攻撃の「高速道路」

悪性 DNS トラフィックの詳細な分析

Akamai

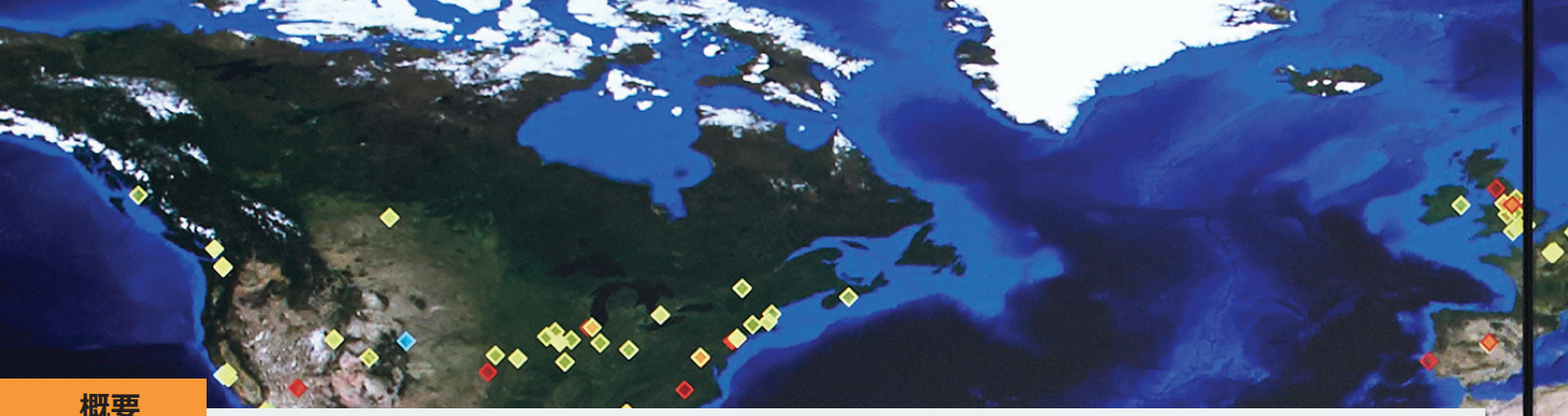
目次

ドメイン・ネーム・サーバー ー 攻撃トラフィックの「高速道路」

ドメイン・ネーム・システム（DNS）はインターネットインフラの黎明期からその重要な要素とされてきました。家庭でも職場でも、私たちがインターネットを容易に利用できるのは、Web 上のアクセス先に正しく到達するために DNS が使用されているからです。攻撃者がたびたびこのインフラを利用して攻撃を仕かけてくるのは驚くことではありません。指令を受け取るまで待機するようにコマンド & コントロール（C2）サーバーを利用したり、コードをリモートで実行してドメインにアクセスし、悪性ファイルをマシンにダウンロードしたりするといった脅威が存在します。DNS はあらゆるところで使用されているため、攻撃基盤の重要な要素となっています。

セキュリティ企業である Akamai の優位性は、企業およびホームユーザー（個人）の DNS 利用状況を調査、システムの侵害や情報漏えいの原因となる悪性 DNS トラフィックから保護できることにあります。このレポートでは、世界各国のホームユーザーやエンタープライズ組織を標的とする悪性トラフィックについて分析を行うことです。悪性 DNS トラフィックを徹底して分析し、攻撃者グループやツールと相関付けることで、組織が攻撃を受ける可能性の高い脅威に関する大きな手掛かりが得られます。このような情報は、セキュリティ対策担当者が防御のあり方を評価し、組織が採っている技法や方法論がその攻撃に対抗できるかどうかのギャップを分析する上で参考になります。これを怠るとセキュリティ侵害を招き、その結果、機密データの漏えいや財務的な損失を招いたり、コンプライアンス違反による罰則を受けたりすることになりかねません。2025 年までにサイバー犯罪のコストは年間 10 兆 5,000 億米ドルに増えることが予想され、組織には攻撃を受ける前の備えが求められます。

エンタープライズユーザーとホームユーザーともに悪性 DNS トラフィックを分析した結果、明らかになったいくつかの攻撃やキャンペーンには、世界各国を移動する Android ベースのマルウェア FluBot の拡散をはじめ、エンタープライズ組織を標的とするさまざまなサイバー犯罪グループの広まりが見られました。最適な例として考えられるのが、イニシャル・アクセス・ブローカー（IAB）が絡む、存在感を増している C2 トラフィックです。この組織は、企業ネットワークに侵入し、RaaS（Ransomware as a Service）グループなどを相手に、そのアクセスの手引きをすることで収益を得る組織です。情報の「高速道路」である DNS に関するこのような活動が目立つようになってきたため、それを読者の方々と共有することに価値があると考えています。



概要

当社のデータによると、10 ～ 16% の組織が、調査期間中いずれの四半期においてもネットワークで C2 トラフィックの発生を確認しています。C2 トラフィックの存在は、攻撃が進行しているか侵入を許した可能性を示しており、情報を盗み出すボットネットから IAB まで、さまざまな脅威が存在します。

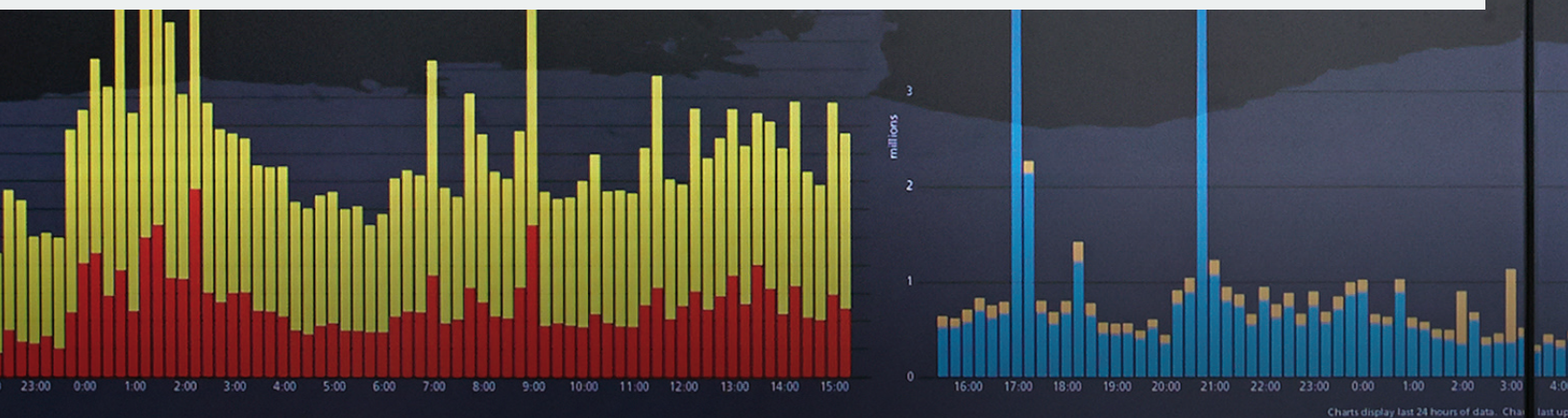
影響を受けたデバイスの 26% が、Emotet や Qakbot に関連するドメインなどの既知の IAB C2 ドメインに接触していました。IAB は、主に初期侵入を実行し、ランサムウェアグループやその他のサイバー犯罪グループにアクセスを手引きする役割をしているという点で、組織にとって非常に危険な存在となっています。

ネットワーク接続ストレージ（NAS）デバイスは、パッチを適用されることが少なく、貴重なデータが保存されているため、悪用の格好の的になっています。当社のデータによると、攻撃者は QSnatch を通じてこれらのデバイスを悪用しており、企業ネットワーク内の影響を受けたデバイスの 36% がこの脅威に関連する C2 ドメインにアクセスしています。

影響を受けた組織の 30% が製造業に属しており、第 2 位の業界の倍の数字にのぼります。このことは、サプライチェーンの問題や日常生活の混乱など、サイバー攻撃が現実に与えている影響を浮きぼりにしています。基本産業や製造などの重要インフラへの攻撃を抑止する力としては、Network and Information Security 2（NIS2）などの規制が考えられます。

ホームネットワークへの攻撃では、コンピューターのような従来のデバイスだけでなく、携帯電話やモノのインターネット（IoT）デバイスも悪用の対象となります。大量の攻撃トラフィックには、モバイルマルウェアや IoT ボットが関係しているものと見られます。

DNS データの分析からは、欧州、中東、アフリカ（EMEA）、ラテンアメリカ（LATAM）、アジア太平洋地域と日本（APJ）で FluBot マルウェアの拡散が始まっていることが伺えました。マルウェアのソーシャルエンジニアリング手法と複数の EU 諸国言語を使用するという手口は、感染の広がりの要因として考えられます。



Akamai DNS トラフィック分析の用語

Akamai の Edge DNS と DNS インフラは、毎日最大 7 兆の DNS リクエストを検出しています。Akamai のユーザーとエンタープライズ組織を守るために、私たちはマルウェアの感染元となるドメインや利用者の情報を盗むおそれのあるサイトに向けられたリクエストをブロックしています。また、これらの悪性 DNS トランザクションの調査により、これらのドメインをマルウェア、フィッシングサイト、C2 の 3 つに分類できるようになり、エンタープライズ組織やホームユーザーにとって最大の脅威を明らかにする詳細な分析もできるようになりました。

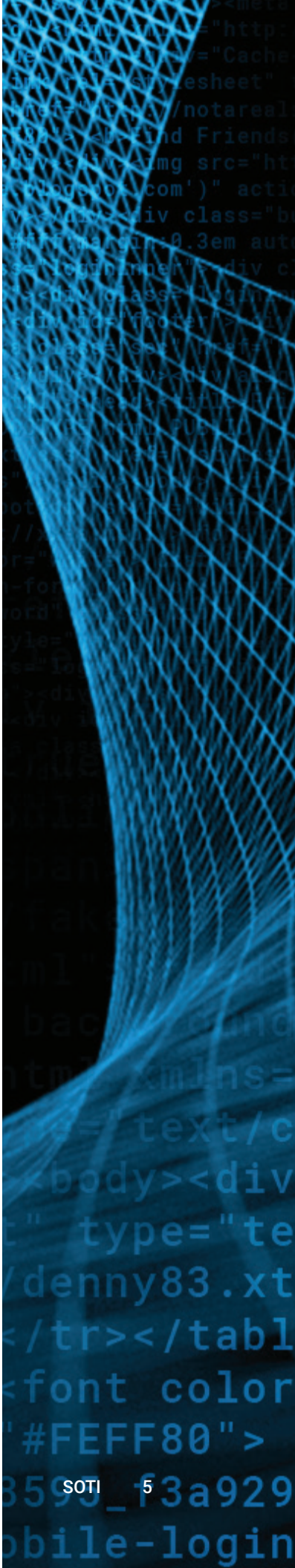
悪性 DNS トラフィックから慎重にデータを抽出することで、この最大の脅威に関する重要な結論を導き出すことができます。私たちは保護対象を大きく 2 つのユーザーグループに分けており、まず、Akamai が保護している企業ネットワーク内のエンタープライズユーザー、そしてもう 1 つがパーソナルネットワークからインターネットにアクセスするホームユーザーです。これらを標的とするボットネットなどの脅威は、悪意をもってデバイスを乗っ取り、クリプトマイニングにより金銭的な利益を得ようとします。

まず、本レポートにおける**フィッシングサイト**、**マルウェア**、C2 の用語の定義を明確にしておきましょう。

フィッシングサイトとは、小売店、銀行、ハイテク企業などに見た目を似せたフィッシングキットに関連するドメインで、ユーザーを騙して認証情報や個人識別情報（PII）を入力させようと試みます。Akamai は DNS を通じたこれらのトラフィックを確認し、エンタープライズユーザーとホームユーザーを個人情報の盗難や損失から保護しています。

マルウェアとは、悪性ファイルとして機能したり、悪性ファイルを格納したりする悪性ドメインのことです。このカテゴリーには、悪性の JavaScript が置かれたサイトや、乗っ取られて望ましくない広告が掲載された Web サイト、そのような広告を掲載したページにユーザーを誘導する Web サイトも含まれます。最新の多くの攻撃では、悪性ファイルを外部ソースからデバイスにダウンロードして初期ペイロードとして利用するか、攻撃の次のステージをダウンロードすることが必要となっています。こうしたトラフィックを見つけてブロックすることは、組織を初期感染や継続的な攻撃から保護するのに役立ちます。

C2 とは、私たちの DNS トラフィック分析において、感染したデバイスと通信して指令を送り、デバイスを制御するドメインを意味します。初期侵入を果たした攻撃者は、感染したシステムと攻撃者が制御するサーバー間に C2 通信を確立し、他のマルウェアのダウンロードや拡散、データ漏えい、システムのシャットダウンやリブートなどの追加の指令を送り、さらにシステムやネットワークのセキュリティを侵害します。C2 トラフィックは、攻撃が継続している間はまだ緩和が可能であるため、これを検知することが重要です。さらに、C2 サーバーに関連するドメインをブロックすることは、C2 通信を阻止し、マルウェアのダウンロードによるさらなる指示や指令を食い止め、ネットワークにおける攻撃者の悪意ある活動の機会を縮小することにつながります。



目前の脅威：組織に広がる悪性トラフィック

Akamai の DNS トラフィック分析によると、2022 年第 4 四半期には、13% のデバイスが少なくとも一度はマルウェアと関連のあるドメインにアクセスを試みています（図 1）。さらに、6% がフィッシングに関連するドメインと通信しています。本レポートで主に取り扱う C2 関連の領域では、第 4 四半期に若干減少しながらも一年を通じて増加の傾向が見られます。

