Datalex

ケーススタディ

distil networks

DistilとF5を統合することにより 高度持続型ボット攻撃(APB)から航空会社のウェブサイトを保護！

「あるウェブスクレイパーは、航空運賃を知るためにできることは何でもやっていました。
ウェブスクレイパーを阻止するための多くの他のソリューションを用いた最初の試みにもかかわらず、ウェブスクレイパーは依然として24時間以内にサイトに戻ってくることが可能でした。しかし、Distilの実装により、ウェブスクレイパーはあっさりと消え去りました！」

Datalex、セキュリティアドミニストレータ、エリック・チェイピン(Eric Chapin)氏

会社名： Datalex
業界： 航空会社向けEコマースプラットフォーム

● Datalex社

アイルランドを拠点とするDatalexは、価格設定、販売、注文管理、カスタマーインサイトを組み合わせて、旅行のあらゆるタッチポイントにおいて競争力のある差別化された小売エクスペリエンスを提供する、統合デジタルコマースプラットフォームを提供しています。

2014年のワールド・トラベル・アワード(World Travel Awards)で「World's Leading Travel Merchandising Solution Provider」に選ばれたDatalexのコマースプラットフォームは、世界で最も革新的な航空会社小売ブランドのうちの数社が主導する、世界の隅々までカバーする10億人超の消費者の旅行市場を実現します。

Datalexの顧客としては、エアリンガス(Aer Lingus)、アバカス(Abacus)、中国国際航空(Air China)、エア・トランザット(Air Transat)、ブリュッセル航空(Brussels Airlines)、コパ航空(Copa Airlines)、デルタ航空(Delta Air Lines)、エーデルワイス航空(Edelweiss)、HPエンタープライズサービス(HP Enterprise Services)、ジェットブルー航空(JetBlue Airways)、フィリピン航空(Philippine Airlines)、SITA、スイスインターナショナルエアラインズ(Swiss International Air Lines)、ヴァージン・アトランティック航空(Virgin Atlantic)、ヴァージン・オーストラリア(Virgin Australia)、中国西部航空(West Air)、ウエストジェット航空(WestJet)が挙げられます。

概要

● 課題

・ウェブスクレイパーがDatalexの顧客のサイトを攻撃し、アップセルやクロスセルの機会を引き抜き、GDS(Global Distribution System:横断的販売網) APIプルコストを増大させていた
・毎日の複数の攻撃がパフォーマンス問題やダウンタイムを引き起こす恐れがあった
・F5 Networksを用いて悪いボットトラフィックを特定・規制することは面倒で非効率的であった

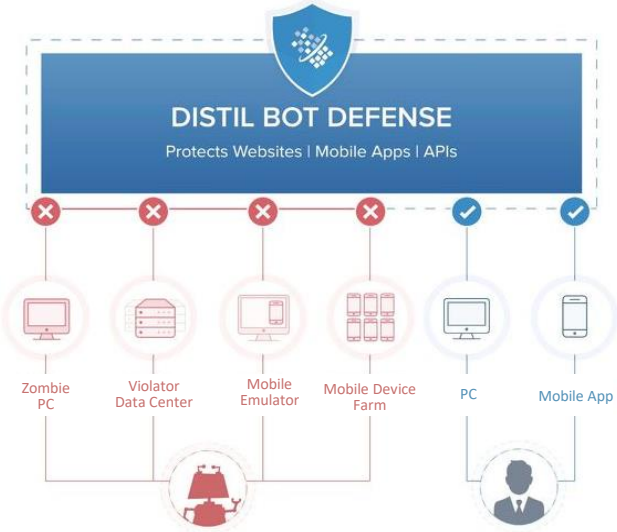
● 導入

DistilのアプライアンスとクラウドCDN(各顧客のホスティングの選好に基づく)

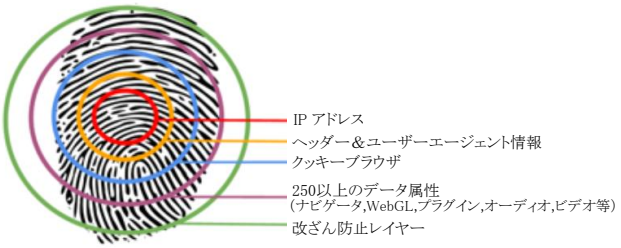
● 結果

・高度持続型ボット(APB)が「諦める」ように追い込んだ
・スクレイパーを排除し、サイトをより信頼性が高くセキュアなものにした
・リソース時間を節約しながら、既存のボット対策ソリューションよりも能力を高めた

世界最高精度(99.9%)の“不正BOT検出率！”



● Distil Networksのハイデフ・フィンガープリント



コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.

