Passive DNS: Deteque の信頼されるリアルタイム脅威インテリジェンス

PIPELINE SECURITY

Passive DNS の利用により、世界中のネットワークから悪質な活動のパターンを発見することができます。お客様の SIEM とセキュリティ分析を強力に後押しする、グローバルな脅威データです。

Passive DNS とは

Passive DNS は、どのホスト名が、いつ、どの IP アドレスに名前解決されてきたかをリアルタイムで示す、常に更新され続けるデータセットです。この重要な情報を持つ単一データポイントを世界中の様々な情報提供者と組み合わせることで、単一のネットワークを監視しているだけではわからない、世界ネットワーク上での潜在的脅威の全容を明らかにすることが可能になります。

Deteque の Passive DNS データ収集者のグローバルネットワークからくる複合データを使用すれば、DNS 名前解決のパターンを明らかにして、スパム、フィッシング、ランサムウェア等のマルウェアの挿入手段である悪質ドメインを運営するためにサイバー犯罪者が使用するパスウェイを示すことができます。

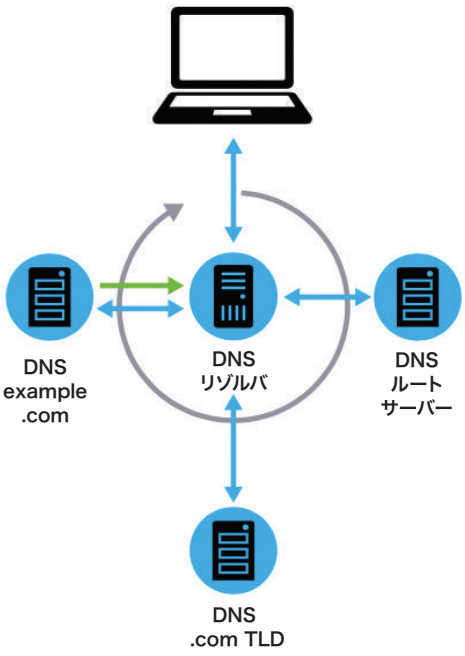
Passive DNS の仕組み

ご登録いただくと、Deteque の API 経由で Passive DNS データベースにクエリーを送り、セキュリティ情報およびイベント管理（Security & Incident Event Management (SIEM)）調査で疑われるドメインと IP アドレスを見ることができます。クエリーにより生成されたデータセットはユーザー自身のツールで更に分析が可能で、それらのドメインや IP アドレスが異常な行動をするあるいは疑わしい活動と関連しているかどうかを確認できます。

ドメインの場合、突然集中的な活動を見せる最近登録されたドメイン、IP アドレスが入れ替わるホスト名または関連付けられたホスト名が頻繁に変わる IP アドレスが考えられます。

Passive DNS のデータを研究すれば、調査員はどのドメイン名が特定のネームサーバーによってホストされているかを追跡できます。更に、ドメイン名が以前はどこを指していたか、また、あるドメイン名の下にどのサブドメインが存在しているかを確認できます。

Deteque ユーザーは、既存の SIEM、分析ツールおよび独自製品との継続的な統合のため、データを恒常的データフィードとして受け取ることも可能です。



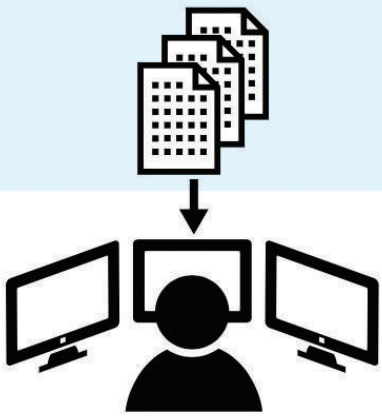
クライアントは、ローカルの DNS リゾルバに問い合わせを行い、ドメインの IP アドレスがキャッシュに含まれていなければ、外部のルートサーバー、トップレベルドメイン（Top Level Domain）サーバー、ネームサーバー自体の順に問い合わせて、サイトへアクセスします。

クライアントが一致するドメインや IP アドレスを受け取ると、再帰セグメントの結果のみが Deteque に自動的に送信されます。当社には、誰が問い合わせを行ったのかはわかりません。