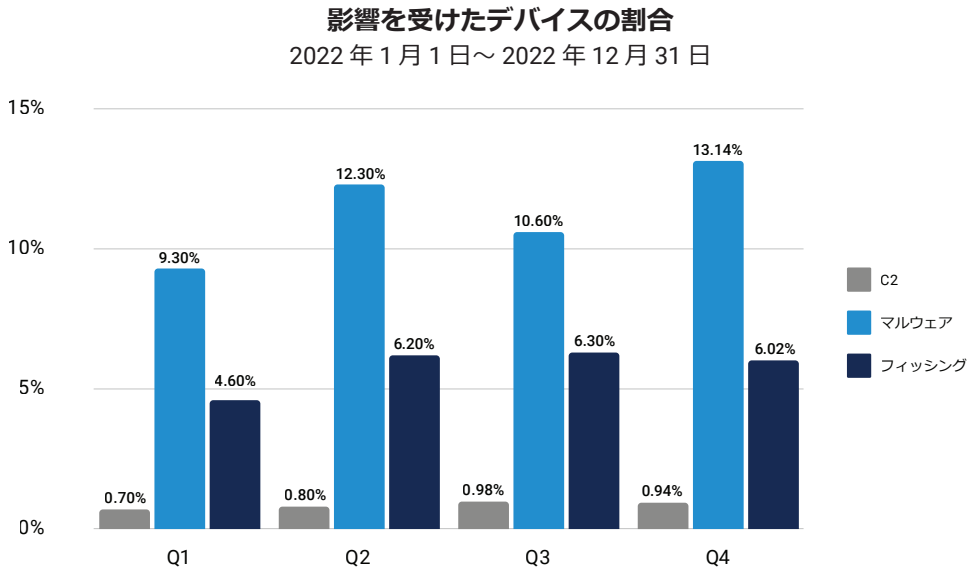


図 1：保護されたデバイスが悪質なアクセス先と接触する傾向が増加

図 1 に示したデータは、悪性ドメインと通信を試みた個別デバイスをカウントしたものです。注意が必要なのは、（攻撃者によりマルウェアのダウンロードに使用される）マルウェアの配布元にアクセスするデバイスと、C2 ドメインにアクセスするデバイスの違いです。後者のデバイスは一般的に、攻撃の実行中に攻撃者とマルウェアが通信を行うために使用され、攻撃サイクルを進めるためにさらにマルウェアのダウンロードに使用されることもあります。この違いはネットワーク侵入の試みにおける違いを示すと考えられます。マルウェアをマシンにダウンロードする最初の試みでブロックされたケースと、侵入に成功した（データによると DNS を経由していない可能性あり）か、攻撃の試みを継続しているケースです。このケースでは、C2 ドメインに到達できれば、攻撃を実行できるようになります。

このレポートで主に注目するのは、攻撃者がデバイスへの侵入に成功したことを示すと思われる C2 トラフィックです。これらの攻撃の広まりを把握するために、異なる視点からデータを見る必要があります。個々のデバイスに注目するよりも、（C2 トラフィックの存在により示される）継続的な攻撃がデータセット内にどれだけ一般的に見られるかを調べることで、組織別にデータを集約することが可能になります。

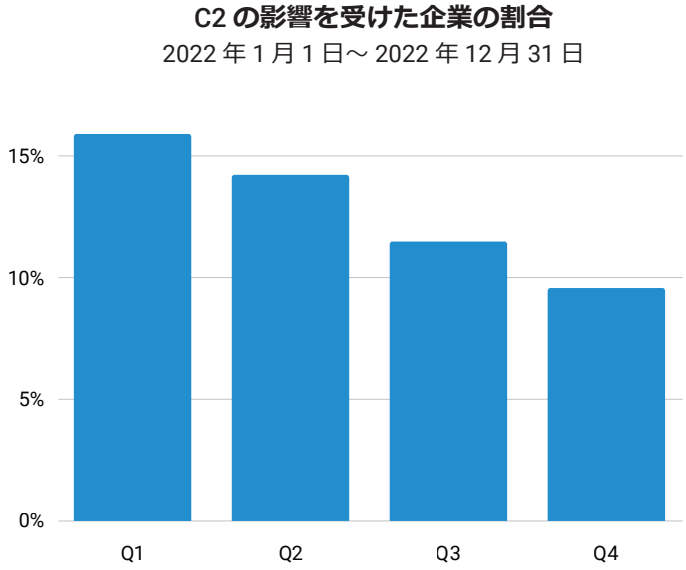


図 2：悪性 C2 トラフィックの分析による、
1 年間に 1 台以上のデバイスが C2 ドメインにアクセスした組織の割合

> **収集した DNS データによると、10 ～ 16% の組織が、特定の四半期に少なくとも一度は、組織のネットワークから C2 トラフィックが外に流れていると見られる事例を経験しています。**

収集した DNS データによると、10 ～ 16% の組織が、特定の四半期に少なくとも一度は、組織のネットワークから C2 トラフィックが外に流れていると見られる事例を経験しています（図 2）。これは、マルウェアがオペレーターと通信を試みていることを示すもので、侵害の兆候と考えられます。この C2 トラフィックは Akamai のソリューションによりアクセス先に到達しないようにブロックされましたが、攻撃に成功すればデータ漏えいやランサムウェア攻撃などの被害が発生したおそれがあります。2022 年上半期時点で検知されたマルウェアは 23 億にのぼり、平均で 1 日に 1,501 件が発見されています。当社の調査では、マルウェアのネットワーク侵入や被害を防止するために DNS を活用する有効性が明らかになっています。

組織への脅威を広げるイニシャル・アクセス・ブローカー

マルチステージ攻撃は、現在のネットワーク攻撃において主要な位置を占めるようになっています（図 3）。攻撃者は相互に連携する（または雇う）ことで攻撃を成功させるチャンスを増やすこともあれば、一度の攻撃でさまざまなツールを組み合わせることもあります。C2 はこうした攻撃を成功させる上で大きな役割を果たします。通信の手段としてだけでなく、ペイロードや次のステージのマルウェアをダウンロードして攻撃を進めるためにも利用されます。Emotet、TrickBot、Ryuk ランサムウェアの攻撃チェーンがそのよい例で、ここ数年に見られるようになったものです。Emotet はまず標的のネットワークに侵入し、初期アクセスを確立すると外部ドメインにアクセスして TrickBot のペイロードをダウンロードして個人データや認証情報などのデータを入手します。攻撃者にとって価値の高い標的とみなされると、マルウェアは C2 サーバーにアクセスして最終的なペイロードとして Ryuk ランサムウェアをダウンロードします。

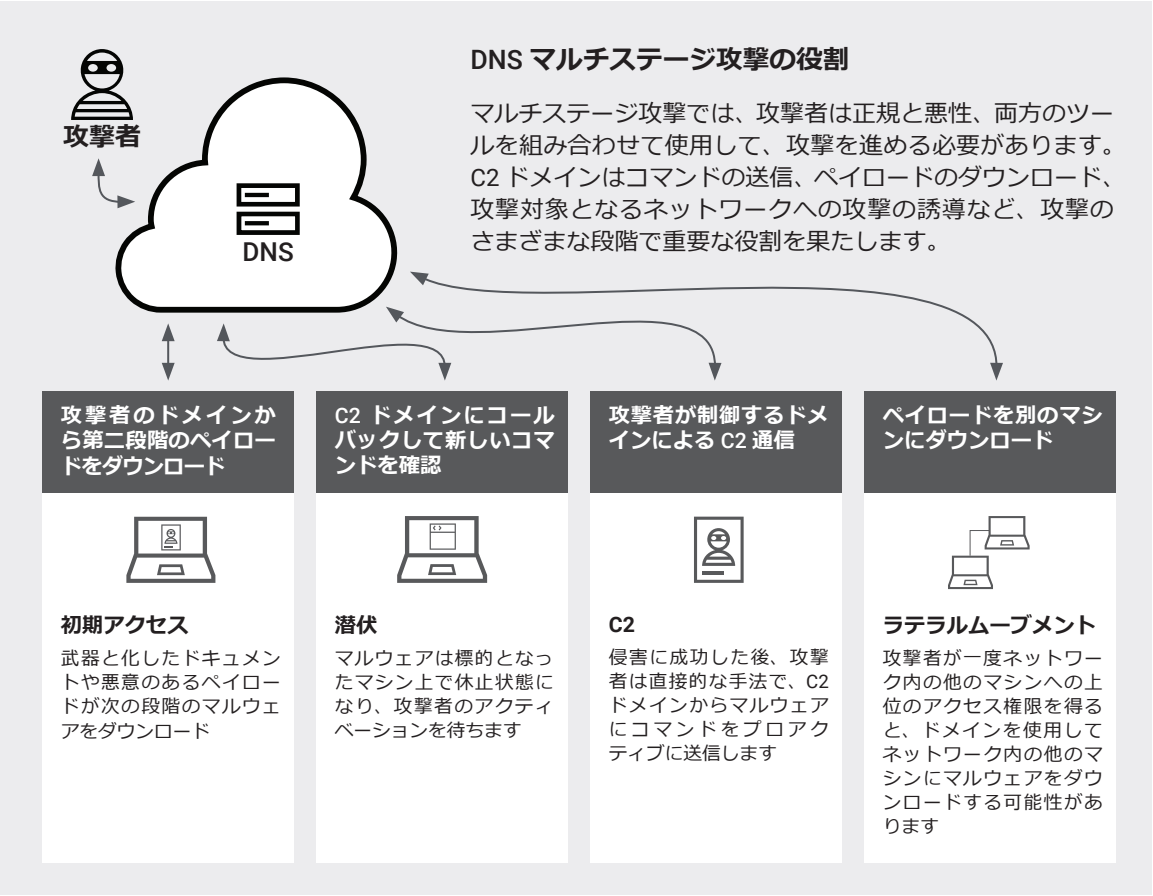


図 3：攻撃の各段階における C2 の役割

この一連の事象は、本レポートの情報をどう見るかを考える上で重要なポイントです。C2 通信は攻撃のさまざまな段階で発生します。私たちが分析した最新のランサムウェアグループ、Conti グループなどが採っている手法では、巧妙な攻撃者は、攻撃のスピードと効率を上げるために、オペレーターを「キーボード操作」のための要員として扱う傾向があるということが分かっています。C2 トラフィックを把握して防ぐことは、進行する攻撃を食い止めるための要となります。

私たちが調査した C2 ドメインは、特定の脅威ファミリーや攻撃者グループへの関与するドメインと、関連のないドメインとに分類できます。このセクションでは、脅威タイプに関連する C2 ドメインに注目し、各グループの能力や方法論に応じたリスクのレベルを評価するための材料を示すことにします。これらのマルウェアファミリーは、攻撃者がどのように攻撃に利用するかに応じて、さまざまな事例に応用できる可能性があることに注意してください。

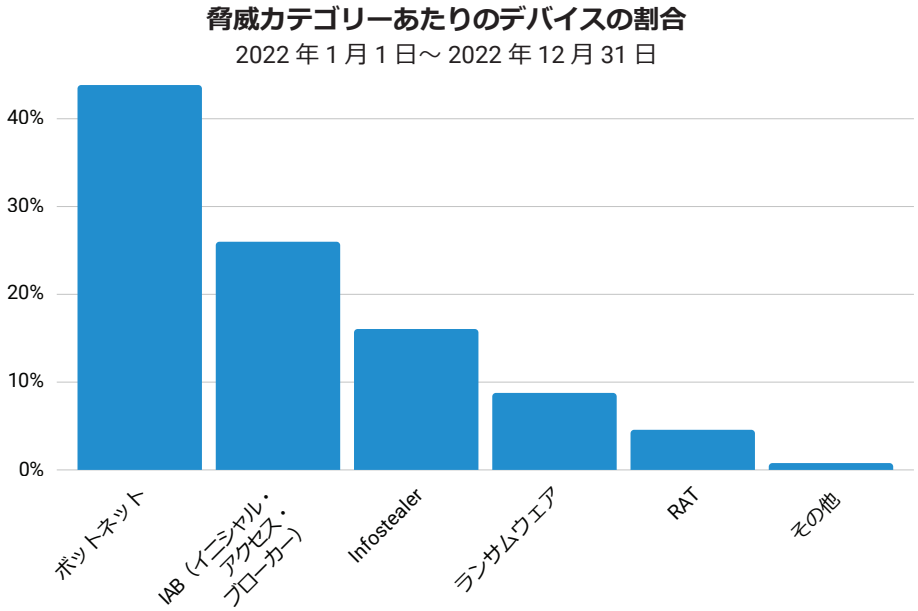


図 4：エンタープライズ組織を標的とするのは主にボットネット、次いで IAB、infostealer

図 4 では、攻撃者グループを IAB、ボットネット、RaaS のグループに分けています。データによると、データ漏えいを目的とするボットネットと同じく、IAB は企業ネットワークの最大の脅威の一つです。

イニシャル・アクセス・ブローカー
IAB は主に、ランサムウェアグループをはじめ他のサイバー犯罪者が組織ネットワークへの足がかりとなる最初の侵入ポイントを提供することを目的としています。

RaaS（Ransomware as a Service）グループ
（技術知識のない者も含めた）他の攻撃者を仲間とし、ランサムウェアソフトウェアを有償で利用するグループです。

