MARKET PERSPECTIVE

クライアントサイドWAF：これからのセキュリティフロンティア

Christopher Rodriguez

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot:：クライアントサイドの脅威と新たなソリューション

2018年、セキュリティ研究者は、オンラインカードスキミングまたはWebスキミングと称される新しい形態のサイバー犯罪を特定した。Magecart（メイジカート）の攻撃は、アプリケーションの機能をサーバーからクライアントに移行させる増加傾向を悪用していた。脅威アクター（サイバー攻撃実行者）は、信頼できるアプリケーションソースに悪意のあるコードを注入した。これは、WAFの保護を導入していないユーザーのブラウザー上で実行することが可能であった。最終的に、この攻撃は企業のWebアプリケーションセキュリティ対策の弱点を露呈した長期に渡るデータ侵害となった。

Takeaways

- クライアントサイドスクリプトは、アプリケーションアーキテクチャにおいて有用なツールであり、ユーザーエクスペリエンス、アプリケーションパフォーマンス、アナリティクス、セキュリティ強化というベネフィットをもたらす。
- スクリプトはユビキタスである。現在のWebサイトには数十種類ものスクリプトがあり、サードパーティのスクリプトが3つのスクリプトのうち2つを占めている場合もある。
- クライアントサイドスクリプトは、多くのステークホルダーが参加する繊細かつダイナミックな機能のエコシステムである。
- クライアントサイドセキュリティには、ベストプラクティスのベースラインがある。しかし、クライアントサイドセキュリティの複雑さと課題は、この脅威ベクトルに対する企業のセキュリティソリューションへの需要を高めるであろう。

Recommended Actions

- 市場で入手可能なソリューションは、機能によって大きく異なる。購入者にとって、最大の関心事は、セキュリティと「壊れないモノ」というビジネス要件のバランスである。
- クライアントサイドの可視化と制御は、多くのベンダーにとって難しく、馴染みのない分野である。市場への新規参入者は、独自のソリューションを構築するか、既存のケイパビリティの連携、もしくは獲得かを選択し、慎重に検討すべきである。
- 多くのIT部門では、クライアントサイドスクリプトや環境についての見識がない。また、セキュリティの問題を理解している者も少ない。デモ、リサーチ、概念実証、試用版など高度な市場教育が必要である。

Source: IDC, 2021

April 2021, IDC #US47623221

市場開拓と市場動向

本調査レポートでは、クライアントサイドの Web アプリケーションファイアウォール（WAF：Web Application Firewall）市場における脅威ベクトル、新たなソリューション、および将来性について分析する。

アカマイ（Akamai）、Cymatic（サイマティック）、PerimeterX（ペリメーターエックス）、Tala Security（タラセキュリティ）は、WAF 保護を拡張してクライアントサイドの脅威に対応し、新たな道を切り開いている。クライアントサイドスクリプトは新たな脅威ベクトルであり、セキュリティ市場はこのニーズに対応するために進化している。

これらのセキュリティソリューションは、一般的に「クライアントサイド WAF」「アンチスクリプト」「スクリプトセキュリティ」などと呼ばれているが、用語の理解について混乱を招く恐れがあるため、以下のオプションを検討すべきである。

- WAF と言うと、Web アプリケーションに適用される特定のコントロールセットを思い浮かべるが、クライアントサイドスクリプトは、アプリケーションセキュリティのパラダイムでは本質的に異なるコントロールポイントである。
- クライアントサイド WAF は、WAF で確立されたセキュリティコントロールとの接続を描写する上で有用な用語であるが、それに比べて「スクリプトセキュリティ」は漠然としており混乱を招く恐れがある。
- アンチスクリプトは、スクリプトを、望ましくない、欠陥のある、あるいは明らかに悪意のあるテクノロジーとして一般化する。しかし、実際にはスクリプトは、アプリケーションアーキテクチャにおける価値ある強力なツールである。

IDC では、これらのソリューションを総称して、クライアントサイド WAF と呼ぶ。これは主に WAF がよく知られている点を考慮したためである。また、クライアントサイド WAF という用語は、将来的にスクリプト以外のクライアントサイドの脅威ベクトルのタイプが拡張される可能性に対応するためである。

