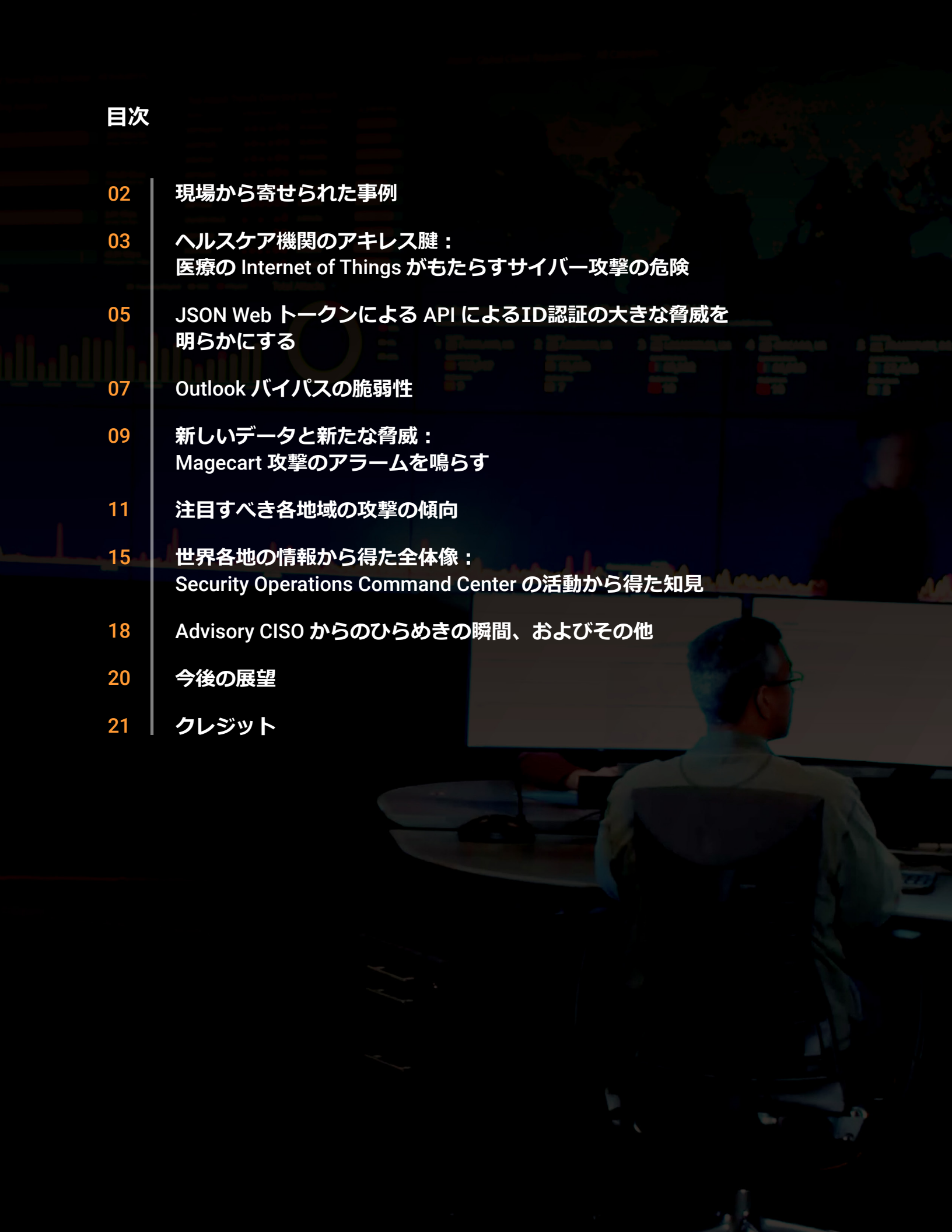
年間レビュー

2023 年のサイバートレンドと今後の見通し

目次



現場から寄せられた事例

このインターネットの現状（SOTI）に関するレポートでは、今年発表したレポートをそれぞれ見ていく形の従来の年間レビューとは異なり、1 つの中心的なテーマにフォーカスしています。それは、「今年気に入ったセキュリティの話題」です。Akamai の Security Intelligence Group（SIG）に属するライターやデータサイエンティストに、過去 10 か月間に取り上げた事例について年間評価を依頼しました。Akamai のセキュリティ調査のブログや、2023 年 SOTI レポートで公開した多数の注目すべき話題や新たな発見から、1 件だけを選び出すのは大変な作業だったでしょう。当社の Advisory CISO および Security Operations Command Center（SOCC）の Vice President にも、今年の攻撃の傾向と 2024 年に反映できる主な知見の考察を依頼しました。

セキュリティ業界および Akamai のセキュリティリサーチ内部では、さまざまなことが起きました。当社のセキュリティ専門家によるリサーチ作業がコミュニティーに対して有用であったことは疑いありません。当社の専用ハブを通じて、セキュリティのプロは知見、緩和戦略、攻撃の傾向など、信頼できるリソースに容易にアクセスし、各自の組織の防御に役立てることができます。当社の RPC ツールキットなどのフリーツールや、無料でオープンソースの Adversary Emulation プラットフォームである Infection Monkey にもアクセスできます。Infection Monkey はマルウェアのように伝播し、ビットを反転すれば簡単に複合化できる形でファイルの「暗号化」もできます。こうすることで、攻撃者がどのようにして環境内を移動できる（できない）かを、現実に即して理解できます。脅威が進化する速度に対応するためには、テストを継続的に行う必要があります。担当者は、前回の侵入テストでの成績だけでなく、現在のネットワークの対応状況も知る必要があります。

2023 年の状況を一言で表すなら、それは「転換（pivot）」ではないでしょうか。攻撃者はセキュリティ対策を回避するために戦術を転換し、新たなアタックサーフェスやまだ侵害されていないターゲットを探し、あらゆる規模や業界の組織に大きな損害を与えました。セキュリティの防御側にも同じことが当てはまり、攻撃を緩和し、組織の保護を改善するために、手直しを加えながら新たな方法を学び続けています。ソリューション、リサーチ、ツールを通じて、私たちはある目標に向けて転換します。それは、実践的な知見と緩和対策を、私たちと同じセキュリティ脅威に対応するセキュリティ担当者に与えるという目標です。

この記事がご参考になれば幸いです。

ヘルスケア機関のアキレス腱：医療の Internet of Things がもたらすサイバー攻撃の危険

私は Badette Tribbey です。SOTI レポートの執筆者の 1 人です。セキュリティ専門家およびデータサイエンティストと協力して、技術上の発見とデータから有用な知見を導き出しています。数学は苦手ですが、数値を使って、攻撃の傾向を確実に見つけ出すことが好きです。