ボットネット
攻撃者がボットネットを利用する目的は、クリプトマイニングや DDoS 攻撃によるデータ漏えい、マルウェアの展開やラテラルムーブメントなどさまざまです。

情報窃取（infostealer）
infostealer はユーザー名、パスワード、システム情報、銀行の認証情報、cookie などの各種データを収集します。

ランサムウェア、リモート・アクセス・ツール（RAT）と infostealer の組み合わせは、さまざまな攻撃ステージで重要な役割を果たします。これらのツールは、経験の浅いサイバー犯罪者であれ、熟練したサイバー犯罪者であれ、裏の世界で容易に入手でき、初期侵入を果たした後、ネットワークに身を潜め、それから攻撃を仕かけてくるため、組織はこれまで以上にサイバー犯罪の被害を受けやすくなっています。これらのグループの分類とともに、攻撃における攻撃者間の交わりや組織に与える影響も明らかにしたいと考えます。

イニシャル・アクセス・ブローカーのグループ

「イニシャル・アクセス・ブローカー」（IAB）と呼ばれるサイバー犯罪者は、主に他のサイバー犯罪者や攻撃者に組織のネットワークへの足がかりとなる最初の侵入ポイントを提供するのが主な役割です。複数のサイバー犯罪者グループが攻撃に用いる手口は似通っており、RDP ／ VPN 関連の脆弱性、総当たり攻撃、認証情報の収集、マルウェアを仕込んだフィッシングメールの送信などの手口が使われますが、IAB はこれらの感染したシステムへのアクセスに特化し、攻撃を完遂するよりも攻撃者グループにそのアクセス情報を売ることを目的としています。LockBit、DarkSide、Conti、BlackByte などの背後にいるランサムウェアグループは、攻撃の一部に IAB を利用しているという報告があります。2023 年度調査によると、初期アクセスの情報の平均売値は約 2,800 米ドルです。

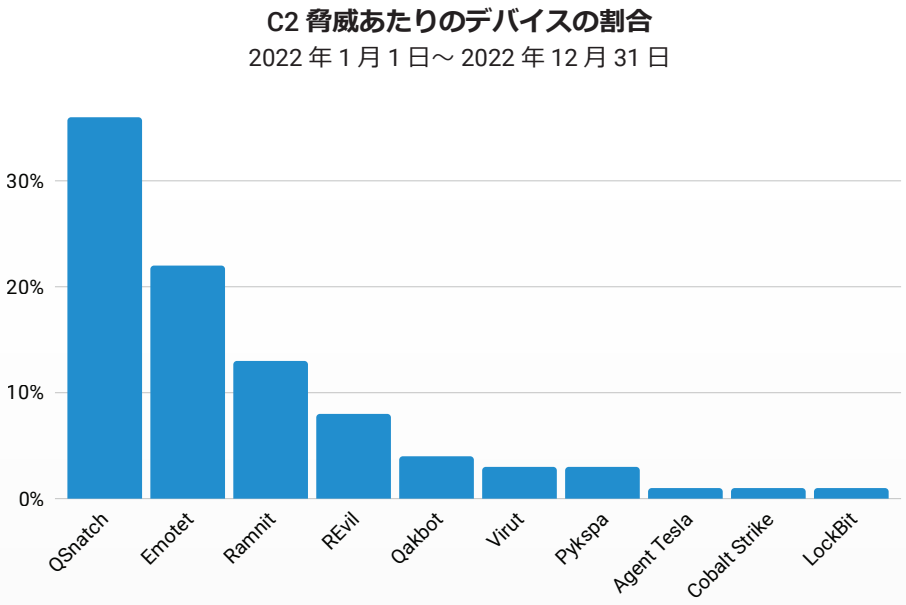
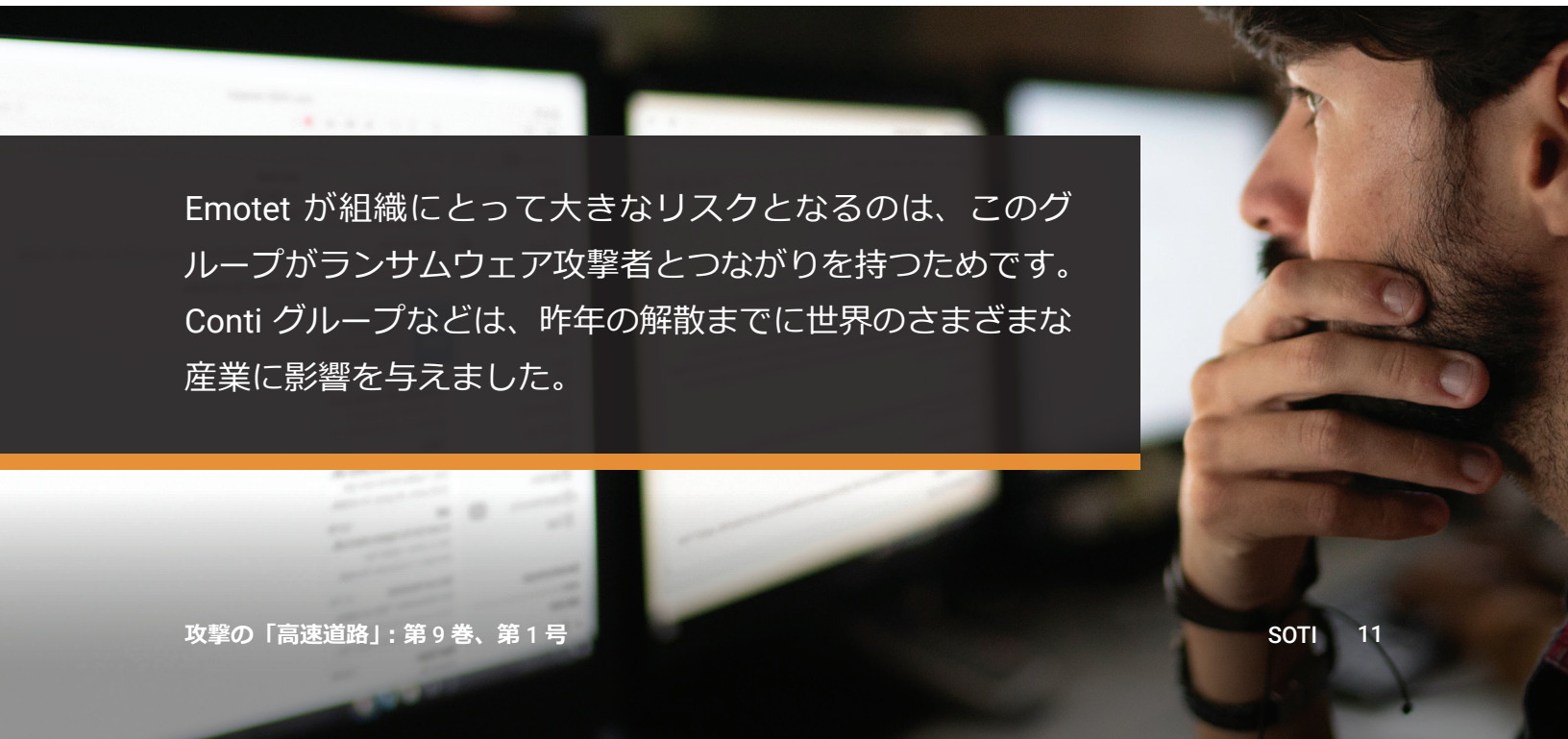


図 5：QSnatch、Emotet、Ramnit は企業ネットワークのトラフィックに見られる上位 C2 マルウェアファミリー

当社の DNS データ（図 5）によると、感染したデバイスの 26% が、Qakbot（感染したデバイスの 4%）や Emotet（感染したデバイスの 22%）などの IAB と関連のあるドメインにアクセスしています。IAB は RaaS ビジネスモデルとサイバー犯罪において重要な役割を果たしています。ランサムウェア攻撃者やサイバー犯罪者がリモートアクセスと認証情報を必要とするのは、被害者のネットワークに侵入するためだけでなく、ネットワークを横方向に移動して潜伏し、アクセス権限を取得するなどの活動のためでもあります。攻撃者は IAB を利用して、時間のかかる予備調査、潜在ターゲットのスキャンや初期感染などの作業を行わせます。闇市場で売られるアクセス権を入手することでその手間が省け、攻撃者が攻撃を仕かけるのに必要な知識や時間のハードルが下がります。こうして、標的にしたい組織への攻撃の可能性が増し、ランサムウェア、認証情報や機密情報の流出、スパイ活動やデータ漏えいなどが生じることになります。

当社のデータによると、Emotet は最も目立つ IAB の一つです。Emotet が組織にとって大きなリスクとなるのは、このグループがランサムウェア攻撃者とつながりを持つためです。この中には、昨年解散するまでに世界のさまざまな産業に影響を与えた Conti グループが含まれます。この数年で Emotet はモジュールを増やし、分散型サービス妨害攻撃（DDoS）やメール窃取の機能を追加し、攻撃目標を拡大しています。Emotet は多くの機能を備えた銀行向けのトロイの木馬／ボットネットから Malware as a Service（MaaS）へと変容し、銀行向けトロイの木馬の IcedID や、TrickBot、ランサムウェアの UmbreCrypt のような脅威を拡散させています。TrickBot グループも Emotet を利用し、Ryuk、ProLock、Conti などさまざまな種類のランサムウェアを配布しています。Emotet が用いる手法の詳細は、このトピックの MITRE ATT&CK フレームワークでご覧いただけます。



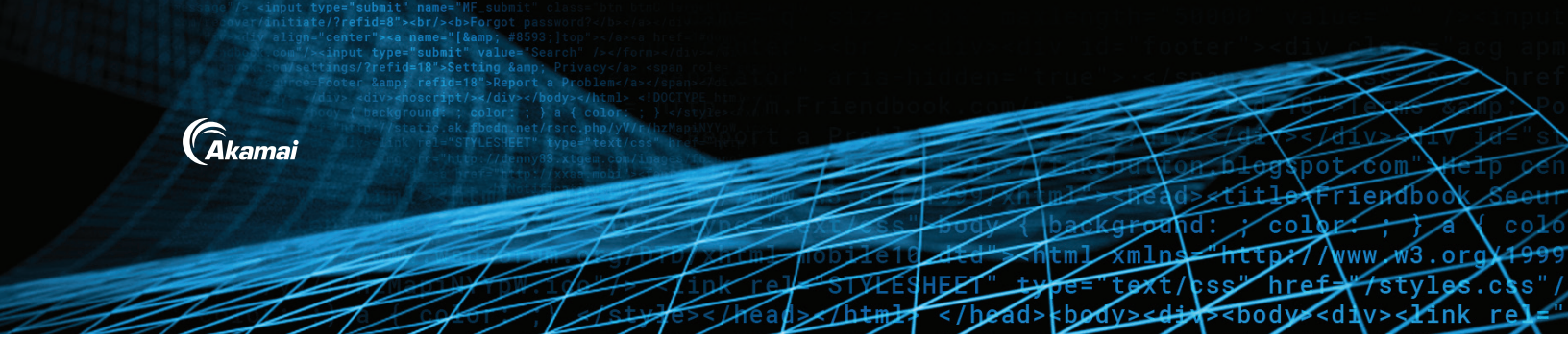
Emotet が組織にとって大きなリスクとなるのは、このグループがランサムウェア攻撃者とつながりを持つためです。Conti グループなどは、昨年の解散までに世界のさまざまな産業に影響を与えました。

データに見られる 2 番目に優勢な IAB が Qakbot です。このグループは Black Basta ランサムウェアグループと手を組んだことで知られています。報告によると、世界各地で 50 以上の組織がこのランサムウェアグループの影響を受けました。Qakbot チームは情報窃取の能力が高く、システムセキュリティの侵害を広める第 2 段階のマルウェアを配布することで知られています。調査によると、Qakbot は Cobalt Strike を利用することで、侵入後にさまざまな悪意ある活動を行い、被害者の環境内にバックドアを設置します。このツールはレッドチームが使用する正規のペネトレーションツールですが、敵対者によっても悪用されています。この手法は近年、IAB による利用が増加しています。MITRE ATT&CK フレームワークでは、この攻撃で Qakbot が利用する手法の詳しい情報を提供しています。

ボットネットのグループ

当社の分析によると、ボットネットは最大の脅威タイプであり、対象となる C2 トラフィックの 44% を占めています。このグループにはさまざまな攻撃者が見られ、いずれのボットネットも同じ性質を持つわけではないことに注意が必要です。比較的穏やかなものには、クリプトマイナーを植え付けるものや、被害者のマシンを利用して DDoS 攻撃を実行するものがあります。それだけでも代償が高く付きますが、私たちがエンタープライズ組織で見つけたボットネットはデータ漏えいやマルチステージ攻撃に利用可能なもので、より大きなリスクをもたらすおそれがあります。ボットネットはネットワークを横断して広がり、TrickBot のようにランサムウェアの展開に使用されるものや、情報窃取や認証情報の収集に特化したものがあります。