文中の社名、商品名等は各社の商標または登録商標です。

● 課題

「悪者がDatalexの顧客のサイトをスクレイピングし、SEO（ Search Engine Optimization)を低下させ、アップセルやクロスセルの機会を引き抜いていた」

旅行業界は、悪いボットやウェブスクレイピングに対して特に脆弱性があります。
「当社の顧客サイトにはスクレイパーにとって貴重なデータがあり、スクレイパーはそのデータを取得する方法において攻撃的になる場合があります」とDatalexのセキュリティアドミニストレータ、エリック・チェイピン氏は述べています。

「スクレイパーはTravelocity やKayak などの他の旅行サイトと運賃を共有するものなので、当業界は一般的にはスクレイパーに対してかなり寛容であり、且つ一部のスクレイパーは「許可」または「ホワイトリスト登録」されているので、運賃についてサイトをスクレイピングすることができます」。「しかし、スクレイパーが規則に従わないか、サイトに深く入り込む場合は、措置を講じる必要があります」とチェイピン氏は説明しています。

持続型スクレイパーは、旅行サイトからコンテンツを盗み、そのコンテンツをスクレイパー自体のサイトに投稿して、SEOの影響力を弱め、広告費を奪うことができます。ウェブスクレイピングボットは、運賃価格を監視するためにも使用されるので、競合他社は、より低価格の運賃を提供することで、より安く売ることができます。

「航空会社業界では、ボットは、顧客の連絡先情報、フライトの変更、搭乗手続きの手順に関する問題を引き起こす場合があり、アップグレードや旅行保険などのアップセルやクロスセルの機会を盗むことによって、ビジネスを引き抜くこともできます。」とチェイピン氏は述べています。

深く掘り下げるスクレイパーが、GDS(Global Distribution System:横断的販売網) APIプルコストを増大させ、パフォーマンス問題を引き起こしていた。

Gartner

The only anti-bot solution to be included in Gartner's Online Fraud Detection Market Guide two-years running

航空会社である顧客の一社には、深く掘り下げる攻撃が殺到していました。「悪意のあるスクレイパーが、非常に激しくサイトを攻撃していました」とチェイピン氏は述べています。「このウェブスクレイパーは、通常よりも深く入り込み、バックエンドの支払コストをつり上げていました。」

チェイピンの説明によれば、航空会社がGDS(global distribution system)に対して激しいAPIプルを行うと、それはビジネスの金銭的コストになります。「このスクレイパーは、当社の顧客のGDSプルコストを増大させており、当社は、マネージドソリューションプロバイダとして、この攻撃を阻止する方法を見つけなければなりませんでした」とチェイピン氏は述べています。

チェイピン氏によれば、より小規模の顧客サイトでさえ、1日に何度もボットによって攻撃され、そのことが顧客サイトの速度を落とすか、顧客サイトをオフラインにすることさえあります。深刻なケースでは、過度のスクレイピングが帯域幅とサーバの使用量を使い果たし、不安定さやダウンタイムさえも引き起こします。

Distil Networksは、平均的な旅行ウェブサイト上のトラフィックの約23%が悪いボットからのもの、即ち、ウェブサイトをパフォーマンス問題や「ブラウンアウト（消費電力増大に起因する電圧降下）」に直面させる可能性があるトラフィックであることを理解していました。

「ウェブスクレイパーは常に航空会社コミュニティに存在していましたが、ウェブスクレイパーが本当にサイトをダウンさせるレベルに進んだのは、ここ2～3年のことにすぎません。最新のスクレイパーは、事実上スクレイパーがDDoS試行であるレベルに達しています」とチェイピン氏は述べています。