今年取り上げた最も注目すべきトピックの 1 つは身につまされるもので、医療の Internet of Things（IoMT）のリスクの高まりです。「セキュリティギャップのすり抜け」と「猛威を振るうランサムウェア」の両方で、ヘルスケアおよび生命科学におけるリスクの概況を調査し、この業界が攻撃を受けやすい理由を検討しました。最も印象深いことの 1 つは、MRI 機器、インスリンポンプ、ウェアラブルなどの IoMT 資産が、患者にとって非常に利便性が高いものである反面、ヘルスケア機関のリスクを大幅に引き上げているという点です。これらの組織はすでに、ヘルスケアエコシステムの複雑性、レガシーテクノロジーの脆弱性、IT およびサイバーセキュリティ関連の人材配置の問題により、境界保護に関して課題を抱えていました。さらに、この環境では、タイミングよくパッチを適用するのは至難の業です。複数のシステムやアプリケーションに対して、様々なベンダーからアップデートが提供されるため、追跡が困難であるためです。

パッチが適用されていない IoMT デバイスはすべての業界において最も脆弱な資産に該当し、ランサムウェアなどの悪性度の高い脅威を招きかねません。IoMT が飛躍的に増加し、それに伴い API の使用も増えるにつれ、その脆弱性も増大し、攻撃者がターゲットにおける足がかりを得る手段となったり、悪用されてデータ侵害が発生したりする可能性があります（図 1）。米国における複数の病院およびヘルスケア機関を対象として実施された Cynerio と Ponemon Institute による調査の共同レポートでは、半数以上が IoMT デバイスのセキュリティギャップによるサイバー攻撃を受けたとされています。

> “この [ヘルスケア] 環境でタイミングよくパッチを適用するのは至難の業です。複数のシステムやアプリケーションのベンダーからアップデートが提供されるため、追跡が困難であるためです。
>
> – Badette Tribbey、Senior Technical Writer、Akamai

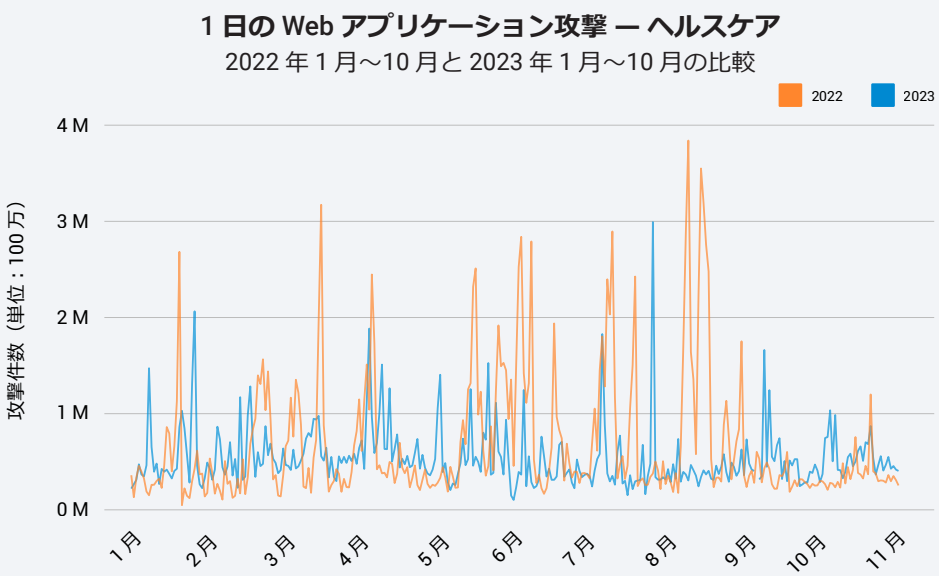


図 1：ヘルスケア/製薬業界における Web アプリケーションおよび API 攻撃は、2022 年から 2023 年の間、散発的に急増しながら常時発生しています。攻撃数は前年比で 21% 減少していますが、2023 年における 1 日あたりの攻撃数の中央値は 2022 年よりも増えています。

ヘルスケア業界の今後の展望

ヘルスケア業界が IoMT を拡大させていくと、医療サービス（遠隔医療や患者のリモートモニタリングなど）にアクセスするために API は引き続き重要な役割を担うことになり、臨床および財務の面で成果の向上につながります。また、健康記録や患者データはダーク Web 上で高い価値があるため、ヘルスケア機関に対する攻撃が減少する可能性は低いでしょう。

これまでに起きたことから今後起きることに視点を移すと、攻撃者がこれからも新たな攻撃を作り出し、攻撃の範囲と複雑性を拡大しようとしていることが明確になります。ゼロデイ脆弱性を利用した、より技術的な攻撃が引き続き増えていくと考えられます。さらに、規制をめぐる状況（Protecting and Transforming Cyber Health Care [PATCH] Act of 2022 など）が変化を続けていることから、当社のソリューションが喫緊のプライバシー、報告、決済、データ主権、耐障害性に関する多数の法律に役立つことを確かなものとする必要があります。最後に、このような CISO にとって攻撃による混乱がさらに増えることが予想されます。彼らは、より少ないベンダーに統合したうえで、ハッカーの滞在時間を最小限に抑えるソリューションの利用に予算をシフトするでしょう。

JSON Web トークンによる API によるID認証の大きな脅威を明らかにする

Lance Rhodes です。2023 年 3 月から、Akamai SIG チームのサイバーセキュリティの執筆者として活動しています。私の仕事の多くはレポートとブログをつなぐ「接着剤」の役割です。ブログ投稿と横断研究の発行と執筆、SOTI レポートのコンテンツとマーケティング資料の執筆に取り組んできました。そしてこのすべてが、毎月の社内外へのニュースレターおよびセキュリティ会議への提出物についてのチームとのコラボレーションに結び付いています。

今年取り組んだブログ投稿の中でも最も刺激的だったものの 1 つが、JSON Web トークン（JWT）の投稿です。この投稿はアプリケーションおよび API に関する SOTI レポート（セキュリティギャップのすり抜け）と直接つながっており、ここでは API によるID認証の標準的手法の 1 つである JWT での認証の不備について詳説しています。JWT の理解を深めていくのは楽しい経験でした。

今年初めにアプリケーションおよび API の SOTI レポートに取り組んだ後、Nitzan Namer と JWT の投稿に取りかかり、ユーザー認証の不備に対する攻撃ベクトルとしての JWT に焦点を当てました。それは Open Web Application Security Project（OWASP） API Security Top 10 のうちのひとつです。SOTI レポートにはこの点のみを取り上げたセクションがありましたが、ブログ投稿では JWT 構造と、特権昇格、データ漏えい、アカウントの乗っ取りなどの最大の脅威から保護するためのベストプラクティスについて、掘り下げて説明しています。