エンタープライズ組織で観測された最大規模のボットネット QSnatch はまさにこれを目的とし、ネットワーク接続デバイスから情報を盗み出します。私たちのデータによると、QSnatch は感染したデバイスの 36% に影響しています。このマルウェアがターゲットとする QNAP は、企業がバックアップやファイルストレージに使用する NAS デバイスの一種です。感染方法はいまだ不明ですが、調査員の推測によると QSnatch の感染経路として考えられるのは、ファームウェア脆弱性の悪用やデフォルトのユーザー名／パスワードを使用するデバイスへの総当たり攻撃です。QNAP を使用する企業には、ファームウェアを最新の状態に維持し（QSnatch に感染すると、パッチのインストールが妨げられ、セキュリティ製品が無効化される可能性があります）、デフォルトのパスワードをただちに変更することを強くお勧めします。QSnatch は攻撃者によって認証情報スクレイピング、パスワードロギング、リモートアクセス、データ漏えいなどに利用されます。貴重な情報が格納されたストレージデバイスは攻撃者の標的とされる可能性があります。これらのデバイスに侵入を許すと、ランサムウェア攻撃を受けた場合にバックアップがない状態で業務を進めなければならなくなります。攻撃の手法や対策については、こちらの CISA アラートで取り上げられています。



RaaS（Ransomware as a Service）グループ

私達の DNS トラフィック分析では、C2 マルウェアファミリーにーにアクセスする感染デバイスの 9% が RaaS グループに関連するドメインにアクセスしていました。このようなサイバー犯罪グループは、（技術知識のない者を含め）他の攻撃者を仲間に加え、使用料金と引き換えにランサムウェアソフトウェアを利用させます。ランサムウェア攻撃を受けた組織には、会社の機密データの損失に限らず、さまざまな被害が出ます。修復と回復のための費用や法務費用、罰金の支払いを余儀なくされる場合もあれば、サービス停止に伴って生産性が低下したり、ブランドや信用に傷がついたりする場合もあります。Cybersecurity Ventures によると、ランサムウェア攻撃のコストは 2031 年までに年間およそ 2,650 億米ドルにのぼると見られています。Akamai のグローバル・ランサムウェア・レポートもランサムウェアによる深刻な被害として、財務的な損失のほか、サプライチェーンの混乱を取り上げ、場合によっては生死に関わる問題にまで発展する可能性を指摘しています。

RaaS グループの中でも悪名高い犯罪集団 REvil は IT 管理ベンダーを標的としたサプライチェーン攻撃を仕かけ、1,500 を超えるマネージドサービス・プロバイダーに影響を与えました。その活動は、ロシア政府がメンバー数名を逮捕したことで停止しています。しかし、解散から数か月後、セキュリティ調査員は REvil のリークサイトが活動を再開し、米国の大学を含む最新の被害者の情報を提供していることを確認しています。調査員は、攻撃を仕かけたのは REvil ではない可能性があると推測し、痕跡を隠すために REvil を名乗っている可能性があると各国に警告しています。手口という観点で見ると、標的に合わせて攻撃の流れを REvil が調整することで知られ、標的についての彼らの知識レベルを伺うことができます。REvil の戦術、手法や手順について詳しくは、MITRE の記事でご覧いただけます。

> **貴重な情報が格納されたストレージデバイスは攻撃者の標的とされる可能性があります。これらのデバイスに侵入を許すと、ランサムウェア攻撃を受けた場合にバックアップがない状態で業務を進めなければならなくなります。**

DNS トラフィックの調査で見つかったもう一つの RaaS グループが LockBit です。Conti が「消滅」した後、LockBit グループは最も活動的な RaaS プロバイダーの一つになっています。こちらのレポートによると、それ以前の期間（2019 年 11 月～ 2022 年 3 月）に、この RaaS は被害を与えた組織数で Conti に続くポジションにつけていました。

LockBit は他の RaaS グループよりも高速な暗号化メカニズムを誇り、LockBit 2.0 で 12,000 社以上の企業に影響を与えたと主張しています。2022 年 6 月、グループは LockBit 3.0 をリリースし、バグ・バウンティ・プログラムなどの追加機能を加えています。また、同グループがターゲットへの初期アクセスを取得するために Log4j 脆弱性を悪用していることが報告されており、パッチ適用の重要性が強調されています。このようなセキュリティの欠陥に対処していない組織は、LockBit に感染するリスクが高くなる可能性があります。LockBit は進化し続けており、最近では三重の脅迫という新しい手口が加わっています。これは、ファイルが暗号化されてリークサイトに公開され、身代金の支払いを拒むと DDoS 攻撃を行うという手口です。

市場のツール

このセクションに取り上げるツールは、攻撃においてシステムへの侵入、情報の入手や特権の昇格まで、特定の役割を果たします。さまざまな攻撃者グループが編み出した手口は、infostealer や RAT のように、多くの場合に通信を行う必要があります。これらのツールをはじめ、攻撃者グループが用いる手法を理解することで、セキュリティ対策担当者は攻撃がどのように始まるのかを理解し、必要な対策を講じることができます。

Infostealer

ユーザー名やパスワード、システム情報、銀行認証情報、Cookie などのさまざまなデータの入手を目的とする infostealer は、攻撃に多く用いられる MaaS ツールの一つです。技術知識やスキルを持たない攻撃者でも、比較的安価に infostealer を入手して攻撃を仕かけることが可能です。

一連の C2 マルウェアファミリーの中で、既知の C2 にアクセスしたデバイスの 16% が infostealer と関連していました。Ramnit（感染したデバイスが 13%）もよく使われる infostealer です。高度にモジュール化しているという強みを活かして、攻撃者は他の機微な情報の窃取や他のマルウェアのダウンロード／展開などのさまざまな機能を最終目的に応じて使い分けたり、さらに進化した攻撃を仕かけたりすることができます。2021 年に Ramnit は銀行向けトロイの木馬の中でも首位にあげられており、最新のニュースによると他のマルウェアが Ramnit と類似のコードを使用していることが伝えられています。

ネットワーク内の infostealer の存在は、ユーザーの認証情報が盗まれるおそれのあることを知らせるサインです。盗まれた収集情報は闇市場で売買され、他の攻撃者が初期アクセスを獲得するために利用されます。ランサムウェアグループは、フィッシングやボットネットを通じて infostealer を展開して有効な認証情報を入手します。また、MaaS を提供する地下フォーラムで infostealer にアクセスするライセンスをレンタルすることもあれば、IAB を通じてネットワークアクセス権を購入することもあります。場合によっては infostealer のオペレーターが IAB となり、収集した高価値の認証情報（VPN や RDP のアクセス権など）を最高値で売ることや、さらに高度な攻撃を仕かける攻撃者に売ることもあります。

リモート・アクセス・ツール

Cobalt Strike は複数の攻撃者グループの活動に悪用されています。この強力な RAT を攻撃者が利用するさまざまな方法には、予備調査、特権昇格、ネットワークのラテラルムーブメント、永続化、侵入後のペイロードのリモート実行（ランサムウェアなど）、データ流出などがあります。主に侵入後のラテラルムーブメントやデータ流出のほか、スピアフィッシングモジュールによる初期アクセスベクトルにも利用されます。このツールを用いることで知られるグループには、Conti、Qakbot、TrickBot、Emotet などがあります。環境内の Cobalt Strike の検出に役立てるため、YARA ルールが設けられ、ツールを悪用しているかどうかの判別に用いられています。

当社のデータによると、Agent Tesla の C2 トラフィックの存在も確認されました。この RAT は闇市場で売られ、入手しやすい価格と使いやすさからサイバー犯罪者にとって魅力的なツールとなっています。攻撃者はこのツールで各種ブラウザーの認証情報の入手、キー入力やスクリーンショットのキャプチャ、キー入力の記録を行うことができます。その顕著な手法の一つであるフォームグラビングは、個人識別情報などの機密情報を収集する手口です。盗んだ情報は ID 盗難や詐欺に利用されます。PCrisk からは Agent Tesla の手法に関する詳細情報とユーザーへの影響が発表されています。

一年を通じて散発するマルウェアキャンペーン

年間を通じて見ると、C2 マルウェアの活動には、ばらつきが見られます（図 6）。典型的な例として、Emotet は、2021 年 11 月の活動再開を受け、2022 年 1 月、2 月に特に活発に活動していました。この活発化による猛攻撃で、Emotet は数か月の休止後に再び以前の地位に返り咲いています。再開後の数か月で、Microsoft による VBA（Visual Basic for Applications）マクロ無効化を回避するというように手法が強化されています。いくつかのレポートによると、Emotet は 2022 年 7 ～ 11 月に再び活動を休止したとされています。私たちのデータでも 7 月には C2 トラフィックが減少し、Emotet のドメインにアクセスする感染デバイスの割合が減っています。このことは、グループの活動が年中続いていたか、あるいはインストールされたマルウェアが以前の古いインフラと通信を続けている可能性を示しています。2023 年の観察により、Emotet グループが本当に休止したかどうかが判断できるでしょう。

上位の C2 脅威別に見た月ごとのデバイスの割合
2022 年 1 月～ 2022 年 12 月

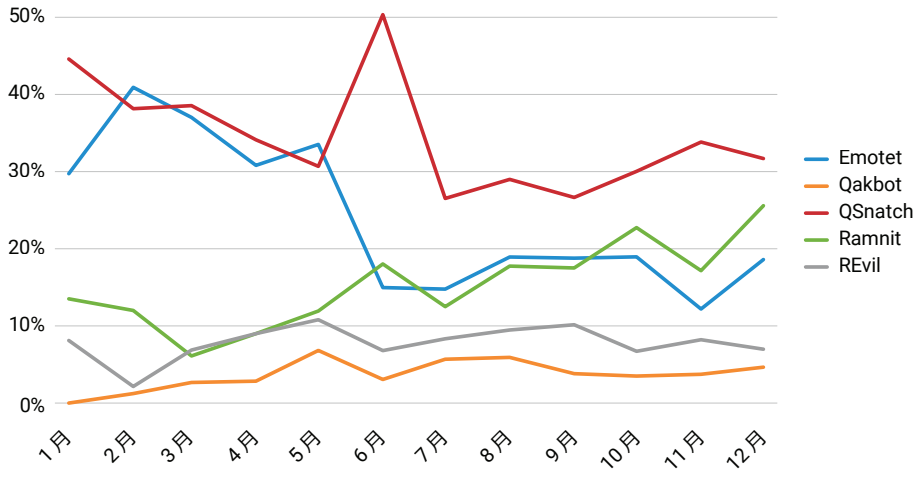


図 6：月別のトレンドグラフから、2022 年を通じて QSnatch が活発であったことが分かる

> **Emotet の活動は 2021 年 11 月の活動再開を受け、2022 年 1 月、2 月には活発に活動しています。この活発化による猛攻撃で、Emotet は数か月の休止後に再び以前の地位に返り咲いています。**

QSnatch は年間を通じて常に活発な状態で、6 月付近をピークにその脅威の広がりが伺えます。NAS サーバーが攻撃者の標的に選ばれるのはいくつかの理由があります。まず、機微な情報が含まれていること。第 2 に、NAS サーバーはパッチが適用されている可能性が低いこと、第 3 に、組織のネットワークで比較的アクセスがしやすく、ラテラルムーブメントのハブとして利用できることがあげられます。セキュリティソリューションの搭載など、この数年で変化も見られますが、サイバー犯罪者はインストールされたセキュリティ製品の無効化や新しい修正による更新の阻止などにより対策を回避しています。このため、これらのデバイスは新種のマルウェアに対して脆弱なままとなります。

データからは、8 ～ 12 月にかけて企業ネットワークにおける Ramnit の増加も見られます。このマルウェアはさまざまな機密情報を盗み出し、情報が他の攻撃者に売られて将来の攻撃につながるおそれがあることから、これは懸念すべき状況です。

QSnatch と Emotet：全地域に共通の脅威

地域ごとの脅威の広がりを知るため、私たちは C2 ドメインにアクセスする各地域のデバイスの割合を調べました（図 7）。それぞれの割合は、地域ごとのデバイス数を基準にしているため、影響を受けたデバイスの数も地域によって違いがあります。興味深いことに、攻撃にはわずかな違いはあっても全地域で似た傾向があります。このため、各地域とも「まとめと提案」のセクションの提案事項やマルウェアグループについての前述のセクションに記された提案事項を参考にしていただきたいと思います。

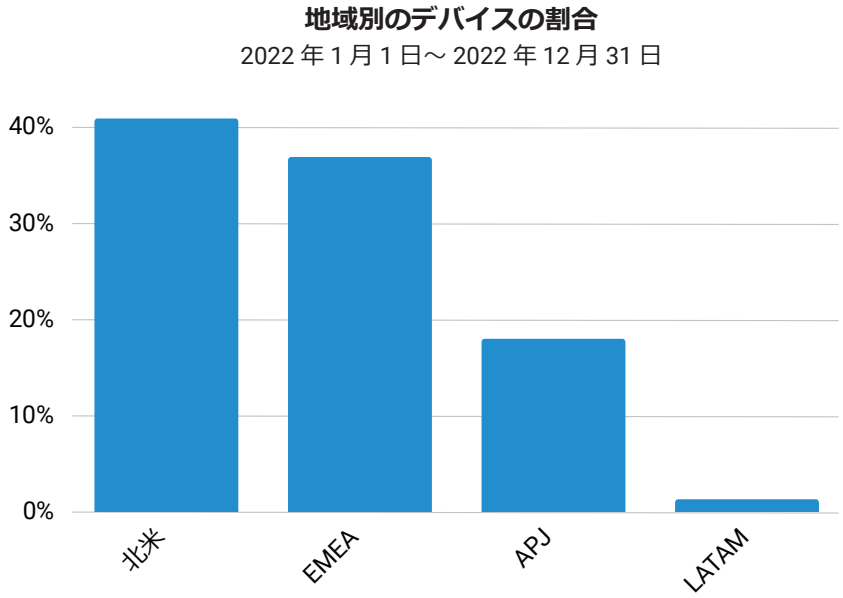


図 7：影響を受けたデバイス数を地域別に見ると、北米が最も多く 41%、次いで EMEA（37%）、APJ（18%）

北米

世界各国の多くの組織が苦慮している最大の脅威グループが QSnatch と Emotet です。北米地域では、影響を受けたデバイスの約 29% が Emotet、33% が QSnatch の攻撃を受けていました（図 8）。Dark Reading のレポートによると、Shodan 検索にあがる 300,000 台の QNAP インターネット接続デバイスは格好の標的ということです。さらに、QNAP などの NAS デバイスはバックアップに使用され、メディアサーバーやファイルサーバーとして利用可能なデバイスです。

