Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

Kaspersky Similarity

Kaspersky Threat Analysis

kaspersky bring on the future

Kaspersky Threat Analysis

Kaspersky Threat Analysis

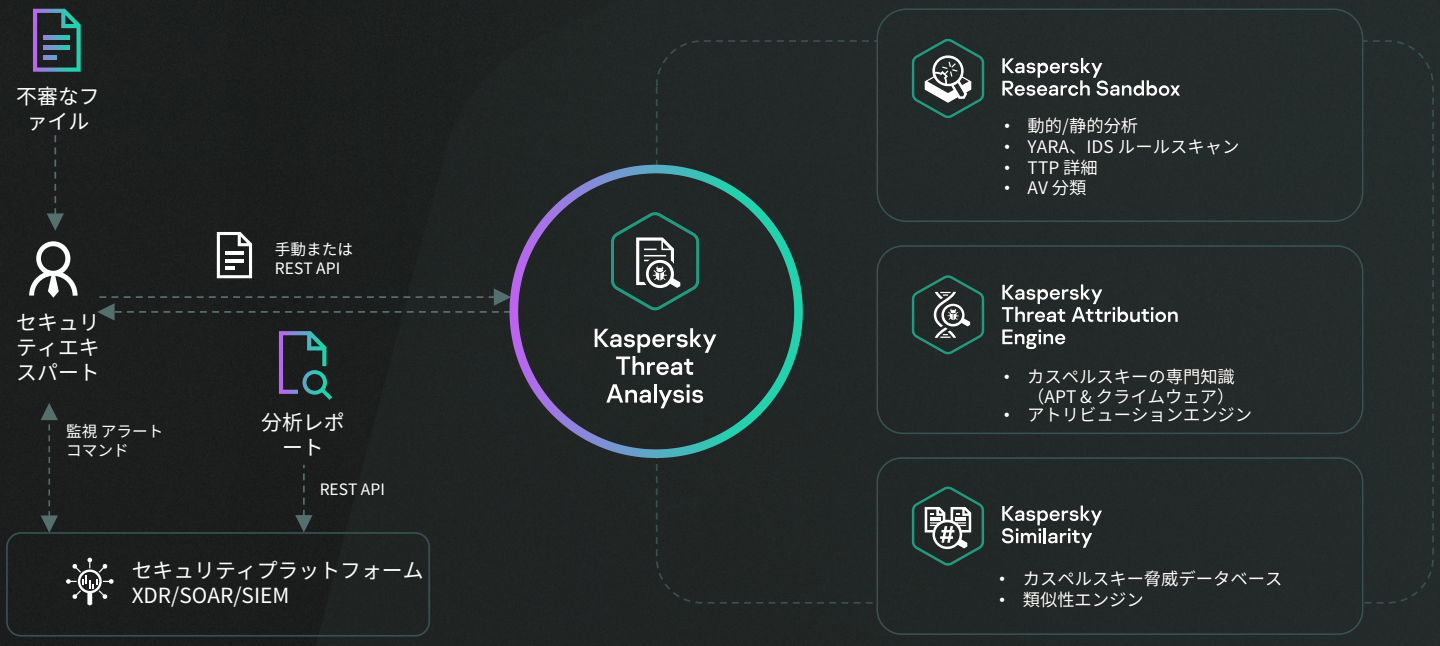
潜在的なサイバー脅威に直面した場合、どのような決断を下すか、それをどれくらいうまく下せるかが重要なポイントになります。今日の標的型攻撃は、従来のアンチウイルスツールだけでは防げません。アンチウイルスエンジンで防ぐことができるのは既知の脅威とその亜種だけですが、その一方で巧妙な攻撃者は、あらゆる方法を自在に駆使して自動検知を逃れます。SOC が日々処理するセキュリティアラートは指数関数的に増えています。毎日大量のマルウェアサンプルが生成される中で、アラートの優先順位付け、トリアージ、検証を効果的に行うのは至難の業です。

脅威インテリジェンス、動的分析、脅威アトリビューション、類似性の各技術を組み合わせることで、これまでには見られなかった悪意のあるオブジェクトの検知に役立つ強力なツールが誕生します。カスペルスキーは、セキュリティ研究者が既存の脅威や新たな脅威に関する情報を常に把握できるように、疑わしいファイルの定期分析を自動化する単一の弾力的なフレームワークを提供しています。

