［インターネットの現状］／セキュリティ

第５巻、第２号

小売業界への攻撃とAPIトラフィック

編集者による概説

この 10 年間でセキュリティ業界に起きた最大の変化の 1 つは、「Akamai はビジネスとは無縁の単なる技術者集団ではなく、ビジネスのあらゆる面で欠かせないサービスを提供している」という認識が広がったことです。業界の中で比較的新しい存在である、セキュリティの専門家にとっては、これは当たり前のように聞こえるかもしれませんが、組織によっては、このような広い視点から見た考え方はまだ浸透していません。セキュリティチームは企業に不可欠な存在であると考えている組織や、他の企業とは切り離して考える組織など、セキュリティチームに対する組織の見方はさまざまです。

セキュリティチームを正当なビジネスパートナーとして見なしている組織にとって、セキュリティチームの重要な役割は、ビジネスが直面するリスクを特定することです。1990 年代、セキュリティチームは、「ノー」としか言わない組織と見られ、セキュリティチームにとっては、まさに「暗黒時代」でした。このような中、セキュリティのリーダーは、品質の向上とリスクの周知に取り組みました。優れたセキュリティチームは、リスクとリスクの評価プロセスを明確に定めているため、私たちがリスクを認識した場合に、**「リスクがあるかないか」**の単なる二者択一的な方法ではなく、どの程度のリスクがあるのか微妙な違いまで説明できます。さらに重要なことは、これらのリスクに対する金銭的コストを理論的に説明できることが多いため、ビジネスリーダーは潜在的コストを評価できます。

しかし、リスクの特定は難しく、**本当に**困難です。ビジネスの意思決定に大きく影響する可能性のある微妙な違いを理解することは、慣れ親しんだ話題でも難しいプロセスです。私たちは、リスクとその影響を過小評価する場合があり、その結果、ビジネスにおける評価を下げたり、問題が発生した場合に責任追及されたりすることもあります。セキュリティの他の多くの面と同様、唯一無二の方法というものはありません。重要なのは、個人と組織に合ったバランスの取れた行動です。

この問題は、全体像がほとんどまたは全く見えない未知の要素や課題に直面した場合にさらに困難になります。今号の**「インターネットの現状／セキュリティ」**レポートで紹介している 3 つの事例では、数多くの組織が本来認識すべきでありながら認識できていない、セキュリティの側面について解説しています。Akamai が実施した API トラフィックに関する調査では、驚くべきことに、ヒット件数の 83% が API の利用によるものであることが明らかになりました。DNS トラフィックの調査では、IPv6 トラフィックの件数が過少にレポートされていることが判明しました。IPv6 に対応しているシステムの多くが依然として、IPv4 を優先しています。最後に、Credential Abuse および小売企業のインベントリを不正使用するボットネットについて Akamai が行った調査では、この問題が増加していることが判明しました。これは注意を要します。

リスク評価で必要となるのは、「認識**すべき**にもかかわらず、認識していない問題は何か」を常に考えることです。これらは単に目に見えないため、把握していない（把握できない）ものです。把握できない問題を少しずつ取り除き、把握できるカテゴリーに移すうえで、本レポートがお役に立てれば幸いです。

目次

TL;DR

- Akamai は、2018 年 5 月から 12 月にかけて 280 億回近くの Credential Stuffing の試みを検出しました。オールインワン・ボットネットなどのツールは、小売企業に対する大規模な攻撃を担っています。
- Akamai の ESSL ネットワークに関する最近の分析では、保護されたコンテンツ・デリバリー・ネットワークのトラフィックの割合は、HTML トラフィックが 17%、API トラフィックが 83% になっていることが判明しました。2014 年の同じ調査に比べて、大幅に増加しています。
- Akamai の分析に基づくと、IPv6 の使用率に関するレポートは、実際より少なく報告されている可能性があります。このことが、「IPv6 は監視する必要がない」という危険な想定につながっています。

概要

今号の「**インターネットの現状／セキュリティ**」レポートで取り上げている 3 つの事例はすべて、ほとんどの組織が調査できていないことです。いくつかの問題が自身の環境にとって重要であることに組織が気付いていないなど、その原因が何であれ、これらの問題を監視するツールがなかったり、このトラフィックを監視するリソースを利用できなければ、このようなトラフィックは多くの場合見過ごされます。

ボットネットによって発生したトラフィックを組織が調査しても、専用の検知ツールを使用しなければ、このトラフィックは、多くの場合、他の種類のネットワーク活動と同じものとして扱われます。ボットネットの開発者と小売部門のセキュリティ担当者は、実際の金銭をめぐる多次元的な戦いを繰り広げており、このような危険性は、小売部門以外の分野にはほとんど見られません。Akamai のチームでは、毎月数百万の Credential Abuse の試行が発生する中で、オールインワン（AIO）ボットツールを確認し、それらのツールを認識しています。

ボットネットによって発生したトラフィックを組織が調査しても、専用の検知ツールを使用しなければ、このトラフィックは、多くの場合、他の一般的なネットワーク活動と同じものとして扱われます。

多くの組織が十分に可視化できないトラフィックとしては、他に API トラフィックがあります。Akamai では、2014 年に Enhanced SSL（ESSL）ネットワークの JSON と XML トラフィックの内部監査を実施しましたが、その結果、トラフィックの 47% が、これら 2 つのプロトコルによるものであることが判明しました。2018 年 10 月に社内のトラフィックについて実施した同様の調査では、トラフィックの 69% が JSON、14% が XML を占め、HTML はわずか 17% でした。

インターネットは IPv6 に徐々に移行していますが、インターネットソサエティによると、上位 1,000 のサイトの 28% が IPv6 に対応しているのに対し、上位 100 万のサイトで IPv6 に対応しているのはわずか 17% です。しかし、Akamai の調査によると、非常に多くのシステムで、IPv6 トラフィックを処理できる場合でも IPv4 が優先されているため、この数字は実際より低く報告されている可能性があることがわかりました。IPv6 は依然として少数派のトラフィックと見なされているため、多くのセキュリティツールにとっても大きなセールスポイントにはなっていません。IPv6 に対応している場合でも、IPv6 空間を監視する価値があると考えている組織はわずかにすぎません。

- Akamai の調査

小売業界に対する大規模な攻撃に利用されるツール

2018 年 5 月 1 日から 12 月 31 日にかけて、Akamai のネットワークで検出された小売業種に対する Credential Stuffing の試行数は 100 億 58 万 5,772 回でした。これらの攻撃は他のすべての業種にも広がっており、Akamai では、8 か月間で 279 億 8,592 万 324 回の Credential Abuse の試行数を検出しました。つまり、毎日 1 億 1,500 万回以上、ユーザーアカウントへの不正アクセスやログインが試行されたことになります。

これらの試行の理由は複雑ではありません。これらの試行を担っている攻撃者は、個人情報、口座残高、資産などのデータを探しており、2021 年までに 4 兆 8,800 億ドル規模に拡大することが予想される、オンライン小売市場から現金を奪うことを狙っています。

Akamai が記録した Credential Stuffing の試行は、ボットによって自動化されています。ボットは、ウェブトラフィック全体の 60% を占めますが、ボットとして実際に断定できるのは半分にも満たず、このことがボットの追跡とブロックを困難にしています。このジレンマは、すべてのボットが悪意のあるものとは限らないという事実と相まって、さらに困難なものになっており、このことは、今年度第 1 号の「**インターネットの現状／セキュリティ**」レポートでも考察されています。

ボットは、ウェブトラフィック全体の 60% を占めますが、ボットとして実際に断定できるのは半分にも満たず、このことがボットの追跡とブロックを困難にしています。

数字を当てる宝くじ

犯罪において、Credential Stuffing 攻撃は数字を当てる宝くじのようなものです。攻撃者は、人々がさまざまなアカウントでパスワードを使い回しているという事実を利用しています。Credential Stuffing 攻撃を受けると、1 つのウェブサイトから不正に入手した認証情報が他の多くのウェブサイトにも転用されます。

