使うユーザーの多くは、中小企業のユーザーに比べて恒常的にeDiscovery検索を行っており、検索したデータを頻繁に抽出していることがわかります。アカウントで検索結果がプレビューされたりエクスポートされる都度、「Office 365 eDiscovery経由の不審な情報抽出」の検知がトリガーされます。攻撃者がeDiscoveryにアクセスできれば、Office 365のコンポーネントすべてをほぼ自在に操れるため、情報が簡単に検索され入手されてしまいます。あるお客様の実例では、社内ネットワークに侵入した攻撃者が、SOCチームの対策状況を監視する目的でeDiscoveryを使っているケースもありました。当社がこの事実を突き止めていなければ、お客様はOffice 365のアカウントが侵害されたことを把握できず、たとえ最初の侵害が修復されたとしても同じ攻撃者に再び足場を確立されてしまっていたでしょう。



中規模企業と小規模企業の検知項目では「Azure ADに対する不審な操作」がそれぞれトップ3、トップ2に入りました。

中小企業の3大脅威に「Azure ADに対する不審な操作」がランクイン

調査結果： 中規模および小規模企業では「Azure ADに対する不審な操作」がそれぞれトップ3、トップ2に入りました。アカウントを乗っ取った攻撃者による権限昇格の可能性を含め、システム環境に何らかの変更が加えられたことを示す脅威です。

考察結果： 大企業では中小企業に比べて、より日常的にAzure ADの保守管理操作が実行されているためか、この項目はトップ10ランク外でした。つまり中小企業は、アラートの内容を注意深く検証し、異常な振る舞いが、アカウントの乗っ取りおよび権限昇格に続く管理者権限の悪用によるものではないことを徹底する必要があります。

脅威項目のトップは「Office 365 Exchangeの高リスク操作」

調査結果： 企業規模を問わず「Office 365 Exchangeの高リスク操作」が、ランキングのトップを占めました。

考察結果： 「Exchangeの高リスク操作」は、機密情報の収集、抽出からスクリプトの実行、バックドアの設置に至るまで、危惧すべき活動が発生したことを示す脅威です。最近の大規模サプライチェーン攻撃でわかるとおり、攻撃者は組織内外でやり取りされるメールを常にチェックし、機密情報にアクセスする機会を虎視眈々と狙っています。この項目の検知は、「当該アカウントでは通常考えられない活動」が発生したことを意味します。発生頻度の低い作業を管理者が実行している可能性もありますが、攻撃者がデータを入手したり次の段階に進むためにOffice 365テナントのExchangeを操作している恐れもあります。

攻撃対象領域をサプライチェーン攻撃に照らし合わせて検証

ここからは、最近発生したサプライチェーン攻撃におけるAzure AD環境共通の攻撃活動（報告ベース）を、当社独自の脅威検知項目に照らし合わせて詳しく見ていきましょう。実際の攻撃者は、汎用的なベンダー製品へのアクセス権を使って多くの組織の社内LANに侵入しました。

サプライチェーン攻撃では、ネットワーク・サンドボックス、エンドポイント、多要素認証(MFA) をはじめとする防御統制の網をすり抜けるために、攻撃者が多大な労力をかけ、高度なスキルを発揮したことが証明されました。以下は、実際に用いられた攻撃手法の一例です。

- 侵入対象の環境を充分下調べし、企業側のサンドボックスやマルウェア分析環境ではないことを徹底確認
- コードサイニング証明書および正規のプロセスを使用し、一般的なエンドポイントコントロール対策を回避
- インメモリードロッパーと呼ばれる斬新な手法を使い、ファイルベースの攻撃分析に検知されずにC2ビーコンを配信
- セキュリティ アサーション マークアップ言語 (SAML) のセッション署名キーの窃取による多要素認証バイパス

エンドポイントの検知と対応 (EDR) ソリューションは近年進化しています。足跡を残さずにEDRを迂回するには、並々ならぬ執着心と卓越したスキルを要したことでしょう。しかし今回の攻撃によって、強い決意と巧妙な手腕をもった攻撃者であればエンドポイントコントロールや防御策を難なく迂回できてしまう、ということも改めて浮き彫りになりました。

サプライチェーン攻撃では、ネットワーク・サンドボックス、エンドポイント、多要素認証(MFA) をはじめとする防御統制の網をすり抜けるために、攻撃者が多大な労力をかけ、高度なスキルを発揮したことが証明されました。

