VECTRA AI, INC.

Security that thinks®

攻撃者の振る舞いに関する業界レポート

VECTRA AI, INC.
Security that thinks®

目次

データセットと統計情報. 3

運用の効率とROI. 5

スコアリング. 7

1万デバイスあたりの脅威のタイプ. 8

1万デバイスあたりの業界別脅威. 11

まとめ. 16

Vectra® AI社が公開した「攻撃者の振る舞いに関する業界レポート」は、Vectra AI社のお客様の企業ネットワークで発生した、アクティブかつ持続的な攻撃者の振る舞いに関する分析結果を報告するものです。

本レポートでは、9つの業界で毎月500万を超えるホストをサポートするVectra Cognito®が取り扱う、350社のサンプルから検知した、様々なサイバー攻撃やその傾向を検証しました。検証にあたっては、攻撃ライフサイクルにおける全ての戦略フェーズを網羅した、学術的なアプローチを採用しています。

数多くの脅威調査レポートが存在しますが、本レポートでは、クラウド環境やデータセンター、そして企業ネットワークにおいて検知された、実際のサイバー攻撃者の振る舞いに関する優れたインサイトを提供します。

セキュリティ業界のレポートは、エクスプロイトや一連のマルウェアといった、既知の脅威に関する統計内容に焦点を当てたり、実際に発生した侵害行為に関する事後的な分析結果を提供しているものがほとんどです。しかし、この「攻撃者の振る舞いに関する業界レポート」では、攻撃ライフサイクルにおける全ての戦略フェーズを網羅した、学術的なアプローチを採用しています。さらに、本レポートでは、業界別のデータを提供することで、業界による違いを浮き彫りにしています。

データセットと統計情報

本レポートで使用するデータは、検知メトリクスの共有に同意した、350社のVectra Cognito導入企業から得られた、匿名化されたネットワークメタデータに基づいたものとなります。Cognitoプラットフォームは、インターネット上でやり取りされるトラフィックや、ネットワークデバイス間のトラフィック、プライベートデータセンターやパブリッククラウドの仮想ワークロードなど、全てのネットワークトラフィックや関連するログを直接監視して、攻撃の疑いがある振る舞いを特定します。

このような分析によって、高度な攻撃フェーズに関する可視性を提供することができます。Cognitoプラットフォームは、境界防御をすり抜けた脅威を検知し、最初の侵害が発生してからの、攻撃の進行状況を観測します。

観測結果

- 2019年7月から12月の6ヶ月間に、全業界の1万台のホストで、平均215件の攻撃者の振る舞いが検知され、その中では、2019年7月の252件が最大となっています。
- コマンド&コントロールの振る舞いが最も多く見られたのは、テクノロジー（1万台あたり138件検知）および教育機関（1万台あたり102件検知）でした。その他については、1万台あたりわずか39件の検知に止まっています。
- TORは、正当なビジネス上の目的にはほとんど用いられないため、どんな企業でも、TORのトラフィックが大量に発生することは稀です。全業界を通じて、ホスト1万台あたりのTOR検知数の平均は3件でした。12月には、ホスト1万台あたりの検知数が19件に跳ね上がりましたが、これはアジア太平洋地域のテクノロジー企業に起因したものでした。
- 金融・保険では、ホスト1万台あたり29件のポートスキャンが検知されましたが、全業界平均では11件となっています。
- 内部偵察行為の検知数が最も低かったのは、政府機関であり、ホスト1万台あたりで32件でした。一方、金融・保険ではホスト1万台あたり最高の93件となっています。
- 7月には、ユーザーのパスワード解読を目的としたファイルサーバー（SMB）に対する総当たり攻撃（brute force）が、ホスト1万台あたり、年間最高となる22回観測されました。残りの期間（8月～12月）のSMB総当たり攻撃は、ホスト1万台あたり14回観測されました。
- 小規模企業（従業員1～3,000名）は、ラテラルムーブメント攻撃を受けるリスクが高くなっています。小規模企業では、ホスト1万台あたり112件のラテラルムーブメント攻撃が観測され、中規模・大規模企業では64件となっています。
- Vectra AI社のお客様は、検知やトリアージ、さらにセキュリティインシデントとホストの関連付けや、優先順位付けなどの自動化を図り、Tier-1のアナリストの負担を38分の1にまで軽減すると共に、セキュリティの運用担当チームが、最もリスクの高い侵害を受けたホストへの対応に集中できるようにしています。

本レポートで使用する主な用語

本レポートでは、可能な限り標準的な用語を使用していますが、一部にはあまり明確でない、または一般には受け入れられていない用語もあります。そのような場合には、Vectra Cognitoプラットフォームでのデータ記述方法に合致した用語を使用します。以下で、これらの用語について説明します。

観測ホスト－様々な特性に基づきホストに対応する一意のインスタンスです。Cognitoでは、各ホストに対する一意のIDを生成することで、IPアドレスに依存することなくホストを特定しトラッキングを行うことができます。ホストは、物理的なデバイスである場合も、仮想またはクラウドのワークロードである場合もあります。

フラグイベント － 検知対象となる個々のアラートを指します。イベントは、単一のポートスキャンやリモート接続アクティビティなど、発生した特定の振る舞いに対応するインスタンスです。

検知 － 攻撃者に特定の振る舞いを誘発させる、1つのインスタンスに対応したイベントの相関関係を指します。検知は、機械学習アルゴリズムモデルをベースに実施され、使用したモデルに従ってラベル付けが行われます。

検知発生ホスト － 全ての検知イベントは、脅威の振る舞いに関する兆候を示す、特定のホストに紐付けられます。各ホストは、攻撃ライフサイクルの複数フェーズにおける、攻撃者の振る舞いに関連した検知結果も合わせた形でスコアリングされます。

この「攻撃者の振る舞いに関する業界レポート」では、業界別のデータを提供することで、業界による違いを浮き彫りにしています。

図1および図2は、本分析の対象となった企業の統計情報を示したものです。図1は、全業界の中で対象業界が占める企業数の割合と、6ヶ月間に検知されたフラグイベントの合計数という、2つの視点で構成したものです。

図2は、分析対象となる小規模、中規模、大規模企業の割合を示したものです。企業の規模については、容易に判断することが可能なため、従業員数に基づき分類を行っています。(大規模 = 25,001名以上、中規模 = 5,001～25,000名、小規模 = 0～5,000名)