Credential Stuffing 攻撃は 2 段階のプロセスを経ます。持ちうる限りの認証情報のペアを使ってログインページでそれが有効かを検証し、一度それが有効なことが検証できれば、そのアカウントを支配します。この 2 番目の段階を一般に「アカウント乗っ取り（ATO：Account Take Over）」と呼びます。

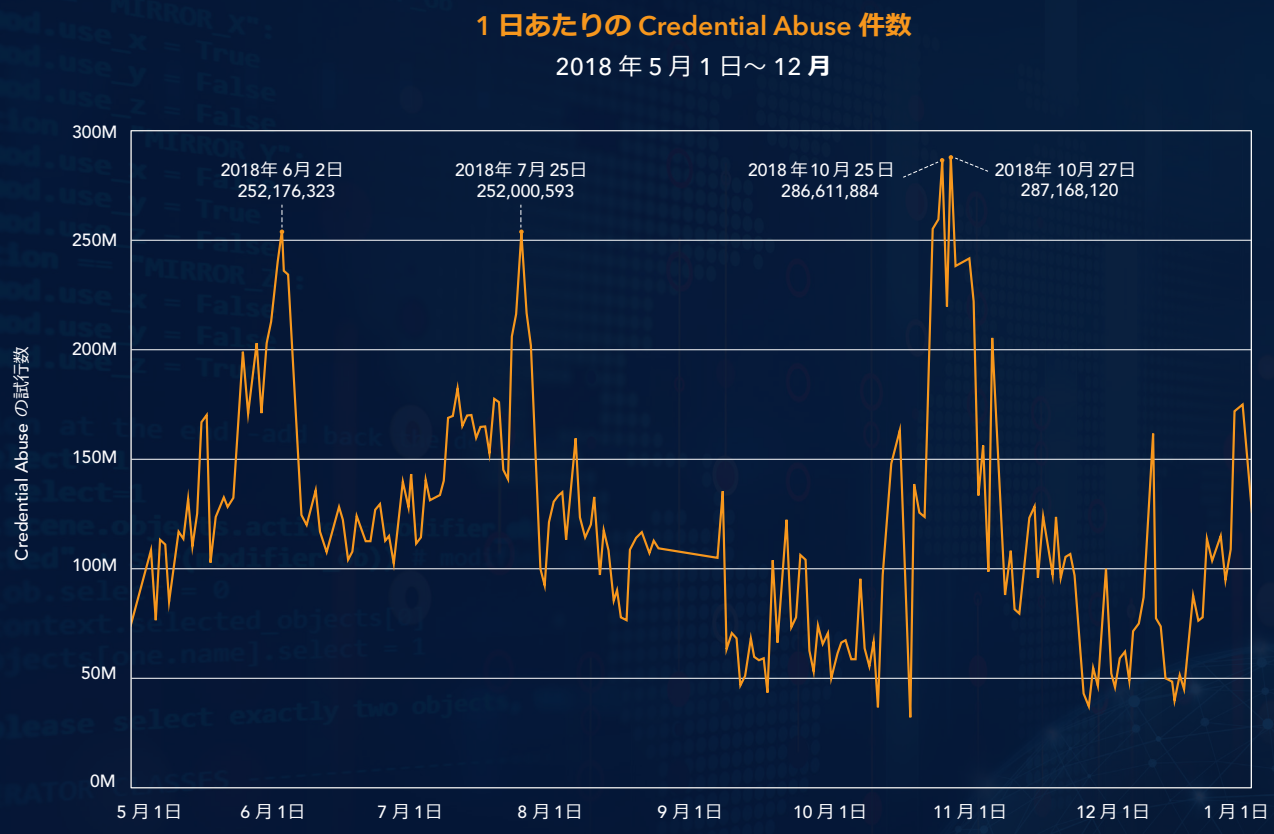


図 1

2018 年 5 月 1 日から 12 月 31 日までの間に、Credential Stuffing が最も多く発生した上位 4 日間

LinkedIn のデータ漏えいにより、1 億 1,600 万ものアカウントが不正アクセスされたことを考えてみてください。犯罪者は、LinkedIn の認証情報を他のウェブサイトでも使用していることを期待しながら、メールアドレスとパスワードを組み合わせたこのリストを利用して、他の多くのウェブサイトを標的にしてきました。これらの Credential Stuffing の試行により、複数のアカウントが乗っ取られる二次被害が発生しています。だからこそ、セキュリティの専門家は、パスワードマネージャーの利用と、ウェブサイトごとに異なる長いパスワード文字列を使用するように強調しているのです。

Credential Stuffing 攻撃との戦いは困難な戦い

Credential Stuffing との戦いは、簡単なものではありません。Ponemon Institute が実施した Akamai の調査の回答者の 71% が、Credential Stuffing 攻撃の防御を強化すれば、正規のユーザーのウェブエクスペリエンスを損なう可能性があるため、このような攻撃を防ぐことは難しいと述べています。

組織からの回答によると、Credential Stuffing の試行数は毎月平均 12.7 回で、試行 1 回あたり 1,252 ものアカウントが標的にされています。これらの試行を担うボットを徹底的にブロックするだけの場当たり的な措置は、最初は意味を持ちますが、このような措置によって、正規のユーザーが影響を受ければ、ビジネスに深刻な損害を与える可能性もあります。

この調査では、回答者の 32% が Credential Stuffing 攻撃を可視化できておらず、30% が Credential Stuffing 攻撃の検出と緩和ができていないと述べています。また、Credential Stuffing 攻撃の抑制と防止のための十分なソリューションとテクノロジーが組織になければ、このような防御に直面した場合に十分に対応できないと、回答者の 70% が述べています。

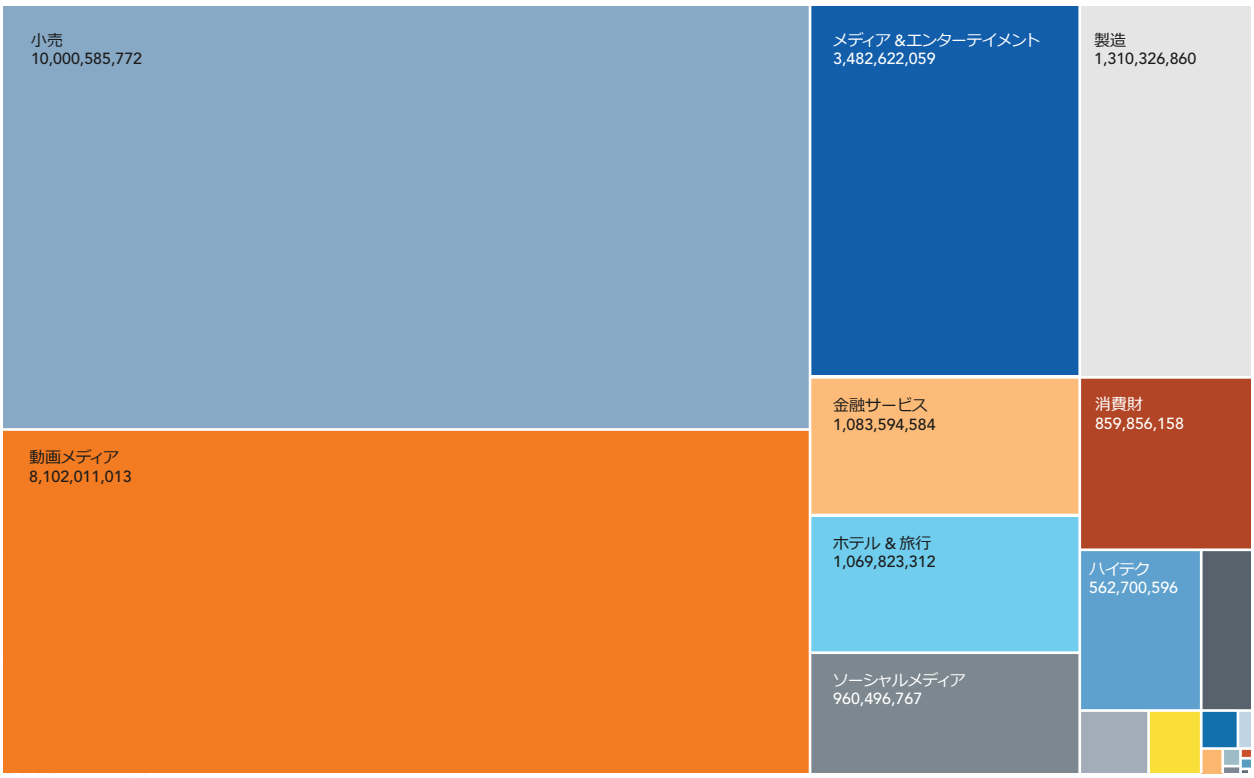
Credential Stuffing 攻撃は、コストを強いる戦いでもあります。このような攻撃に伴う年間のベースラインとなるコストの合計は、アプリケーションのダウンタイムで 170 万ドル、顧客の喪失で 270 万ドル、IT の作業工数で 160 万ドルになります。