概況

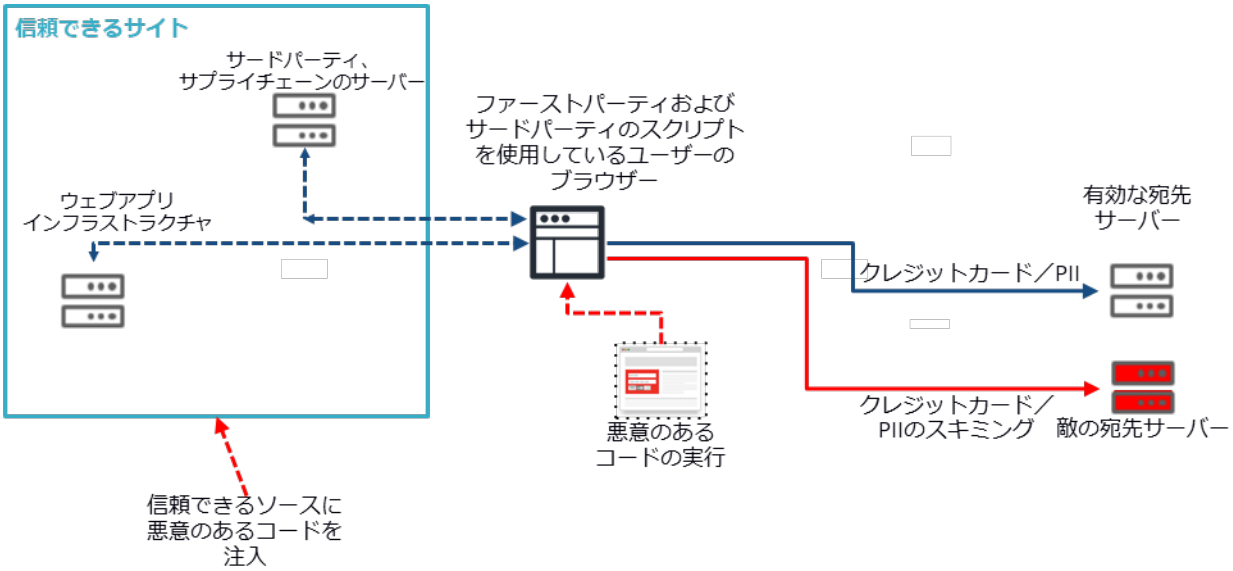
2018 年、決済カードデータをスキミングする新たな手法が登場した。これはハッカー集団「Magecart（メイジカート）」の仕業とされている。Magecart の攻撃は、新しい脅威ベクトル、すなわちクライアントのブラウザーで実行されるスクリプトを悪用したものであった。調査の結果、攻撃キャンペーンが検知され、Magecart 集団が、チケットマスター、NewEgg、ブリティッシュ・エアウェイズなどの大規模なオンライン企業の Web サイトを数か月に渡って侵害していたことが判明した。

Magecart のキャンペーンは、クライアントサイド攻撃を利用して Web スキミング（オンラインカードスキミングまたはフォームジャッキングと呼ばれることもある）を実行するものだった。脅威ベクトルの中でも、Web スキミングは、特に目につきやすいものに数えられており、この脅威ベクトルによって、ウォータリングホール攻撃やクリプトジャッキングなどの他の攻撃が可能になってしまう。これらの攻撃の目的はさまざまであるが、全体的に見て、クライアントサイドセキュリティは、大規模かつ長期的なデータ侵害につながる情報窃盗キャンペーンとなる可能性がある。

Figure 2 は、クライアントサイド攻撃のライフサイクルの概要を示したものである。悪意のあるコードは、WAF による保護が及ばないブラウザーで実行されることに留意していただきたい。また、悪意のあるコードは、サードパーティとファーストパーティの両方のソースに注入される可能性がある。

