2021 年 11 月 15 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai 脅威レポート：
API の脆弱性が企業から個人まで重大なリスクになっていると警鐘
API セキュリティの課題と現状をグローバルに検証
2020 年から 2021 年の攻撃トレンドも明らかに

世界で最も信頼されているソリューションで安全なデジタル体験を提供する Akamai Technologies, Inc.（NASDAQ：AKAM）は、アプリケーション・プログラミング・インターフェース（API）の日々変化する脅威の状況に関する最新の調査レポートを発表しました。Gartner 社によると、API は 2022 年までに最も頻度の高い攻撃ベクトルになると予想されています。この「API：すべての人々をつなぐアタックサーフェス」レポートは、Akamai の「SOTI インターネットの現状／セキュリティ」シリーズの最新号です。本レポートでは、Akamai と Veracode の研究者とのコラボレーションも取り上げており、Veracode の Chief Research Officer である Chris Eng 氏のゲストエッセイも収録しています。

API は、異なるプラットフォーム間をすばやく容易につなぐためのパイプラインとして設計されています。利便性とユーザー体験を重視した結果、API は多くのビジネスにとって欠かせないツールとなりましたが、同時にサイバー犯罪者の格好のターゲットにもなっています。本レポートでは、ソフトウェア開発ライフサイクル（SDLC）およびテストツールの改善にもかかわらず API の 脆弱性が生じてしまう、避けがたいジレンマに注目しています。API セキュリティは、製品やサービスの市場投入を急ぐ中で後回しにされがちです。多くの組織は従来のネットワーク・セキュリティ・ソリューションをそのまま使用していますが、こうした従来のソリューションは、API に起因する広範囲のアタックサーフェスを防御するようには設計されていません。

「認証の不備やインジェクションの欠陥、シンプルな設定ミスまで、インターネット接続アプリを構築する人々は、API セキュリティについて多くの懸念を抱えています」と、Akamai Security Researcher であり、「SOTI インターネットの現状／セキュリティ」レポートの執筆に参加している Steve Ragan は語っています。「API 攻撃は検知されにくく、検知されても報告されていないことが多々あります。DDoS 攻撃やランサムウェアはいずれも重要な問題とみなされますが、API に対する攻撃は軽視される傾向があります。その大きな理由として、巧妙に実行されたランサムウェア攻撃ほど派手ではない方法で犯罪者が API を攻撃に利用するからです。とはいえ、無視できる問題ではありません」

API の脆弱性がどの部分にあるかは、必ずしも明確ではありません。たとえば、API はモバイルアプリに隠れて見えないことが多いため、操作される危険はないと考えがちです。開発者は、ユーザーがモバイル・ユーザー・インターフェース（UI）でしか API を操作しないと思い込んでいますが、このレポートで指摘しているように、常にそうとは限りません。

Veracode の Chief Research Officer である Chris Eng 氏は次のように述べています。「OWASP のトップ 10 と OWASP API セキュリティのトップ 10 を比較すると、後者の目的は API 固有の「脆弱性とセキュリティリスク」に対処することですが、よく見ると、すべて同じ Web 脆弱性を少し異なる順序で、少し異なる言葉を使って説明しているだけです。さらに API コールは簡単にすばやく（意図的に）自動化できます。― つまり、開発者と攻撃者の両方にとって諸刃の剣というわけです」