「F5 Networksを用いて悪いボットや人間によるウェブサイトトラフィックを特定・規制することは面倒で非効率的であった」

全てのスクレイパーが悪者という訳ではないので、良いスクレイパーと悪いスクレイパーを見分けることは多くの労力を要することがあります。「良いボットが当社の顧客の運賃を推奨できるように、良いボットをホワイトリスト登録する能力があることを確認しなければなりません」とチェイピン氏は述べています。

これまでDatalexはF5 Networksのボット対策ソリューションを使用していましたが、チェイピン氏によれば、このソリューションは、ページ又はセッションに対するパケットを特定することによってスクレイパーを阻止しようとしていたため、ソリューションを調整することがより困難になっていました。

「F5は、パケットを特定することによって何らかの基本レート制限を行うことも可能でしたが、現在、レート制限を通じて出てくるのはボットブロックの10%未満です」とチェイピン氏は述べています。「以前のソリューションは一度だけで終わってしまうものでしたが、Distilは段階的な方法なので、もっと多く検出することができます」とチェイピン氏は説明しています。

F5 Networksは、一部の普通のスクレイパーを阻止するのに役立ちましたが、顧客サイトに深く入り込むボットには不十分でした。「持続型スクレイパーを阻止するためには、F5よりも高性能のソリューションが必要であることが分かっていました」とチェイピン氏は述べています。「当社はDistilを見つけ、POCを行いました。当社は、Distilがサイト上に実装されるとすぐに、悪いボットを阻止していました。実際、調整が完了した後では、Distilは今までのところ、許可されたスクレイパー以外のすべてのスクレイパーを排除しています」

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.

文中の社名、商品名等は各社の商標または登録商標です。

● Distil Networksを用いた結果

「Distil NetworksはF5 Networksを補完して高度持続型ボットを阻止」

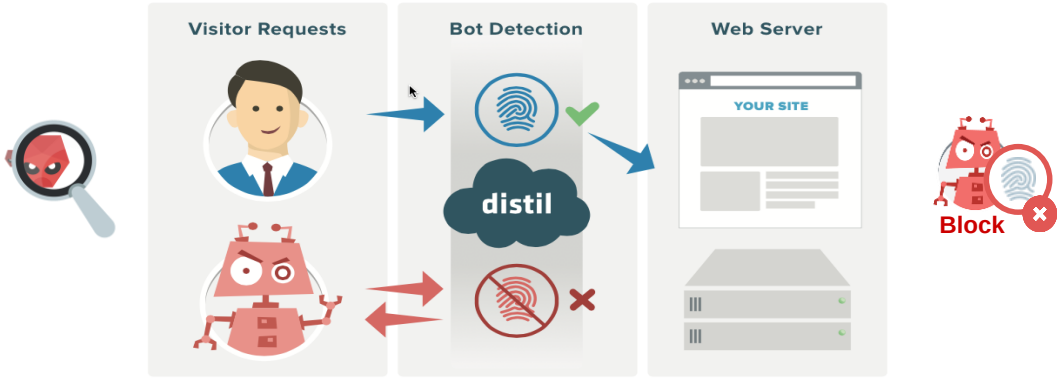
チェイピン氏は、その他のネットワークソリューションにはF5 Networksを使用していますが、F5 Networksのボット対策ソリューションは、レート制限またはシグネチャ検出についてはDistilが提供するようなきめ細かい制御を提供しなかった、と述べています。

更に、F5 Networksは、よりIP中心であったため、犯罪になるIPであればブロックしますが、悪者が数百のIPにわたってボット攻撃を拡散するか、ピアツーピアネットワーク、又は匿名プロキシから入ってくる場合は機能しません。Distilは、基本レート制限に依拠するのではなく、デバイスフィンガープリンティング、各ドメインのウェブトラフィックの挙動モデル化、ならびに自動JavaScript検出及びその他の高度なブラウザ検証ツールを使用します。

「F5 Networksは最初の攻撃を検出しますが、一部のスクレイパーは、そのトラフィックをすぐに変更して、複数のIPやより多くのセッションにわたって拡散し、正規のユーザのように見せることができます」とチェイピン氏は述べています。