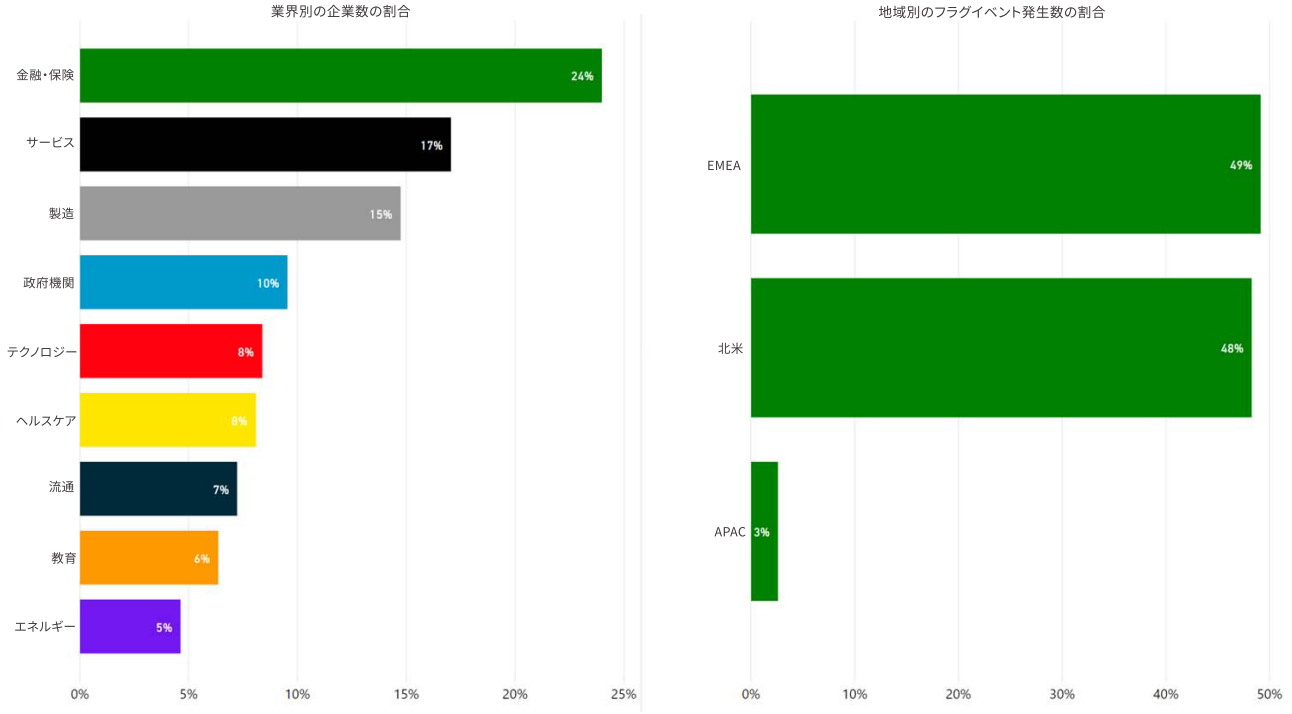


図1：業界別の企業数の割合と地域別のフラグイベント発生数の割合

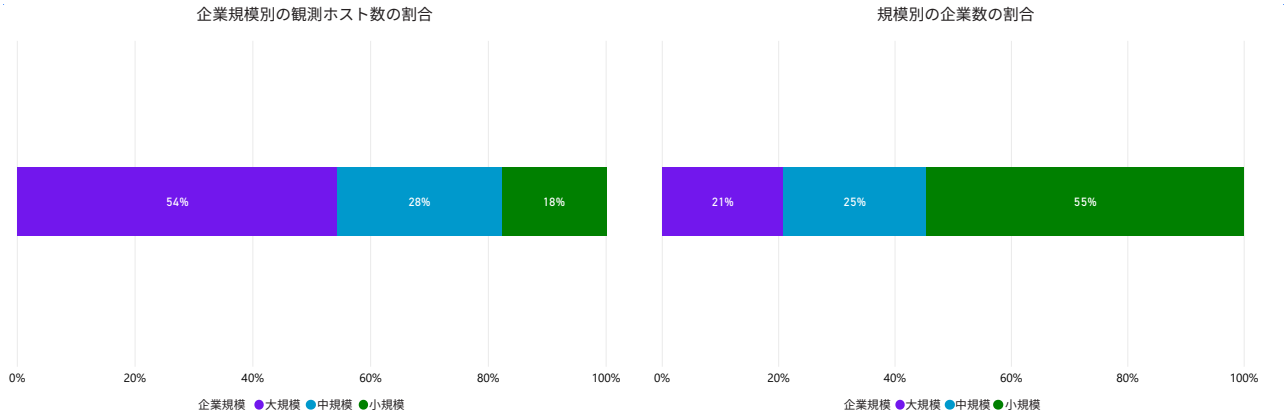


図2：企業規模による特性

運用の効率とROI

サイバーセキュリティ対策は、運用効率の確保に向けた持続的な取り組みと言えます。リスク、脅威、そして攻撃者は無限に存在しますが、企業側には有限のリソースしか存在しません。このため、セキュリティ製品を評価する際には、常にその効率や企業の現状の運用に対する影響を、考慮に入れる必要があります。

ネットワーク侵害に対する検知は、時間との勝負になります。損害を軽減するためには、重要なアセットが盗難にあったり被害を受ける前に、攻撃をリアルタイムに検知する必要があります。従来、標的型攻撃の検知と対応は、非常に時間を要するプロセスであり、膨大な量のアラートを手作業で仕分けるためのセキュリティチームの存在が不可欠でした。

Vectra AI社が提供するCognito Detect™は、AIを駆使して、非常に高速に脅威の継続的な検知と優先付けを行います。このような攻撃者の振る舞いは、侵害を受けたデバイスと紐付けられ、さらに一般的な攻撃の対象や大規模な攻撃キャンペーンとも紐付けられます。数千に及ぶ脅威の兆候は、数10のデバイス上での攻撃者による数百の振る舞いにまで絞り込まれます。これらの脅威は、広範な攻撃キャンペーンの1つになり得ます。

分析対象となるネットワークの規模には大きなばらつきがあり、最小数100デバイス程度から、最大は40万以上のデバイスで構成されるネットワークに至るまで、様々な形態が存在します。

このような差異を考慮し、データについては、1万程度のデバイスとワークロードを持つネットワークを想定して平準化を行い、ネットワーク内の脅威の存在を均等かつ容易に比較できるようにしました。IoTデバイスやスマートフォン、タブレット、ラップトップなど、IPアドレスを持つデバイスについても、サーバーや仮想ワークロードと同様に監視対象となります。

図3は、2019年7月から12月の6ヶ月間における、業界別の検知件数で、ホスト1万台を想定して平準化したものになります。

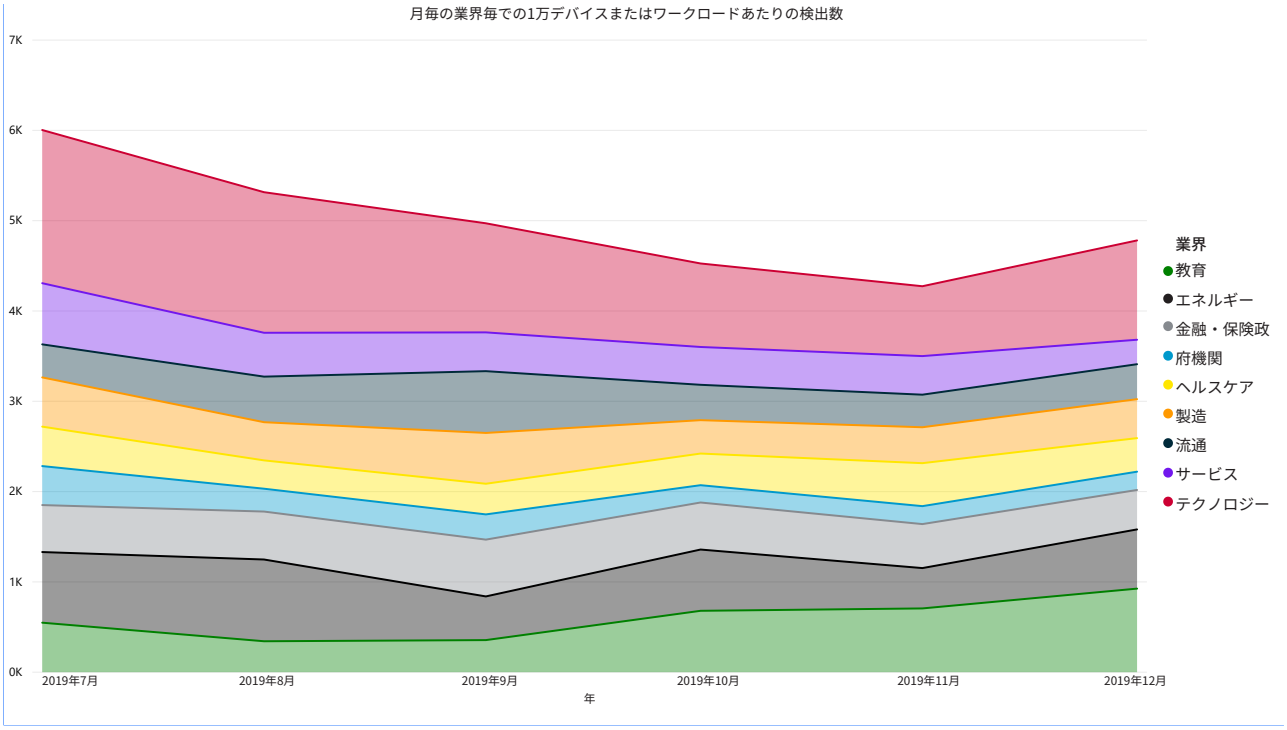
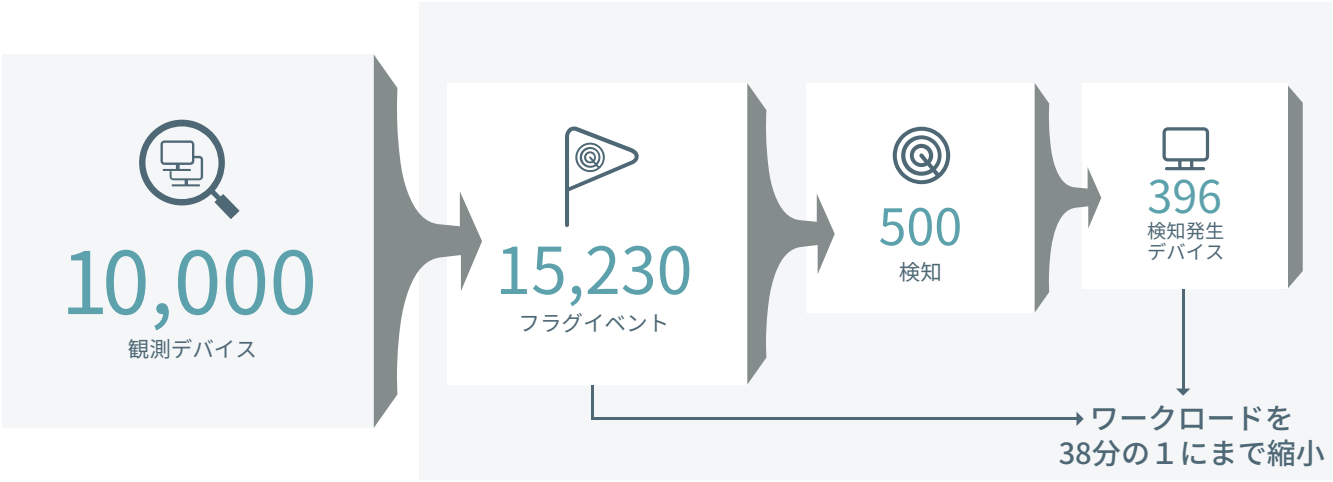