その他にも北米地域で注目すべき脅威として Ramnit、Qakbot、REvil があげられます。これは、Emotet のような IAB がランサムウェアなど、他の感染手法を採用することを考えると興味深い点です。

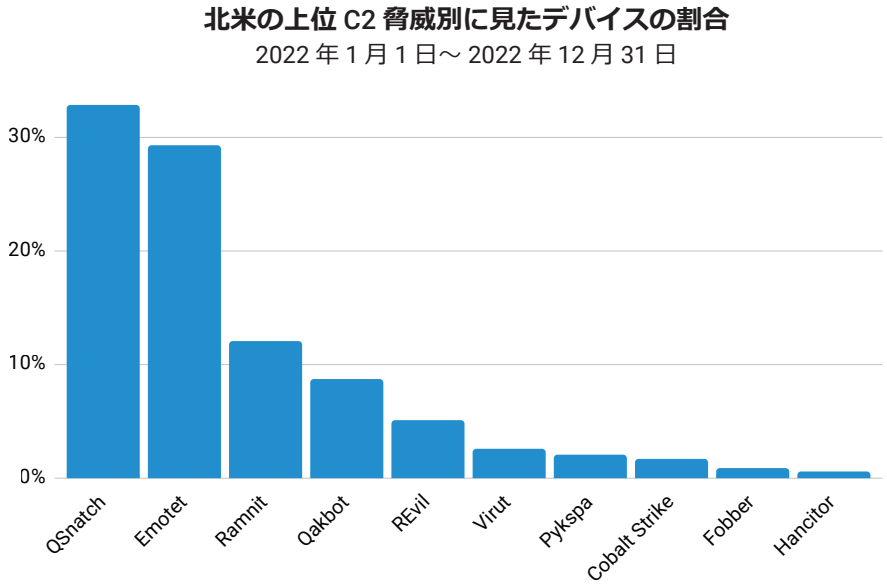


図 8：北米地域の組織で影響を受けたデバイスの大多数が QSnatch、Emotet、Ramnit に関連するドメインに一度以上アクセスしている

ヨーロッパ・中東・アフリカ

EMEA は北米に次いで影響を受けたデバイスの割合が多い地域です。地域内の上位の脅威（図 9）には QSnatch（28%）、Ramnit（21%）が含まれます。この地域での Ramnit の活発な動きは、オペレーターが過去にイタリア、英国、フランスの銀行と金融機関を標的としたこともあり、特に驚くことではありません。その標的の一つとして、EU 諸国が主要ターゲットとなっていました。実際、Ramnit の影響を受けたデバイスの数を全世界で比べると、いまだに EMEA 諸国が最大規模の感染数となっています。それに加えて、同地域は Emotet による感染も 19% と高い水準です。

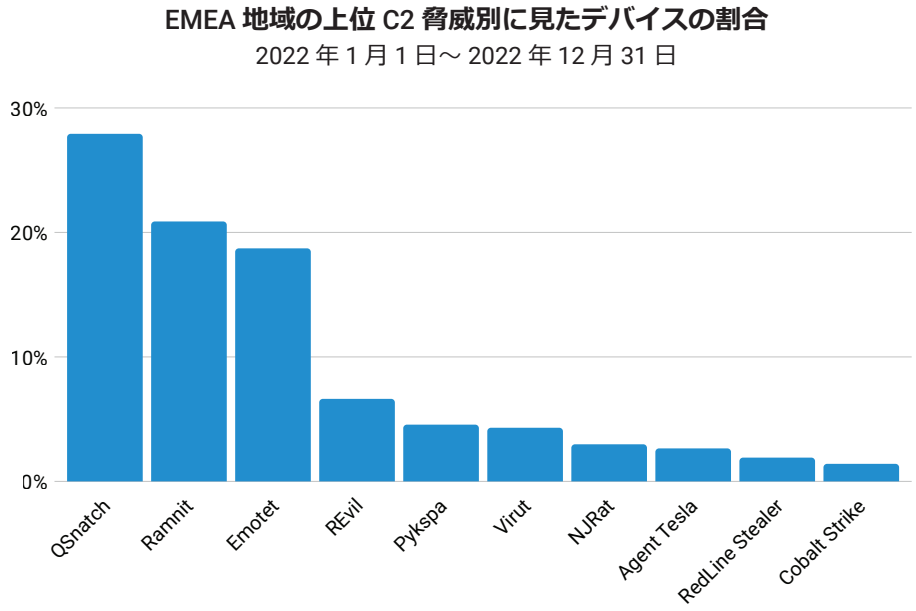


図 9：EMEA は他地域よりも Ramnit の C2 関連ドメインにアクセスするデバイスが多く、組織のリスクが特に高い

アジア太平洋および日本

APJ 地域では QSnatch の感染が大きな影響を与えています（図 10）。各地域の感染数を比較すると、この地域は QSnatch に感染したデバイス数が北米に次いで第 2 位となっています。一方、APJ 地域は、REvil や LockBit といったランサムウェアにも注意する必要があります。どちらも、この地域で影響を受けたデバイスで見られた脅威の中でも上位 5 位に入っています。昨年には REvil のメンバーが逮捕されましたが、その数か月後にはこのマルウェアによる攻撃が確認されています。コードにアクセスできる旧メンバーが REvil を復活させようとしている可能性もあります。LockBit や REvil など（主に金銭を目的とする）ランサムウェアの脅威の存在は、もはや驚くような話ではなくなってきました。RaaS オペレーターが Emotet などの IAB を利用し続ける限り、ランサムウェアは各業界や地域の企業にとって重大なセキュリティ課題であり続けるでしょう。

APJ 地域の上位 C2 脅威別に見たデバイスの割合

2022 年 1 月 1 日～ 2022 年 12 月 31 日

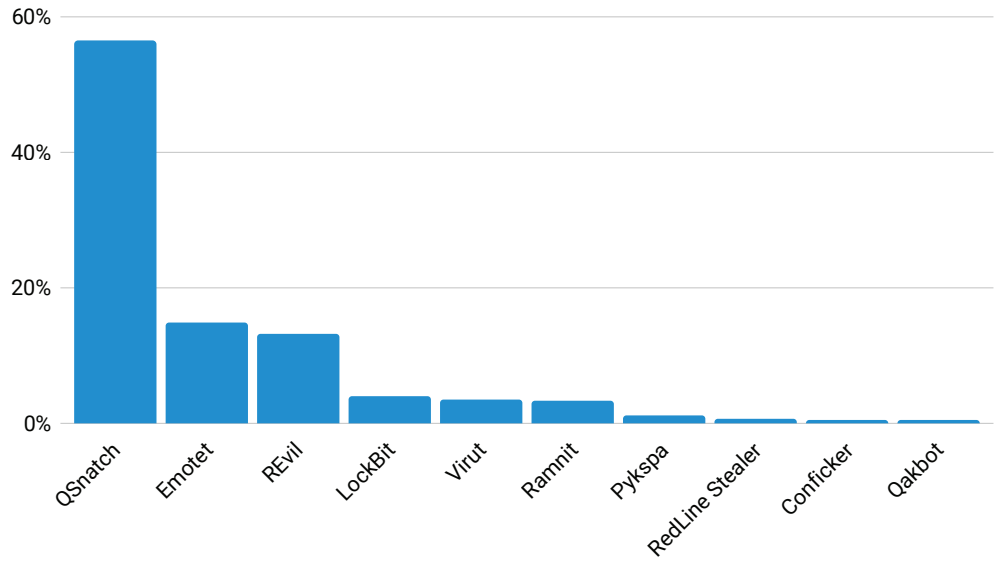


図 10：地域内で QSnatch の感染が多数確認された

ラテンアメリカ

続いて LATAM 地域の傾向を見てみましょう。ここは影響を受けたデバイスの数が最少の地域ですが、標的にされることが少ないというわけでも、影響を受けないというわけでもありません。世界的な傾向と同じく、QSnatch と Emotet による影響を受けています（図 11）。この地域を調べただけでも、Agent Tesla、Virut、Ramnit が有力な脅威となっていることがわかります。

LATAM 地域の上位 C2 脅威別に見たデバイスの割合

2022 年 1 月 1 日～ 2022 年 12 月 31 日

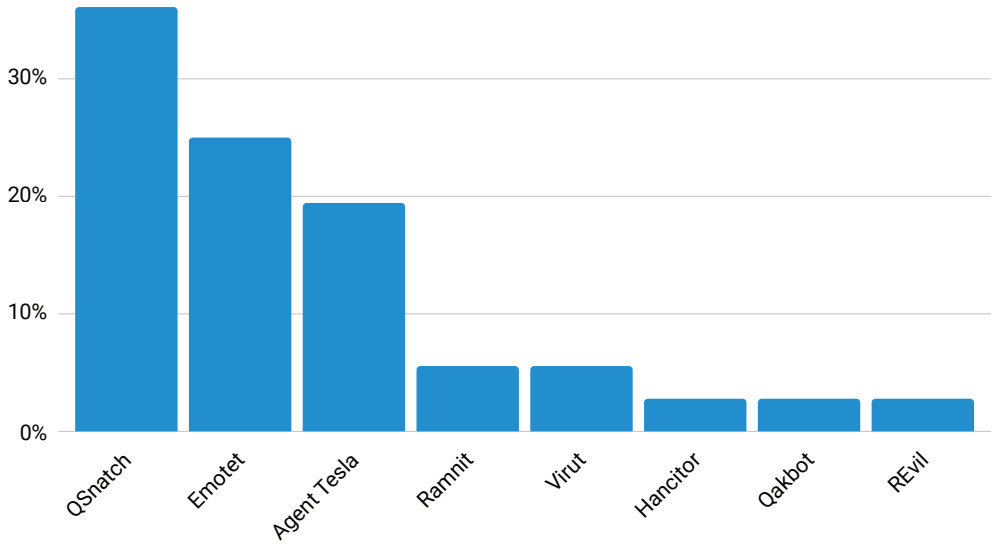


図 11：LATAM 地域とも一致する世界的な傾向

地域ごとの内訳は、類似点を見つけるだけでなく、それぞれの地域に特有の脅威を見つけるためにも重要です。QSnatch は常に最上位の脅威ファミリーですが、これに次ぐ上位 4 つの脅威は、地域によって変動があるものの Emotet、REvil、Ramnit、Agent Tesla の組み合わせです。地域ごとの脅威の違いに基づいて、どのような脆弱性管理を行い、侵入テストチームが何に注力すべきかを判断することができます。

業界・業種別のトレンド：IAB とボットネットの影響が大きい製造業

業界ごとにトレンドを分析することで、各業界のリスクのレベルと、業界どうしの比較を確認することができます。ここでは影響を受けたデバイスの数でなく、顧客毎にデバイス数を集約して業種別に影響を受けた企業数を割り出しています（図 12）。収集した DNS データによると、悪性の C2 トラフィックの影響を受けた組織の 30% 以上が製造業でした。さらに、ビジネスサービス（15%）、ハイテク（14%）、商業部門（12%）も影響を受けています。当社の DNS データに基づく上位 2 業界（製造およびビジネスサービス）は、Akamai のグローバル・ランサムウェア・レポートで分析した Conti ランサムウェアの被害を受けた上位業界とも一致しています。そのレポートでは、Conti ランサムウェアの被害を受けた企業を詳しく分析し、業種、収益、地域別に分類して、存在感を増しているこの脅威の攻撃のトレンドを明らかにしています。

> **収集した DNS データによると、悪性 C2 トラフィックにより影響を受けた組織の 30% 以上が製造業部門でした。さらに、ビジネスサービス（15%）、ハイテク（14%）、商業部門（12%）も同様に影響を受けています。**