図 2

動画メディアとメディアおよびエンターテインメントに対する試行数（116 億回）

業種別 Credential Abuse 試行数

2018 年 5 月 1 日～ 12 月 31 日



上位の市場セグメント

全般

2018 年の 8 か月間で Akamai が検出した Credential Abuse の試行数は 279 億 8,592 万 324 回でした。図 2 は業種別の内訳です。面積の大きさは全体における割合を表しています。各ボックスの上部には、Akamai が調査した業種別のデータを表示しています。右下隅のエリアには業種のラベルが表示されていませんが、これらは、自動車や公共部門など、同時期の Credential Abuse の試行数が 2 億 5,000 万回未満の業種です。

小売が Credential Abuse 攻撃の最大の標的になっており、次いでストリーミングメディアを提供する企業（81 億 201 万 1,013 回）になっています。他のメディアおよびエンターテインメント企業では 34 億 8,262 万 2,059 回、製造業のサイトでは 13 億 1,032 万 6,860 回になっています。Akamai では、今後のレポートでメディアのサイト全般に対する攻撃を調査する予定です。

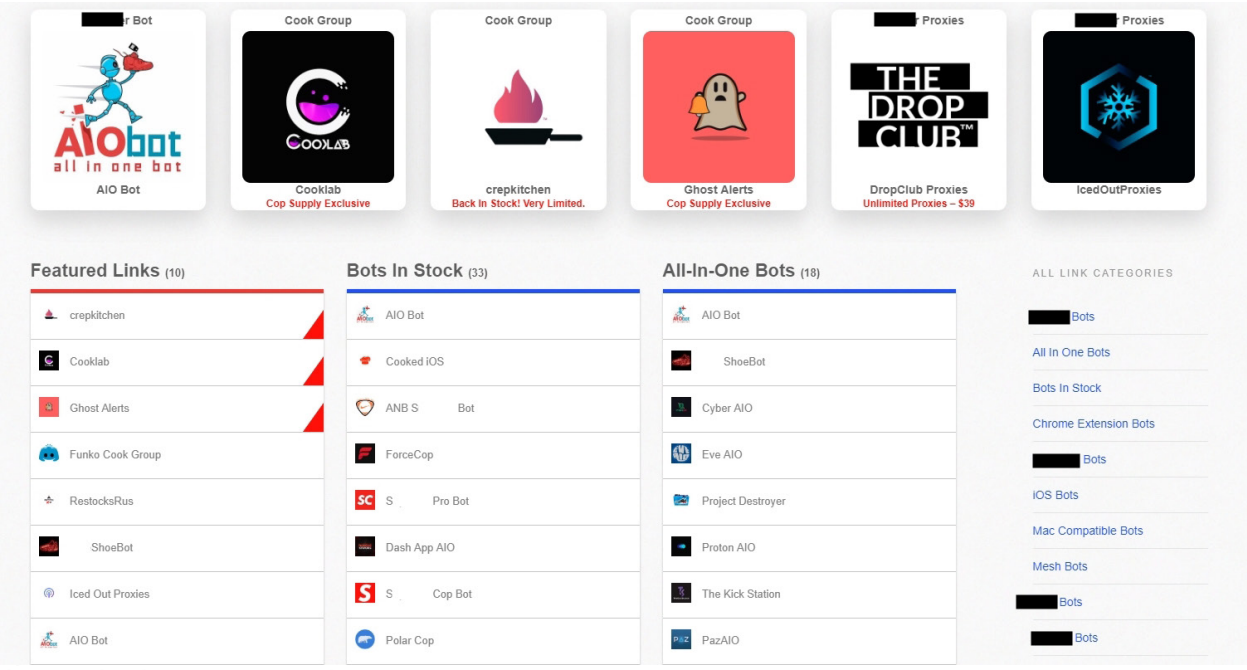
小売

小売業は、レポート対象期間の 8 か月間で Credential Stuffing の試行数が 100 億回になっており、調査したデータの中で最大の標的になっています。この業種では、アパレル業界が 37 億回で、同時期で最も標的となった業種になっています。

では、小売、特にアパレル業界がこのような標的として狙われる理由は何でしょうか？答えは簡単です。お金です。

図 3

市場で流通している AIO ボットの例、プロキシ、ホストサービスなどを提供



BrandZ Top 100 によると、トップ 10 のアパレルブランドだけで、1,113 億ドルもの市場規模がありますが、アパレル単独のリセール（再販）市場の規模は約 10 億ドルです。トップ 10 のアパレルブランドの市場規模と比べると、リセール市場は小さい規模ですが、それでも膨大な利益を生む市場です。実際、このようなアフターマーケットは活気づいており、毎日の取引額は 200 万ドルにもなっていると、リセール業者のプラットフォームの StockX は述べています。

小売業界、特にアパレル業界では、Credential Stuffing の試行と購入にしばしば関係するボットをオールインワンボット（AIO）と呼んでいます。これらのボットは、さまざまな回避術を利用して、すばやい購入を可能にする多機能ツールで、120 を超えるオンライン小売企業を標的にしています。AIO は簡単に入手でき、特定の小売店を念頭に設計されています。

AIO が存在する主な理由は、リセール市場に参入するためだけでなく、ユーザー名とパスワードのリストを使用して、特定のウェブサイトのアカウントとプロファイルのアクセス情報をすばやくチェックできることです。

小売業界を標的にする犯罪要素には、乗っ取りに成功したアカウントに対するさまざまな不正行為があります。不正アクセスしたアカウントに関連付けられている個人情報や独自のステータスには価値があります。

小売企業は、ブランド認知戦略の一環として、割引コードや限定版の商品を馴染みの顧客に提供することがよくありますが、犯罪者が Credential Stuffing の試行に成功すれば、これらの特典がすべて買い占められ、後で転売するなど、悪用されてしまいます。特別販売では、馴染みの顧客が優先されることがよくありますが、これらの顧客のアカウントが標的になれば、犯罪者に先に購入されてしまいます。