この投稿が、セキュリティ研究者、技術担当者、JWT ユーザーおよび管理者にとって継続的に使用されるリソースとなればよいと Nitzan と話したことを覚えています。投稿の構造上のスタイルで、その望みが叶うようにしました。JWT の基本事項を最初に取り上げ、その後、6 件のシナリオが続き、共通する同じ脅威の例を示し、それぞれに対するベストプラクティスを述べています。基本事項として、JWT が JSON オブジェクトとして共有する情報を含むトークンを発行して、API を保護する方法を説明しています。各トークンは暗号化ではなくエンコードされ、ヘッダー、ペイロード、検証用署名（サーバーがトークンを発行した後にデータが改ざんされていないことを認証する）で構成されます。

> “ブログ投稿では JWT 構造と、特権昇格、データ漏えい、アカウントの乗っ取りなどの最大の脅威から保護するためのベストプラクティスについて、掘り下げて説明しています。
>
> – Lance Rhodes、Cybersecurity Writer、Akamai

6 件のシナリオは、以下のとおりです。

1. 検証なしでサーバーがトークンを使用できるようになっている
2. 異なるアプリケーションに同じ秘密鍵を使用している
3. 弱い署名アルゴリズムを使用している
4. 短く、低エントロピーの秘密鍵を使用している
5. 機微な情報を JWT のペイロードに保存している
6. 鍵の悪用

JWT は最も一般的な検証フォーマットの 1 つです。このフォーマットでは多数のミスが発生する可能性がある広範なアタックサーフェスが生じるので、適切なセキュリティ対策の導入が不可欠です。これらのシナリオでは JWT への最も一般的な脅威の一部を示していますが、シナリオはこの他にも多数あり、攻撃手法は絶えず進化しています。

JWT は暗号化されず、セキュリティを念頭に実装されてもいない

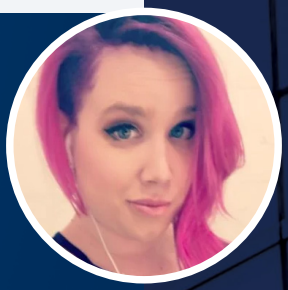
このブログの投稿内容の最大の要点は、JWT は暗号化されず、セキュリティを念頭に実装されてもいないということです。このように普及している認証トークンがこれほど脆弱であるのは信じがたいことです。JWT のメリットの一部は、何度もサインインせずに多数の Web アプリケーションや API を使用できることです。SOTI レポートでも JWT ブログ投稿でも、実際利用されている JWT のアルゴリズムを Akamai トラフィックで分析した結果、理論的には安全性が低く非対称アルゴリズムほど保護能力が高くないのにもかかわらず、最もよく使われるのは対称アルゴリズムであると突き止めました。両資料には、例えば Akamai の顧客の 54.8% が HS256 アルゴリズムを使用していることが示されていますが、これは対称アルゴリズムです。

対称アルゴリズムが選ばれることが多いのは、おそらく、ユーザーが必要とするのが 1 つの鍵だけで、非対称アルゴリズムにはより多くの計算リソースが必要となるためです。JWT の暗号化バージョンである JSON Web Encryption も、あまり普及していません。ほとんどの企業が JWT を使い、計算にかけるパワーを節約することを選びます。

要点：利便性、コスト、速度は、セキュリティよりも優先されがちです。これは私たちセキュリティ研究者やライターの仕事の重要性を思い起こさせる重要な点です。効率と安全性のバランスを取るには、優れたセキュリティのリサーチおよびプラクティスが必要です。

> このように普及している認証トークンがこれほど脆弱であるのは信じがたいことです。
>
> – Lance Rhodes、Cybersecurity Writer、Akamai

Outlook バイパスの脆弱性



こんにちはご機嫌いかがでしょうか。私は Tricia Howard です。SIG のブログを担当しています。技術記事の中心に身を置き、当社の研究者、コーポレート・コミュニケーション・チーム、法務部門（何より重要）と協力してタイムリーに効率よく情報をつなぎ合わせて記事を完成させます。私の仕事の一番良いところは、当社の研究者たちがとても素晴らしい仕事をするので、それを自慢できることです。

私が今年執筆を依頼された中で、これが最も難しかったと言えます。私たちのチームがこの 1 年間で成し遂げたすべての素晴らしいことの中から、1 つだけお気に入りを選ぶことなどできません。それでも 1 つだけ選ばなければならないので、著名な（または悪名高い）Outlook バイパスの脆弱性に関する Ben Barnea の投稿を選びました。Ben は私が知る中で最も聡明な研究者であり、たった 1 つのスラッシュでパッチ全体を壊す方法を見つけ出しました。信じられないし、不可能とさえ思われますが、実は可能で、彼はそれをやってのけました。

オリジナルの脆弱性では、不正な攻撃者がカスタム通知音を伴う Outlook のインバイトを送信できました。同時にこの通知音が攻撃のパスとなり、攻撃者のサーバーに接続可能になり、NTLM の認証情報が提供されます。これは本当によくないことで、これで攻撃者は認証情報に対するブルートフォース攻撃やリレー攻撃を行うことができます。そして当然ながら、こうしたことから特権昇格につながり、この後何が起きるかはご存じのとおりです。最悪なのは、この脆弱性はゼロクリックであり、この攻撃を実行するためにユーザー操作は不要だということです。この背後には何か強力な仕組みがあり、特に、この発生元がロシアで広まっており、ヨーロッパのさまざまな政府機関に忍び込んでるとしたら、危険というほかありません。

パッチは 3 月に公開されました。これは、攻撃者が、悪意のある人物のサーバーに接続するために PidLidReminderFileParameter にカスタムパスを指定する能力を取り除くものです。このパッチではそのかわりに、インターネットに接続しようとしているパスがどうかを確認する MapURLtoZone 機能を使用します。接続が試行されると、従来の通知音が鳴り、カスタム通知のファイル・パス・オプションが排除されます。これにより、理論的にはリモート攻撃者がこの脆弱性を利用するチャンスがなくなります。攻撃者と攻撃対象との接続を確立するためには、最終的にインターネットに呼び出す必要があるからです。

> 防御側は毎日多忙で、そのうえ、新しいゼロクリック特権昇格の脆弱性に気を配らなければなりません。
>
> – Tricia Howard、Senior Technical Writer、Akamai

パッチの阻止

ここからがさらに面白くなります。こう言っては何ですが、愉快とも言えます。優れた研究者の常として、Ben は脆弱性が本当にもう悪用されないかを確かめようとしました。単純な言い方ですが、MapURLtoZone には基本的に許可と拒否という 2 つのオプションがあります。つまり、インターネットに向けて呼び出すか、呼び出さないかです。大部分は、パッチは意図したとおりに動作しました。パスがローカルに思われる場合でも、MapURLtoZone はパスがインターネットに到達するものと認識し、その動作をブロックしました。

