Response Policy Zone サービス:

悪意あるサイト、不正利用されているサイトに対するセキュリティを改善

PIPELINE SECURITY

脅威インテリジェンスは2分毎に更新され、サイバー犯罪者が、データの窃盗、詐欺の行為、正当なシステムの悪用目的で使用するドメインをブロックします。RPZ は、悪意あるドメインをブロックし、あらゆる企業においてベストプラクティスを開発するのに役立つパワフルなツールです。

RPZ とは

毎日、何百万人ものユーザー、マシンからマシンへのアップデートや IoT デバイスが、ウェブサイト、クラウドアプリケーション、E コマースサイトやその他のオンラインサービスへシームレスに接続するため、ドメイン名システムと関連するインフラストラクチャに頼っています。

接続は瞬間的に確立されるため、マルウェア、ランサムウェアやボットネットをインストールするために利用されたり、サイバー犯罪者によって不正使用されているドメインに接続してしまう危険性があります。

セキュリティ専門家は、悪意あるドメインと IP アドレスへ名前解決することを防ぐことで悪意あるサイトへのアクセスをブロックするResponse Policy Zones(RPZ)を使用してこの危険を軽減することができます。

Deteque の調査員と自動システムは、実際に悪意活動をしているドメイン、活動開始前だがレピュテーションの低いドメインと不正利用されている IP アドレスを識別するため、インターネット全体から情報を集めて脅威インテリジェンスを提供します。

RPZ の仕組み

RPZ がない場合、クライアントは、ローカルの DNS リゾルバに問い合わせ、ドメインの IP アドレスがキャッシュに含まれていなければ、外部のルートサーバー、トップレベルドメインサーバー、ドメインサーバー自体の順に問い合わせて、サイトへアクセスします。このプロセス内には悪意あるドメインを除外する検査はないため、このプロセスでは正当なサイト、悪意あるサイトの双方が返ってきます。

クライアントが RPZ を有効化したネームサーバーへの問い合わせを開始すると、再帰 DNS 正引きの各段階が分析され、既知の悪意あるドメイン、アドレスとネームサーバーを識別します。RPZ がセキュリティリスクを検知した場合、DNS サーバーは「存在しません」といった種類の返答を返し、危険へのアクセスを防ぎます。

組織それぞれで、ユーザーへの警告ページをカスタマイズし、セキュリティに関する意識向上とベストプラクティスの研修メッセージを載せることもできます。組織にいる者全員がオンラインセキュリティへ貢献することを確実化するのは重要なステップです。

PRZ はデータ問い合わせサービスとして提供され、実質的にはお客様のための DNS ファイアウォールとして機能します。5千人以上のユーザーを対象に大規模な商業運営をしている組織は、IXFR による Deteque のドメインベースのレピュテーションデータの利用も可能です。

利益と機能

・迅速な導入

特別なハードウェアは不必要です

・スピードと正確さ

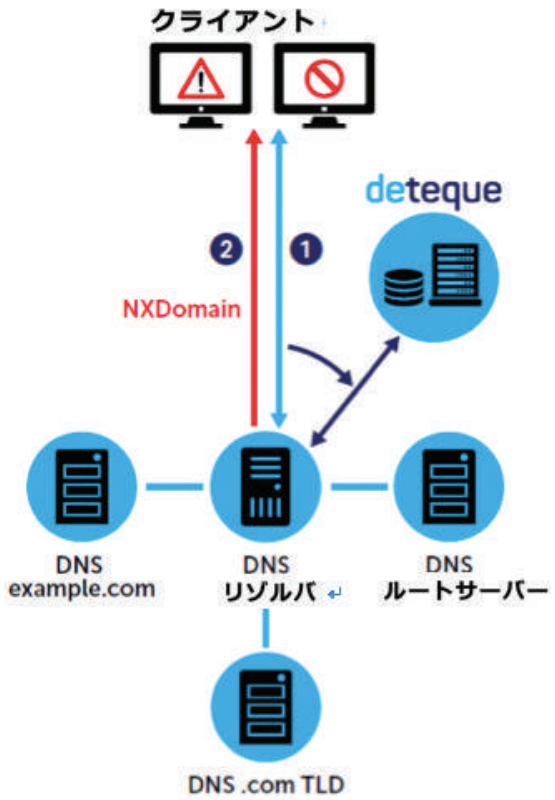
継続的に監視し、2分毎に配信されます

・確実性と信頼性

Deteque の調査員はお客様のために脅威インテリジェンスを更新すべく常に努力を怠りません

・簡単な統合

業界標準形式のデータフィードとして利用可能で、特別なカスタマイズは必要ありません



❶ クライアントがローカル DNS リゾルバに問い合わせると、リゾルバはまず Deteque RPZ に問い合わせます

❷ Deteque RPZ が悪意あるドメインを識別すると、ローカル DNS リゾルバはドメイン問い合わせをブロックし、ユーザーへ警告を送信することもできます

PIPELINE SECURITY
www.pipelinesecurity.jp
〒103-0014　東京都中央区日本橋蛎殻町 1丁目35–8グレインズビル1F
Tel: 03-4405-5766　hello@pipelinesecurity.jp
deteque A division of SPAMHAUS

