新サービス「Threat Intelligence Data Feed（TIDF）」で脅威をさらに見える化

2023年5月11日

インターネットをより安全にするという使命のもと、WhoisXML APIは、組織のセキュリティインテリジェンスやシステムを補完し、脅威のより広い見える化と対応の迅速化を実現する新サービス「Threat Intelligence Data Feeds（TIDF）」を開始しました。

「TIDFがあれば、周知の悪質なプロパティを網羅的に把握できます。サイバー犯罪が急速に拡大している現在、悪意あるイベントを検知して脅威の種類ごとに分類し、組織の迅速な対応を支援する広範囲の脅威インテリジェンスが求められています。TIDFは、まさにそのようなニーズに応えるものです。」とWhoisXML APIのCEOであるJonathan Zhangは述べています。

幅広い脅威の見える化と対応の迅速化を実現

TIDFは、以下の10個のデータフィードで構成されています。

- 悪意あるIPv4アドレス
- 悪意あるIPv6アドレス
- 悪意あるドメイン名
- 悪意あるURL
- 悪意あるファイルハッシュ

- ホストファイルの拒否リスト
- ドメイン名の拒否リスト
- IPv4アドレスの拒否リスト
- IPv6アドレスの拒否リスト
- Nginx ngx_http_access_moduleに対応したIPv4/IPv6の拒否リスト（CIDR表記）

これらのデータは標準化されたCSVおよびJSONの形式で提供されるため、ほとんどのシステムと互換性があります。既存のサイバーセキュリティシステムに容易に統合でき、悪意あるインジケーターを検出した際にはすぐにブロックできます。

脅威をタイプ別に分類

各ファイルに含まれるインジケーターは脅威の種類ごとに分類され、より深い分析や攻撃アクターの帰属特定に役立つ高付加価値のインテリジェンスをもたらします。カテゴリーは以下の通りです。

- **攻撃**：SSHブルートフォースなどの悪意ある攻撃に関連したセキュリティ侵害インジケーター（IoC）。
- **ボットネット**：マルウェアに感染したコンピューターのネットワークに含まれるホストの一覧。
- **コマンド＆コントロール（C&C）サーバー：**ボットネットやマルウェアと通信しているC＆Cサーバーのリスト。
- **マルウェア**：悪意あるソフトウェアの配布に関連するホスト名、URLおよびファイルハッシュ。
- **フィッシング**： フィッシングに関与したドメイン名、URL、ホスト名。
- **スパム**： スパムコンテンツのホストまたは送信に関与したプロパティ。
- **Suspicious**：大量のデータのリクエストまたはスクレイピングといった疑わしい行為に関連しているウェブプロパティ。

- **Tor**：Torの出口ノードとして機能するホスト。
- **Generic**：上記のカテゴリーに該当しない悪意のインジケーター。

TIDFは、最新の脅威情報でさまざまなスペシャリストのサイバーセキュリティ対策をお手伝いします。組織のセキュリティチームやネットワーク管理者は、TIDFでゼロトラストポリシーの実装拡大、ネットワークセキュリティの強化ができます。法執行官やセキュリティ研究者は、TIDFのデータから洞察を得て捜査やOSINT分析を深めることができるでしょう。

TIDFのファイルは毎日更新されるため、お届けする情報は常に最新かつ適切に保たれています。

また、お客様のニーズに合わせた柔軟な価格設定とパッケージをご用意しています。

Threat Intelligence Data Feed（TIDF）の詳細につきましては、こちらまでお気軽にお問い合わせください。ファイルのサンプルはこちらでダウンロードしていただけます。