図3

手作業によって、全ての攻撃者の振る舞いや侵害を受けたホストデバイスを調査する場合に比べ、Cognitoでは、セキュリティ分析の対象となる調査のワークロードを38分の1にまで縮小することができます。

Tier-1セキュリティアナリストの作業負荷の削減



業界別の観測されたデバイス1万あたりのワークロードの削減効果

業界	認識したイベント	検知数	検知されたデバイス	極めて危険	高い危険性	ワークロードの削減効果
教育	12,666	617	650	11	34	19x
エネルギー	18,617	598	338	8	16	55x
金融・保険	19,510	511	361	8	20	54x
政府機関	9,328	249	268	6	12	35x
ヘルスケア	15,423	381	411	7	16	38x
製造	17,064	431	323	6	15	53x
小売	9,437	421	283	7	24	33x
サービス	14,679	430	365	12	20	40x
テクノロジー	18,100	1,193	634	12	23	29x

スコアリング

Vectra AI社が提供するCognitoは、各デバイスやワークロードを長期間にわたり監視し、不審な振る舞いのあったデバイスやワークロードと検出結果を紐付けします。検知スコアとそれが発生した時間は、ホストデバイススコアにおける重要な入力値となります。

Cognitoのスコアリングは、脅威スコア（threat score）と信頼度スコア（certainty score）という2つの動的な基準によって構成されています。これらは報告のあった個々の検知結果とホストに対して適用されます。

検知結果の脅威スコアは、セキュリティイベントが確かなもの（例えば、スパムやデータ流出が発生した場合など）であった場合、どの程度の損害を与える可能性があるかを示すものです。脅威スコアは、その損害の可能性で計測されるため、最悪のシナリオを反映するものとなっています。

検知結果の信頼度スコアには、それまで観測された証拠を基に、特定のセキュリティイベントが発生し得る確率が反映されます（例えば、スパムが発生する確率や、データ流出が発生する確率などです）。

信頼度は、実際に検知された脅威の振る舞いと、正常な振る舞いの差異に基づき決定されます。このため、個別に検知された結果に関する信頼度スコアは、時間と共に変化します。

検知結果は動的に変化するものであり、該当スコアの変動は、紐付けされたデバイスのスコアにも影響を与えます。また検知結果には、対象が大きな影響を及ぼす可能性のある振る舞いであることが、高い信頼性をもって表示されるため、セキュリティアナリストは、危険性の高いスコアを確認して調査の優先順位を決定することができます。

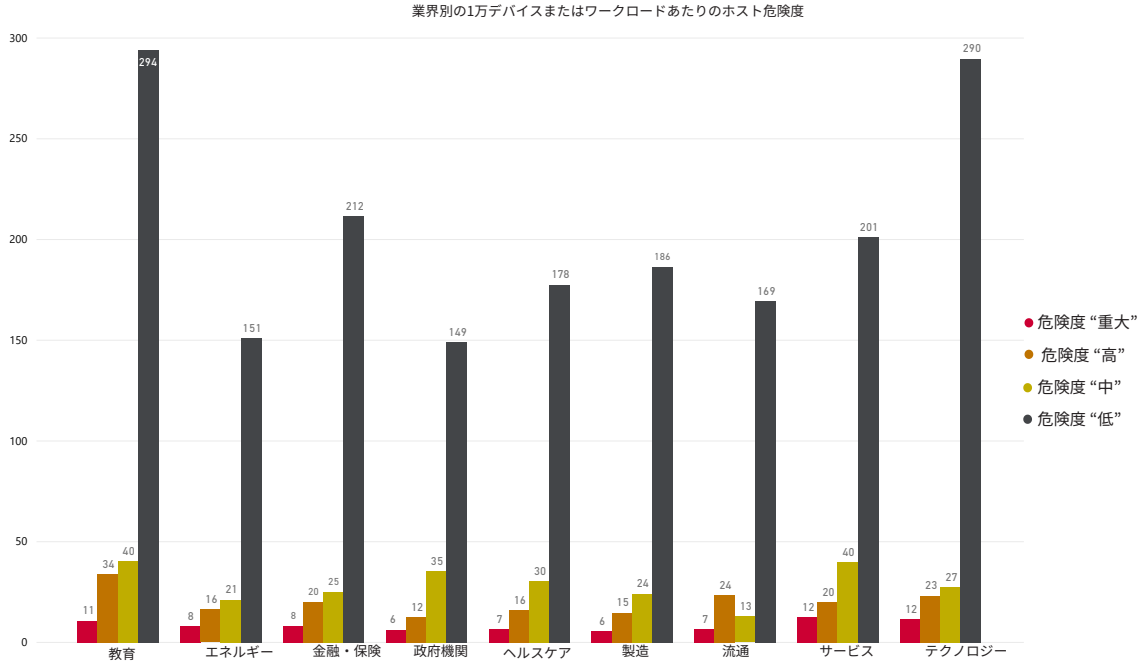
ホストデバイスのスコアに影響を与える他の要因としては、観測された検知結果の重複や、サイバー攻撃がその目的に向け、現在進行中であることを示す検知結果の組み合わせなどがあります。

全ての検知タイプには、数日から1ヶ月の存続期間があります。検知結果が繰り返し発生しない場合、ホストデバイスのスコアはゼロに向け減少していきます。検知結果は、存続期間が経過すると無効になり、ホストデバイスのスコアに影響を与えないようになります。

デバイスおよびワークロード 1万あたりの検知結果概要

平均すると、1ヶ月間監視した1万のデバイスおよびワークロードあたりのホストの危険度の最大値は、“重大”が8で、“高”が20でした。これらのデバイスやワークロードは、企業にとって大きな脅威となっていることが明らかであり、セキュリティアナリストによる迅速な対応が必要となります。

Vectra AI社は、ホストデバイスの危険度に関する統計を業界別に分類し、それぞれの業界と全体的な平均値に対する危険度別に、デバイスとワークロードの数を比較評価しました。



例えば、テクノロジーおよび高等教育機関における“低”の危険度の数は、通常の割合より50%高くなっています。これは、攻撃ライフサイクルの早い段階で、攻撃に関わる振る舞いが発生したことを表しています。しかし、このような状況は、必ずしもデータ盗難のような、より“重大”な攻撃のステップを示すものではありません。

対照的に政府機関の場合には、“高”または“重大”と判定されたホストの数は少なくなっていますが、これは攻撃のライフサイクル全般にわたって、振る舞いの進行度が低いことを示しています。