Response Policy Zone サービス：
悪意あるサイト、不正利用されているサイトに対するセキュリティを改善

PIPELINE SECURITY

脅威インテリジェンスには下記が含まれます
オンライン詐欺、障害、搾取には様々な形があるため、Deteque の RPZ は、新しいタイプの脅威とサイバー犯罪者による DNS プロセスの新しい乱用手法を考慮し、常に進化を続けています。

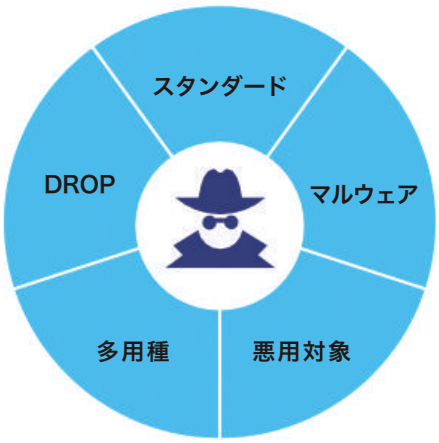
DROP – Do not Route Or Peer（ルートまたはピア禁止）
プロフェッショナルなスパマ業者やサイバー犯罪者によってハイジャックされたことが知られている、または、地域インターネットレジストリによって直接犯罪組織に割り当てられた IP アドレスの範囲です。
ISP からサイバー犯罪者が借りている IP 範囲のリストも含んでいます。

標準
Deteque のセキュリティ調査員は、新しく登録されたドメインを常に監視し、サイバー犯罪活動への繋がりを識別するための自動システムを利用しており、疑いのあるドメインを迅速にリストに載せることが可能です。

マルウェア
Deteque のセキュリティ調査員のグローバルチームは、犯罪ネットワーク、悪意あるドメインと不正利用されている IP アドレス間の繋がりを追跡します。RPZ のデータは、通常 DDoS 攻撃の前兆となるボットネットのビーコン通信を遮断することで、DDoS 攻撃に対する防御に役立たせることも可能です。
Deteque の調査員は、マルウェアを解析調査して Domain Generation Algorithms（ドメイン生成アルゴリズム）のドメインとそれらのドメインが利用され始める時を明らかにし、ボットネット指揮統制サーバーの接続ポイントとして犯罪者が利用を始める前に、それらのドメインをブロックすることができます。

悪用対象
概して正当なものであるのに、不正利用や不法侵入によってスパム業者が悪用しているドメインです。「悪用された正当なもの」と呼ばれ、ドメインの所有者は正当な運営者でありながら、サーバーは不法侵入されているものを指しています。

多様種
これには、匿名化された通信による望まないネットワーク使用を制限するため、Tor exit ノードのブロックなど多岐にわたる脅威の種類を含んでいます。また、未承諾で送られてくる一斉送信 E メールの送信者が制御しているまたは使用できるようになっているとみられることが理由で Spamhaus ブロックリストに載っている IP アドレスも含まれています。



Deteque の RPZ サービスは
脅威の先に立つため進化を続けます

従業員のセキュリティ意識
悪質なドメインへの接続を防ぐことは重要です。さらに良いのは、これまで冒してきた危険を従業員に知らせることです。RPZ は悪質なドメインをブロックするだけでなく、ブロックされた返答を使い、お客様のセキュリティトレーニングと意識向上プログラムに基づいてカスタマイズした警告メッセージを即座に送信することができます。

Domain レピュテーション - Deteque のアプローチ
Deteque のセキュリティ調査員のグローバルチームは、犯罪ネットワーク、悪意あるドメインと不正利用されている IP アドレス間の繋がりの追跡を行い、既知あるいは疑われるドメインのブロックリストを提供することにおいて、長年の経験を持っています。このドメインベースのデータは、リストに載っているドメインに接続しようとしたのがどのマシンかを示すことにより、ネットワーク上で感染しているコンピューターを識別するのにも役立ちます。
DNS ファイアウォールとしての RPZ は、既知の悪質なサイトへのアクセスを軽減し防ぐのに非常に効果的なレイヤーとなります。2 分毎に更新される RPZ は最新の脅威インテリジェンスを提供し、お客様のセキュリティを強化して既知の悪質サイトへのアクセスを防ぎます。

Deteque – Spamhaus の一事業部
Deteque は Spamhaus の一事業部で、DNS 悪用への対抗に打ち込むセキュリティ研究者のコミュニティとサービスプロバイダーの世界的ネットワークと繋がりを持っています。
Deteque は 2008 年以来、リアルタイムで組織を守るため DNS 関連の脅威インテリジェンスを収集、照合および提供することで、ネットワーク安全確保の最前線に立ってきました。

PIPELINE SECURITY
www.pipelinesecurity.jp
〒103-0014　東京都中央区日本橋蛎殻町 1丁目35–8グレインズビル1F
Tel: 03-4405-5766　hello@pipelinesecurity.jp
deteque A division of SPAMHAUS