Akamai お客様事例

アジアの大手通信企業が脅威から API を保護

自社環境内のすべての API を可視化して保護

管理されていない API を探索

API 保護を強化

機微な情報のセキュリティを確保

モバイルデバイスの普及に伴い、アジアの通信業界は、より良いデジタルサービスに対する顧客の需要に応えるために、新しいテクノロジーの開発とネットワークの拡大に大きく投資しています。水面下で、API は次のものをもたらしています。

- DevOps チームのプロセスを促進しながら通信業界を変革するために必要な接続性
- 携帯電話サービス、インターネットアクセス、その他の通信製品を地域全体の顧客に提供するための基盤
- よりパーソナライズされたソリューションを提供し、最終的に顧客体験を改善する能力

この地域をリードするある通信企業は、API により、新しいデジタル音声およびデータソリューションを提供する大きなチャンスが生まれると考えています。5G 時代が近づくにつれ、同社はテレフォニーだけでなく、ビッグデータ、AI、IoT、その他の新たなデジタルアプリケーションにも目を向けています。一方、API については、その数だけでなく、リスクも増大していることも理解しています。2022 年と 2023 年に他の大手通信プロバイダーが API 攻撃の影響を受けているのを目の当たりにした同社は、Noname Security（現在は Akamai 傘下）と手を組みました。

Telecommunications Company

所在地

アジア

業種

ネットワーク事業者

ソリューション

Akamai API Security

Akamai

すべての API とそのリスクを可視化する必要性

多くの組織のセキュリティチームが、API とそのリスクに対する可視性の欠如に悩まされています。Akamai の調査結果によると、API の完全なインベントリーを作成している組織のうち、どの API が機微な情報を返すかを知っている組織の割合は、わずか 10 分の 4 です。Akamai の API セキュリティソリューションの探索モジュールを使用したところ、Akamai の顧客である通信企業も同様の課題を抱えていることがわかりました。

Akamai と提携する前、この顧客の API セキュリティ制御は主に従来の API 管理プラットフォームと Web アプリケーションファイアウォール（WAF）で構成されていました。アプリケーションセキュリティと API 探索の観点から見れば、この形態は理にかなっていました。しかし、いずれのソリューションも、今日の攻撃手法から API を包括的に保護するために必要とされる高度なセキュリティ制御と可観測性を提供するものではありませんでした。その主な理由の 1 つは、すべての API が WAF や API ゲートウェイのようなプロキシを経由してルーティングされるわけではなく、これらの管理されていない API は攻撃者にとって魅力的なターゲットとなっていることです。

しかし、API インベントリーの正確な監査が行われるとしても、同社にはリクエストの運用や管理を行う際に正常に動作しながら API を保護する機能が必要でした。簡単に言えば、組織のセキュリティチームが環境内の悪性のふるまいを手動で特定するのは非現実的です。

リアルタイムで保護する必要のある API エンドポイントは数百（場合によっては数千）にも及びます。一般的に使用されている AppSec ソリューションは通常、顧客の環境内のすべての API コールに対応することはできません。そのため、適切な API ランタイム保護機能がなければ、企業の IT 環境はサイバー攻撃に対して脆弱なままになる可能性があります。

すべての API を把握し、API の脅威からのセキュリティを確保するためのソリューション

手を組んだ両社は第 1 段階としてパイロットを展開して、社内の API を特定し、設定を評価し、API を通過するデータのタイプを把握しました。この顧客はすぐに、探索の実行速度、正確なインベントリー調査結果、およびツールによる機微な情報の露出の特定に感銘を受けました。

パイロットでプラスの成果が得られたため、同社は Noname API Security Platform（現在は Akamai API Security の一部）の対象範囲を社内外の API 環境全体に拡張しました。これにより、本番環境の隠れた API も明らかになり、環境が直面している最も差し迫った脅威が発見されました。

同社は、将来の攻撃から API を保護するために、主要なセキュリティ脆弱性に対する強力な防御を必要としていました。Akamai API Security を展開したことで、同社は疑わしいふるまい異常を検知し、インシデント対応プロトコルをリアルタイムでトリガーできるようになりました。これにより、修正プロセスに必要な情報を得るために事後的なレポートやアクセスログを利用する必要がなくなります。Akamai API Security で疑わしいふるまいが検知されると、この顧客の API ゲートウェイ、SIEM システム、その他の情報セキュリティエンジンに報告され、セキュリティチーム全体に情報が提供されます。同社は、ユースケースと脆弱性の重大度に応じて、従業員に問題を手動、半自動、または完全自動で修正させることができます。

 | サポート | | 公開日：2024 年 9 月