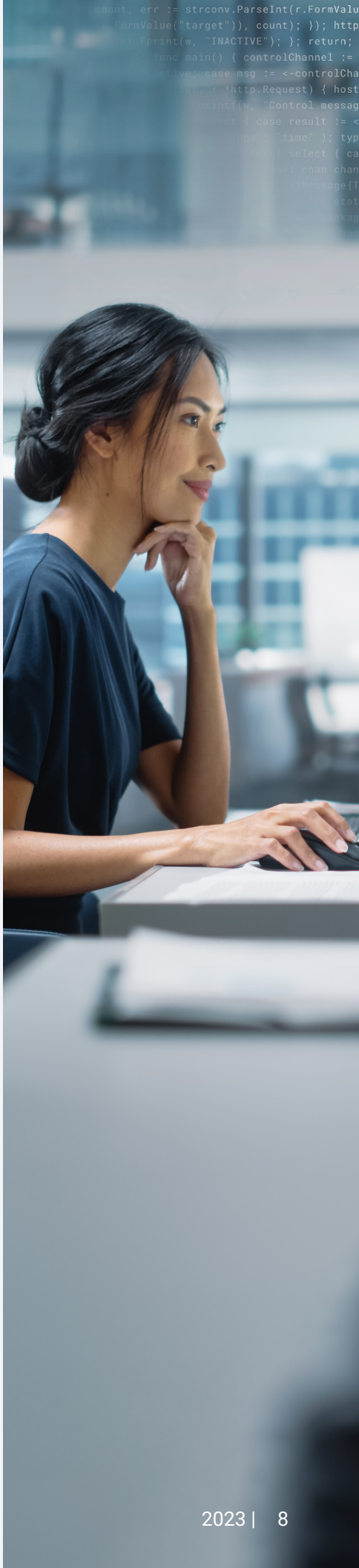
Ben はパス名の末尾に「/」に追加してみることにしました。MapURLtoZone に予期されていないものを指定すると、それを許可するか拒否するかを決定しなければなりません。スラッシュの追加は認識されず、そのために 0 が返され、関数によってこのパスはローカルで信頼できると解釈されました。その後は、残った脆弱性を意図した通り実行できるようになりました。これはカスタムパスで、CreateFile を行おうとするものです。

これがすべてです。スラッシュを 1 つ追加しただけで、**重大**な脆弱性に対応するパッチ全体が、まったくの役立たずになってしまいました。このパッチはおそらく、サイバー専門家がこの脅威を排除するために数日または数週間から数か月の時間と労力をかけて作成したものですが、1 つのスラッシュによって無効にされたのです。

分析してみると、元の攻撃がどれほど洗練されていたか、舌を巻くほどです。攻撃者は Magnus Carlsen 級の巧みさで長期戦を戦っています。スラッシュだけでパッチを無効化できたことから、攻撃者らはバイパスする方法を自力で見いだしたと推測できます。固定概念にとらわれることなく考えて、Ben がそれを発見したのは本当に素晴らしいことです。

だからこそ、こうしたバグを発見する研究者たちは、セキュリティコミュニティーの活力源なのです。防御側は毎日多忙で、そのうえ、新しいゼロクリック特権昇格の脆弱性に気を配らなければなりません。セキュリティ研究者は、毎日の生活においてテクノロジーやインターネットの活用が増えている中で、実質的な変革を起こそうとしています。

この素晴らしいチームの一員となり、世界で最も優れた考えを持つ人々と働けることを誇りに思います。私たちのブログ、X（旧 Twitter）のポスト、SOTI を読んでくださった方々に感謝いたします。そして Akamai SIG 内部および外部の研究者には、あらゆる作業内容、分析、発見に感謝します。来年は何が待ち構えているか、楽しみです。



新しいデータと新たな脅威：Magecart 攻撃のアラームを鳴らす

Chelsea Tuttle です。Akamai で働いて 8 年近くになります。過去 4 年間の SOTI に取り上げられたデータを担当するデータサイエンティストとして、大部分の時間をデータのクリーニング、調査、分析、視覚化に費やしています。データ処理以外には、SOTI の執筆者と密接に連携し、データが示すストーリーの伝達を支援しています。ビッグデータは複雑で、履歴データのレポートからメリットを得られるので、新しいデータセットを追加することはあまりないのですが、今年は追加しました。2023 年を振り返ると、この新しいデータセットについて公開したいくつかの事例がお気に入りとして思い浮かびます。この調査に伴う学習の機会が楽しかったからです。

私たちは、ネットワーク全体で確認された攻撃の試行回数について報告することに集中しすぎるあまり、潜在的な脆弱性の保護や攻撃の阻止に必要なデータを報告する重要な機会を逃しがちです。今年 SOTI レポートに追加したデータセットの 1 つは、攻撃の量ではなく、潜在的な脆弱性の領域に焦点を当てたという点で他とは異なり、注目に値します。このデータセットは、Akamai Client-Side Protection & Compliance が毎日数十億の Web ページスクリプトを隅々まで監視することによって提供された観察結果から派生しています。私たちが監視する潜在的な脆弱性の領域の 1 つは、Web サイト上で利用されているファーストパーティーとサードパーティーのスクリプトの数です。ファーストパーティスクリプトの使用がセキュリティを保証するものではなく、使用しているサードパーティースクリプトに脆弱性があるとは限りませんが、サードパーティーを信頼して Web ページスクリプトをホストするなど、外部への信頼を高めると、セキュリティプロファイルへのリスクが高まります。Akamai は、あらゆる業界でサードパーティースクリプトの使用が増加したことで生まれた、利便性とセキュリティとのギャップを埋めるべく取り組んでいます。

2023 年 6 月の「コマース業界における脅威トレンドの分析」SOTI レポートで示したように、今年の Akamai リサーチの注目領域の 1 つは近年の Magecart 型の Web スキミング攻撃です。具体的には Magecart 攻撃がデジタルコマース業界に侵入し続けている様子を調べています。このタイプの攻撃では、悪性の JavaScript コードインジェクションを使用して、クレジットカード情報などの機密性の高いユーザー認証情報をデジタルコマース Web サイトのショッピングカートから盗み出します。このタイプの攻撃は攻撃者にとって比較的容易ですが、消費者には大きなリスクが生じ、検知はますます困難になっています。これらの Magecart などの Web スキミング攻撃は、Web サイトの利用者や所有

> “Akamai は、あらゆる業界でサードパーティースクリプトの使用が増加したことで生まれた、利便性とセキュリティとのギャップを埋めるべく取り組んでいます。
>
> – Chelsea Tuttle、Senior Data Scientist、Akamai