Deteque が受け取るデータポイントのサンプル

ホスト名 www.example.com
解決先：IP 93.184.216.34
日時：時間と日付
初めて見られた日時：時間と日付

世界中の協力者から照合され、重複除去されたデータポイント



精製されたデータは、クエリーを介し、または継続的データフィードの形で、リアルタイムインテリジェンスとしてお客様の調査に活用いただけます

プライバシーとコンプライアンス

サブスクライバーから受け取るデータには個人情報（Personally Identifiable Information (PII)）は含まれないため、Deteque との協力関係のためにお客様の組織、顧客あるいは従業員への不正侵害が発生することはありません。全てのデータは、暗号化されて Deteque へ送信され、当社の側で処理が完了すると即時に削除されます。

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

Passive DNS: Deteque の信頼されるリアルタイム脅威インテリジェンス

PIPELINE SECURITY

お客様の組織を守るグローバルインテリジェンス

Passive DNS は、お客様の調査力を高め、特定のドメインがお客様のネットワークへ接続するのをブロックしたり、お客様のホスティング環境に関するリスクを評価するなど、組織を守るための積極的決断を可能にします。

Passive DNS を使用すると下記のことが可能です。

- お客様のホスティングプロバイダーが使用している IP ブロックとネームサーバーに関係ある他のドメインと組織を検出することでホスティングネットワークの健全性が明らかになります。
- 疑わしいドメインの履歴と IP アドレス関係を明らかにすることで、それらのドメインを調査できます。
- 類似ドメインを分析して潜在的脅威を評価できます。
- 類似ドメインとなりすましドメインによる著作権やブランドの侵害を検知できます。
- Deteque のデータセットを独自の自動レピュテーションベースのツールに統合できます。

理想的な Passive DNS の選択

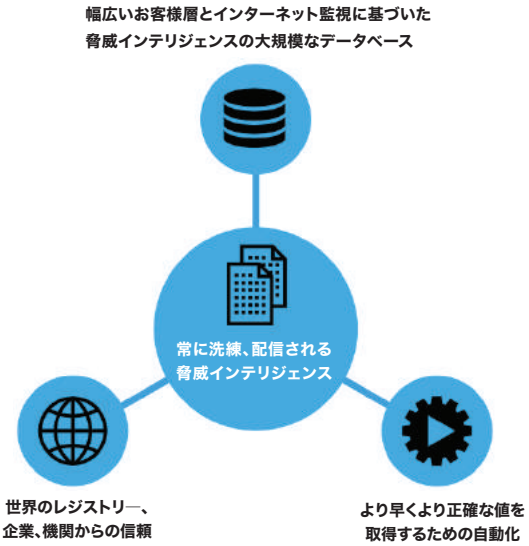
ユーザー分類	使用方法	入手方法
情報セキュリティ専門家および サイバーインシデント対応分析者	特定の IP 範囲のデジタルフォレンジックと調査または DNS クエリーと応答との関係の分析	Web ポータル
SOC/SIEM チーム、セキュリティベンダー および専門家ユーザー	生のデータセットの頻繁な複数のクエリーおよび ソフトウェアとセキュリティプラットフォームへの統合	API 経由のクエリー
大規模企業、セキュリティ研究者 および法執行機関	新しい悪質ドメインや新たに出現した脅威あるいは サイバー犯罪のトレンドを割り出すための、生の再帰 DNS トラフィックの継続的な監視	継続的なデータフィード

Deteque について

Deteque は Spamhaus の一事業部で、DNS 悪用への対抗に献身するセキュリティ研究者のコミュニティおよび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。Deteque は、Passive DNS に加え、サイバー犯罪者がデータの窃盗、詐欺の実行および正当なシステムを不正利用するために使う悪質ドメインと IP をブロックする Response Policy Zones (RPZ) 脅威インテリジェンスも照合、提供しています。

Spamhaus の一事業部

Spamhaus は、皆の保護に役立つデータを世界中の様々なネットワークと組織が提供する、信頼される第三者として機能しています。このモデルによると、Spamhaus は現在 30 億個のユーザーメールボックスを守り、インターネット上で送信されたスパムとマルウェアの大多数をブロックしています。Spamhaus のデータは、インターネットのサービスプロバイダー、E メールサービスプロバイダー、企業、大学、政府および軍のネットワークの大半によって使用されています。



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