imperva

CASE STUDY

Keystone RVは Imperva DDoS Protection を使用して大規模DDos攻撃を阻止

概要

インディアナ州に本社を持つ Keystone RVは北米を代表するRV車メーカーです。同社のブランドはMontana、Cougar、Outbackなどがあり高速道路で最も多く見かける名前です。

- 即時に解決する救世主
- 迅速な脆弱性評価と開発
- 期待以上の結果

業種 その他 ウェブサイト
www.keystonerv.com

DDoS攻撃により、コーポレートサイトやパートナーサイトがダウン

Keystone RVはコーポレートサイトと1万社のディーラーを対象としたパートナーポータルサイトを保持しています。同社はディーラーから、コーポレートサイトとパートナーポータルにアクセスできないとの報告を受け始めました。Keystone社のネットワークおよびセキュリティ管理者のMark Widman氏はウェブホスティングプロバイダーに連絡すると、DDoS攻撃を受けていることがわかりました。DDoS攻撃の原因は不明で、Keystone社はDDoS攻撃でよくあるサイバー攻撃者からの「身代金要求」を受け取っていませんでした。また、同社はサイバー自警団や政治的ハクティビストを刺激するような不適切な行動もしていませんでした。Keystoneは無作為に仕掛けられたDDoS攻撃の犠牲になったものと思われました。当初、Keystoneのウェブホスティングプロバイダーはもっと多くの Web アプリケーション ホスティング リソースを ウェブサイトに割り当てようとしました。ホスティングプロバイダーは多くのウェブサーバーを追加して、多数のアプリケーションに帯域を割り当てました。しかし、Widman氏はホスティングプロバイダーのこの解決策は「攻撃によって崩壊しており、当社は非常に困難な状況に陥りました」。

「攻撃を受けた時、回線帯域の100倍にもなりました。それに対し、Impervaが攻撃を阻止し、ウェブサイトの稼働を確保することができました。Impervaのサポートチームは素晴らしく、Impervaの導入前に戻ることはできません」

ITおよびセキュリティ管理者
Mark Widman氏

すぐに結果が得られる迅速な評価と導入

Keystoneは過去には DDoS攻撃に合ったことがなく、セキュリティチームは実現可能な解決策を早急に調査する必要がありました。チームは有償と無償のDDoS防御サービスを見つけましたが、チームのITソリューションパートナーはImpervaを推奨しました。Widman氏によれば、無償サービスはKeystoneのサイト運営を保証できない上に、有償サービスの当初の価格が「あまりにも高額であった」ため、無償サービスを直ちに除外しました。Widman氏は木曜日の午後4時にImpervaに連絡を取ってImpervaに事前情報を与えてkeystoneのDNS情報を更新した後、早期にウェブのトラフィックをImpervaのクラウドセキュリティインフラ経由でリダイレクトすることができました。2時間後の午後６時までにウェブサイトは稼働し、攻撃を完全に防ぐことができました。

ImpervaがSYNフラッド攻撃とその後の攻撃を撃退

Impervaからの情報によれば、KeystoneのウェブサイトはSYNフラッドとして知られているDDoS攻撃の大きな標的となっていたことが分かりました。分散型SYNフラッド攻撃中は、標的であるコンピュータ処理を妨害するために、複数の攻撃ソースがSYN要求として知られる膨大な数の接続要求を標的のコンピュータに送り付けます。攻撃中には、Keystoneのウェブの帯域幅の使用が通常レベルの100倍以上になりました。ImpervaはネットワークDDoSの防御機能によりDDoS攻撃をなんなく軽減しました。Imperva Cloudは世界中に分散しているデータセンターネットワークを通じてルートトラフィックを運営しているため、ホスティングプロバイダーのインターネット帯域幅のキャパシティを越えた攻撃に拡張対応できます。Impervaのセキュリティオペレーションセンター（SOC）のエンジニア—は、攻撃トラフィックの大多数は東欧からのものだとWidman氏とチームに教えました。Widman氏はImperva SOCエンジニアと協力して、攻撃中の特定地域からのアクセスを制限しました。その結果、好ましくないウェブアクセス要求を除外するのにも役立ちました。Impervaを導入してから２日後にはDDoS攻撃は止みました。Keystoneはその翌月も二回の継続攻撃に合いましたが、ImpervaはDDoS攻撃も撃退することができました。一連のDDoS攻撃の後に、ウェブのアプリケーションがImpervaによって安全に守られているため、Keystoneのセキュリティチームは脅威から開放されました。Widman氏は「Impervaは救世主だ」とコメントしています。

期待以上のテクニカルサポート

Keystoneのセキュリティチームは、当初から Impervaの営業とサポートスタッフに感心していました。「私たちが一緒に仕事した誰もが、知識豊富で対応が早かったです」。
また、Imperva SOCはセキュリティポリシーの設定、モニタリング、チューニングを含む導入のあらゆる面を管理しています。Keystoneがポリシー変更を要求した場合、セキュリティアラート通知に関して問い合わせた際は「ポリシー変更は45分以内に行われるなど、Impervaのサポートエンジニアは素晴らしい」と述べています。

Impervaはウェブ攻撃を阻止し、アプリケーションのアクティビティを可視化

KeystoneはImpervaのDDoS Protection Serviceに加えて、Imperva Cloud WAFも導入しました。従って、Keystoneのウェブサイトは強力なDDoS攻撃を阻止するだけでなく、SQLインジェクション、クロスサイトスクリプティング（XSS）、ディレクトリトラバーサルなどのウェブアプリケーション攻撃に対しても安全を確保します。Keystoneのセキュリティチームはユーザとボットの両方がサイトを攻撃し、機密データにアクセスしようとしていることを知って驚きました。Imperva DDoS ProtectionはKeystoneのセキュリティチームに安心感を与えるだけでなく、そのサービスはウェブアプリケーション稼働の可視性を非常に高めています。通知項目には脅威の種類、攻撃者のIPアドレス、ウェブブラウザ、地理的位置が含まれています。また、Keystoneのセキュリティ管理者はオンラインポータルにログインして、標的URLや侵害の引き金となった脅威パターンなどの追加情報の閲覧もできます。高機能なダッシュボードにはセキュリティ、パフォーマンス、設定情報が表示されます。KeystoneのウェブサイトははImpervaによってDDoS攻撃から将来も守られます。Keystoneにとって、Impervaは費用対効果が高く、同社のセキュリティ担当者は簡単な事前情報フォームに記入して、社内のDNSホスティングプロバイダーに連絡してDNS設定を更新するだけで容易にロールアウトが可能です。Widman氏は「Impervaのサービスは全ての面で傑出している」との見解をコメントしています。