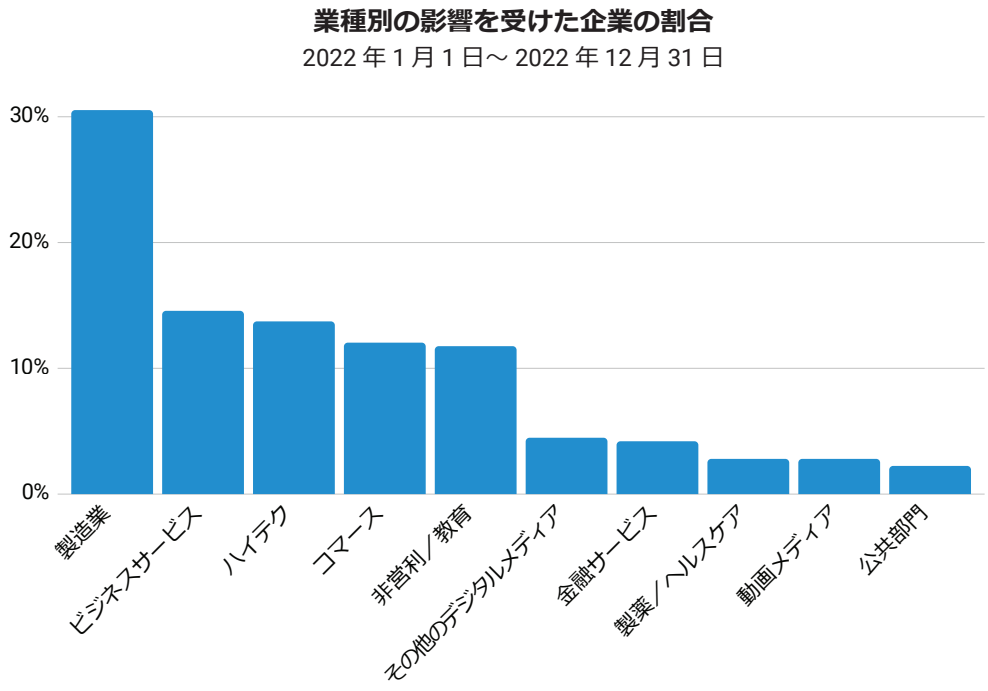


図 12：製造、ビジネスサービス、ハイテクは C2 感染の影響を最も受けている産業

製造業が各種の C2 攻撃に大きく影響を受けている事実は、この業界が重要な社会基盤であり、攻撃の成功によりサプライチェーンの混乱など実世界への被害が起きる可能性があることから懸念すべきことです。データからは製造業への影響が最も大きい理由を見つけることはできませんが、この業界における脅威タイプを詳しく調べることで何かヒントが得られるかもしれません。

いくつかの国では、製造などの重要産業のセキュリティを強化する規制を導入しています。EU 全域の NIS2 規制はサイバーセキュリティ基準とセキュリティ要件を強化するもので、リスク分析や情報システム・セキュリティ・ポリシー、サプライ・チェーン・セキュリティ、主要機関（エネルギー、輸送、銀行、保健など）のインシデント管理を規制しています。対象となる業種も広くカバーしています。

製造業の上位 C2 脅威別に見たデバイスの割合
2022 年 1 月 1 日～ 2022 年 12 月 31 日

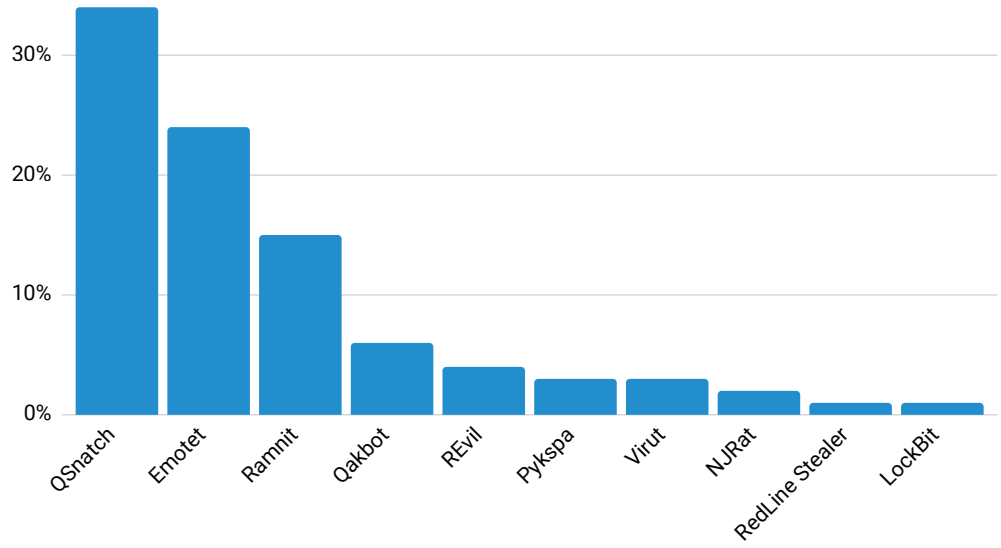


図 13：製造業における C2 脅威ファミリーの
うち上位にランキングされるのは QSnatch、Emotet、Ramnit

製造業界を詳しく見ると、この業界の組織がアクセスする C2 関連ドメインの上位に、QSnatch、IAB、Ramnit が入っています（図 13）。組織のネットワークに IAB が存在することは、攻撃者が潜在的な標的の情報を集めており、マシンに侵入してアクセスが可能になれば、RaaS グループなど他のサイバー犯罪者にデータが売られることを意味するものと考えられます。さらに、この業界の脅威となる C2 マルウェアのリストには infostealer も含まれます。注意したい脅威の一つである RedLine Stealer は、認証情報やクレジットカード情報などのブラウザー情報を収集することができ、今では毎月 100 ～ 150 ドルのサブスクリプションで購入可能な MaaS となっています。Group-IB の調査によると、この infostealer は 2021 年下半期から 2022 上半期までに SSO アカウントを含む可能性のあるログを推計 35,585,412 件集めたと見られています。また、この infostealer に関連する C2 ドメインは 2022 年第 3 四半期だけでも 409% 増加しています。

業界のトレンドには常にアンテナを張っておく必要があります。サイバー犯罪者はあらゆる業界に攻撃の手を広げることから、ある業界で起きていることは多くの場合、ほんの足がかりにすぎません。ある業界で最も利用されているテクノロジーに攻撃が集中することもあれば、お金を払ってくれる可能性が高い対象や、最高値が付きそうな対象が狙われることもあります。これまでにサイバーセキュリティにあまり投資をしてこなかった業界への攻撃も見られています。重要なのは、隣家からの煙を見たら自分の家の火災予防システムを点検するのが良策であるということです。

ホームユーザーへの攻撃

攻撃者がエンタープライズ組織を標的とするのは、ネットワークへの侵入が成功すれば多額の見返りが得られるからです。さまざまなツールや手法を使い、エンタープライズ組織を周囲から侵害して潜り込み、機密情報を盗み出すこともあります。こうした企業ネットワーク内の infostealer や IAB などの脅威については先のセクションで説明したとおりです。しかし、家庭のネットワークでは、どのような脅威が用いられてどんな結果になるのか、状況が異なります。

ホームユーザーは多くの場合、企業環境ほどセキュリティが高くないのが特徴ですが、これらのユーザーからは企業ほどの見返りは得られません。攻撃者はこのことを理解しており、家庭の機器により簡単に感染する能力から利益を得る方法を探しています。例えば、可能な限り多くのデバイスに感染させようとターゲットを絞らずにばらまくという大規模なキャンペーンを展開する一方、企業には的を絞った攻撃をします。これらの家庭機器が大規模なボットネットの一部となると、これらのゾンビデバイスを利用して無数のサイバー犯罪活動を実行します。ユーザーが知らない間に、スパムや DDoS 攻撃などを組織に仕かけるのです。また、ボットネットの攻撃を成功させるか、サイバー犯罪者に自分のボットネットを使ってもらうためには、可能な限り多くのデバイスを感染させる必要があります。そのほかにも、攻撃者がホームユーザーを攻撃して利益を得る手法として、感染したデバイスをクリプトマイニングの演算リソースとして使うという方法もあります。

> **これらの機器が大規模なボットネットの一部となると、これらのゾンビデバイスを利用して無数のサイバー犯罪活動を実行します。ユーザーが知らない間に、スパムや DDoS 攻撃などを組織に仕かけるのです。**

ボットネットからの大量のトラフィックを示すホームネットワーク

焦点をホームユーザーに移し、ホームネットワークの悪性 DNS トラフィックを調査するために、過去 6 か月間に悪性のフラグが付けられた数百万のクエリーの匿名サンプルを分析し、どのような脅威に注意すべきかを明らかにしました。一目して上位の脅威はボットネットが関係し、攻撃者がさまざまな目的で IoT を利用していることが伺えます。以降のセクションでは、この点について説明をします。

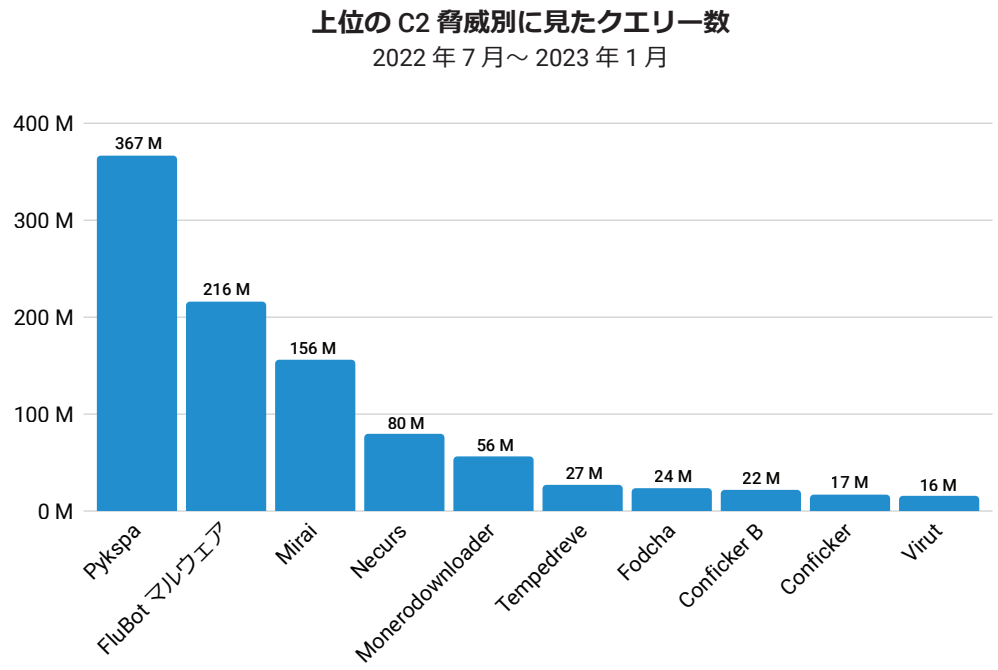


図 14：ホームネットワークの DNS トラフィックに見られるボットネットのうち上位にランキングされるのが Pykspa、FluBot マルウェアと Mirai

Pykspa：ソーシャルメディアから伝播

データを調べた結果、Pykspa は全世界でフラグ付き DNS クエリーが 3 億 6,700 万件にのぼりました（図 14）。この脅威は Skype から広がり、影響を受けたユーザーの連絡先に悪性リンクを送ります。状況によっては、Twitter をブラウザーのタブで開くと、マルウェアへのダウンロードリンクを含むツイートが作成されることもあります。また、C2 通信を確立するためにドメイン生成アルゴリズム（DGA）も利用します。過去に、その v2 が DGA のサブセットを用いて検出を回避し、ネットワークに長期間潜んでいたことが確認されています。

攻撃者はバックドア機能を使用してリモートシステムに接続し、ファイルのダウンロードやプロセスの終了といった任意のコマンドをさまざまな方法（ドライブのマッピングやネットワーク共有など）で実行します。Pykspa は Skype 設定にもアクセスしてユーザーの個人情報を収集します。特にマルウェア対策ソリューションに関連する文字列などを含む特定の Web サイトへのアクセスも妨げようとします。面白いことに、このマルウェアはユーザーの Skype のインターフェース言語を調べ、英語、ドイツ語、フランス語、スペイン語、イタリア語を含む対象言語であれば、その言語でスパムメッセージを発信します。

FluBot：Android が対象のマルウェアボットネット

FluBot マルウェアは Pykspa に次ぐ C2 マルウェアです。主にテキストメッセージ経由で Android スマートフォンに感染し、ユーザーに悪性リンクのクリックを促してマルウェアをダウンロードさせようとします。伝播手法として、FluBot マルウェアはユーザーの連絡先リストを C2 サーバーにアップロードするほか、同様のソーシャルエンジニアリング手法によりユーザーの連絡先も送信します。FluBot がデバイスに存在する場合、ユーザーの銀行情報や財務情報が流出するリスクがあります。このマルウェアは、ユーザーが正規の銀行アプリにアクセスすると、代わりに偽のページを表示します。こうして、これらの認証情報が個人情報の盗難や詐欺取引に利用されるおそれがあります。

このマルウェアはさまざまなソーシャルエンジニアリング手法を利用します。例えば、ユーザーに荷物の配送状況を確認するリンクをクリックさせたり、ボイスメールがあることを知らせて偽のボイスメールアプリをダウンロードさせるという手口があります。また、偽のセキュリティ更新通知を送り付け、そのリンクをクリックするように仕向けるという手口もあります。ユーザーがリンクをクリックすると、アプリをダウンロードするよう指示が出ます。するとアプリは連絡先リストへのアクセスや通話などの許可を求めてきます。この脅威が特に危険であるのは、アクセシビリティサービスの許可を要求して攻撃者が画面のタップ操作を制御できるということです。そうなると、さらにアプリをインストールできるようになります。このマルウェアを除去するためには、デバイスを出荷時の状態にリセットする必要があります。

Mirai：IoT デバイスの能力を大規模な攻撃に利用

当社の調査では、Mirai は FluBot マルウェアに僅差で続き、フラグ付きの DNS クエリーは 1 億 5,600 万件でした。telnet ポートが接続可能な状態になっている IoT デバイスを標的とする Mirai は、最大手の DNS プロバイダーへの DDoS 攻撃によって知られるようになりました。この自動で伝播するワームの標的になるデバイスは、デフォルトのユーザー名とパスワードを使用している脆弱なデバイスです。一時は 100,000 台以上のゾンビデバイスを生み出し、攻撃者がこれを利用してハイプロファイルのターゲットに DDoS 攻撃を仕かけていました。以前の攻撃では 145,000 台のデバイスを利用してテクノロジー攻撃を実行しています。これは、脆弱なデバイスが不正なデバイスと化してサイバー攻撃に利用され、エンタープライズ組織の大規模な混乱を招くおそれがあるという例の一つです。