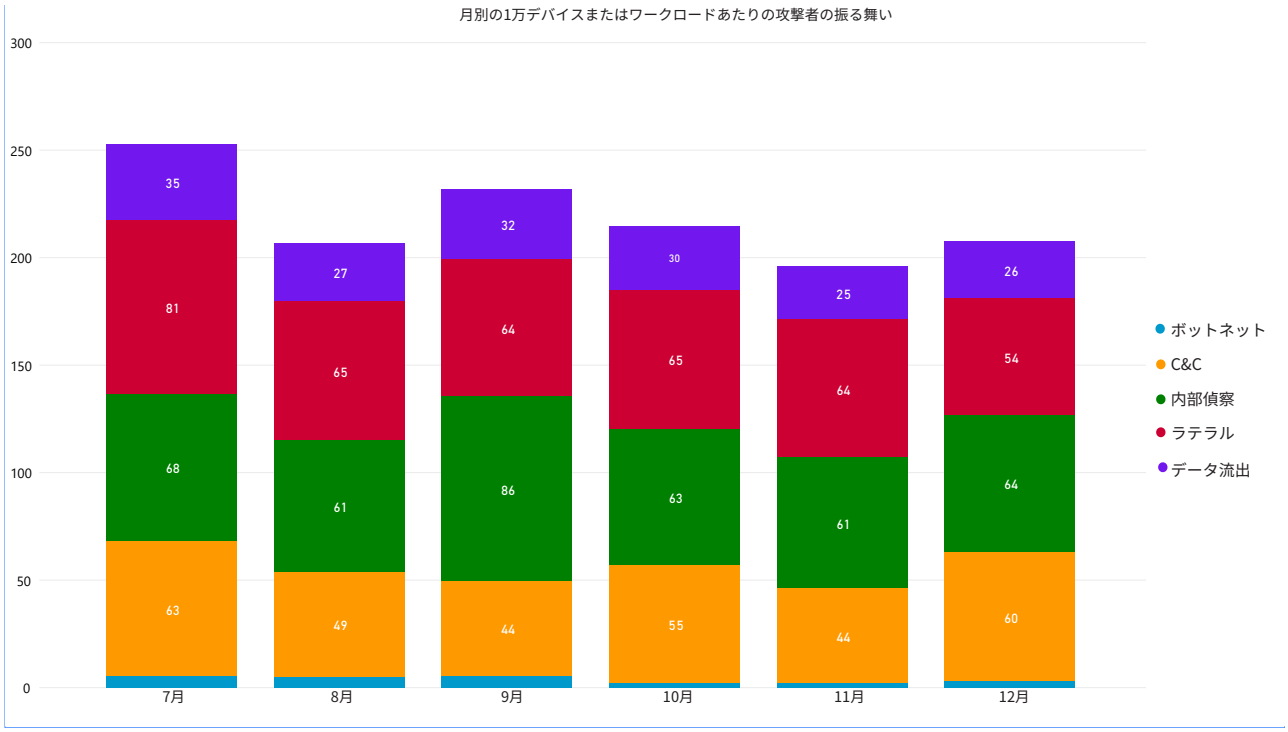
1万デバイスあたりの脅威タイプ

さらに詳細を把握するために、検知結果の統計内容を業界別に振り分けました。以下の図は、攻撃ライフサイクル全体での脅威の振る舞いを示しています。このような振る舞いは、企業におけるエクスポージャーやリスクに関する強力な指標となり、これによってセキュリティアナリストは、最も重要な対象に集中する形で時間を使えるようになります。

各攻撃が、全てのステップを踏むわけではありませんが、多くの場合、攻撃は相互に関連しながら段階的に進行し、最終的に金銭的な損失やデータの流出、データの破壊という結果に繋がります。

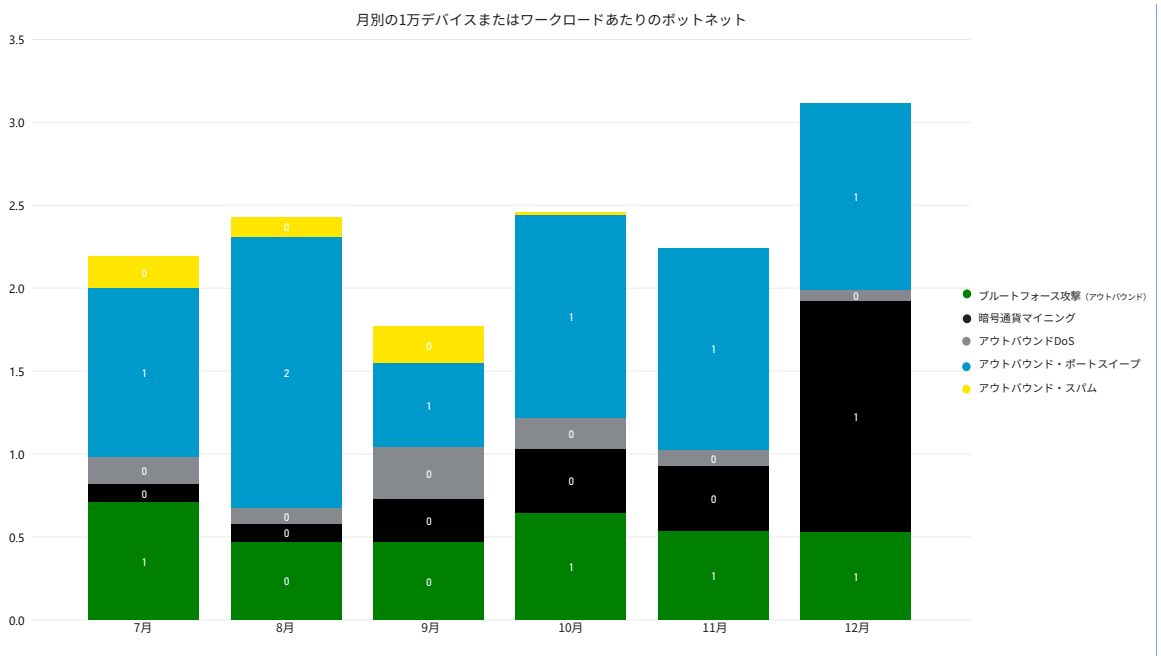
こちらのデータは、実際に攻撃者の振る舞いが進行中であることを示しています。コマンドアンドコントロール（C&C）や内部偵察といった活動は、多くの場合攻撃の初期段階で発生するため、攻撃が拡大する前に迅速に緩和措置を取ることができます。これらの振る舞いは、一般的に最も多く検知される対象です。

ラテラルムーブメント（横方向の移動）は、攻撃ライフサイクルの終盤に発生します。サイバー犯罪者は、サーバーにアクセスできる管理者の認証情報を盗み出し、企業内部で足場を固めようとします。これらのタイプの検出結果を受け、インシデント対応チームによる高優先度のアクションを確実に遂行させることで、データ流出による取り返しのつかない損害の発生を未然に防ぐことができます。



ボットネット

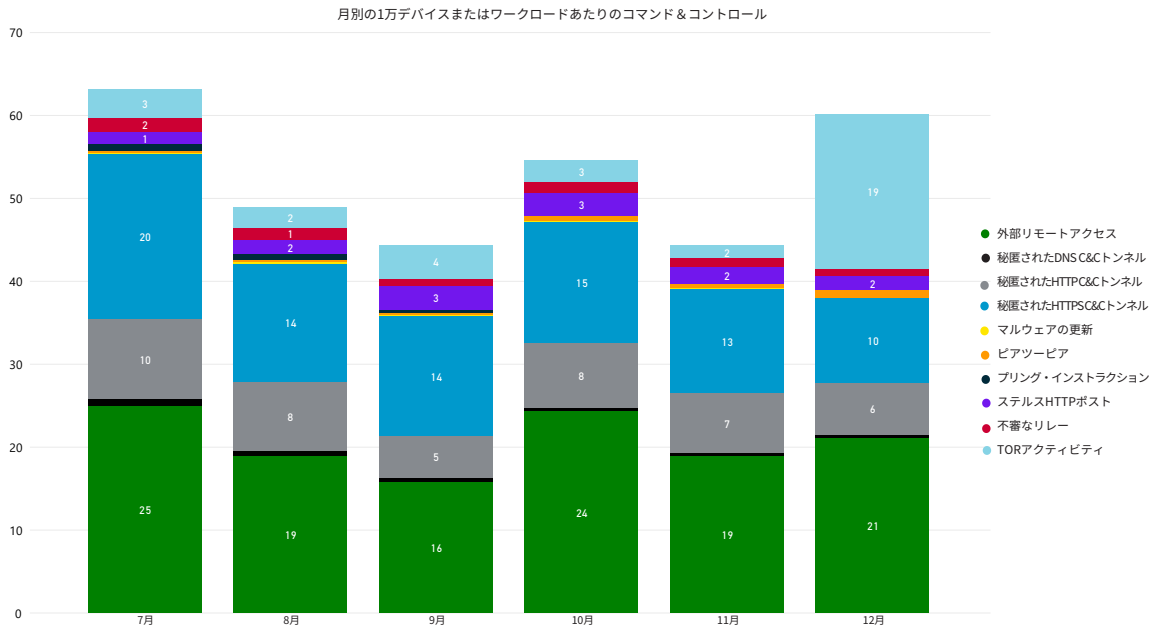
ボットネットは、デバイスがボットハーダー（bot herder）に対して利益を提供するよう仕向ける、場当たり的な攻撃です。感染したデバイスが、不正な価値を生み出すために使用する手段には、ビットコインのマイニングからスパムメールの送信、偽の広告クリックに至るまで様々な内容があります。ボットハーダーは、利益を得るために、デバイスやネットワーク接続、さらに悪評を受けていない割り当て済みIPアドレスを使用します。