者が気づかないうちに発生することが多く、攻撃者は一般に、脆弱または旧式のソフトウェアを使用するデジタルコマース Web サイトを選びます。

最近の Magecart の亜種

Akamai の研究者が確認した最近の Magecart キャンペーンでは、多数の Magecart の亜種が見られます。2023 年 6 月の SOTI レポートでは Magecart クライアント側攻撃に焦点を当て、オープン・ソース・ライブラリのサードパーティースクリプトで見つかった脆弱性の悪用により、サプライチェーン攻撃を招いたとしています。この SOTI レポートの執筆直後、Akamai の研究者が新しい Magecart 型キャンペーンを発見した方法に関するブログ投稿を公開しました。このキャンペーンでは、正当な Web サイトを悪用して他のサイトを攻撃していました。このキャンペーンの攻撃対象の Web サイトには、基本的に 2 セットありました。正当なサイトがハイジャックされてホストとして使用され、攻撃者が制御するサーバーとなり、脆弱なコマースサイトがクライアントサイド Web スキミングで攻撃されます。8 月には、Akamai の研究者が別の新しい Magento キャンペーンを発見した様子を紹介する 2 番目のブログ投稿を公開しました。このキャンペーンでは、隠されたサーバーサイド・テンプレート・インジェクションにより、デジタル・コマース・サイトを悪用して被害者の支払い状況を入手していました。

Akamai のリサーチャーたちが、正当な Web サイトを悪用して他のサイトを攻撃する Magecart 型の新しいキャンペーンを発見しました

Akamai SIG の最新の Magecart ブログ投稿では、攻撃者が Web サイトのデフォルトの 404 エラーページを操作して悪性のコードを隠すための新しい難読化手法について説明しています。Akamai の研究者は、この新しいキャンペーンには 2 つの高度な隠ぺい手法が追加されていることを発見し、攻撃者が攻撃チェーンを延長して検出を防ぐために使用している開発戦術を明らかにしました。

2023 年も終わりに近づいた今、新しいデータと新たな脅威から得られた研究とレポートのすべての機会を振り返ると、この先 2024 年にある新しいデータと学習の機会に期待せざるを得ません。

注目すべき各地域の攻撃の傾向

私は Charlotte Pelliccia です。2023 年に SOTI チームに加わりアジア太平洋および日本（APJ）、ヨーロッパ、中東、アフリカ（EMEA）地域の事例を紹介しています。私たちの APJ および EMEA のスナップショットは、グローバルな SOTI レポートの姉妹編です。ここでは、2023 年に取り上げた攻撃の傾向の中でも顕著なものをいくつか挙げて、今年初めに公開したスナップショットのデータを更新します。

Web アプリケーションおよび API 攻撃 – 2 つの業界の事例

当社の最新の金融サービスおよびコマース SOTI レポートにもあるように、APJ において金融サービスは Web アプリケーションおよび API 攻撃の標的となっている第 1 位の業界です（第 2 位はコマース）。2023 年 6 月のレポート以降、金融サービスへの攻撃は 45 億件にも上りました（37 億件から 22% 増加）。そして 2023 年 3 月のレポート以降、コマースへの攻撃は 12 億件から 19 億件へと 58% 増加しました。各業界内での内訳は比較的一定しています（図 2）。

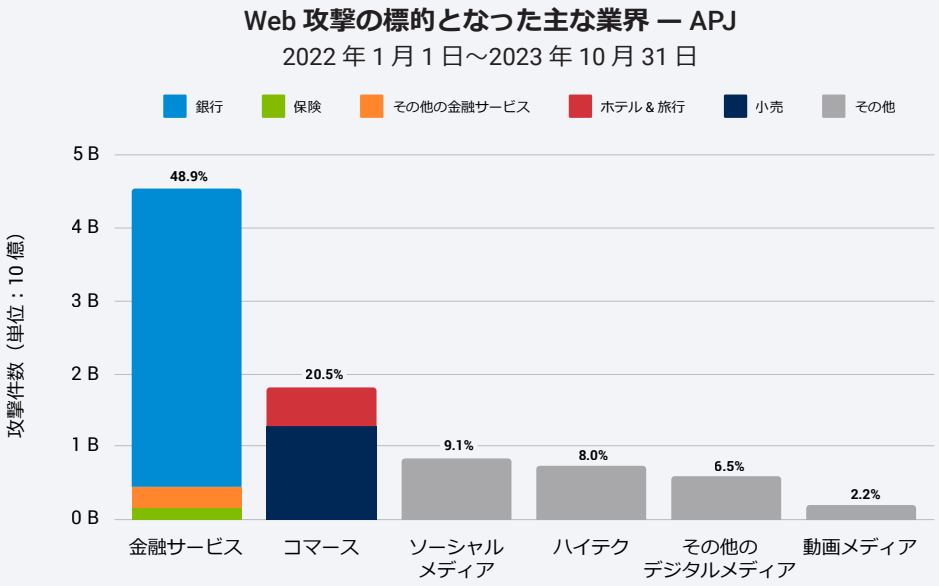


図 2：2023 年 10 月までの APJ での業界別 Web 攻撃

> 組織がリスクへの理解を深め、ツールとベストプラクティスを微調整するためには、地域別の攻撃トレンドを可視化することが重要です。
>
> – Charlotte Pelliccia、Cybersecurity Writer、Akamai

同時期の EMEA において、コマースは Web アプリケーションおよび API 攻撃を最も多く受けた業界であり、2023 年 3 月のレポート以降、最高で 65 億件の攻撃を受けました（46 億件から 41% 増加）。製造業が 4 位から上昇し、金融サービスを抜いて 3 位になりましたが、金融サービスへの攻撃は 2023 年 6 月のレポート以降 70% 増加し、10 億件から 17 億件に達しました。ここでも、各業界内での内訳は比較的一定しています（図 3）。

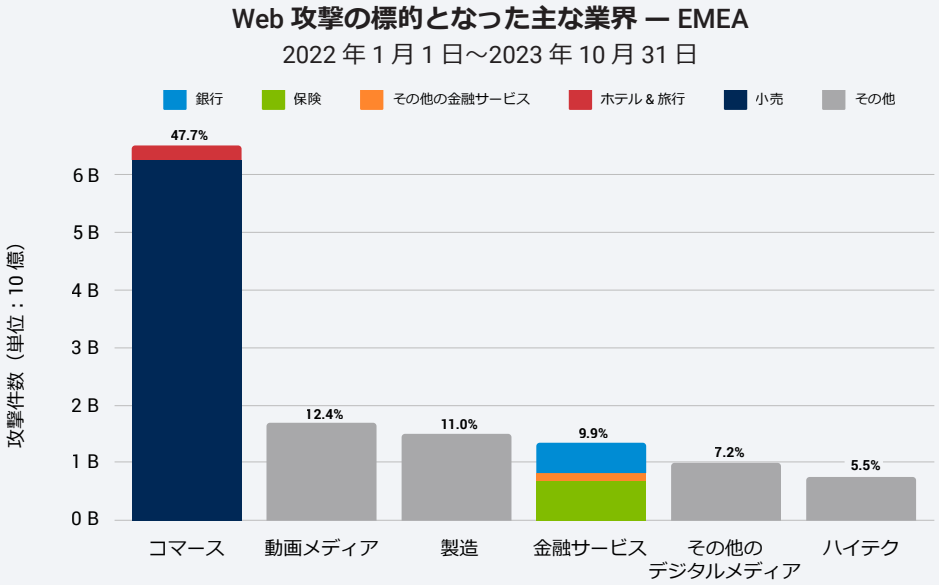


図 3：2023 年 10 月までの EMEA での業界別 Web 攻撃

悪性ボットが多用されている

以前のレポートで見てきたように、APJ は引き続き悪性ボットの活動において北米に次いで 2 位です。2022 年 1 月から 2023 年 10 月の APJ において攻撃を受けた上位 3 つの業界は、コマース（27.4%）、動画メディア（15.0%）、金融サービス（14.3%）です。EMEA では、すべての悪性ボットの活動のほぼ半分（50.1%）がコマースを標的としており、その他のデジタルメディアが 15.3%、動画メディアが 12.2% と続きます（図 4）。