サンドボックスなどの従来の脅威分析技術に加え、 Kaspersky Threat Analysis は最新のアトリビューション技術や関連する類似性技術も提供しています。効率的な脅威分析を実現するハイブリッドなアプローチにより、十分な情報に基づいて判断を下し、インフラのセキュリティを確保できるようになります。

Kaspersky Threat Analysis には、統一された Web インターフェイスと RESTful インターフェイスの両方があり、ユーザーは具体的なパラメータを設定して疑わしいオブジェクトを効率的に解析できます。複数の脅威分析ツールを組み合わせることで、あらゆる角度から状況を分析することが可能になり、包括的で詳細なレポートを利用して迅速かつ効果的に対応することができます。

仕組み



サンドボックス技術

は強力な動的分析ツールであり、ファイルサンプルの発生源の調査や、ふるまい分析に基づく IOC の収集、従来のアンチウイルスツールでは検知されない悪意のあるオブジェクトの特定を可能にします。

クラウド版とオンプレミス版をご用意しています。

Sandbox

Kaspersky Research Sandbox は、20 年以上かけて進化してきたカスペルスキーのラボ内サンドボックス環境から直接開発されています。このサンドボックスには、カスペルスキーが脅威に関する調査を通じて蓄積してきたマルウェアのふるまいに関するあらゆる知識が組み入れられており、毎日 42 万件以上の悪意のある新規オブジェクトの検知を可能にしています。ふるまい分析と堅牢な反回避技術にヒューマンシミュレーション技術を組み合わせたハイブリッドアプローチを提供します。

この技術をオンプレミスに配置すると、データが組織の外部にさらされるリスクを防ぐことができます。オンプレミスの Kaspersky Research Sandbox では、分析用のカスタム実行環境を作成して実際の環境に合わせて調整することもでき、脅威検知の精度と調査スピードが向上します。

使用すべき理由

アンチウイルスツールで検知されない疑わしいファイルが悪意のある特性を示すのは、その動作中だけです。Kaspersky Research Sandbox はファイルのふるまいをエミュレートして、危険な動作を際立たせます。