コマンド&コントロール

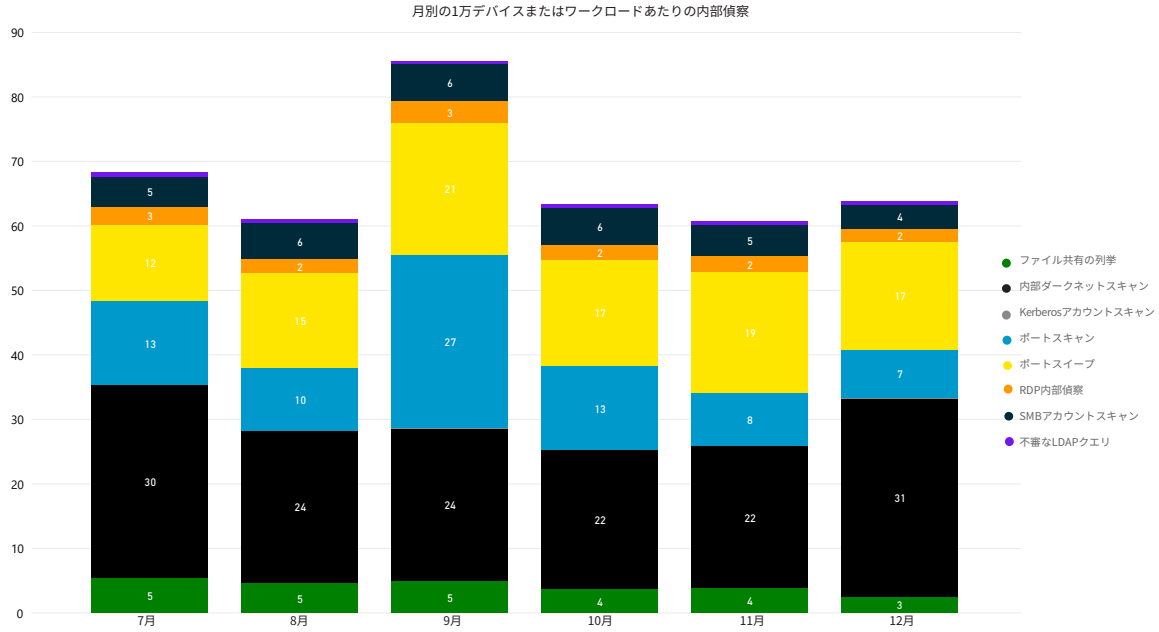
C&Cトラフィックは、デバイスが外部の悪意ある不正者の制御下にあるような場合に発生します。ほとんどの場合、デバイスはボットネットの一部になっているか、あるいはアドウェアやスパイウェアがインストールされているため、その制御は自動化されています。

稀なケースではありますが、最も重大となるのは、悪意のある部外者がデバイスをマニュアルでコントロールできる場合です。これは最も脅威のレベルが高いケースであり、特定の企業を標的にした攻撃であることを意味しています。



内部偵察

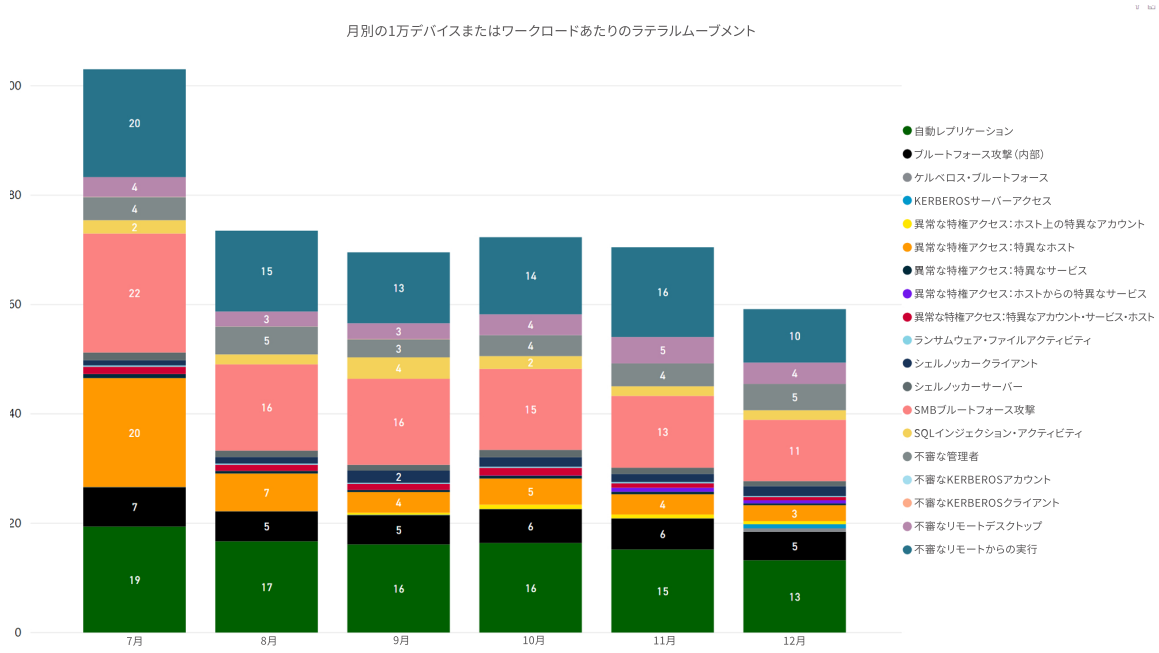
内部偵察攻撃者の振る舞いは、デバイスがエンタープライズインフラストラクチャーのマッピングに使用された場合に発生します。この行動は、標的型攻撃の一環である場合がほとんどですが、ボットネットが内部から他のデバイスに拡大を試みている場合もあります。検知できるタイプは、システムやネットワークポート、ユーザーアカウントに対する、ファストスキャン（Fast Scan）とスロースキャン（Slow Scan）です。



ラテラルムーブメント

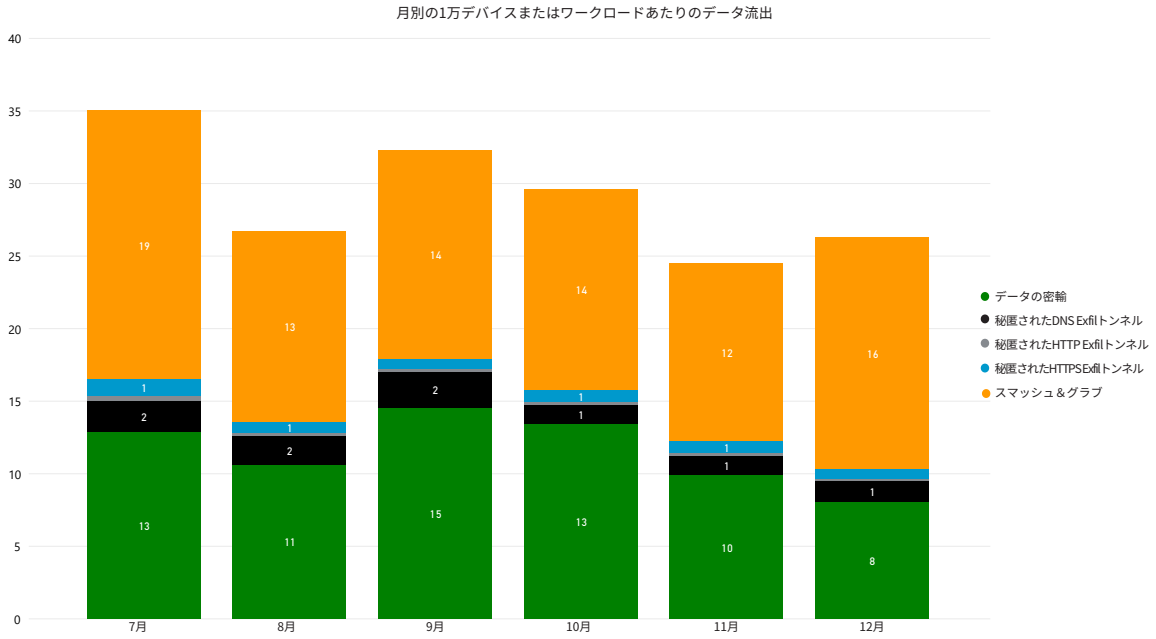
ラテラルムーブメントは、システム内を横方向に移動し、標的型攻撃の拡大を試みる不正行動です。アカウント認証情報の盗難や、他のデバイスからのデータの盗難といった試みを行う場合もあります。