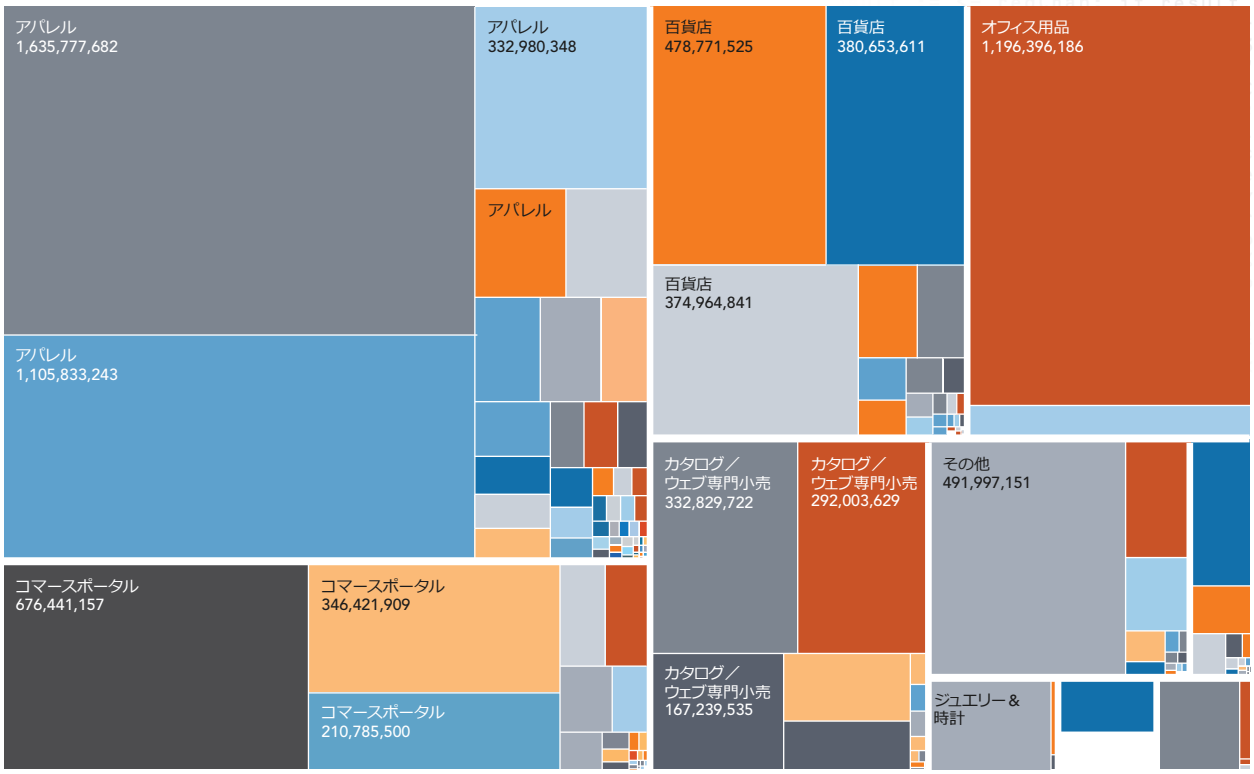
小売り企業は、AIO の試行が成功しても、全く気付かないことが多く、商品の需要があるときに、オンライン販売と記録的な取引数が痕跡として残るだけです。AIO によって、このような「在庫の一掃」が自動化され、それが流通市場を賑わしていることや、顧客から情報をかすめ取るのに使用されたことに小売企業が気付くケースは、ほとんど（または全く）ありません。

小売の販売サイクルにおけるボットの問題は、組織的な問題になっていることです。問題なのは、商品がすぐに売り切れることではなく、誤った成功感を生み出すことです。AIO が使用されると、小売企業が顧客獲得や付加価値販売野の機会を得ることができなくなり、成長とブランド認知が妨げられます。AIO により在庫不足が人工的に生み出され、売上の指標や在庫の追跡も歪められます。情報と小売り業者の評判がリスクにさらされることで、小売企業の顧客と投資家に損害を与えることになります。

犯罪者が Credential Stuffing の試行に成功すれば、これらの特典がすべて買い占められ、後で転売するなど、悪用されてしまいます。

小売業界の詳細

Credential Abuse
小売業界（業種別）、
2018 年 5 月～ 12 月



アパレル業界以外の小売業界内で、Akamai が Credential Stuffing の試行回数を追跡した結果、ダイレクトコマース（14 億 2,700 万回）、デパート（14 億 2,600 万回）、オフィス用品店（13 億回）、ジュエリーや時計などのファッション（1 億 2,972 万 5,233 回）となりました。図 4 の色分けされた各ボックスは、各業界を表しており、業種別に白の線でグループ分けされています。たとえば、左上のボックスは、単一の業種が 16 億 3,600 万回の攻撃を受けたことを表しています。

ボットと攻撃者は、小売だけでなく、複数の標的を念頭に置いて、これらの Credential Stuffing 攻撃と試行を実行しています。ダイレクトコマース（単一の商品またはブランドを提供する小売企業）の場合、標的の中心は、既存の履歴があるアカウント、収集可能な個人情報、特別な取引やプロモーションなどです。同じことがデパートにも言えますが、デパートのクレジット明細が漏洩すると、それを利用して取引が簡単にできるため、犯罪者にとってはさらに旨みがあります。

図 4

レポートの対象期間中、すべての Credential Abuse 攻撃の 6% が 1 つの業界を標的

Credential Stuffing を試行して、オフィス用品店や小売企業に対して ATO が成功すると、攻撃者は取引や個人情報の詳細、注文書（PO）や連絡先などの他の関連情報にアクセスできるようになり、アカウント保持者がビジネスメール詐欺（BEC）攻撃やスピアフィッシングのリスクにさらされます。

ジュエリーやアクセサリーの市場の顧客は富裕層が多く、犯罪者にとって、個人情報の詳細や口座残高の「商品価値」は高いためです。これらの業界も格好の標的です。

レポート対象期間に Akamai が金融機関に対する Credential Stuffing の試行回数を追跡した結果、10 億 8,000 万回になりました。これらの試行は、すべて犯罪目的です。こうした攻撃者は、流出した認証情報と金融口座の照合を企んでおり、Credential Stuffing を試行して ATO が成功すると、金銭の流出や、金融情報の売買などの被害を受けることになります。

レポート対象期間に Akamai がホテルと旅行業界に対する Credential Stuffing の試行回数を追跡した結果、1,069 億回になりました。これらの攻撃は複数の標的に対して実行されています。この業界には、小売や金融機関の標的も含まれており、個人情報に加え、ポイントなどの特典やプロモーションなどの情報もアカウントから盗まれています。飛行機やホテルの特典アカウントに不正アクセスしたり、割引価格で予約した部屋を正規の値段や利幅を上乗して再販売したりするなど、犯罪者は巨額の金を稼いでいます。

レポート対象期間に Akamai が金融機関に対する Credential Stuffing の試行回数を追跡した結果、10 億 8,000 万回になりました。これらの試行は、すべて犯罪目的です。

地域

最後に地域別に見てみましょう。図 5 に示すように、Credential Stuffing トラフィックの発信源では、米国が群を抜いており、次いでロシア、カナダ、ブラジル、インドとなっています。AIO ボットの多くは米国で開発されているため、米国がトップになっていることを見ても特に驚くことではありません。

標的についても、米国がトップで、追跡された Credential Stuffing 攻撃は 224 億 7,000 万回です。次いで、カナダ（20 億 1,000 万回）、インド（11 億 6,000 万回）、ドイツ（7 億 9,200 万回）、カナダ（4 億回）となっています。