FIGURE 2

Web スキミング攻撃の構造（ブラウザー）



Source: Akamai, 2021

インダストリアルダイナミクス

クライアントサイド WAF は、成長の可能性が高い新興市場である。このテクノロジーは、アプリケーション開発手法の変化に起因する新たな脅威ベクトルに対応するものである。近年、アプリケーションの機能はサーバーからクライアントへと移行しており、この傾向は今後も衰えそうにない。サーバーからクライアントに機能が移行されることで、サーバーからのパフォーマンス要求は軽減されるため、パフォーマンスの向上とエンドユーザーのインタラクティブなエクスペリエンス向上が可能になる。その結果、スクリプトは、インタラクティブなオンラインエクスペリエンスを実現するツールとして、ますます人気が高まっている。スクリプトは、トラッキング、アナリティクス、ユーザーエクスペリエンス、セキュリティなど、合法的な目的で多岐に渡って使用されている。ある試算によると、Web サイトには 15 種類以上のスクリプトが含まれていると言われており、スクリプトは現在、Web サイトのいたるところに存在している。

さらに、JavaScript はシンプルであるため、IT 部門以外の専門家がスクリプトを採用するのを促すことになった。スクリプトを使用すると、IT 部門以外の事業部門でも、さまざまな目的のためにコードを作成し、Web 資産に挿入できるようになる。また、サードパーティのサービスの統合や挿入も簡単にできるようになる。しかし、特に WAF などの必須ツールに注力し続けている企業では、スクリプトのセキュリティ面はほとんど見落とされている。

全体的に見て、この脅威はよく理解されていない。脅威のカテゴリーで最も広く議論されている侵害は、ほとんどがサードパーティのスクリプトである。その良い例が Magecart のキャンペーンだ。このケースでは、Magecart のハッカーは、ターゲットにした企業のサプライヤーパートナーのコードにアクセスし、信頼できるスクリプトに悪意のあるコードを挿入したのである。企業によっては、この脅威ベクトルは「ゴールポストの移動（moving the goalposts：こっそりと一方的に変更する）」の実行であると考えるかもしれない。大規模のオンライン企業が、すでに直面している多種多様な脅威に対して Web サイトのセキュリティを確保することは容易なことではなく、パートナーのシステムの脆弱性をも考慮しなければならないことは、実質的に不公平だと思われる。サードパーティのスクリプトが最も問題となるのは、IT 部門がパートナーのコード、更新、変更を可視化できず、管理できないからである。

残念ながら、Web スキミングは問題の一部でしかない。サードパーティのスクリプトは、ほとんどの Web ページに存在するスクリプトの 1 つの層にすぎないためである。参考までに、アカマイの研究者の推定では、スクリプトの約 67%がサードパーティ製であるということである。結局のところ、ほとんどの Web ページは、内部のステークホルダーとサードパーティのスクリプトから成るエコシステムである。これらの内部システムは、サーバーが乗っ取られてしまうと、悪意のあるコードを出してしまう可能性もある。

リスクの低減に役立つと思われるベストプラクティスが、いくつかある。まず重要なのは、サードパーティのスクリプトの厳格な管理である。また、定期的なコードレビューやアプリケーションテストも信頼性の高い手段である。さらに、IT 部門はサブリソース完全性（SRI：SubResource Integrity）などの技術を活用して、スクリプトの変更をハッシュ化して検知できる。これらの選択肢は必要な保護のベースラインを提供できるが、これまでは高度な脅威アクターが、検知を逃れるために常に高度で巧妙な戦術を使っていることが明らかになっている。そのため、SRI やその他の手法はスタートとしては有効なものではあるが、高度な攻撃に対しては限界がある。

さらに、脅威アクターは強制されない限り、その活動を中断する可能性が低い。大きな話題となった Magecart の攻撃以降、ハッカーたちはこれらの攻撃をさまざまな方法で改変してきた。たとえば、ハッカーはバナー広告を介して悪意のあるコードを注入する手段として、広告主のネットワークを狙う可能性がある。また、GitHub などのコードリポジトリーを狙う方法もある。これらのリポジトリーには、オープンソースのライブラリやコードスニペットが含まれており、一般的に Web アプリケーションで使用することから、多くの企業で再利用され、信頼されている。そのため、これらの信頼できるソースは、安全な Web サイトに悪意のあるスクリプトを注入するための手段となってしまう可能性がある。