2016 年、Mirai の背後のグループがソースコードを公開しましたが、これは法執行機関がオリジナル版の作者にたどり着く（そして逮捕する）のを妨げるためと思われます。これをきっかけに他のグループが Mirai のコードを使い始め、システムへの感染を可能にするなどの修正や機能強化を追加しています。コードを公開したことにより、新たな変種の Okiru、Satori、Masuta、PureMasuta など、DDoS 攻撃を意図したものも加わるようになりました。感染したデバイスを再起動することも効果はありますが、マルウェアは絶えずデバイスをスキャンしているため、パスワードを変えない限り再度感染する可能性があります。

Necurs：マルウェア配布とアクセス権の販売

Necurs ボットネットは 2012 年にはじめて確認され、過去 6 か月のフラグ付きクエリーは 8,000 万件でした。Dridex、TrickBot、Locky などの他のマルウェアペイロードを配布する機能を持ち、家庭と組織にとって深刻な脅威となります。このボットネットについて特に注目すべきもう一つの点は、感染したコンピューターへのアクセス権を売ることで他のグループがレンタルボットネットを利用した攻撃を行えるようになることです。多くのボットネットと同様、DGA を使用して複数のドメインに C2 サーバーを展開し、ブロックされたドメインがあっても攻撃を続けることが可能です。

ランサムウェアや銀行向けトロイの木馬の配布だけでなく、Necurs はロシアのデート詐欺、偽薬物販売などのさまざまなスパム攻撃にも使用されています。調査の間、Microsoft がこのボットネットの動きを監視したところ、わずか 58 日のうちに約 380 万件のスパムメールメッセージが送られていました。2020 年の法執行機関とセキュリティコミュニティーとの連携により、Necurs ボットネットの活動は排除されました。

Monerodownloader：マイニングボットネット

攻撃者が利益を得るために用いる多くの手法の一つに、クリプトマイニング用のマシンに侵入して利用する方法があります。仮想通貨 Monero がサイバー犯罪者に人気を高めていることは、この通貨を入手するボットネットが増えている理由の一つです。攻撃者がこの通貨を好むのは、チェーンの閉鎖性と匿名性から追跡されにくいことが理由です。Monerodownloader については情報が少ないものの、その手法として情報の収集やペイロードを送信する C2 サーバーへの接続などが含まれます。

パッチが未適用のシステムは、Monero クリプトマイナーなどの脅威の影響を受けます。他の同様の Monero 通貨マイナーも脆弱性を悪用し、無料ソフトを装ってマイナーをダウンロードさせ、ネットワークを横断して他のデバイスを感染させて多額の金銭を得るものがあります。このラテラルムーブメントはホームユーザーよりも企業環境に多く見られるものの、この手法からクリプトマイナーが感染規模を最大に広げようとしていることが伺えます。

地域別上位の脅威：ボットネットによるホームネットワークへの影響が続く

ここで地域別のデータから、ホームネットワークの DNS トラフィックに基づく地域別のボットネットの活動を明らかにし、この傾向に寄与するいくつかの要因を考えてみます。

北米

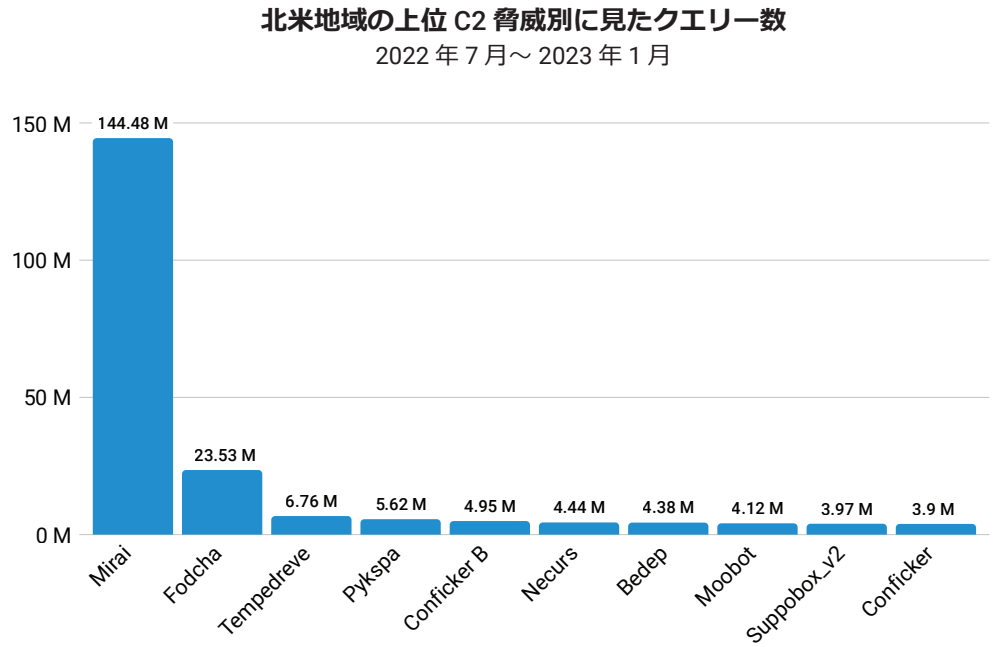


図 15：Mirai が北米で脅威であり続ける理由として、脆弱な IoT デバイスの存在が考えられる

北米では、Mirai ボットネットに関連する 1 億 4,400 万件以上のクエリーがホームネットワークで発生しています（図 15）。このボットネットは、ユーザー名とパスワードがデフォルトのままの脆弱な IoT デバイスを標的とします。この地域から大量のクエリーが送られるのは、家庭内での IoT デバイスの人気が高く利用の多いことが理由と思われます。2022 年だけでも米国では世帯あたりのネットワーク接続デバイスは平均 22 台にのぼるという報告があります。この数字は前年の 25 台よりやや減少しています。北米の IoT デバイスによる接続は増加が予測され（2025 年までに 54 億）、脆弱な IoT デバイスを悪用する Mirai や同種のマルウェアの脅威が増す可能性が高い状況です。

ホームユーザーに与えるこれらの脅威の影響として、サイバー犯罪者が家庭機器を利用し、ユーザーの知らないうちに犯罪が行われることがあげられます。しかし、組織においても DDoS 攻撃をはじめ、Mirai などのボットネットから行われる悪性のスパムキャンペーンも深刻な問題です。最善の対策として、機器のデフォルトのユーザー名とパスワードを必ず変更し、Mirai や同種の攻撃から保護することが重要です。

ヨーロッパ・中東・アフリカ

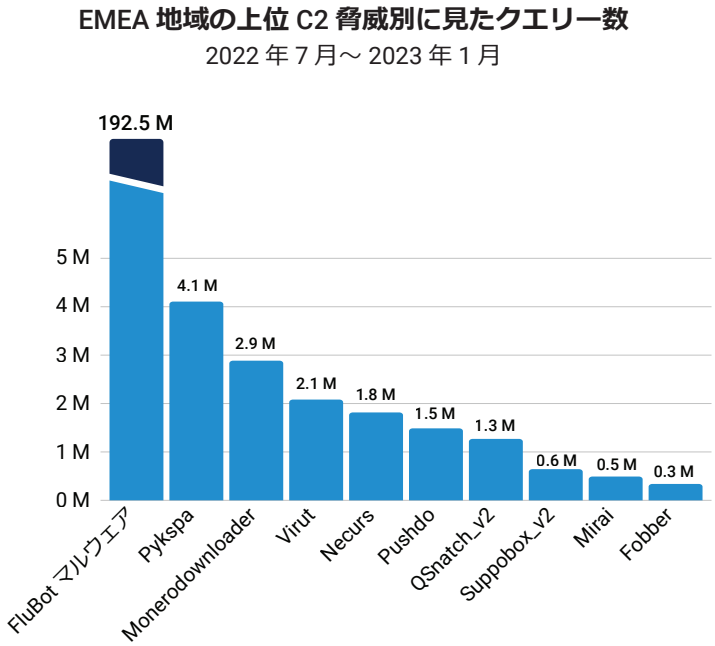


図 16：EMEA 地域における FluBot マルウェア感染の原因としては、その伝播の手口の巧妙さと複数の欧州言語を利用したソーシャルエンジニアリング手法が考えられる

FluBot マルウェアが山火事のように EMEA 地域に広がっていると言っても過言ではない状況です。この地域に見られる大量の DNS クエリー（約 1 億 9,300 万）は際立っています。Akamai による DNS トラフィックの調査から、これらの感染が EMEA 地域で発生していることが分かりました（図 16）。一つの要因として、攻撃者が連絡先リストに SMS を送るフィッシング手法であるスミッシングの広がりがあります。さらに、これはパッケージ配布に関連したアプリや本当はマルウェアであるボイスメールアプリをダウンロードさせようと試みます。このほかにも、FluBot は追加の権限を要求し、ユーザーに気づかれずに銀行や金融機関の認証情報を記録します。報告によると、スペイン、ドイツ、フィンランド、英国などのユーザーが標的になっています。SMS が EU 圏の他の複数の言語（ドイツ語、ハンガリー語など）でも書かれていることも、このマルウェアが欧州で拡大している多くの要因の一つです。

ラテンアメリカ

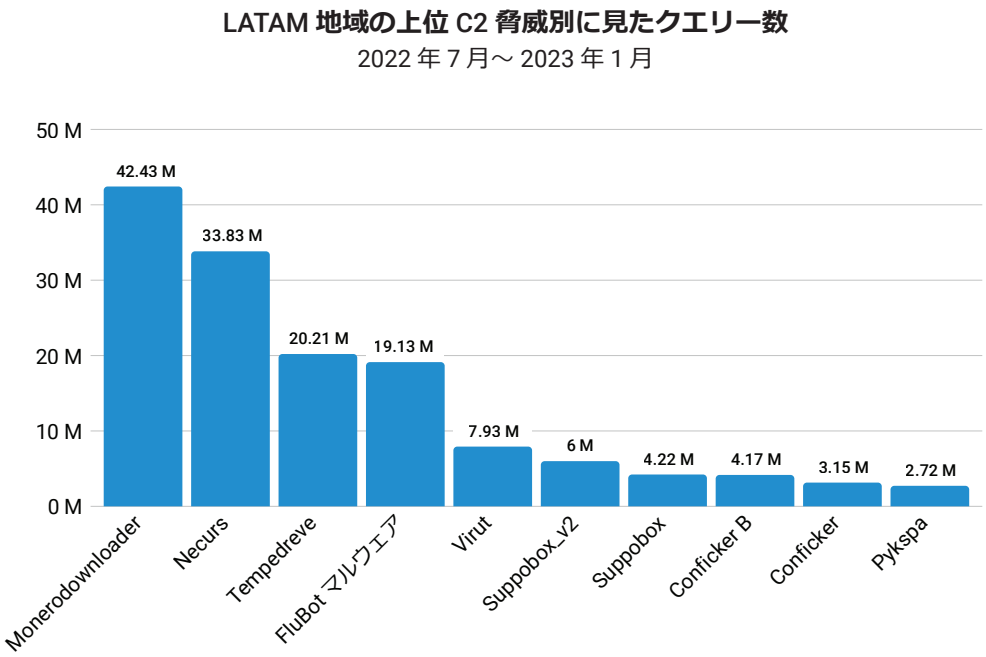


図 17：ラテンアメリカ地域で Monerodownloader クリプトマイニングボットネットが上位の脅威になるのは、仮想通貨の使用率が高いことが要因と思われる

北米や EMEA と異なり、LATAM 地域はさらに多くの形でボットネットが広がっています（図 17）。クリプトマイニングボットネットの Monerodownloader はフラグ付きクエリーが 4,200 万と、活発なボットネットグループのリストの最上位にあり、これに Necurs（3,400 万）、Tempedreve（2,000 万）が続きます。この地域はインフレ率が高く振込払いが多いことから仮想通貨の利用率が高く、これが Monerodownloader などのボットネットが上位を占める理由と考えられます。サイバー犯罪者はユーザーに気づかれることなくデバイスをマイニングに悪用し、金銭を得ることができます。また、DNS トラフィックに見られる上位の脅威に FluBot があがるということは、トラフィック量の多い EMEA 地域外にもこのボットネットが広がっていることを示しています。