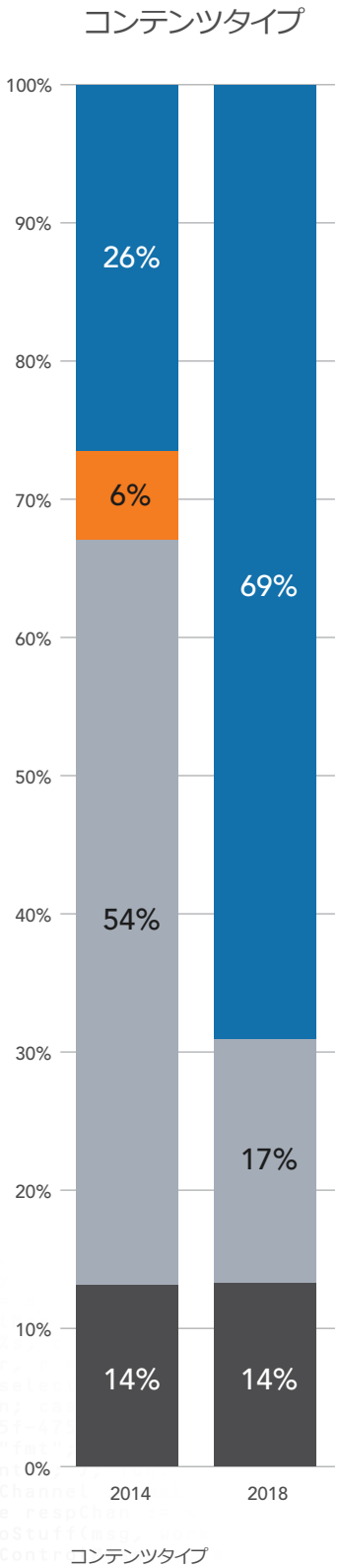
まとめ

Credential Stuffing 攻撃と ATO は、リセール市場におけるゲームに利用されることがあり、これらの攻撃のほとんどが、ビジネス詐欺や、個人情報や金融情報の収集、闇市場での売買や取引に集中しています。

このような攻撃を止める唯一の方法は、ボットの検出と緩和の精度を上げ、ウェブサイト間で認証情報を共有させないようにすることです。パスワードの使い回しを止めなければ、Credential Stuffing と ATO は犯罪に利用され続けます。

図 5

2018 年 5 月 1 日～ 12 月 31 日に追跡された Credential Stuffing 攻撃の発信元の国



API トラフィックの増加

2014 年、Akamai の調査担当者は、次のような比較的簡単な質問をしました。「Akamai のネットワークの HTTPS トラフィックの中で、API の割合は HTTP と比較してどれくらいですか？」この質問で知りたかったのは、トラフィック（ひいてはインターネット全体）のどの部分が機械のためにフォーマットされたコンテンツか、その中のどの部分が人間の操作によるものなのか、また、どの部分が、人間の操作が直接介入せずにデータが自動的に交換されているかということです。当初、Akamai のトラフィックに占める API トラフィックの割合は少ないと想定していましたが、Akamai による統計の情報分析の結果、API トラフィックはすべてのレイアウトとデータトラフィックの 47% を占めることが判明しました。

これは大きな発見であり、これをきっかけに、4 年にわたり多くの活発な議論がなされました。その結果、API トラフィックを再度確認することを最近決定しましたが、結果はまたしても驚くものでした。API として分類されるトラフィックは、現在すべてのヒット数の 83% になっており、HTML トラフィックは 17% まで低下しています。

このようなトラフィックパターンの変化は、セキュリティ業界にとって分岐点になっています。これまで、トラフィックのオリジンであるサーバーとシステムの保護に利用されてきた制御の多くは、ブラウザーのトラフィックの監視に振り分けられてきました。同じ制御を API トラフィックに応用するのに必要なメカニズムとしては、堅牢性が低く、設定が困難で、特定の環境では利用できない場合があります。

調査したトラフィックは、Akamai コンテンツ・デリバリー・ネットワークである ESSL ネットワークから得たものです。このネットワークは、銀行や小売などの安全な取引用に主に設計されています。このセクションで使用されているデータ、条件、定義の詳細については、付録の説明を参照してください。

JSON が重要

このレポートの目的である、API トラフィックの Akamai の定義は、ESSL ネットワークの JSON または XML のコンテンツタイプを含む、すべての HTTPS レスポンスです。これには、ブラウザーベースのトラフィックが含まれる場合がありますが、Akamai の調査で判明したことは、これはトラフィックのごく一部であり、主要な測定には大きな影響がないことでした。このレポートでは、調査対象の 10 日間のヒット数が 100 万回を超える組織に限定しています。

図 6

アプリケーションからの XML トラフィックは 2014 年以降、ほとんどなくなっている

API トラフィック、特に JSON は、一般に単独のアトミックリクエストに基づいています。つまり、各リクエストは、ストリームまたはマルチパートリクエストの一部ではなく、スタンドアロンのデータグラムであることです。対照的に、ページの構成に必要な HTML は比較的小さい場合がありますが、依存する画像や他のコードは一般に非常に大きく、数百のオブジェクトで構成されています。

HTTPS トラフィックの Content-Type を見ると、JSON が最も一般的な単一の Content-Type であることがわかりました。これまで、JPEG や GIF などの画像ファイルは、ESSL ネットワークのトラフィックの大部分を占めていましたが、Akamai が最近実施した測定によると、これらの 2 つのファイルタイプのトラフィックを合計しても、JSON ほどではないことが判明しました。一方、すべての画像タイプのトラフィックを 1 つに合計すると、JSON よりも大きくなります。

Akamai の ESSL ネットワークは、API トラフィックを主な用途として処理するために急速に進化しているといっても過言ではないでしょう。その理由は、メディアやハイテク業界では非常に大きなトラフィックが消費されるためです。こうした業界は、多くの場合、ニュース、天気予報、ストリーミングメディア、ゲームのサービスを提供するビジネスです。

全体的に、JSON トラフィックは現在 HTML トラフィックの 4 倍になっていますが、上位 5 社の企業を分析から除外したとしても、JSON は、HTML の 2 倍のトラフィックを占めています。API トラフィックが、消費と生産の両方を担うあらゆる規模の組織のトラフィックの大部分を占めていることは、議論の余地はありません。