問題に対するアプローチは、ベンダーごとに少し異なっている。市場のトレンドであるソリューションは、主に JavaScript タグを介して展開されており、スクリプトが実行される前にセキュリティ機能を挿入することができる。ソリューションは、そこから大幅に分岐する。主なケイパビリティには、スクリプトや通信（送信元と送信先など）の可視化とマッピングが含まれる傾向がある。その他のケイパビリティとしては、脆弱性の管理、ポリシーの適用、悪意のある活動や疑わしいイベントの検知などがある。また、鍵や埋め込みデータの暗号化、コードの難読化、サンドボックス化、およびその他の防御的手段など、より高度なケイパビリティも考えられる。現時点では、主要なセキュリティケイパビリティを十分に可視化し、自動化するというアプローチがとられる傾向が見られる。時間の経過と共に、より高度な検知手段が重要視される可能性はある。それは、エンドユーザーのエクスペリエンスを妨げたり、あるいは Web サイトの機能を「破壊」することなく、十分なセキュリティを提供するためである。

ベンダーの動向

現在、クライアントサイド WAF には商用製品／サービスがいくつかあり、その範囲やケイパビリティはさまざまである。デジタル・AI（旧称：アークサン）、Source Defense（ソースディフェンス）、Cymatic、Tala Security、PerimeterX、ChameleonX（カメレオンエックス：2019 年にアカマイが買収）など、いくつかの市場専門家が存在する。また、広範な Web アプリケーションセキュリティのポートフォリオを持つ市場専門家もいる。たとえば、アカマイでは総合的な Web アプリケーションと API（Application Programming Interface）のセキュリティポートフォリオによってマルチベクトル攻撃から保護するアプローチの一環として、2020 年に Page Integrity Manager を発表した。同様に、PerimeterX は 2019 年に、同社のエンタープライズボット管理ソリューションを補完するものとして、製品／サービスの提供を開始した。最も新しい参入者は、2021 年 3 月に新しいソリューションを発表した Cloudflare（クラウドフレア）である。これらの企業にはボット管理のバックグラウンドがあり、クライアントサイドのセキュリティシグナルを熟知させるのに役立つ可能性があると、IDC は指摘している。ボット管理をうまく行うのは難しいため、ベストオブブリードのソリューションでは、ボットの不審な挙動を検知し、分類するために（JavaScript を含む）複数の技術が採用される傾向がある。

クライアントサイド攻撃は、検知が難しい場合がある。ただし、いったん検知されれば、企業とその顧客が被る金銭的負担という観点から、その脅威は極めて明確に把握できる。たとえば、この種のデータ侵害は、盗まれた顧客記録の件数で測定される場合が多い。この分野の既存競合他社は、スクリプトベースの脅威検知と低減において、高い有効性を実証した。これを受けて、脅威アクターは他の場所に力を注ぐようになり、その結果、業界内はモグラたたきゲームのような状態になっている。攻撃者の目的は、攻撃対象に適した、セキュリティ保護されていない、あるいはセキュリティ保護の低い Web サイトを発見することである。Magecart の攻撃が有名になったにもかかわらず、市場における脅威ベクトルの認知度がまだ低いため、脅威アクターは新たなターゲットを見つけることが可能となっている。これらの要因はすべて、脅威ベクトルに対する認知が高まり、当然のものとなれば、セキュリティ保護の需要が増し、今後数年間でさらに多くのベンダーを市場に呼び込むことになるであろう。

市場戦略

クライアントサイドの脅威は、攻撃ベクトルが有効であると、サイバー犯罪者が考える限り、大規模オンライン企業にとっての課題となるであろう。しかし、この攻撃はランサムウェアのような大規模なブロードキャスト攻撃に比べると、ターゲットが絞られているタイプの攻撃である。ターゲットとされた企業のほとんどが、スクリプトベースの攻撃の検知と低減に手間取っている。また、これらの問題に対する市場の認知度を高めるためには、時間と労力がかかる。ベンダーは、継続的な教育、デモンストレーション、および概念実証テストを通じて認識を高める力量を問われることになる。