製品の特徴

Windows、Linux、Android 環境でのオブジェクト分析の自動化

カスタムイメージにより、Windows オペレーティングシステムとアプリケーションにまたがる脅威分析が可能（実際の環境に適用されるもののみ）

ファイルの実行中に取得された指標とデータに基づく脅威スコアにより、分析されたオブジェクトの危険度を提示

先進の反回避技術とヒューマンシミュレーション技術

手動のサンプルアップロードと、自動化されたワークフローとの連携を可能にする強化された REST API

200 種類を超えるファイルの分析に対応し、詳細な分析レポートを提供

ネットワークトラフィックのスキャン用の Suricata カスタムルールを追加し、既成の Suricata ルールと併用可能

MITRE ATT&CK による TTP 抽出のための 1000 以上の独自のハンティング

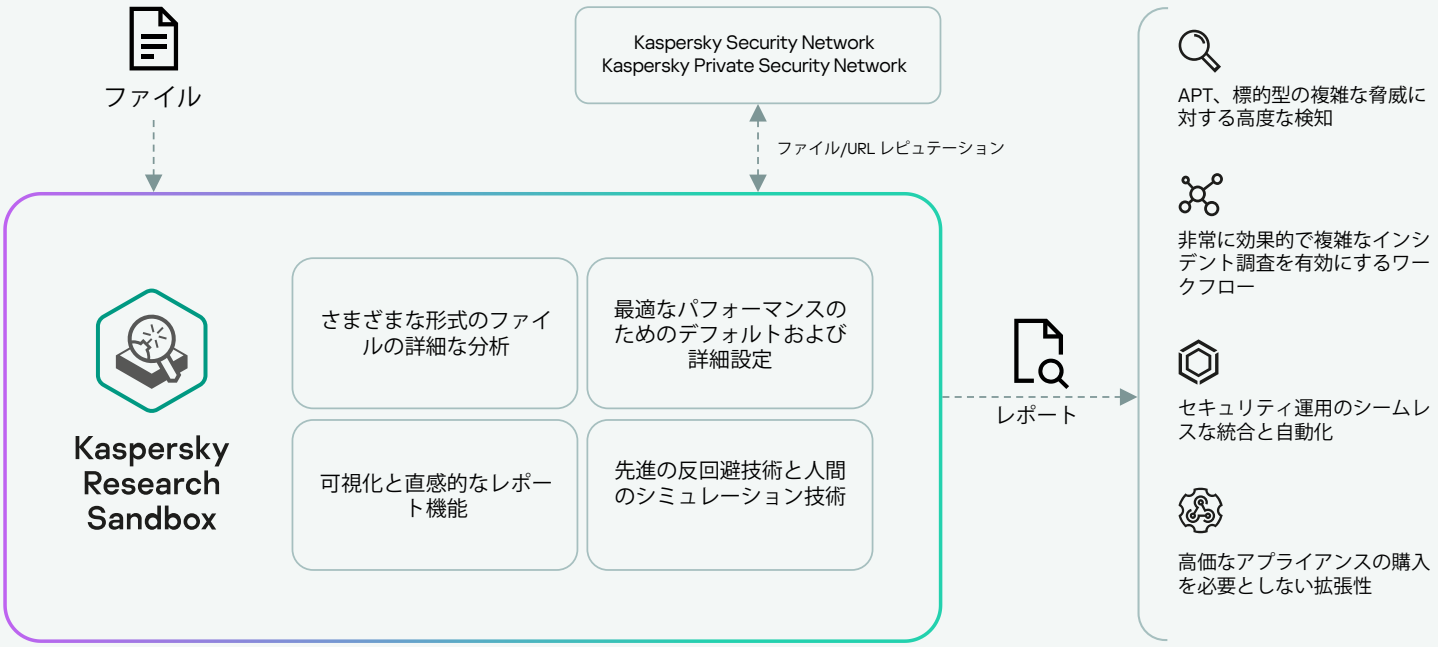
インタラクティブモードのサポート（2024 年第 1 四半期を予定）

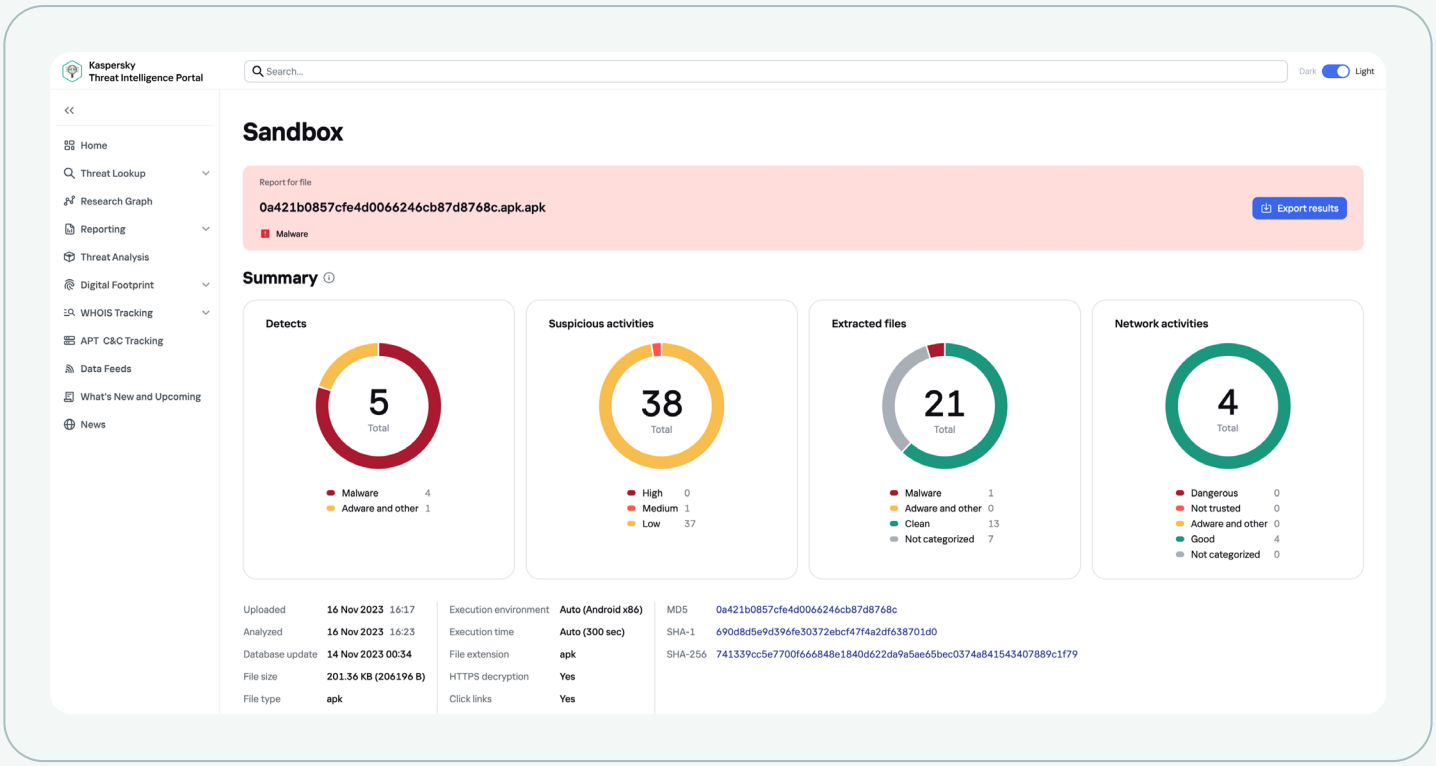
本製品はベアメタル展開に対応します。必要なパフォーマンスに応じてハードウェアを構成でき、拡大可能です。少なくとも 1 つの独立した ISP 接続（フォールトトレランスのためには 2 つ以上を推奨）と各チャネルに 100Mbps が必要です。

