kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

常に進化を続ける IT 上のセキュリティ脅威を追跡、分析してその被害を軽減することは、大変な作業です。脅威インテリジェンスは情報セキュリティ業界に新たな収益源と言われているものの、すぐれたバリューを提供しています。脅威インテリジェンスのなかでも、おそらく最も注目が集まり、争点の的になっているのが脅威属性です。

製品の特徴：

- 数百のAPT攻撃とサンプルのデータを集めたリポジトリに素早くアクセスできます。
- 脅威の優先順位付けとアラートのトリアージを効率的に自動化したり手動で実行できます。
- 公になっていない攻撃者とサンプルを追加し、プライベートコレクションに保存されたファイルに類似したサンプルを検知するよう製品に「学習」させることができます。
- 手動のサンプルアップロードと、統合用のオープンAPI、自動化されたワークフローが利用できます。
- 安全な隔離環境に実装することで、システムやデータを保護するだけでなく、コンプライアンス要件にも対応できます。
- すべての送信で高いプライバシーと機密性を維持することで機密情報の漏洩を防止します。

そして、それには明確な理由があります。きわめて巧妙な脅威は、調査やリバースエンジニアリングプロセスが複雑なため、脅威を検知してから対応するまでの時間は、多くかかるのが一般的です。多くの場合、それだけの時間があれば攻撃者は目的を十分に達成できます。適切でタイムリーな属性によって、数時間かかっていたインシデント対応時間を数分に短縮できるだけでなく、誤検知の数も減らすことができます。

標的型攻撃の特定、攻撃者のプロファイリング、そしてさまざまな脅威アクターの属性要因の作成には時間と労力がかかり、それが数年におよぶこともあります。うまく機能する属性を作成するには、長年蓄積した大量のデータと、調査経験のあるリサーチャーで構成されたスキルの高いチームが必要です。一般的に、リサーチャーはさまざまなグループのアクティビティを追跡して情報の断片をデータベースに保存します。データベースは貴重なリソースとなり、ツールとして共有できます。

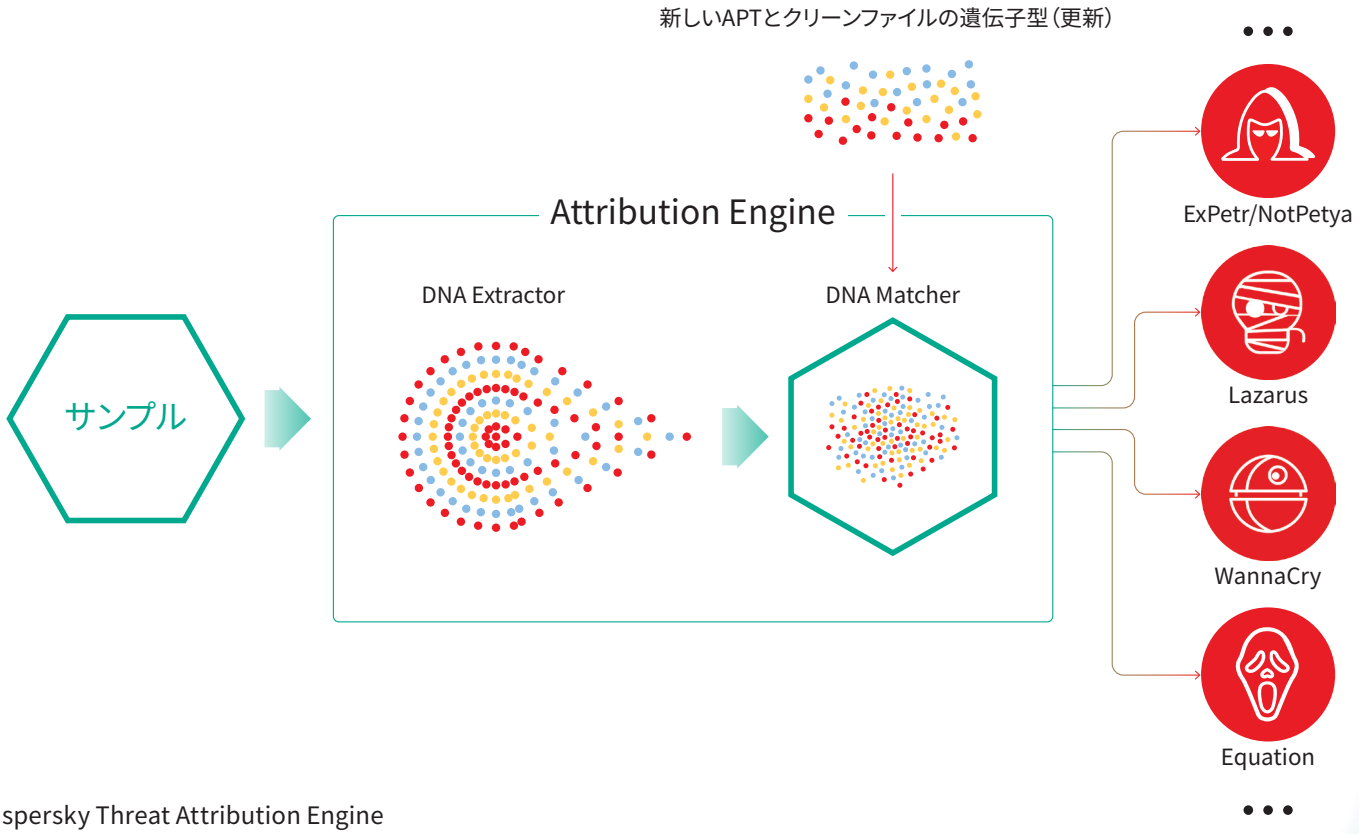
Kaspersky Threat Attribution Engineには、過去22年間にわたってカスペルスキーのエキスパートによって収集されたAPTマルウェアサンプルとクリーンなファイルを含むデータベースが組み込まれています。カスペルスキーでは、毎年、600件を超える脅威アクターとキャンペーンを追跡し、120以上のAPTインテリジェンスレポートをリリースしています。カスペルスキーの継続的な調査によって、6万以上のファイルを含む大規模なAPTコレクションを実現しています。これによって誤検知フラグの検出を改善し、自動化ツールを使うことで属性の精度を最大限に高めています。