今後は、自社独自の製品やケイパビリティを導入する企業が増えると思われる。アカマイは 1 年前に Page Integrity Manager を発表した。Page Integrity Manager は、個人識別情報（PII：Personally Identifiable Information）が送信され、アクセスされるブラウザーに読み込まれたスクリプトによって生じる攻撃対象の拡大に対応するものである。2020 年、新型コロナウイルス感染症（COVID-19）の感染拡大により、経済活動におけるインターネット利用が加速したため、クライアントサイドの脅威がブラウザーで急増した。

Cloudflare は、Cloudflare Page Shield という新しいソリューションを最近市場に投入したことを発表したが、このソリューションに先立ち、同社は Tala Security との技術提携によって、この脅威ベクトルに対応していた。

Cloudflare は、独自のクライアントサイドセキュリティケイパビリティの開発を決定したが、このアプローチは、他社にとっては簡単なものではないかもしれないと IDC は指摘している。市場のほとんどのベンダーは、クライアントサイド WAF ケイパビリティの開発において、JavaScript クライアントを活用したボット検出技術を優先している。レガシーの WAF ソリューションには、このようなケイパビリティや、クライアントサイドコードに関するその他の実績がない。

Web アプリケーションおよび API セキュリティの製品ラインを強化しているベンダーにとって、専門的なソリューションの獲得は、競争条件を整えるための最良の選択肢となる可能性がある。アカマイによる ChameleonX の買収は、特定用途向けのテクノロジーとクラウドスケールを組み合わせることで得られる潜在的なベネフィットの一例である。アカマイの Page Integrity Manager は現在、毎日 64 億回のスクリプト実行を分析し、毎月 37 億回以上のページビューを保護し、毎週、約 4,000 万件の不審な、または悪意のあるエンドユーザーのインタラクションを検知している。アカマイはリアルタイムの通知、根本的原因の分析、即時軽減、自動化ポリシーの作成を提供することができる。

IDC の見解

クライアントサイド攻撃は、攻撃ベクトルが有効であるとサイバー犯罪者が認識している限り、長期に渡ってセキュリティ格差を拡大していくであろう。その大きな要因は、クライアントサイドの脅威ベクトルが十分に理解されていないことである。これまで、WAF ソリューションは、

Web サーバーをターゲットとした Web アプリケーショントラフィックを分析することで機能していた。しかし近年、JavaScript が普及したことによって、かなりの機能がクライアントブラウザーに移行されている。ところが、多くの企業はこの事実を見落としていたり、Web 機能のクライアントブラウザーへの移行によるリスクやセキュリティの影響に関して適切な評価を行っていない。

この種の攻撃は、ランサムウェアなどの大規模なブロードキャスト攻撃に比べてターゲットを絞って設定しているため、さらに市場の混乱を招いている。たとえば、ほとんどの企業は WAF や DdoS（Distributed Denial of Service）低減ソリューションによって対処される攻撃の種類は、よく理解している。また、望ましくないボットや悪意のあるボットがもたらすセキュリティリスクも、多くの企業に認識されている。しかし、API セキュリティやクライアントサイドセキュリティなどの新しい分野は、単に目に見えないだけで、それゆえ海中の氷山のように、重大なリスクをもたらす新たな分野である（Figure 3 を参照）。

FIGURE 3

Web アプリケーションと API セキュリティの氷山

Source: IDC, 2021

企業が潜在的な脅威ベクトルを理解すると、複数のドメイン、Web ページ、Web アプリケーションを含む複雑な IT 環境で実行されているスクリプトをカタログ化して理解するプロセスは、非常に困難な作業となる。Magecart の攻撃が発生したとき、注入された悪意のあるスクリプトを検知するプロセスでは、変更を検出するためのコードを 1 行ずつ手作業で確認する必要があった。現在は、研究者が根本的な問題やベストプラクティスを理解しているため、プロセスの合理性は高まっている。しかし、ターゲット企業の多くは、スクリプトベースの攻撃を検知して低減するのに手間取っているという点に変わりはない。脅威ベクトルを理解するのに時間がかかり、さらに既存のセキュリティギャップやエクスプロイトを特定するのにも時間がかかるためである。その