Akamai が最近実施した測定によると、これらの 2 つのファイルタイプのトラフィックを合計しても、JSON ほどではないことが判明しました。

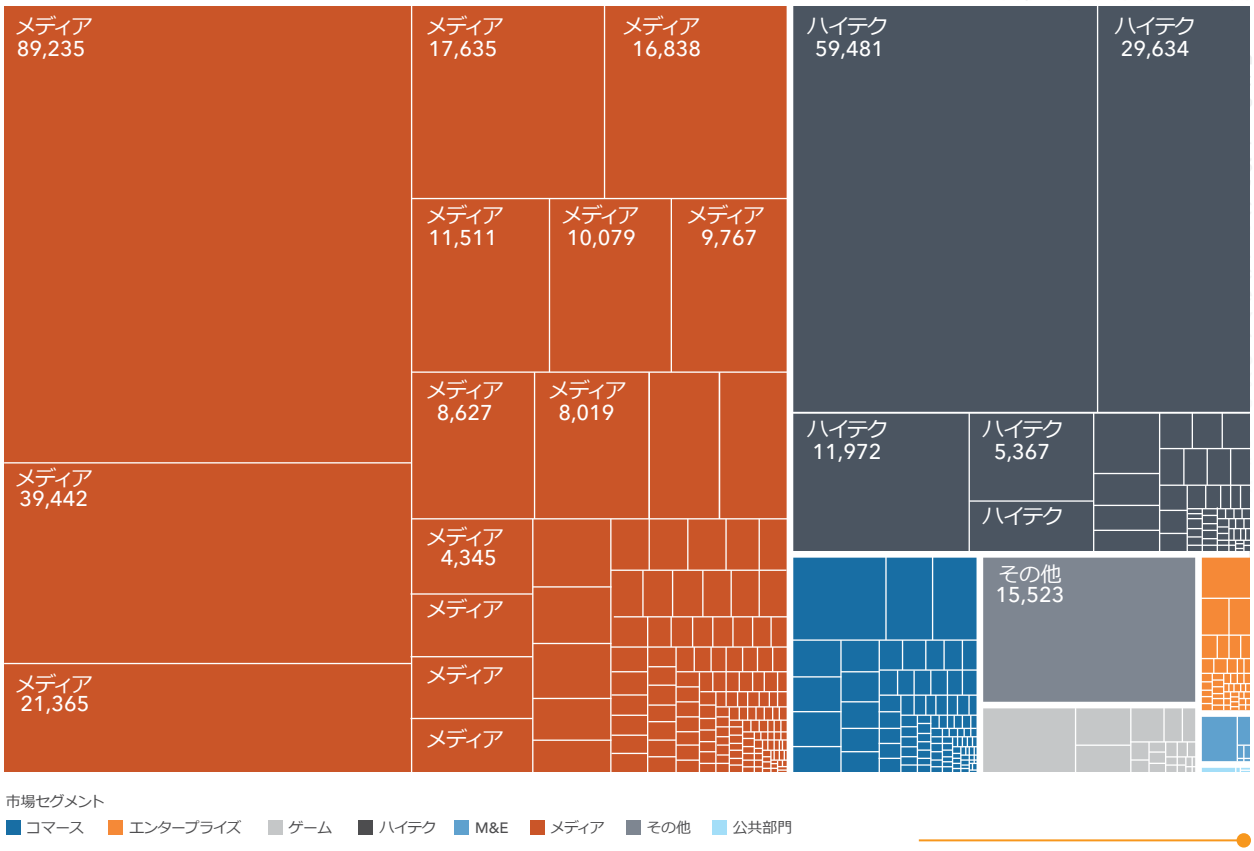


図 7

各業界でもメディア業界は群を抜いて API を使用している

図 7 では、API トラフィックの分布を示しています。メディアがヒット数全体の約 3 分の 2（63%）を占めていることが一目でわかります。これは、膨大な数のユーザーによるものだけではなく、API トラフィックを利用するメディアサイトの数が多いことにもよります。API トラフィックが次に多いのは、ハイテク業界です。業界の分類は、Akamai の分類とトラフィックを基準にしており、業界の基準とは完全に一致しないことがあります。

セキュリティの問題は別にしても、API トラフィックが増加していることは、パフォーマンスの観点からも重要です。キャッシュが可能である割合（Akamai などのコンテンツ・デリバリー・ネットワークのサーバーに保存されたキャッシュから引き当てて利用できるトラフィックの量）は、HTML ヒット数と API ヒット数の間で比較できます。記録されたヒット数の 3 分の 1 は「no-store」とマークされたため、キャッシュできませんが、API トラフィックのキャッシュヒット率は HTML トラフィックを実際に大きく上

回っています。これは、大量の API トラフィックが顧客のオリジンサーバーからオフロードされており、エンドユーザーのエッジサーバーから送信されていることを意味します。これにより、オリジンサーバーとインターネットバックボーンの両方の負荷全体が大幅に軽減されます。

JSON ドキュメントの大部分は、ブラウザーで消費されていません。スマートフォン、アプリケーション、組み込みデバイス（ゲーミングコンソール、ストリーミングデバイス、スマートテレビなど）の API トラフィックは 66% 以上を占めています。対照的に、すべてのブラウザーを合計しても、API トラフィックのわずか 27% にすぎず、その他については 1 桁台の割合です。

スマートフォンは、大量の API を使用しており、携帯電話網を使ってインターネットに接続する必要があります。この通信は主にプログラムによって駆動されているため、携帯電話のアクセスは、HTML より API からのものが大部分を占めます。携帯電話網からの API リクエストの割合は 37% で、HTML（18%）の 2 倍です。

この点について Akamai が実施した API と HTML トラフィックの調査の大部分は、記録したヒット数を中心としたものでしたが、各タイプの通信に必要なビット数とバイト数についても議論の重要な部分です。API と HTML のオブジェクトは、平均して 1 KB をわずかに下回るサイズですが、API トラ

JSON ドキュメントの大部分は、ブラウザーで消費されていません。スマートフォン、アプリケーション、組み込みデバイス（ゲーミングコンソール、ストリーミングデバイス、スマートテレビなど）の API トラフィックは 66% 以上を占めています。

User Agent 別 API トラフィック

タイプ	UA	%
ブラウザー	Chrome	13%
	Mobile Safari	8%
	Firefox	2%
	Internet Explorer	2%
	Edge	1%
	Safari	1%
	IE Mobile	0%
非ブラウザー	その他	66%
	CFNetwork	3%
	Apache HttpClient	2%

図 8

API トラフィックの大部分はカスタムアプリケーション用であるため分類は困難

フィックの上限値は大きく異なります。JSON トラフィックでは、API トラフィックの 95 パーセンタイルの 18 KB ですが、HTML トラフィックでは 105 KB です。これは、一般的な TCP セグメントが 1,400 ～ 1,500 バイトであり、サイズの大きいオブジェクトは単一のセグメントに収まらないためです。少数のセグメントであれば、Akamai サーバーで使用される単一のラウンド・トリップ・タイム（RTT）輻輳ウィンドウで一緒に送信できます。このため、18 KB のメッセージは単一の RTT の初期ウィンドウに収めることができますが、105 KB のメッセージでは不可能です。その結果、HTML トラフィックが大きくなると、複数の RTT で転送されるようになりますが、JSON トラフィックは、新しく確立されたコネクションでも、大部分が単一の RTT 内で転送されます。

注目点

Akamai ネットワークの API ヒット数は、この 4 年間で、HTTP トラフィックの半分以下から、HTML ヒット数を押しのけてトラフィックの 83% を占めるまでに増加しました。セキュリティの専門家にとっては、これは極めて重要です。API ヒット数の増加にすべてのツールが対応できるわけではなく、防御態勢の中で、悪意のあるトラフィックの主な発信元を見落とす場合があるからです。サーバーのパフォーマンス面を担当するチームメートにとっても、JSON と XML トラフィックを考慮しなければ、重要な要素を見逃す可能性があります。

サーバーのパフォーマンス面を担当するチームメートにとっても、JSON と XML トラフィックを考慮しなければ、重要な要素を見逃す可能性があります。

アプリケーションは従来型のウェブページとは異なります。レイアウトとスタイルの情報はビルド時にすでに組み込まれているため、これらの情報は不要です。代わりに、アプリケーションでは、ニュースの更新、天気予報、スポーツなど、更新されたデータと画像をリクエストしています。また、ゲームやストリーミングシステムの更新の場合もあるため、最新リリースを知ることができます。個々のリクエストを見ると、受信しているデータのサイズは非常に小さいものですが、これらのリクエストの量は時間とともに増加していきます。

IPV6 は過少報告されているのか？

DNS 再帰リゾルバーにおける IPv6 の普及状況

このセクションでは、ドメイン・ネーム・システム（DNS）再帰（リカーシブ）リゾルバーでの IPv6 の採用状況について見ていきます。再帰リゾルバーとは、インターネットエコシステムの重要な構成要素です。再帰リゾルバーはホスト名と IP アドレスの名前解決のためにクライアントから利用され、レスポンスをキャッシュし、名前解決の遅延と権威サーバーの負荷の両方を軽減します。

Akamai では、2018 年 6 月の Akamai プラットフォームでの IPv6 の採用状況についての統計を以前に報告しました。Akamai プラットフォームで確認されたデュアルスタックの組み込みホスト名のコンテンツリクエストの平均的割合は約 45% で、2 年前より大幅に増加しています。分析対象のネットワークトラフィックは、クライアント（エンドユーザー）とエッジ間のトラフィックであり、エッジネットワークでの IPv6 が普及していることを示しています。Akamai では、DNS 再帰リゾルバーと権威サーバー間のデータについて調査し、インターネットの重要な構成要素での普及状況を確認しました。

Akamai の権威ネームサーバーでの DNS トラフィックの統計データの概要からは、これらのトラフィックの大部分は依然として IPv4 であることがわかりました。2017 年 7 月時点では、IPv6 のトラフィックの割合はわずか 11% で、コンテンツ・デリバリー・ネットワークにおける IPv6 の割合の 45% よりも大幅に低くなっています。Akamai では、これらの重要な構成要素で IPv6 の普及率が大幅に低くなっている理由を理解するために、Akamai の DNS トラフィックについて詳細に調査しました。

2017 年 7 月時点では、IPv6 のトラフィックの割合はわずか 11% で、コンテンツ・デリバリー・ネットワークにおける IPv6 の割合の 45% よりも大幅に低くなっています。