アジア太平洋および日本

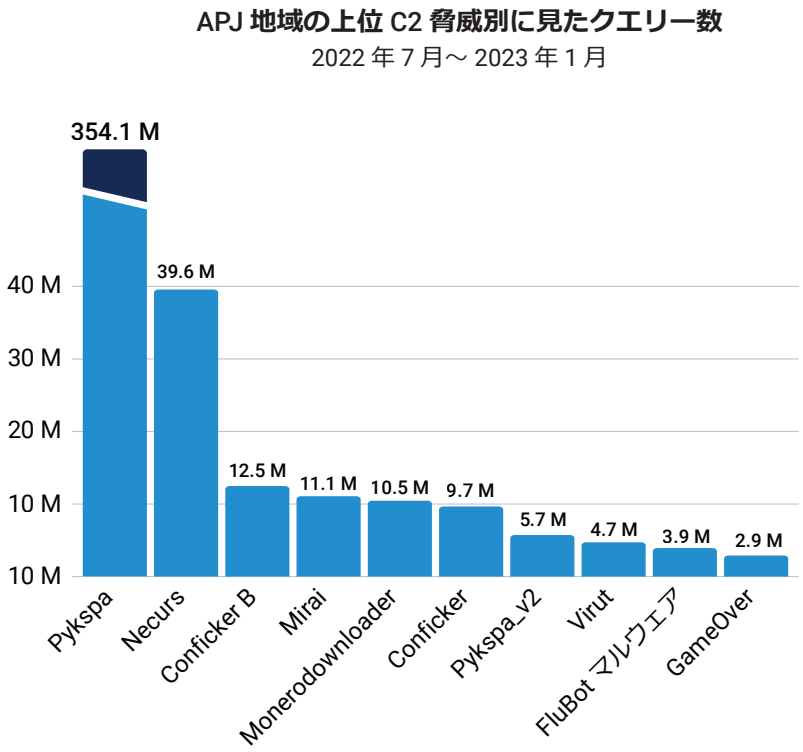


図 18：APJ 地域で大きな脅威となっている Pykspa と Necurs

APJ 地域では Pykspa に関連するクエリーが 3,500 万件以上にのぼります（図 18）。2019 年のブログ記事で、Pykspa が選択式の DGA メカニズムを利用して長期間検出を逃れていることを取り上げました。記事にあげたドメインは主に東アジア地域で見つかったものでした。Necurs などのボットネットに関連するクエリーが見られたことも、システムが他のマルウェアに感染していることの大きな兆候です。

フィッシングの現状に関する概要

DNS トラフィック分析の最終パートでは、フィッシングキットと、フィッシングキャンペーンを成功させる上でのフィッシングキットの重要な役割について見ていきたいと思います。フィッシングが今なお、これまで以上に活発であることは、攻撃者の手法が進化を続け、多くの個人情報がオンラインにあふれている状況を反映しています。攻撃者はフィッシングを本物らしく見せるソーシャルエンジニアリングの手法を用いています。そしてデータは、これらの攻撃の成功率が依然として高いことを示しています。Akamai がホリデーフィッシング詐欺について調べた結果、発見を逃れ続けるための新たな手法や戦術が明らかになりました。今までにない手法として、偽の「ユーザーの声」を利用した詐欺や、HTML のアンカーを使う新しい手法で有効なユーザーのみを詐欺サイトにアクセスさせるものがあります。

コロナ禍よりテレワークが増えたこともフィッシング攻撃の検知防止を難しくしており、個人と組織は常に警戒をして自らを守るステップをとることの重要性が増しています。さらに、ソーシャルメディアの拡大とインターネット接続デバイスの増加も攻撃者にとって機会を拡大する要因です。

金融サービスを狙うフィッシングキャンペーン

フィッシング詐欺で悪用／なりすましの被害を受けた企業を調査するにあたっては、いくつかの方法でデータ収集が行えます。キャンペーンの総数と被害者の数を相関付けました。これにより、特定のフィッシングキャンペーンの成功率と、標的となっている業界の割合を確認できます。

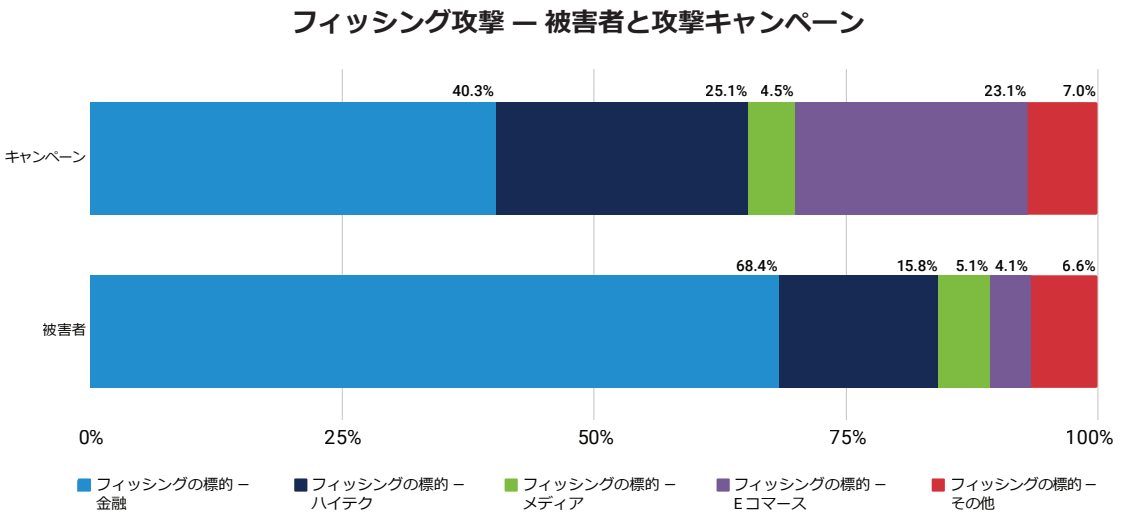


図 19：大多数のフィッシングキャンペーンが金融サービス業界を標的としている（2022 年第 4 四半期）

私たちの調査では、金融とハイテク部門がキャンペーンの数と被害者の数とも上位に位置しています（図 19）。金融サービス機関の顧客を標的とするキャンペーンは 40.3%、被害者は 68.4% となっており、2022 年第 4 四半期には金融サービスに対する攻撃が大きな効力を発揮していたことを示しています。金融サービス関連のレポートの「差し迫る敵：金融サービスに対する攻撃の分析」では、フィッシング攻撃が金銭獲得を目的とし、主に金融サービスとその顧客を標的することに注目しています。これらの攻撃を受けると、ブランドや信用に傷がつき、顧客の信頼を失うなどの影響が出ます。フィッシングは問題修正のための組織のリソースも費やします。

e コマース分野へのフィッシングキャンペーンは 2022 年第 4 四半期に 23% の割合でした。実際の被害者よりもキャンペーンの数が多いものの、この業界が標的とされていることには注意が必要です。ユーザーは、個人情報や銀行情報を狙うサイバー犯罪者に警戒する必要があります。

フィッシングツールキット：フィッシング詐欺の支援ツール

大規模フィッシング攻撃を可能にしているのが、フィッシングツールキットの存在です。フィッシング Web サイトの展開と保守にフィッシングツールキットを使用することで、技術知識がなくてもフィッシング攻撃を実行できるようになります。

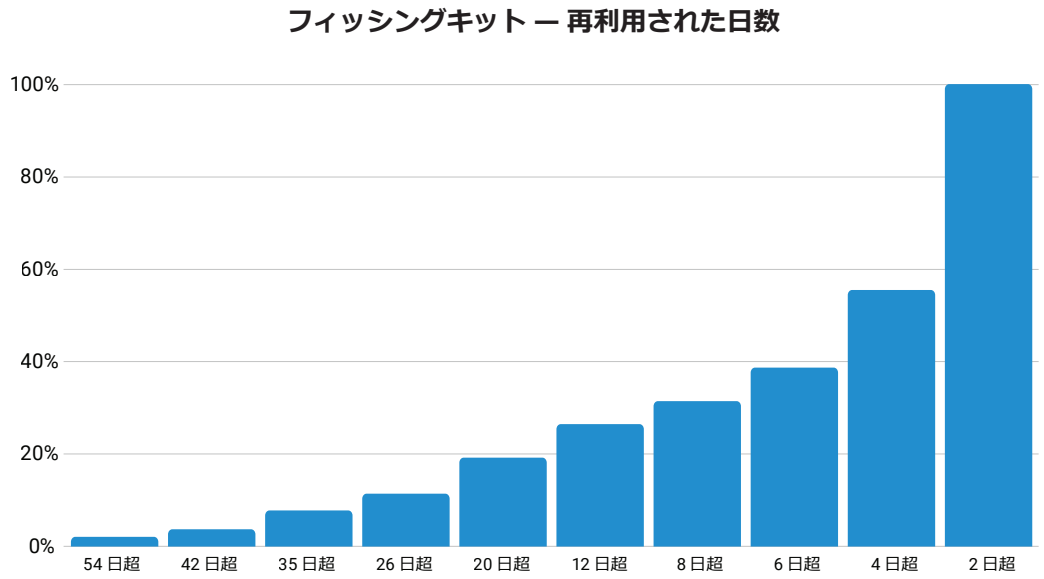


図 20：フィッシングツールキット（再利用された日数別、2022 年第 4 四半期）

新規攻撃キャンペーンの開始に使用されている 300 種類のフィッシングツールキットを追跡調査したところ、2022 年第 4 四半期は追跡対象キットの 2.04% が 54 日間以上再利用されていました（図 20）。さらに 55.5% が 4 日間以上、そして 100% が 2 日間以上再利用されていました（2022 年第 4 四半期）。

まとめと提案：最新の攻撃に対処するためのプロアクティブな対策

以上、脅威グループと攻撃者の手法を取り上げてきましたが、続いてこれらの情報をどのように活かすかを検討します。まずは、組織内または第三者に提供される DNS の管理方法を考えてみます。大規模な組織や複雑な組織では、DNS の管理専門の事業者を利用することは意義があります。いずれにしても、利用する DNS のパフォーマンスと保護を監視する必要があります。次に、必要になる各種の制御について見ていきましょう。DDoS 防御、マルウェア攻撃とスクレ―ピング、ラテラルムーブメント、データ流出が主に緩和すべき対象です。このようなデータ移動のプロセスに従い、あらゆる段階で解消可能な重大な脆弱性を見つけるサイバーセキュリティモデルは、サイバーキルチェーンと呼ばれることが多くあります。

本レポートに取り上げた攻撃手法に対処するためのプレイブックの構築を検討してください。侵入テストチームやレッドチームとともに、IAB と同じツールと手法（Qakbot や Emotet、QSnatch などのボット、LockBit などのランサムウェア）をラボ環境で使うかどうか、また Cobalt Strike などのツールの使用も検討する必要があります。セキュリティの制御がこれらのタイプの攻撃を効果的に警告して食い止められることも重要ですが、対処するチームのトレーニングも重要です。

Cobalt Strike がネットワークで見つかった場合は、ただちにインシデントレポートを作成して調査するのが賢明です。これはレッドチームが用いるツールですが（その場合も調査をして報告の必要があります）、これらのトラフィックの存在は、他の RaaS 攻撃者や脅威アクターが侵入し、緩和可能な攻撃が続いていることを示すことから、警告を発する必要があります。

セキュリティ・オペレーション・センターの運用を検討し、ネットワーク内の IAB 関連の脅威による偵察の可能性を示すプロセス（bits、Wget、cURL など）の追跡方法を決めるようにします。重要なのは何がダウンロードされたかを明らかにし、実行中のものを停止することです。その上で IAB のトリガー（LNK ファイル、マクロ、VScript など）を調査し、どこから侵害が始まったのかを明らかにします。

最新の Akamai リサーチをセキュリティ・リサーチ・ハブでご確認いただけます。

手法

コマンド & コントロール攻撃トラフィック

本レポートのデータは、Akamai の Secure Internet Access（SIA）製品により生成された、コマンド & コントロール（C2）攻撃トラフィック関連のデータです。SIA はクラウドベースのセキュア Web ゲートウェイで、ユーザーデバイスをインターネットに簡単、安全に接続することが可能です。レポートで取り上げた 2 つのタイプのデータは、ユーザー数の多いエンタープライズ組織と個人のホームユーザー向けのインターネットプロバイダーからのセキュリティ・アラート・データを反映したものです。このデータを、それぞれ影響を受けたデバイスの数とクエリー数に応じて評価しています。影響を受けたデバイスは、既知の確認された C2 ドメインに一度以上アクセスしたデバイスのことです。同じく、C2 クエリーは既知の確認された C2 ドメインに一度以上アクセスしたクエリーです。Akamai セキュリティチームはこのデータを社内で使用して攻撃を調査し、悪性のふるまいが認められれば顧客に知らせ、追加情報を Akamai のセキュリティソリューションにフィードバックさせています。

クレジット

共同執筆者

Or Katz

Eliad Kimhy

Badette Tribbey

校閲およびテーマ別寄稿者

Tanya Belousov

Shiran Guez

Ophir Harpaz

Stiv Kupchik

Grace Wang

Steve Winterfeld

データ分析

Ronan Ballantine

Gal Kochner

Chelsea Tuttle

マーケティング・出版

Georgina Morales Hampe

Shivangi Sahu

その他の「インターネットの現状／セキュリティ」レポート

高い評価を受けている Akamai の「インターネットの現状／セキュリティ」レポートのバックナンバーおよび今後のリリースについて：akamai.com/soti

その他の Akamai 脅威リサーチ

以下のリンクから、最新の脅威インテリジェンス分析、セキュリティレポート、サイバーセキュリティリサーチをご確認いただけます。常に最新情報を把握するためにお役立てください：akamai.com/security-research

このレポートに掲載されているデータ

このレポートに引用されているグラフや図のハイクオリティバージョンを以下のリンクからご覧いただけます。これらの画像は、出典元として Akamai を明記し、Akamai のロゴをそのまま残すことを条件に、利用および引用が可能です：akamai.com/sotidata

Akamai ソリューションの詳細

エンタープライズ組織を標的とする脅威に対処するための Akamai ソリューションの詳細を Secure Internet Access Enterprise ページでご覧いただけます。消費者および SMB 市場のサービスプロバイダーの方は、ISP 向けの Secure Internet Access サービスをご覧ください。

Akamai はオンラインライフのカとなり、守っています。世界中の先進企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、世界中の人々の生活、仕事、娯楽をサポートしています。広範に分散したエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、Twitter と LinkedIn で Akamai Technologies をフォローしてください。公開日：2023 年 3 月