「当社の顧客のサイトのうちの1つに対してあるスクレイパーは、Distilに対して同じ分散攻撃を試みました。Distilはその調整がよりきめ細かく、その攻撃者のシグネチャを知っていたので、スクレイパーは手も足も出ませんでした。」

● 高精度なBOT検出システム



● 自動化ボット検出が管理上の重い負荷を緩和する

チェイピン氏は、ボット検出ソリューションの中で、Distilの自動化のレベルは唯一無二のものである、と述べています。
Distilを用いることで、チェイピン氏のチームは、許容レベル、限界を容易に設定し、悪いトラフィックをブロックする方法を指定することができます。
ソリューションを展開するのに必要なNOCの対話は、ほんの一握りしかなく、他の競合ソリューションでは、レベルの設定やメトリックの調整に時間が掛かり、より持続的なボットを阻止するには依然として非効果的である場合があります。

「Distilは、当社の環境でこれまでに実施した中で最も容易な実装のうちの1つでした。一度実装されると、このシステムはそれ自体を最適化します。当社では、ボットの追跡とは対照的な、より戦略的な仕事に従業員の時間を移動させることができています。」

● 高度なスクレイパーを排除することで、サイトをこれまで以上に安定したセキュアなものにする

「サイトに対する迷惑な攻撃を排除することは、サイトの安定性を維持し、バックエンドのインフラコストを低減するのに役立ちます。1つの大きな攻撃によってサイトがダウンする可能性がある当社の小規模顧客の場合は特に、スクレイパーを追い払うことで、判定性が大幅に向上します」とチェイピン氏は述べています。

「最初の顧客にDistilを実装したところ、ウェブトラフィックが50%以上減少し、現実の人間のユーザには何の影響もなかったことが分かりました」とチェイピン氏は述べています。平均すると、悪いボットを排除することで、Datalexの顧客サイトへのトラフィックが20～30%減少しました。
「顧客のサイトにDistilを置けば、悪いボットがなくなることを確信することができます」とチェイピン氏は述べています。

● 高度持続型スクレイパーが「諦める」ように追い込んだ

「Distilは今までのところ、顧客サイト上の手に負えないすべてのウェブスクレイピングを完全に排除しており、このことは、航空会社業界には最も持続的なスクレイパーのうちのいくつかがあることを考えると、素晴らしいことです」とチェイピン氏は述べています。

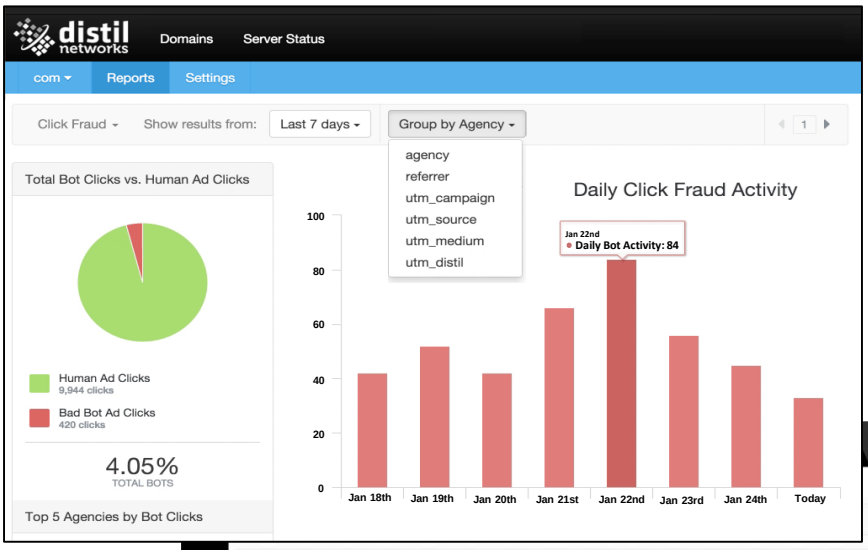
「あるウェブスクレイパーは、航空運賃を知るためにできることは何でもやっていました。ウェブスクレイパーを阻止するためのF5を用いた最初の試みにもかかわらず、ウェブスクレイパーは依然として24時間以内にサイトに戻ってくることが可能でした。しかし、Distilを実装した後、ウェブスクレイパーはあっさりと消え去りました」とチェイピン氏は述べています。