サプライチェーン攻撃について：こちらの動画で最近の侵害事例を詳しく解説しています。今すぐ視聴する

サプライチェーン攻撃の流れ

今回のサプライチェーン攻撃では、企業側の防御策が手薄な攻撃対象領域が標的となりました。

サプライチェーン攻撃 / SolarFlare拡散におけるネットワークからクラウドへの侵入経路

1

SolarWinds製品のバックドア(Sunburst)を使用

- DNS応答を介してC2への初期接続を確立
- Cobalt Strikeのダウンロードにより、C2への接続経路を確保

2

ドメイン管理者権限の取得

- ネットワークを偵察し、ドメイン認証情報を物色
- 認証情報を使ってSolarWinds製品内部を横移動

3

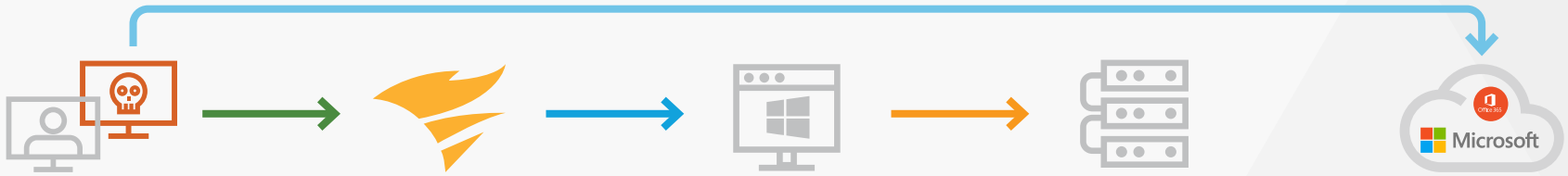
SAMLサイニング証明書の窃取

- ドメイン管理者権限を使ってADFSの認証を突破

4

Azure ADとMicrosoft Office 365にアクセス

- 偽造トークンでAzure ADの管理者アクセス権を取得
- 設定と承認を変更し、永続的アクセスを確立
- ネイティブツールを使って電子メールにアクセス



ステップ3（偽造トークンを使ったMicrosoft Azure ADと Office 365へのアクセス）に関する考察

攻撃者は多くの場合、主にビジネスメールやドキュメントにアクセスするために偽のアクセス権を利用し、標的組織のクラウドテナント内部に侵入していました。オンプレミスからクラウドへの移動は、これまで観測されてきた典型的な攻撃活動とは逆の動きです。今回の攻撃でも、社内LANを標的にした攻撃パターンと同様、コマンド&コントロール、ラテラルムーブメント（横移動）、情報窃取のいずれかを目的としたものと思われる複数の攻撃活動が確認されました。

今回の攻撃者が最初に取った行動のひとつが認証インフラの侵害もしくは改変でした。これによりSAMLトークンを偽造し、MFAをはじめとするセキュリティ対策の仕組みを迂回しながらAzure ADとOffice 365の環境に侵入できます。

偽造トークンでサインインすると、当社の検知サービスで「**Azure ADの不審なサインオン**」（C2カテゴリーの脅威）がトリガーされます。これにより、アカウントで通常発生するパターンとは明らかに異なるログインが発生したことを通知し、警戒を促します。この項目は、前述の総合トップ10リストには入っていませんでした。

このことから、大半のお客様では、社内Microsoft環境への異常なアクセスは頻発しておらず、もし検知された際は充分な精査が必要であることがわかります。最後の教訓は「単にデータを収集するだけではなく、そのコンテキストを推論できなければ真の可視化とは言えない」ということです。疑わしいと同時に攻撃者にとって好都合な振る舞いを理解しなければなりません。そのためには想定される振る舞いだけでなく、目の前で進行している攻撃の脅威モデルについても把握する必要があります。

ステップ3で考えられる別の攻撃手法：信頼情報の改変

認証インフラ突破の可能性としてもう1つ考えられる手口が、信頼関係の改変です。信頼関係を改変するには、必要な権限を備えたアカウントを侵害する、またはすでに侵害されたアカウントに権限を追加する必要があります。後者の場合、アカウントに管理者権限が追加されると、当社の検知サービスで「**Azure ADの冗長アクセス作成**」に関する検知（こちらもC2カテゴリーの脅威）がトリガーされます。特権アカウントを使って信頼関係の設定を改変すると、「**Azure ADに対する不審な操作**」（ラテラルムーブメントカテゴリーの脅威）に関する検知がトリガーされます。前述の調査結果を見ると、この検知項目は、企業規模を問わず当社のお客様全般で検知された脅威のトップ10に入っています。