Kaspersky Threat Attribution Engineでは、誤検知率をゼロにしながらサンプルの類似度を比較するという独自のアプローチをとっています。新しい攻撃を既知のAPTマルウェアや過去の標的型攻撃、ハッカーグループと素早く関連付けることで、深刻度がそれほど高くないインシデントのなかからリスクの高い脅威を見つけ出し、保護対策をタイムリーに実施して攻撃者がシステム内に足掛かりを得るのを防ぎます。

仕組み

Kaspersky Threat Attribution Engineでは、過去に調査したAPTサンプルや関連付けられたアクターとコードの類似度を自動的に比較することで、マルウェアの「遺伝的特徴」を分析します。「遺伝子型」、つまり分解したファイルの小さなバイナリの断片とAPTマルウェアのサンプルデータベースを比較することで、マルウェアの出自、脅威アクター、および既知のAPTサンプルとのファイル類似度を報告します。さらに、セキュリティチームが公になっていないアクターとオブジェクトをデータベースに追加してKaspersky Threat Attribution Engineに学習させることで、プライベートコレクションにあるファイルと類似するサンプルを検知できるようになります。Threat Attribution Engineでは、過去には数年かかっていた属性処理がわずか数秒で終わります。

また、処理済みの情報や送信されたオブジェクトへの第三者のアクセスを制限する、安全で隔離された環境に配置することができます。Threat Attribution Engineを他のツールやフレームワークに接続して属性を既存のインフラストラクチャや自動化されたプロセスに実装したりするためのAPIインターフェースも用意されています。



Kaspersky Threat Attribution Engine

関連するAPT攻撃の詳細な情報はKaspersky APTインテリジェンスレポート[1]でご覧いただけます。カスペルスキーのAPTインテリジェンスレポートを購読していただきますと、弊社が実施した調査結果、確認された情報、また公表されていないすべての脅威に関する情報、およびさまざまな形式（OpenIOC、STIXなど）で提供される技術データなどへのアクセスを提供します。

Kaspersky Threat Attribution Engineは、効果の高いインシデント管理プロセスを確立することで、国のサイバーセキュリティ機関や民間のセキュリティオペレーションセンター（SOC）のためのKasperskyのポートフォリオを拡張および強化します。

Kaspersky Attribution Engineでは以下のような機能によりセキュリティ業務を大幅に改善できます。

- ファイルを迅速に既知のAPT攻撃と関連付けることで、サイバーインシデントの意図、方法、ツールを解明する
- 攻撃の直接の対象なのか、二次的な被害者なのかを素早く評価して適切な封じ込め手順と対応手順を準備する
- カスペルスキーのAPTインテリジェンスレポートで提供されている、APT攻撃に関する実用的な脅威インテリジェンスに従って脅威を効果的かつタイムリーに軽減する

1 カスペルスキーのAPTインテリジェンスの購読レポート機能は製品とは別に購入する必要があります

サイバー脅威ニュース：www.securelist.com
ITセキュリティニュース：blog.kaspersky.co.jp/category/business/
中小企業向けITセキュリティ：kaspersky.co.jp/small-to-medium-business-security
大規模企業向けITセキュリティ：kaspersky.co.jp/enterprise

www.kaspersky.co.jp

実証済みの品質、独立性、透明性をお約束します。カスペルスキーは、安全な世界を作り上げ、テクノロジーを活かして人々の暮らしを良くすることを目指しています。そのために、世界中の誰もがテクノロジーの無限の恩恵を受けることができるよう、セキュリティサービスを提供しています。安心できる未来のために、サイバーセキュリティをお届けします。

詳しくは、kaspersky.co.jp/transparencyをご覧ください

Proven.
Transparent.
Independent.