「Distilは、当社がバックエンドのインフラコストを低減するのを支援し、可用性を高め、顧客サポート時間を減少させています」とチェイピン氏は説明しています。「セキュリティ側では、Distilは、ブルートフォース攻撃、脆弱性スキャニング、サイトに対するその他の攻撃から保護するのに有用なツールです。」

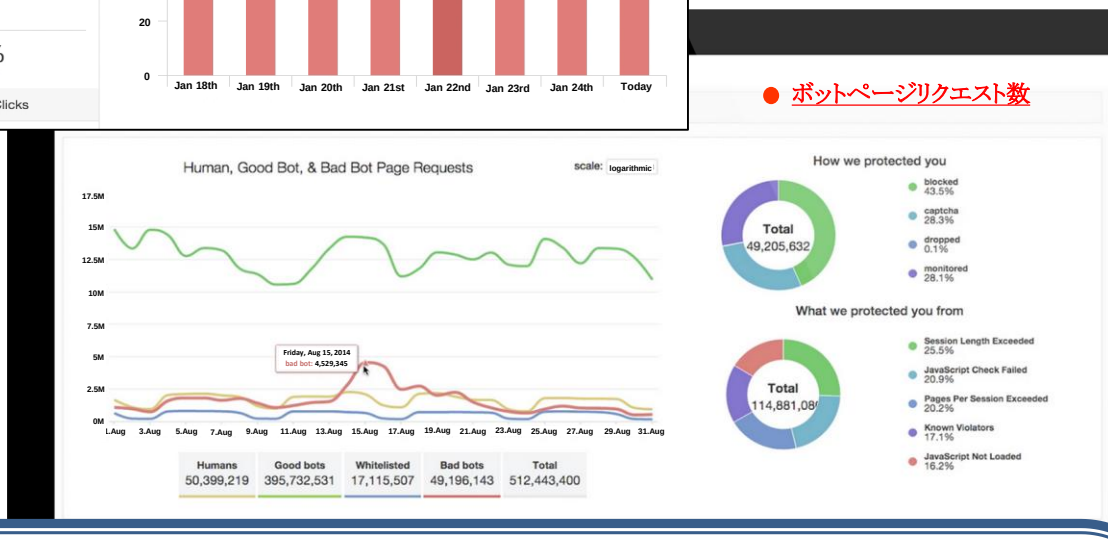
コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.

文中の社名、商品名等は各社の商標または登録商標です。



● 日毎のクリック詐欺の件数を可視化



● ボットページリクエスト数

Fortune 500 & Alexa Global
10,000 Customers
Distil Networksは世界で最も成功しているウェブサイトから信頼されています！
（実績の一部）

● Distil Networksについて

ボットの検出及び軽減のグローバルリーダーであるDistil Networksは、悪いボット、API悪用、詐欺からウェブアプリケーションを保護する、唯一の簡単で正確な方法です。Distilを用いれば、正規のユーザに影響を及ぼすことなく、悪意のあるトラフィックの99.9%を自動的にブロックします。

Distilのウェブセキュリティは、ウェブスクレイピング、ブルートフォース 攻撃、競争上のデータマイニング、アカウント乗っ取り、オンライン詐欺、不正な脆弱性スキャン、スパム、中間者 攻撃（MITM）、デジタル広告詐欺、ダウンタイムからウェブサイトを防御します。

DistilのAPIセキュリティは、ウェブブラウザ、モバイルアプリケーション、及びIoT接続デバイスにサービスするAPIを含む、全てのタイプのAPIを保護します。
DistilのAPIセキュリティは、開発者の誤り、統合によるバグ、自動化されたスクレイピング、ウェブ及びモバイルのハイジャックからAPIを防御します。

Distil Networksの詳細については、http://www.distilnetworks.comをご覧になるか、
Twitterで@DISTILをフォローしてください。

コーネットソリューションズ株式会社
Cornet Solutions
(TEL) 03-5817-3655 (代)
www.cornet-solutions.co.jp

Copyright 2020 Cornet Solutions K.K.

文中の社名、商品名等は各社の商標または登録商標です。