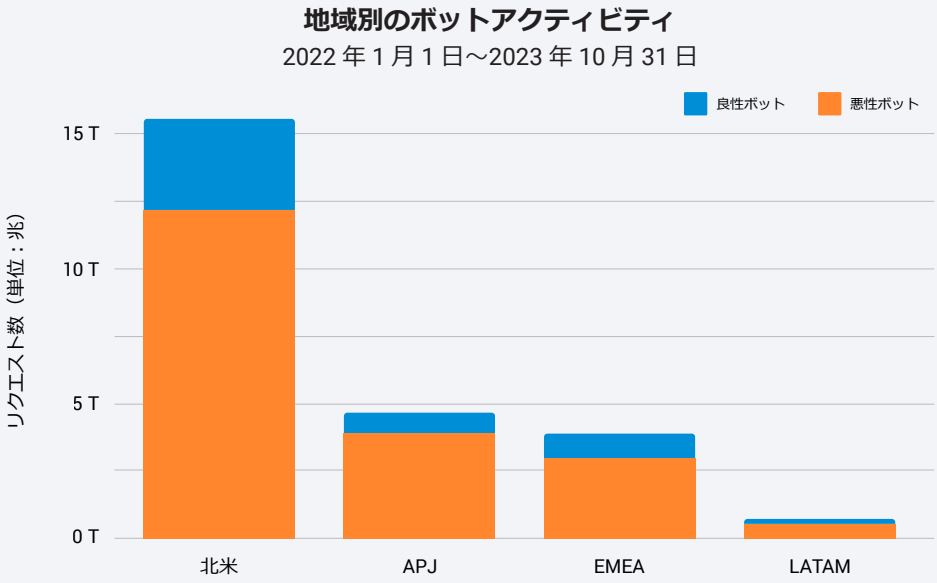


図 4：悪性ボットの使用はすべての地域で広まっており、良性ボットの使用を大きく上回っている

> ボットと DDoS 攻撃の変化に関する SOCC の見解について、以下のエッセイをお読みください。

EMEA は DDoS 攻撃の地域シフトの標的になっている

2023 年のレポートからは、攻撃者が EMEA に真正面から狙いを定めていることが明確になっていますが、その理由の一部は現在の地政学的状況にあります。代表的な例として、EMEA における金融サービス、ギャンブル、製造業界への分散サービス妨害（DDoS）攻撃イベントの件数は、その他すべての地域の件数の合計を上回っています（図 5）。

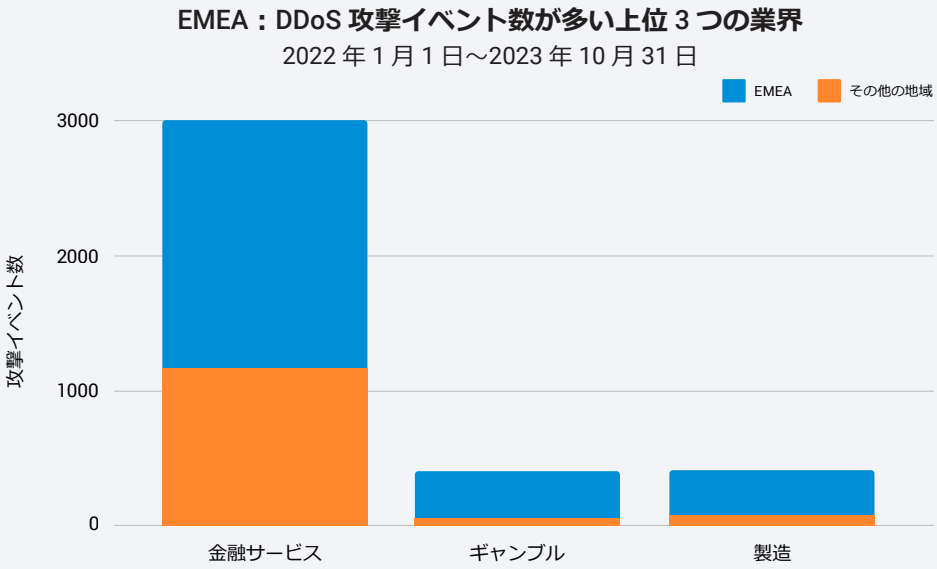


図 5： EMEA はこれらの業界だけで他の地域の合計より多くの DDoS 攻撃を受けている

今後の展望

攻撃者が Web、ボット、DDoS 攻撃で成功を収めている間は、これらが多用されると考えるのが理にかなっています。事実、これら 3 つのベクトルはすでに進化を遂げ、強度を維持したり増したりしています。（CL0P などのランサムウェアグループが）Web アプリケーションへのゼロデイ攻撃をランサムウェア手法と組み合わせて、DDoS 攻撃を追加することで、三重に脅迫する手口が生まれました。ボットによる Web スキャルピングは、ほぼすべての大手航空会社のイベントやチケット販売において新たな標準となりました。また、API のビジネスロジックを狙う API 攻撃が登場しています。

それに応じて、規制による監督と報告義務が世界中の業界で増加し続けています。攻撃を受けない地域や業界はないからです。目的は、サイバーセキュリティに関する法律を、進化する脅威の状況に合わせて最新に維持することです。組織は、報告要件を満たすよう目を配り、多層防御によってリスクを緩和する体制を整える必要があります。

世界各地の情報から得た全体像：Security Operations Command Center の活動から得た知見

Roger Barranco です。Global Security Operations の Vice President を務めています。私は 10 年ほど Akamai で働いており、マネージドセキュリティ業務を担当しています。これは世界中の 6 つの SOCC で運用され、素晴らしいチームが運営しています。私がサイバーセキュリティのキャリアを始めてそれにのめり込んだのは、この分野が興味深く、常に変化している市場だからです。2023 年はこれを裏付ける良い例です。

Akamai SOCC はこれまでにないほど多忙を極め、2023 年の終わりには、処理するセキュリティチケットの数は昨年より約 30% 多くなるでしょう。ここでは、当社のマネージド・セキュリティ・サービスの顧客との対応から得た、2024 年に向けて組織が留意すべき主な知見を紹介します。