攻撃者の足元をさらに固めたり、標的となるデータに近づくために、他のデバイスを侵害する場合もあります。攻撃ライフサイクルにおける段階で考えると、プライベートのデータセンターやパブリッククラウドに侵入する前段階に該当します。



データ流出

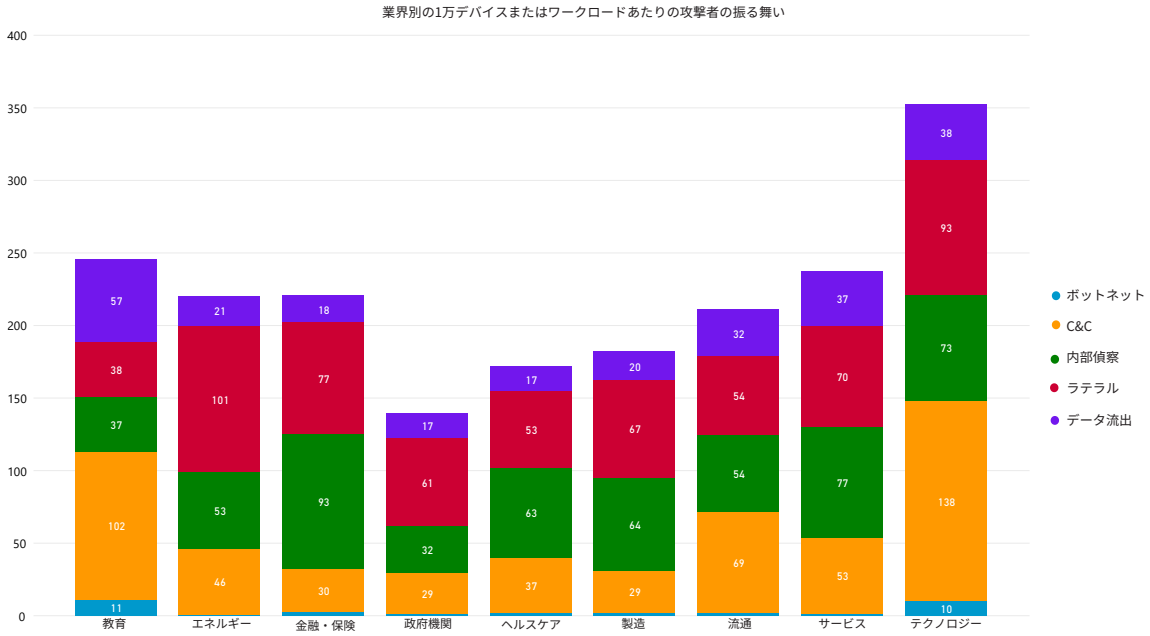
データ流出（exfiltration）に関連した不審な振る舞いは、転送自体を秘匿するような方法でデータを外部に送信する場合に発生します。通常の正当なデータ転送であれば、転送を秘匿するような技術を使用する必要はありません。データを転送しているデバイス、データの転送先、データの量、送信に使用する技術などが、データ流出を把握する上での指針となります。



1万デバイスあたりの業界別脅威

以下のチャートは、各業界で発生した脅威に関する検知数を示しています。このビューでは、1万デバイスあたりの各業界での脅威内訳と、どの業界で最も多くの検知数が発生したかを総数で示しています。

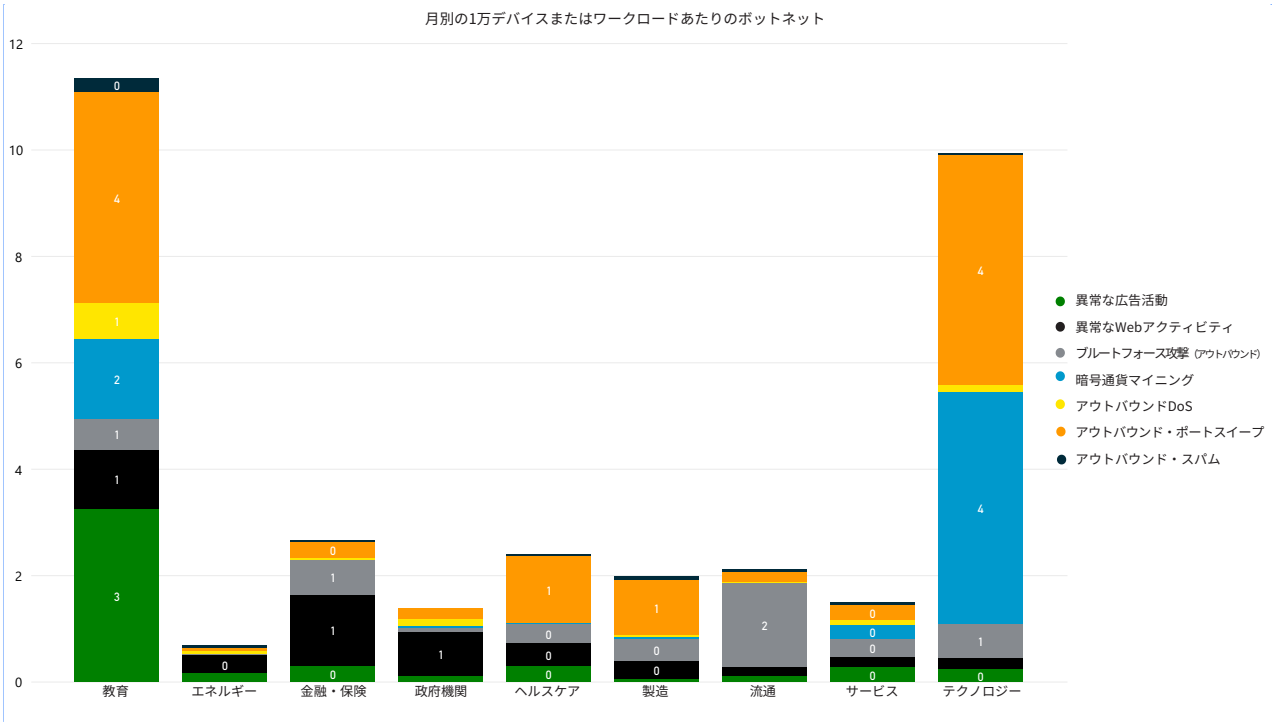
テクノロジー業界と教育機関が高い割合を示していますが、その要因となっているのは、C&C（教育機関）および内部偵察（テクノロジー）の発生件数の多さです。



業界別のボットネット

教育機関は、場当たり的なボットネット攻撃の温床となっています。大学自体がオープンであることや、学生の好奇心が原因となってこのような状況が発生しています。教育機関では、クリプトマイニングや異常な広告、さらにWebアクティビティといった脅威が常に蔓延しています。

2019年の後半、テクノロジー企業におけるボットネットの活動数が急増しました。テクノロジー企業の場合、ホストや不正な振る舞いの全体状況から見れば、ボットネット攻撃は相対的に少ないと考えられますが、最近では、クリプトマイニングやアウトバウンドのポートスイープが目に見えて増加してきています。