最初に、デュアルスタックのリゾルバーの重要性に注目しました。なぜなら、IPv4 と IPv6 の DNS リクエストの相関関係を比較する方法や、IPv4 と IPv6 の両方のトラフィックを生成する単一の再帰リゾルバーを特定する方法がないことが分かっていたからです。そのため、Akamai では、複数のインタフェースを利用できる場合（デュアルスタッキングなど）、再帰リゾルバーが状況に応じて、単一のホスト名の解決に複数のインタフェースを使用するという事実に着目しました。Akamai では、2017 年 7 月からの DNS トラフィックのログ（42 万 9,000 個の一意の再帰リゾルバー IP アドレスを記録）を使用し、「Characterization of Collaborative Resolution in Recursive DNS Resolvers（再帰 DNS リゾルバーにおける共同解決の特性）」ホワイトペーパーに記載されている方法に基づいて、IP アドレスを最初にクラスター化しました。

クラスター内の IP アドレスは、同じ DNS 解決の中で観測されているため、相互に関連しています。このため、IPv4 アドレスと IPv6 アドレス両方を持つクラスターには、デュアルスタックのリゾルバーが含まれている可能性があります。クラスターの 6% は、デュアルスタックのクラスターで構成されていると考えられます。デュアルスタックのクラスターは、他のクラスターよりも少し大きくなる傾向があるため、2017 年 7 月時点では、すべての再

帰リゾルバーの 7% がデュアルスタックであると推定されます。再帰リゾルバーで IPv6 トラフィックの普及が遅い主な理由の 1 つは、オペレーターが IPv6 アドレスでリゾルバーを構成していないことであることがわかりましたが、理由はそれだけではありません。そこで、デュアルスタックのクラスターに注目し、DNS 解決にデュアルスタックのクラスターで使用されているインタフェースを調査しました。再帰リゾルバーの 7% だけがデュアルスタックですが、それらは、トラフィック量の最も多いリゾルバーとなっています。DNS トラフィックのログを見ると、デュアルスタックのクラスター全体で、DNS クエリーの 37% を送信していました。では、IPv6 の DNS トラフィックが 11% 未満である理由は何でしょうか？デュアルスタックのクラスターでは、明らかに IPv6 より IPv4 が使用されています。Akamai では、クラスターごとに、DNS クエリーで使用されている IPv4 インタフェースと IPv6 インタフェース比率を計算しましたが、その結果、中央値で取った比率は 11:1 であることが判明しました。これは、このクラスターの 10% 未満が IPv4 よりも IPv6 を優先していることを示しています。この結果から明らかになったことは、再帰リゾルバーに使用されている IPv6 の割合が低いもう 1 つの理由は、デュアルスタックのリゾルバーが、IPv6 よりも IPv4 で DNS クエリーを送信していることです。

このような結果に影響を与えている可能性のある要因は複数あります。1 つ目の理由は、多くのドメインで IPv4 と IPv6 の委任の数に一貫性がないことです。再帰リゾルバーの IPv4 の委任の数が IPv6 よりも多いと、委任の間でクエリーが均一に分散していても、IPv6 よりも IPv4 が多く利用されると考えられます。

2 つ目の理由は、多くの再帰リゾルバーのソフトウェアパッケージが、レイテンシーとは逆に、優先度の重みづけが軽くなるよう定義します。IPv6 の接続性が悪いと、高遅延になるため、再帰リゾルバーで IPv4 が使用される可能性があります。最後の理由は、再帰リゾルバーのオペレーターが、慣れ親しんだ技術として IPv6 よりも IPv4 を使用するようにポリシーを決定している場合があることです。

DNS 再帰リゾルバーでの IPv6 の普及率は、エッジでの IPv6 の普及率に比べて低いように思われます。これには、さまざまな原因がありますが、多くの作業が必要であることも考えられます。権威 DNS サーバーのオペレーターがすべきことは、権威 DNS サーバーが IPv4 と同じ数の IPv6 委任のオプションを提供するようにし、IPv6 委任のパフォーマンスを IPv4 委任と同等にすることです。再帰リゾルバーのオペレーターがすべきことは、IPv4 を優先するポリシーが再帰リゾルバーに設定されているかどうかを確認し、それらをすべてデュアルスタックとすることです。

DNS 再帰リゾルバーでの IPv6 の普及率は、エッジでの IPv6 の普及率に比べて低いように思われます。

IPv4/IPv6 アドレスの指定のパターン

デュアルスタックの再帰リゾルバーのクラスターの調査では、将来 IPv4 アドレスと IPv6 アドレスを速やかに関連付けるのに使用される可能性のある、IP アドレス指定のパターンを確認しました。

このデータでは、デュアルスタックのリゾルバーの IPv4 アドレスと IPv6 アドレスの関連付けに様々な方法がとられていることを確認できました。その方法は、(i) IPv4 オクテットを IPv6 アドレスの最後の 4 へクテットとして組み込む（例：1.2.3.4 を 89ab::1:2:3:4 として組み込む）、(ii) 最後の IPv4 オクテットと最後の IPv6 へクテットを等しくする（例：1.2.3.4 と 89ab::4）、(iii) 最後の 4 へクテットに組み込むのではなく、IPv6 アドレスに、そのまま IPv4 アドレスを組み入れる（例：1.2.3.4 と 89ab::1:2:3:4:5678）です。

また、同じ自律システム（AS）内のデュアルスタックのリゾルバー間での IP アドレスの増加にもパターンがあることも確認しました。これは、デュアルスタックのリゾルバーを明確に識別するためにも役に立ちます。たとえば、IPv4 アドレスを IPv6 でシフトして割り当てている場合、IPv4 と IPv6 の両方で増加してみえます。例えば「w.x.y.z」を「a:b:c::${z+c}」としているケース（C は定数）。オペレーターは、IPv4 ／ IPv6 アドレス指定で明らかにさまざまなパターンを使用しています。自律システムで先験的なパターンを確認できれば、デュアルスタックのリゾルバーの IPv4 側と IPv6 側の照合に役に立つ可能性があり、検出プロセスを大幅に簡素化できます。

再帰リゾルバーの IP のクラスターでキャッシュポイズニングを防御

前述の DNS の再帰リゾルバーの IP アドレスのクラスターに話を戻すと、多くのクラスター（38%）には、2 つまたはそれ以上の IP アドレスが含まれており、単にデュアルスタックのリゾルバーの数以上となっていることが確認できました。それどころか、再帰リゾルバーのオペレーターは、複数の IPv4 または複数の IPv6 アドレス（あるいは両方）を同じ DNS 解決で使用しています。このような大きいクラスターは、我々が観察した DNS クラスターの約 72% にもなっています。

多くのクラスターには IP アドレスが 2 つ含まれていますが、クラスターの中には、IP アドレスが普通に 10 個を超える非常に大きいクラスターもあります。

このような挙動には、物理ハードウェア間の負荷分散など、複数の理由がありますが、セキュリティ上のメリットがあることも挙げられます。例えば、カミンスキー攻撃などの DNS キャッシュポイズニング攻撃では、再帰リゾルバーにより送られる DNS クエリーと一致するスプーフィングされた DNS レスポンスが必要になることがあります。DNS クエリーを照合する必要がある DNS レスポンスの領域には、(i) ソース IP ／ポート、(ii) 宛先 IP ／ポート、(iii) DNS の問い合わせ、(iv) DNS トランザクション ID があります。DNS 再帰リゾルバーのクラスター内では、特定の DNS クエリーがクラスター内の任意の IP アドレスから送信される場合があります。

このため、他のフィールドに加えて、一致する DNS 応答をスプーフィング（偽装）しても、そのクラスターから正しい宛先 IP アドレスを推測する必要があります。多くのクラスターには IP アドレスが 2 つ含まれていますが、クラスターの中には、IP アドレスが普通に 10 個を超える非常に大きいクラスターもあります。これにより、DNS キャッシュポイズニング攻撃が非常に困難になります。これらのことから、再帰リゾルバーのクラスターは、キャッシュポイズニングのリスクを緩和する有効な方法です。