> 報告されている手口を見ると、攻撃者の共通目的は「メールやドキュメントに含まれる情報の窃取」であったと考えられます。

ステップ4（メールの盗み見による情報窃取）に関する考察

報告されている手口を見ると、攻撃者の共通目的は「**メールやドキュメントに含まれる情報の窃取**」であったと考えられます。情報を窃取するには、アクセス確立後、さらなる活動（ラテラルムーブメントに相当する活動）が必要です。攻撃者は、侵害されたアカウントの認証情報を既存のアプリケーションまたはサービスプリンシパルに頻繁に追加していた、とされています。この行動が発生すると、前述の「**Azure ADに対する不審な操作**」に関する検知がトリガーされます。

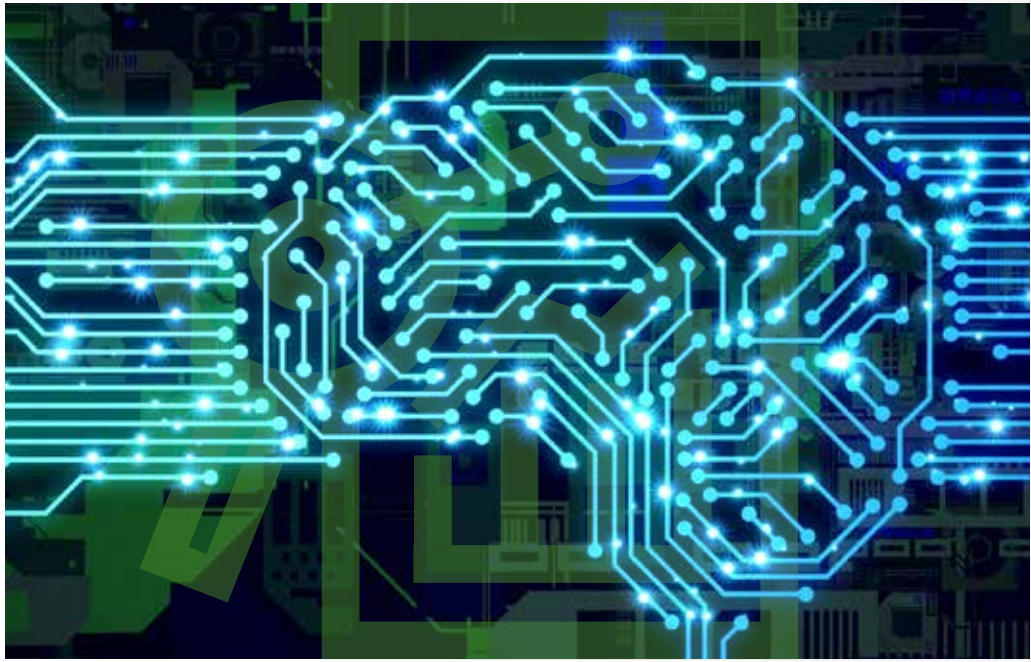
攻撃者が新たなアプリケーションやサービスプリンシパルを追加し、任意のアプリケーションに承認を付加することもあります。その場合は「**Azure ADでの不審なOAuthアプリケーション**」に関する検知がトリガーされます。サプライチェーン攻撃の最終段階を見ると、企業として想定されるもしくは許可されているAzure AD関連の改変操作、および不正な改変操作に関する明確なビジョンを確立し、ここに挙げた2つの攻撃対象領域に対しても注意・警戒を怠ってはならないことがわかります。

違いを見極める：「正規」アカウントによる振る舞いの徹底理解

攻撃者の振る舞いと社内の特権アカウント利用者の振る舞いは、一見すると似通っています。この違いを認識できないと前述のような攻撃シナリオの標的となり、実際、これまで数々の企業が被害にあってきました。同様の理由で、組織の30%が毎月、アカウント乗っ取り被害にあっています。前述のとおり、明確な敵意を持った攻撃者は、防御策やエンドポイントコントロールを迂回する方法を何とかして見つけ出します。つまり「ビジョンと可視性を整備する」という基本に立ち返り、許可された使用にもとづく振る舞いと、攻撃者が取るであろう振る舞いの違いを見極める必要があります。しかし、難しく考える必要はありません。

実用的なAIを駆使することで、Azure ADとOffice 365のアカウントにおける可視性ギャップ（死角）を埋め、適切なデータをもとに普段と異なる振る舞いを検知できます。ご紹介した脅威検知のトップ10項目および、その意味合いについて今一度振り返ってみてください。クラウド環境で発生する怪しい添付ファイルのダウンロードや転送動作、または危険もしくは不審な操作を把握できていますか？もしそうでない場合は、可視化することをお勧めします。

Cognito Detect for Office 365は、皆様のOffice 365およびAzure AD環境で、通常と異なる挙動を検知します。ぜひ詳細をご確認ください。



実用的なAIを駆使することで、Azure ADとOffice 365のアカウントにおける可視性ギャップ（死角）を埋め、適切なデータをもとに普段と異なる振る舞いを検知できます。

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