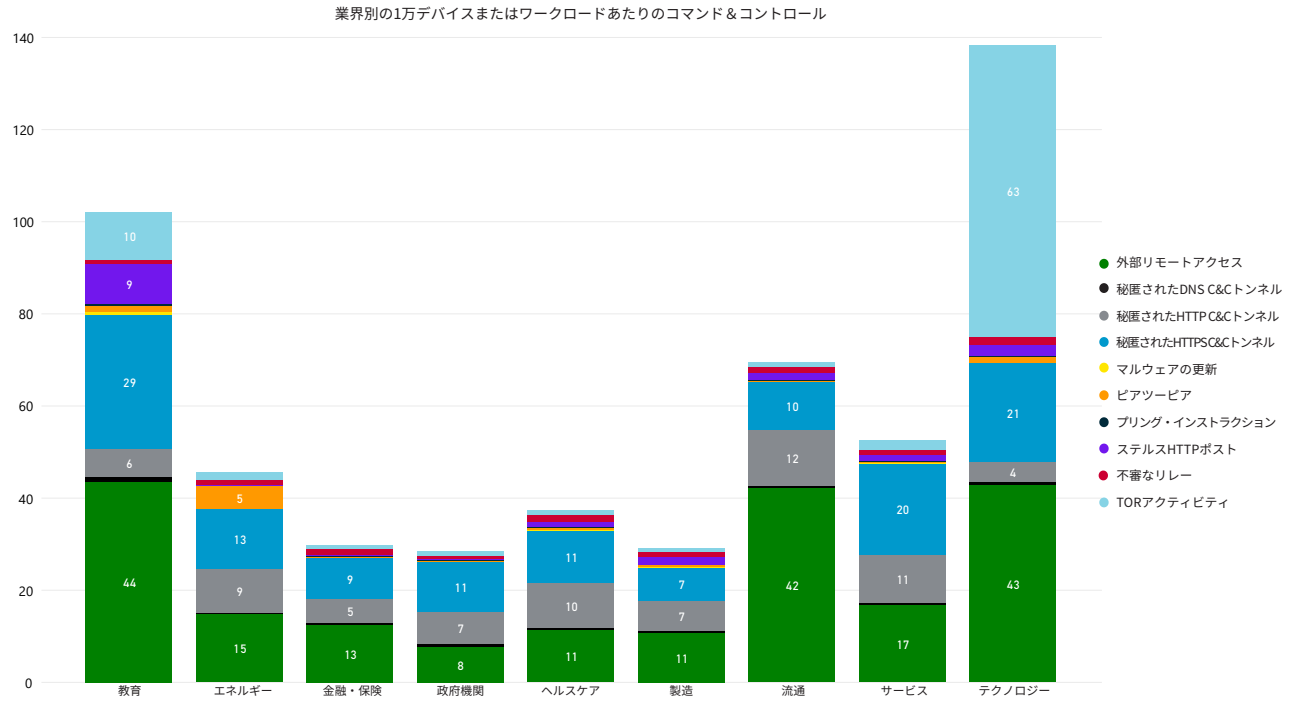
業界別のC&C

テクノロジー業界は、膨大な数の外部リモートアクセスや秘匿されたHTTPSトンネルによって、2019年のトレンドを作ったと言っても過言ではないでしょう。そして、過去6ヶ月にわたりテクノロジー業界のトレンドを追っているのが、教育機関と小売業界です。これらの業界では、特に外部リモートアクセスが高い数値を示しています。

リモートワーカーは、オフィスワーカーと同様に重要な社員として、どの業界の企業にも在籍しているため、その業務を支える外部からのリモートアクセスは、全ての業界において共通に発生しています。リモートワーカーは、リモートデスクトップ・アクセスソフトウェアを使って、外部からホストにアクセスします（GotoMyPCやRDPなど）。一方、攻撃者は、C&Cサーバーに接続し、人間のオペレーターからコマンドを受け取るようなリモートアクセス機能を持ったマルウェア（MeterpreterやPoison Ivyなど）を使用して、ホストをコントロールするという戦術を使います。

一部のソフトウェアに見られる秘匿されたトンネルの使用は、一見無害に思えるかもしれませんが、その真の意図はセキュリティコントロールをバイパスすることにあるため大きなリスクとなり得ます。秘匿されたトンネルは、高度な攻撃者が境界のセキュリティコントロールを擦り抜けるために悪用する標的型攻撃の一部で使用されます。

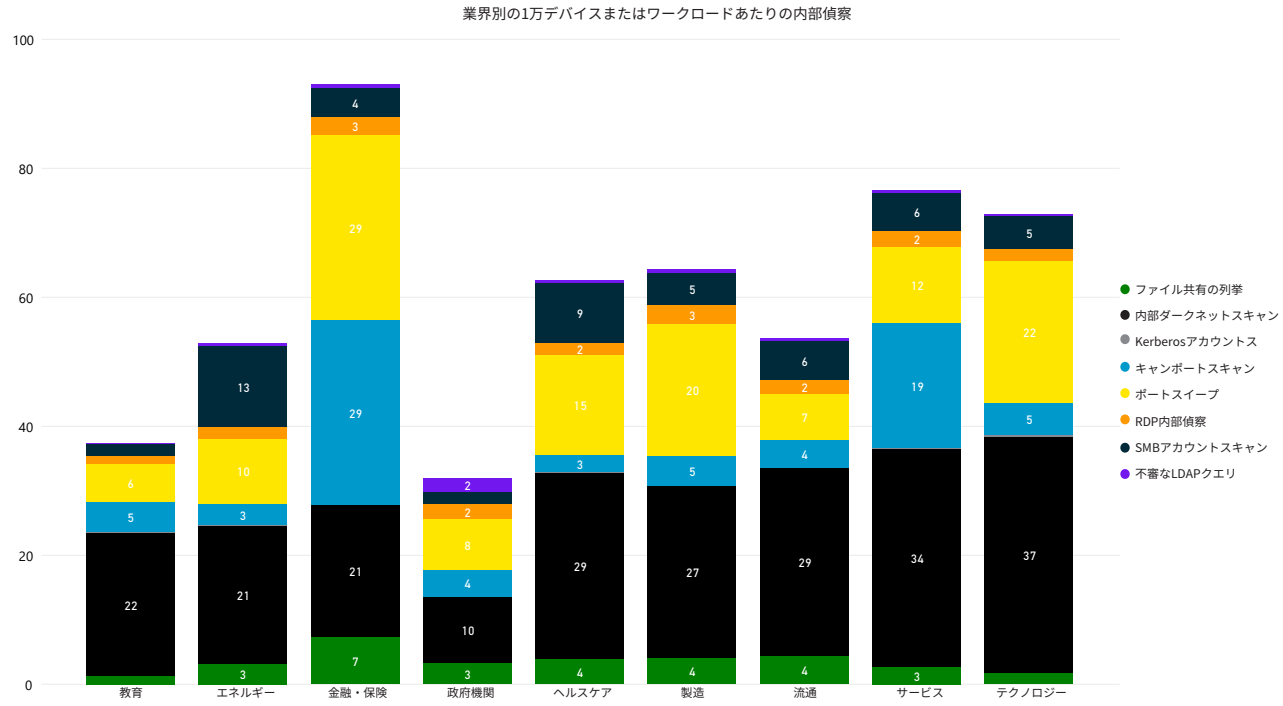
2019年後半、新たに見られたのが、TORトラフィックの急増です。TORは正当なビジネス上の目的にはほとんど用いられないため、大量のTORトラフィックが見られることは、どんな企業においても稀です。全業界を通じて、ホスト1万台あたりのTORの検知数は平均3件でした。12月には、ホスト1万台あたりの検知数が19件に跳ね上がりましたが、これはアジア太平洋地域のテクノロジー企業に起因するものです。



業界別の内部偵察

サイバー攻撃の世界では、多くの場合、よりシンプルなテクニックが複雑なテクニックに勝るというが結果が見られます。金融機関や保険会社における内部偵察の傾向を見ると、1万ホストあたりのポートスイープの数が、業界平均の11件に対して、29件という数値になっていることが分かります。ポートスイープ自体は簡単な仕組みであり、侵入を拡大するという目的を果たすためのネットワークマッピングに必要なものです。

ポートスイープの一環である、ネットワークに存在しないIPアドレスのスキャン（内部ダークネットスキャン）は、内部偵察行動における最も一般的な手法です。内部ダークネットスキャンによって、ネットワーク内にあるアセットマッピングシステムや新しいネットワークに移動し、以前は利用可能で、現状は多くのサービスの接続に失敗したホストがどれであるかを把握することができます。ほとんどのダークネットスキャンは、脆弱性スキャナーやアセット検出システムといった内部システムから発生しますが、システム内での低速な内部偵察は、ネットワークにおける標的型攻撃の始まりである場合があります。