今後の展望

我々、セキュリティチームとセキュリティの専門家は、事業部門とより統合された形で成長していくことを望んでいます。それは今後、数年間における課題です。我々セキュリティ部門はこれまでの「ノーと言うだけの部門」という認識から脱却しました。セキュリティ業界全体は成長してきましたが、まだまだ成長の余地はあると考えています。我々セキュリティのチームと専門家は、いまあらゆることに関わっています。ビジネスの計画と成長に関してもセキュリティが中心的な役割を果たしています。

今号の**「インターネットの現状／セキュリティ」**レポートで取り上げている事例では、見落とされがちなセキュリティの側面に注目していますが、それは日常業務においても重要です。紹介している事例は、今後の四半期ごとや数年ごとに予想される事象の背景になります。

最も注目すべき事例の 1 つは、API に関する事例です。API トラフィックは HTML トラフィックを凌駕しており、セキュリティチームとビジネス部門は、この新たな現実に対処することが求められています。前述のように、現在使用されている多くのツールでは、このようなトラフィックの種類の変化に対応できないため、それがセキュリティの盲点を生んでいます。モバイルデバイスの急増と IoT 技術の進化により、この傾向がすぐに衰えることありません。このような課題と変化にビジネスがどのような選択をしていくかによって、その影響は計り知れないものになります。

API の事例について、Credential Stuffing レポートでは、認証情報の使い回しによるリスクの増加によって、さまざまな市場に影響を及ぼす可能性があることを実証しています。セキュリティの専門家が複数のアカウントで同じ認証情報を使用しないことを推奨してきたのは、これが初めてではありませんが、古くからの習慣はなかなか直りません。今回は小売業界に焦点を当てましたが、このような攻撃の影響を受けるのは小売業界だけではありません。Credential Stuffing が他の市場や業界に及ぼす影響や、アカウント乗っ取り攻撃によるビジネスへの破滅的な影響は理解されておらず、無視されているのが現状です。

インターネットを取り巻く環境は急速に変化しており、これらの傾向は大きな変化の始まりにすぎません。セキュリティチームと専門家は、既存の枠にとらわれない考え方を常に心がけ、ユーザーとビジネスの安全と安心を守る新たな方法を開発することが求められます。

API トラフィックは HTML トラフィックを凌駕しており、セキュリティチームとビジネス部門は、この新たな現実に対処することが求められています。

付録：手法

一般注意事項

「**インターネットの現状／セキュリティ」レポート**」レポートでは、製品に関する言及を最小限に抑えるようにし、データの収集場所と取集方法の説明に必要な製品のみに留めています。最近のレポートでは、読者が実例のデータと統計データを文脈の中でとらえることができるように、データ収集の説明から展開するようにしています。

今号で報告しているテーマ、特に API トラフィックに対する Akamai の取り組みについては、Akamai のソリューションと、Akamai のコンテンツの中で使用している用語の両方に深く関連しているために、後述の議論の中で取り上げることが必要であると感じました。インターネット技術のコミュニティのさまざまな分野で使用される用語の変化は予測がつかないため、ここで Akamai での具体的な用法について明確にしておくことが重要です。

小売業界に対する大規模な攻撃に利用されるツール

このレポートで Credential Abuse の問題の説明に使用されているデータは、Cloud Security Intelligence（CSI）という内部ツールから提供されています。このツールは、Akamai の複数の製品ラインのデータのリポジトリです。このデータは一時データであり、90 日以内に削除されます。データセットの総量は現在 9 ペタバイトを超えており、今も増加しています。

Credential Abuse の試行は、メールアドレスをユーザー名として使用しているアカウントに対するログイン試行の失敗として識別されます。実際のユーザーではタイピングできないような Credential Abuse の試行を識別するには、2 つのアルゴリズムが使用されます。最初のアルゴリズムは、特定のアドレスに対するログインエラーの数をカウントする単純なボリュームを基にしたルールです。Akamai では、数百の組織のデータを相関分析にかけているため、単独の組織のみで検出が可能な内容とは別物です。

2 つ目のアルゴリズムでは、Akamai のボット検知サービスから提供されるデータを応用して、既知のボットネットやツールからの Credential Abuse を識別します。綿密に設定されているボットネットでは、多くの標的にトラフィックを拡散する、スキャンに非常に多数のシステムを使用する、時間をかけてトラフィックを拡散するなどの方法で、ボリュームに基づいた検出を回避できるようにしています。

綿密に設定されているボットネットでは、多くの標的にトラフィックを拡散する、スキャンに非常に多数のシステムを使用する、時間をかけてトラフィックを拡散するなどの方法で、ボリュームに基づいた検出を回避できるようにしています。

API トラフィックの増加

他の大規模な組織と同様、Akamai のインテリジェント・エッジ・プラットフォームは画一的な存在ではありません。Akamai の根元は「コンテンツ・デリバリー・ネットワーク」であり、現在提供している多くのソリューションはここから発展しています。

Enhanced SSL（ESSL）サービスは、元々は Payment Card Industry の Data Security Standard（PCI DSS）の要件を満たすネットワークセグメントを分離するために開発されました。商用、小売企業、金融機関向けに開発された ESSL ネットワークには、PCI や他の規制およびコンプライアンス分野で必要な物理、論理、デジタル制御の機能が追加されています。その名前にもかかわらず、ESSL は TLS などの最新の暗号化方式にも対応しています。

ESSL の登場以来、暗号化された安全なシステムをすべてのトラフィックで使用したいという願望は、今や当たり前の基準になっています。このような変化を受け、現在では Akamai が提供するすべてのトラフィックの 20% 近くが ESSL ネットワークを使用しています。Akamai では、トラフィックの測定にビット数ではなく、ヒット数を使用していますが、換算すると約 8Tbps になります。ESSL は、現在では Akamai の主要ネットワークの 1 つになっており、HTTPS ベースのトラフィックの大部分を提供しています。

Akamai では、API と HTML トラフィックを分析するために、2018 年 10 月の 10 日間を対象に、ESSL ネットワークのトラフィックを調査しました。その後、対象期間を短くして同様のクエリーを実行しましたが、ほぼ同じ傾向が示されました。

クエリーは、特に API と HTML トラフィックを検索しており、API トラフィック（JSON + XML）または HTML の形式以外のトラフィックや画像などは含まれていません。Akamai では、ヒット数（リクエスト／レスポンス）とトラフィック（送信されたボリューム：ビット数とバイト数）を意図的に区別しています。

ESSL の登場以来、暗号化された安全なシステムをすべてのトラフィックで使用したいという願望は、今や当たり前の基準になっています。

クレジット

インターネットの現状／セキュリティチーム

Tony Lauro（Senior Manager、セキュリティ戦略 -「小売業界に対する大規模な攻撃に利用されるツール」）
Martin Flack（Principal Architect -「API トラフィックの増加」）
Moritz Steiner（Principal Architect -「API トラフィックの増加」）
Kyle Schomp（Performance Engineer Senior II -「IPv6 は過少報告されているのか？」）
Rami Al-Dalky（インターン -「IPv6 は過少報告されているのか？」）

編集スタッフ

Martin McKeay（Editorial Director）
Amanda Fakhreddine（Sr. Technical Writer、Managing Editor）
Steve Ragan（Sr. Technical Writer、Editor）

制作

Benedikt Van Holt（アートディレクション）
Brendan John O'Hara（グラフィックデザイン）
Georgina Morales Hampe、Kylee McRae、Murali Venukumar（プロジェクトマネジメント）

Akamai *Intelligent Security Starts at the Edge*

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 /24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com/jp/ja/、blogs.akamai.com/jp/ および Twitter の @Akamai_jp でご紹介しています。全事業所の連絡先情報は、www.akamai.com/jp/ja/locations.jsp をご覧ください。公開日：2019 年 2 月。