DDoS 攻撃は変化している

攻撃を受けている顧客の数は年々増えていますが、攻撃の手法は過去と現在では異なっています。まず、攻撃を受ける顧客の資産のタイプと量が変わりました。たとえば、同一または類似のエンドポイントに対する 10 件の攻撃ではなく、顧客のネットワーク空間にある異なる IP に向けた 100 件の攻撃が行われます。このような攻撃はレイヤー 3 だけでなく、レイヤー 7 も同時に標的にします。さらに、DNS に対する攻撃が飛躍的に増加し、その大半は有効なクエリー攻撃で、顧客の DNS インフラを容易に疲弊させてしまいます。不要な DNS トラフィックが数メガバイトあるだけで、エンタープライズには多大な負荷がかかります。また、やっかいなことに Mirai の活動が復活し始めています。Mirai は Internet of Things (IoT) の力を利用して広範な妨害を引き起こすことで知られています。

今日の脅威の概況では、エッジに強力な仕掛けを組み込んで攻撃に対応するだけでは不十分です。組織には、このワークロードに対処し、状態を維持しながらこれらの各エンドポイントに独自の保護を実装する、堅固なクラウドレベルのセキュリティサービスが必要です。このような状況で、Akamai はプラットフォームとサービスの両面で優れています。多層からなるセキュリティを適用して、あらゆる種類のサイバー攻撃から防御することができます。実地経験を積んだ専門家が各顧客の差異や傾向を調査し、具体的な方法で監視や緩和を行い、悪性のトラフィックを停止し、予期されたクリーンなトラフィックを通過させます。

> Akamai SOCC はこれまでにないほど多忙を極め、2023 年の終わりには、処理するセキュリティチケットの数は昨年より約 30% 多くなるでしょう。
>
> – Roger Barranco、Vice President of Global Security Operations、Akamai

ボットとの容赦ない戦い

Credential Abuse は緩和が困難です。必要なトラフィックの中から不要なトラフィックを見分けるのは難しく、顧客にはそれぞれ独自のバックエンドがあり、異なる緩和対策が必要だからです。さらに、Credential Abuse を実行する攻撃者は最もスキルが高く用心深い部類に属しています。これは、Credential Abuse が成功すれば最も容易に収益を手にできるからです。これらのボット攻撃は危険でコストがかかるので、Credential Abuse 防止ソリューションを備えておくことが重要です。特に、悪性ボットの使用が増え続けている金融サービス業界やコマース業界ではなおさらです。

引き続き攻撃者の対象となる EMEA

ウクライナ侵攻以降、EMEA（特にヨーロッパ）は、さまざまな業界の数および攻撃タイプのカテゴリーにおいて、米国に代わってサイバー攻撃を最も受けている地域となりました。その最たるものが DDoS です。この変化は、攻撃者の多くが国家であるか国家の支持者であり、彼らがヨーロッパに向ける集中力は衰えないという事実を示唆しています。

攻撃者は巧妙さを増している

汎用ツールを利用して運を天に任せて攻撃を仕掛けたり、DDoS ボットネットを 1 時間 10 ドルで借りてビデオゲームの対戦相手を負かしたりするような、スクリプトキディが主な脅威であった時代は終わりました。今日、攻撃者はさらに巧妙になり、特定のターゲットに絞って集中しているように思われます。戦略を練り、時には 1 年にもわたる偵察を事前に行い、攻撃を工夫して認識した弱点を利用しようとします。攻撃者達が下準備を整えた結果、今日の攻撃の持続時間は、わずか数分しか継続しないことが多かった過去数年の攻撃よりも長くなりました。

> 攻撃者達が下準備を整えた結果、今日の攻撃の持続時間は、わずか数分しか継続しないことが多かった過去数年の攻撃よりも長くなりました。
>
> – Roger Barranco、Vice President of Global Security Operations、Akamai

サイバーと運用を調整するためのベストプラクティス

これらの課題にもかかわらず、お客様はサイバーと運用の連携に関する 2 つのベストプラクティスに従い、Akamai を顧客のサイバーチームの延長として活用することで、作業の効果を向上させ、自らを保護できます。まず、攻撃中ではなく、平時に SOCC と提携し、防御対策をプロアクティブに構築します。こうすることで、本番環境に影響を与えることなく攻撃を事前に緩和でき、お客様は回避した攻撃の細部についてのフォローアップレポートを受け取ることができます。

次に、運用の準備状況とバックアップ計画にプロアクティブに取り組みます。たとえば、テストの中で、異なるプラットフォームにルーティングしたり、ルートから外したりできるかを把握しておく必要があります。5 分間の攻撃で、運用の問題から顧客には 1 時間の損害が発生します。つまり、運用面で準備しておくことは、サイバー問題のみの対応に準備することと同等に重要なのです。

今年は、サイバーセキュリティが常に変化している様子が特に強くうかがわれ、この傾向は継続すると予測されます。良いニュースは、これらの知見を応用すると、顧客は先回りして 2024 年に自分の組織を保護できることです。

Advisory CISO からのひらめきの瞬間、およびその他

私は Steve Winterfeld です。Akamai の Advisory CISO です。Nordstrom 銀行の CISO や、Charles Schwab のインシデントレスポンスおよび脅威インテリジェンス担当ディレクターを務めました。現在は、Akamai のパートナー様が顧客を確実に防御できるようにする業務や、当社がどこに能力を集中すべきかを判断する業務を担当しています。

今年は、驚くような傾向がいくつかありました。また、私たちの戦略を更新するために使える、データで裏付けされた傾向もいくつかありました。私が選ぶ今年の上位 9 件の事例には、いくらかのひらめきの瞬間、いくつかの予期されたニュース、そしてまったく変化しないと思われるものがありました。

ひらめきの瞬間

- 総計すると 10～16% の組織が少なくとも四半期に 1 回はネットワーク内でコマンド & コントロール（C2）トラフィックが発生しています。さらに、感染したデバイスの 26% がイニシャルアクセスブローカーに関連するドメインにアクセスしました。
- ランサムウェアの脅威概況に関しては、過去 6 か月にゼロデイおよびワンデイ脆弱性が頻繁に悪用されるなど、攻撃手法に気がかりな変化が見られました。
- Akamai の調査によると、複数のランサムウェアグループの被害を受けた組織では、最初の攻撃から 3 か月以内に後続の攻撃を受ける確率が 6 倍近くに上ることが判明しました。

予期されたニュース

- API のビジネスロジックを狙う API 攻撃は検知と緩和が困難です。そのため、個々のリクエスト単位での判断はいっそう難しくなっています。
- 組織は、新しい Payment Card Industry Data Security Standard（PCI DSS）v4.0 要件およびデジタル・オペレーショナル・レジリエンス法（DORA）規制に準拠する必要があります。