上、四半期ごとにスクリプトの 75%が変更されるため、脅威ベクトルは動く標的のように変化する。スクリプトが変更されるたびに、新たな脆弱性や悪意のあるコードが導入される可能性がある。

しかし、時間は本質的要素である。すでに、既知となっているクライアントサイド攻撃による侵害は長く続いており、攻撃者に数か月分のヘッドスタートを与えてしまい、その間に、数多くのクレジットカードやその他の PII（Personally Identifiable Information：個人特定情報）が盗まれてしまう。攻撃が検知されると、攻撃者は勝手に Web サイト上のオンライン店舗を閉め、新たな被害者に向けて初めからやり直す。基本的に、クライアントサイド攻撃は検知までに膨大な時間がかかり、このバランスの悪さがサイバー犯罪者にとって大きな利点であるため、検知時間は削減しなければならない。

このように、セキュリティ業界にとって時間は、問題に対する買い手の意識を啓発し、向上させるための最大のハードルとなっている。ベンダーにとっては、継続的な啓発、デモンストレーション、および概念実証テストを通じての意識向上が課題である。たとえば、アカマイは Page Integrity Manager の無料体験版を提供している。このソリューションは、対象となる Web ページのスクリプトエコシステムの概要と、さまざまなスクリプト、脆弱性、およびリスク要因の分析を提供している。他のベンダーも、体験版やデモンストレーション、啓発用リソースを提供している。

IDC は、これらのアプローチを高く評価している。概念実証ほど、事態の緊急性、あるいはセキュリティソリューションの価値や有効性を伝えるものは他にない。ベンダーにとっては、潜在的なプレミアムサブスクリプションへの転換という明確なベネフィットがある。購入者にとっても、これまでほとんどの企業が完全に盲点としていた脅威ベクトルを可視化することで、大きなベネフィットを獲得することになる。

さらに近い将来、IDC では、クライアントサイド WAF 市場をモニタリングし、WAF、DDoS 低減、ボット管理、オンライン詐欺防止などの既存市場への影響を把握する予定である。クライアントサイドセキュリティの盲点が解決されれば、セキュリティコントロールポイントとしてのクライアントサイドの潜在的な可視性とエンフォースメントケイパビリティの影響について、より深い議論が必要となるであろう。

参考文献

関連調査

- *IDC FutureScape: Worldwide Future of Trust 2021 Predictions*（IDC #US46912920、2020 年 10 月発行）
- *Pervasive Application Edge Defense: An Application-Based Framework for Trust*（IDC #US46810219、2020 年 9 月発行）
- *IDC Market Glance: Software-Defined Secure Access, 2Q20*（IDC #US46291520、2020 年 5 月発行）
- *Worldwide Internet Defense Forecast, 2020-2023: Infrastructure and Application Security Drive Business Value*（IDC #US46022619、2020 年 2 月発行）
- *Security Convergence at the Edge: Emerging Pervasive Data Defense and Response Platforms*（IDC #US46075520、2020 年 2 月発行）

Synopsis

本調査レポートでは、クライアントサイド WAF 市場の脅威ベクトル、新たなソリューション、そして将来性について分析している。Web 環境で実行されるクライアントサイドスクリプトをターゲットとした脅威について、完全に理解している IT 組織はほとんどない。サイバー犯罪者は、莫大な金銭的利益を得る手段として、クライアントサイドスクリプトを標的にし、捕まることなく悪意のあるコードを密かに実行している。今後、このような脅威ベクトルがより顕著になるにつれ、企業のクライアントサイド WAF ソリューションの需要は着実に高まっていくと考えられる。

「クライアントサイドスクリプトは、これからのセキュリティフロンティアである。サイバー犯罪者は、金銭目的で執拗に攻撃をしかけてくる。そして、企業のデジタルセキュリティスタックに新たな格差を見出した」と、IDC Network Security Products and Strategies のリサーチマネージャーである Christopher Rodriguez は述べている。

IDC 社 概要

International Data Corporation（IDC）は、IT および通信分野に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。50 年にわたり、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。

現在、110 か国以上を対象として、1,100 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っています。

IDC は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com