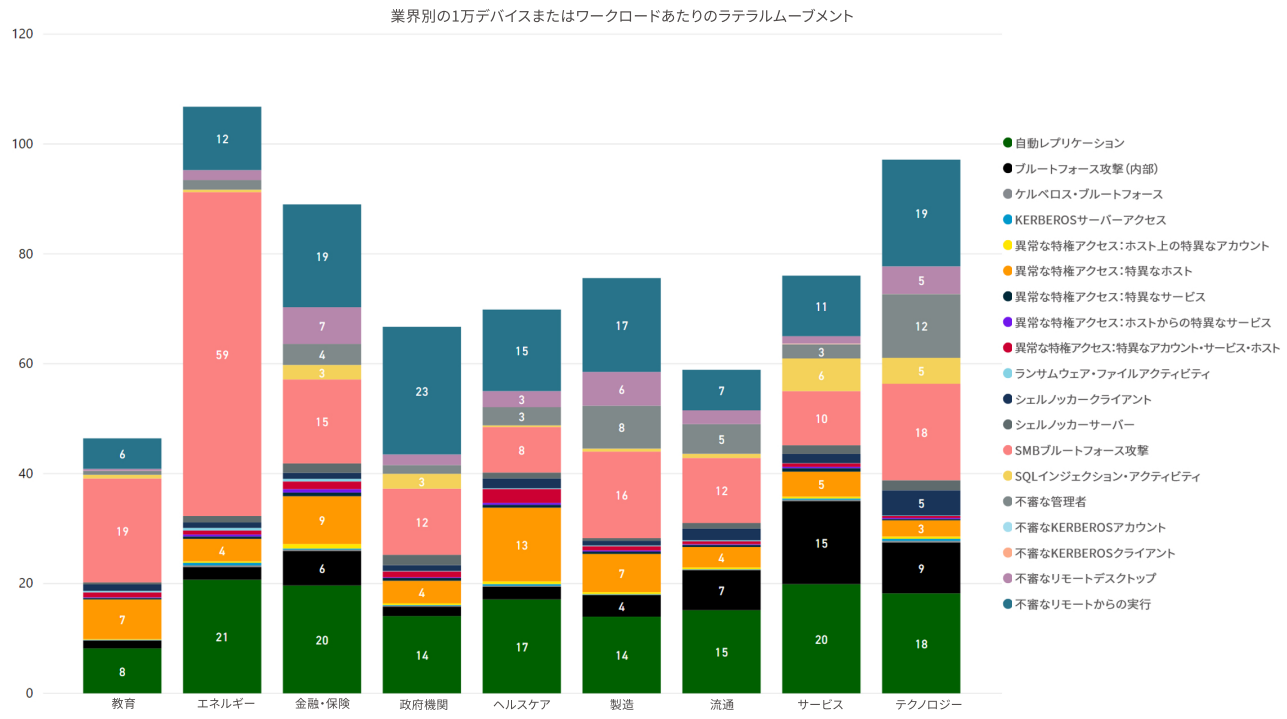


業界別のラテラルムーブメント

再び派手な攻撃テクニックが、全ての業界で見られるようになっています。7月にはSMB総当たり攻撃が、年最高となる1万ホストあたり22件観測されています。それ以外の月（8月から12月）のSMB総当たり攻撃は、1万ホストあたり14件となっています。

SMB総当たり攻撃では、デバイスからファイルサーバーにアクセスするために、同じアカウントを使って複数回ログインを試みます。他のアカウント、特に権限の高い認証情報（ユーザー名とパスワード）を首尾よく入手して行くことが、標的型攻撃に見られる典型的な進め方です。たとえ設定の誤りが原因で発生したケースでも、検知した振る舞いは標的となるシステムに大きな負荷をかけるため、早々に排除する必要があります。

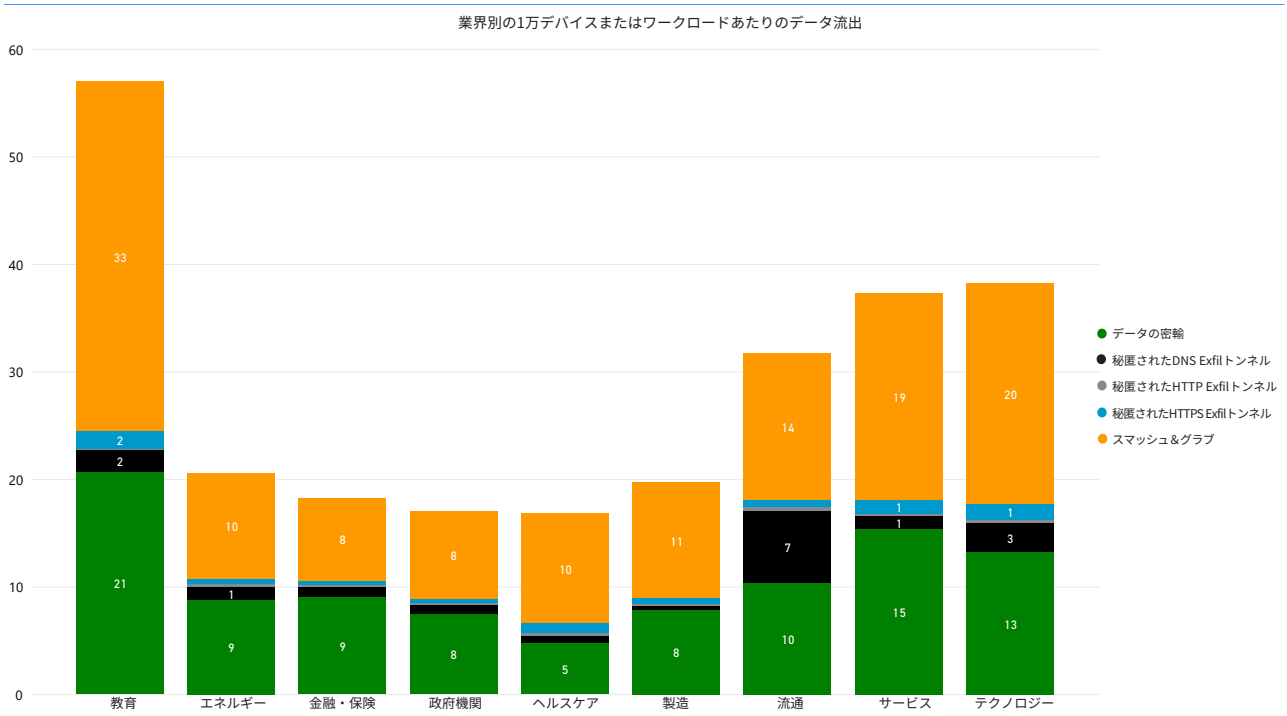
小規模な企業では、1万ホストあたり112件のラテラルムーブメントが観測されていますが、中規模、大規模企業における検出数は64件となっています。大規模な企業よりも小規模な企業の方が、内部を容易に移動できるということかも知れません。2019年におけるランサムウェア攻撃の大部分が、小規模企業を標的としており、攻撃者が気付かれることなく、どれだけ容易にポイントaからポイントbに移動できるかを示す好例と言えます。



業界別のデータ流出

全業界において、スマッシュ&グラブ（Smash-and-grab）は、最も一般的なデータ流出の振る舞いとなっています。通常この振る舞いは、デバイスが対象環境において正常ではないと考えられる相手先に、短時間の内に大量なデータを送信することによって発生します。データがアップロードされた先の外部サービスが、IT部門によって認可されたものでない場合、業務上の潜在的なリスクが高まります。教育機関では、スマッシュ&グラブの振る舞いが最も多くなっており、データ流出の振る舞い全体もまた大きく伸びているのが分かります。

データ流出の振る舞いの中で2番目に位置するのは、データの密輸（smuggler）で、全ての業界に共通して観測されます。この振る舞いは、内部ホストが1つまたは複数のサーバーから大量のデータを取得し、さらにそのデータを外部システムに送信した場合に発生します。大量のデータを短期間に取得し外部に送る行為は、単純に偶然の産物かもしれませんが、外部へのデータ転送は、さらなる調査を行う意義を持つ十分な事象と言えます。



まとめ

明白かつ重要で緊急を要する、重大なセキュリティ要件があります。それは、自社のネットワークが侵害を受けているかどうかを把握できる能力です。防御に失敗すれば、攻撃者が内部に侵入してきますが、レガシーなネットワークセキュリティの連携は、この要件に向け決して十分なものではありません。

企業全体での包括的な脅威の検知と対応は、数多くのリスクに晒されている現代のデータ環境にとって不可欠であり、さらに、これらのリスクは以前にも増して高まっています。ギャップを埋めるためには、実態を把握できる適切なコンテキスト備えた適切なデータを入手して、継続的に侵害を検知できるようにする必要があります。

Vectra AI社が提供するCognitoは、当初からこのような問題に対応できるよう設計されたものです。Cognitoは、セキュリティアプリケーションに対して、ホスト名やビーコンの存在、アカウントの特権レベルなど、固有のコンテキストで強化した信頼度の高いネットワークデータ（つまり、全ての通信で発生している事象に関する知識）を提供します。

Coginitoは、大規模なエンタープライズネットワークに対しても、効率的に拡張することが可能であり、現在、そして将来においても、ユーザーやデータセンター、クラウド環境を全方位で可視化することができます。

最後に、Vectra AI社が実施した分析およびレポートのために、ネットワークメタデータの共有にご協力頂いた企業の皆様に御礼申し上げます。
ありがとうございました。

VECTRA AI, INC.

Security that thinks®

お問合せ：

製品、ソリューションなどに関するお問い合わせは、info-japan@vectra.ai までお願いします。

© 2020 Vectra AI, Inc. All rights reserved. Vectra、Vectra AI社のロゴ、CognitoおよびSecurity that thinksは、Vectra AI社の登録商標です。Cognito Detect、Cognito Recall、Cognito Stream、Vectra Threat LabsおよびThreat Certainty Indexは、Vectra AI社の商標です。その他の会社名、製品名およびサービス名は、一般に各社の登録商標またはサービスマークです。

IR_AttackerBehavior_062420