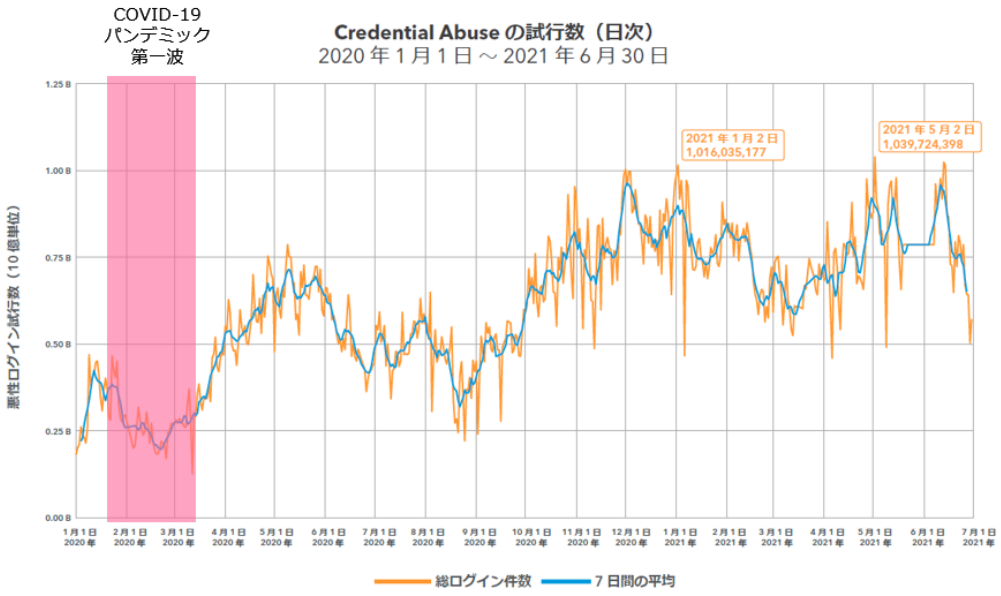
急増する攻撃トラフィックは引き続き API の脆弱性を標的にしている

Akamai は、2020 年 1 月から 2021 年 6 月の 18 か月間の攻撃トラフィックを検証し、合計 110 億件以上の攻撃が試行されたことを確認しました。62 億件の試行を記録した SQL インジェクション（SQLi）が Web 攻撃トレンドリストの首位となり、それにローカル・ファイル・インクルージョン（LFI）が 33 億件、クロスサイトスクリプティング（XSS）が 10 億 1,900 万件で続いています。

これらの攻撃のうち、純粋な API 攻撃が占める割合を突き止めるのは困難ですが、今日のオンライントラフィックの大部分は API ベースであるのが事実です。またソフトウェアのセキュリティ改善に取り組む非営利団体の Open Web Application Security Project（OWASP）がリリースした「API Security Top 10 list（API セキュリティのトップ 10 リスト）」は、このレポートで取り上げた調査結果の大半を裏付けています。

その他の本レポートの概要は以下のとおりです。

- 2020 年 1 月から 2021 年 6 月の 18 か月間に記録されたパスワードリスト型攻撃 (Credential Stuffing 攻撃) は絶え間なく続いていますが、2021 年 1 月と 2021 年 5 月には、ピークとして 1 日あたり 10 億件以上の攻撃が記録されました。COVID-19 の感染拡大の影響を受け世界各国でロックダウンが始まった 2020 年初頭の水準と比較すると、現在は攻撃試行数が約 2 倍の水準で推移していることもこの調査結果からは見て取れます。



- 米国は、この期間の Web 攻撃の標的国の首位となり、2 位の英国の 6 倍近いトラフィック量を記録しています。
    - 米国は攻撃元国としてもトップとなり、ほぼ 4 倍のトラフィックを記録してロシアから首位の座を奪っています。
- DDoS トラフィックは 2021 年これまでのところ目立った変化はなく、2021 年第 1 四半期にピークを記録しています。Akamai は、DDoS イベントを 2021 年 1 月に 1 日 190 件、3 月には 183 件を記録しています。

Akamai の 2021 年度「API：すべての人々をつなぐアタックサーフェス」レポートをお読みください。「インターネットの現状」ページで公開しています。

セキュリティに携わる方々にご利用いただけるように、Akamai の脅威リサーチャーの見解や、変化する脅威の状況に関して Akamai Intelligent Edge Platform から得られる知見をご紹介する Akamai の脅威リサーチハブもご用意しています。

アカマイ について：

Akamai はオンラインライフを守り、力強く支えています。世界中の先進企業が Akamai を選び、安全なデジタル体験を提供することで、何十億もの人々の生活、仕事、娯楽を支えています。世界で最も信頼されている最大規模の Edge プラットフォームにより、Akamai はアプリ、コード、体験をユーザーに近づけ、脅威を遠ざけます。Akamai のセキュリティ、コンテンツデリバリー、エッジコンピューティングの製品とサービスの詳細については、www.akamai.com と blogs.akamai.com 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。