> これらの知見は、セキュリティプログラムの訓練や、冗長なツールやギャップがある場所の確認に役立つ優れたガイドとなります。
>
> – Steve Winterfeld、Advisory CISO、Akamai

まったく変化しないと思われるもの

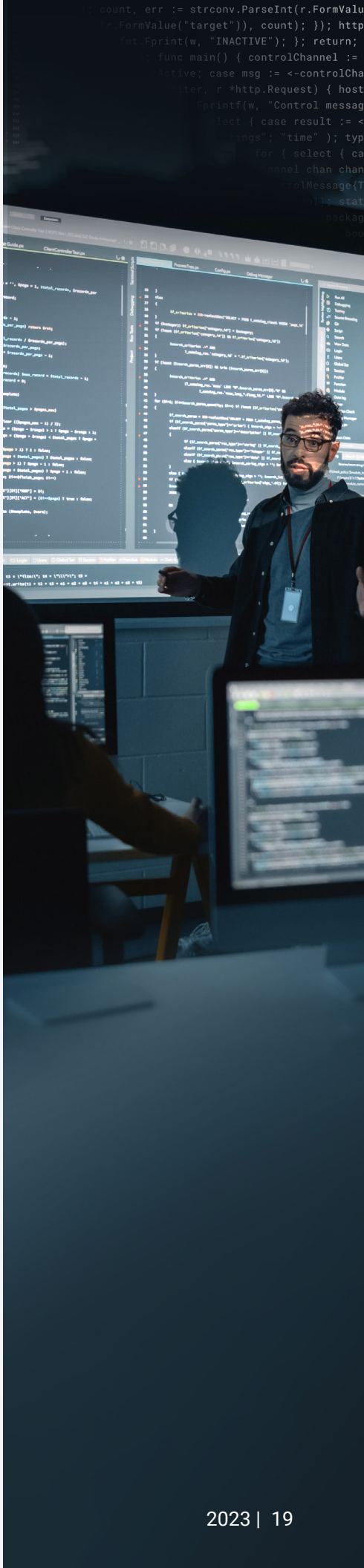
- ボットと API 攻撃の数は増え続け、DDoS 攻撃は新しい記録を更新していきます。
- 最も攻撃を受ける業界は金融サービス、ハイテク、コマースとなるでしょう。
- ローカル・ファイル・インクルージョン（LFI）は、最も利用頻度の高い攻撃手法です。
- 最も DDoS 攻撃を受ける地域は、北米からヨーロッパへと移り変わっています。

私が考え直すきっかけとなった 1 つの発見は、C2 通信からの侵害の検証済みの指標でした。特に悩んだのは、マルウェアがすでにシステムに侵入し、通信を確立した後に、高い頻度で初回検出が発生していることでした。このことから、影響を最小化するためには、予防対策と迅速な検知とのバランスが重要であることが浮き彫りになります。

私が最も驚いた傾向は、ソーシャルエンジニアリングによる攻撃からゼロデイの使用への転換です。ここ数年、私たちの技術的な防御は強度を増し、トレーニングと監視によってスタッフを強化する必要があると感じていました。しかし今年見られるゼロデイへの移行を受けて、来年どこに人員を配置するかを熟慮する必要があります。

最もアンフェアに思われる攻撃は、すでにランサムウェア攻撃に対処中である組織やランサムウェア攻撃から回復中である組織への攻撃です。危機的な状況に過剰反応して、実施中の防御監視からリソースを引き抜くのは簡単です。この調査は、防御を緩めるわけにはいかないことを強く思い起こさせるものです。

これらの知見は、セキュリティプログラムの訓練や、冗長なツールやギャップがある場所の確認に役立つ優れたガイドとなります。プレイブック／プロセスの更新、トレーニングの開催、侵入テスト計画の強化、リスク・ポートフォリオ・レビューのサポートのための演習を促進できます。サイバーセキュリティはチームスポーツなので、これらの知見は内部パートナー（法務や IT チームなど）およびベンダーとの議論を推進するためにも有益です。また、National Institute of Standards and Technology（NIST）、MITRE ATT&CK 知識ベース、OWASP Top 10 などの参考資料やツールも優れたリソースです。



今後の展望

将来を予言することは不可能ですが、DDoS や API 攻撃が 2024 年に蔓延することは予測できます。より大規模なボットネット群を構築し、新たな手法を開発するために絶えず活動し、国家からの影響力を受けることで、DDoS は拡大していきます。この要因とランサムウェアの進化があいまって、法規制と回復力の発端となるでしょう。

大半の業界において、API の実装の推進力となるのは、変革です。その急速な拡大は、意図せずにアタックサーフェスの拡大と脆弱性の増加、シャドー API、ゾンビ API、API の悪用を招きます。Web アプリケーションと API への攻撃が大幅に増加すると予期されます。LFI などの標準的な攻撃とサーバーサイド・リクエスト・フォージェリ（SSRF）やサーバーサイド・テンプレート・インジェクション（SSTI）などの新たな手法の両方がその原因となります。そのためにラテラルムーブメントを検知して影響を緩和できるツールが必要になります。

最後に、一部の業界や地域固有の傾向を除き、熟練したサイバーセキュリティの専門家が全体的に不足すると予期されます。機械学習や大規模言語モデルの人工知能によっていくらか軽減されるとしても、全体的には、必要な人材を見つけて維持することは非常に困難になります。そこで、オンデマンドの人材確保や必要性の低い職務向けのマネージドサービスについてベンダーと提携することになります。

Akamai SIG では、蔓延している脅威や新たに登場するセキュリティリスクに警鐘を鳴らし続けます。私たちは当社のプラットフォームとチャネルを通じてセキュリティコミュニティーと連携し、脅威インテリジェンスの取り組みを支援します。そして 2024 年には、SOTI レポートが 10 周年を迎えます。新しいデータセット、視覚効果、組織を保護し続けようとするセキュリティ専門家をサポートできる主要な知見を導入して、引き続きレポートを改善していきます。

来年もさらなる知見を紹介できると期待しています。そのときまで、皆様が危険にさらされないことをお祈りいたします。

クレジット

共同執筆者

Roger Barranco
Tricia Howard
Charlotte Pelliccia
Lance Rhodes
Badette Tribbey
Chelsea Tuttle
Steve Winterfeld

校閲およびテーマ別寄稿者

Kimberly Gomez
Reuben Koh
Emily Lyons
Richard Meeus
Carley Thornell

データ分析

Chelsea Tuttle

マーケティング・出版

Georgina Morales Hampe
Emily Spinks

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は、**akamai.com/soti** をご覧ください。

その他の Akamai 脅威リサーチ

akamai.com/security-research では、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通じ、常に最新情報を把握できます。

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

Akamai の脅威対策ソリューションの詳細については、**セキュリティソリューション**のページをご覧ください。