Kaspersky Research Sandbox は、特許取得済みの独自技術を基盤に構築されています（特許番号：US10339301）。マルウェアの実行がトリガーされる状況を正確に作り出すことで、研究者が疑わしいファイルや URL を一度の試行で分析できるようにします。

検知から逃れるために、悪意のあるファイルはまず、現在の環境が仮想マシン内かどうかを調査します。そして、サンドボックスが機能しなくなるまで活動を停止します。そのような場合、特許取得技術により仮想マシン内の時間の流れが加速され、悪意のあるコードが実際より早く実行せざるを得なくなります。

Kaspersky Research Sandbox 運用スキームの概要





詳細な分析レポート

分析が完了すると、Research Sandbox から分析対象サンプルのふるまいと機能に関する詳細なレポートが提供されるため、適切な対応手順を定義できます：

サマリ	ファイルの実行 / URL の閲覧結果に関する一般的な情報。
検知名	ファイルの実行中に登録された検知のリスト（AV およびふるまい検知）。
トリガーされたネットワークルール	実行されたオブジェクトからのトラフィックの分析中にトリガーされた Suricata ネットワークルールのリスト。
実行マップ	一連のオブジェクトアクティビティとアクティビティ間の関係をグラフィカルに表現したもの。
疑わしいアクティビティ	登録された疑わしいアクティビティのリスト。
スクリーンショット	ファイルの実行 / URL の閲覧中に取得されたスクリーンショットのセット。
読み込まれた PE イメージ	ファイルの実行 / URL の閲覧中に検知された、読み込まれた PE イメージのリスト。
ファイル操作	ファイルの実行 / URL の閲覧中に登録されたファイル操作のリスト。
レジストリオペレーション	ファイルの実行 / URL の閲覧中に検知された、OS レジストリで実行されたオペレーションのリスト。
プロセスオペレーション	ファイルの実行中に登録されたプロセスとファイルとのインタラクションのリスト。
同期オペレーション	ファイルの実行 / URL の閲覧中に登録された、作成された同期オブジェクト（ミューテックス、イベント、セマフォ）のオペレーションのリスト。
ダウンロードされたファイル	ファイルの実行 / URL の閲覧中にネットワークトラフィックから抽出されたファイルのリスト。
ドロップされたファイル	実行されたファイルにより保存（作成または変更）されたファイルのリスト。
HTTPS / HTTP / DNS / IP / TCP / UDP など	ファイルの実行 / URL の閲覧中に登録されたネットワークセッション / リクエスト詳細。
ネットワークトラフィックダンプ（PCAP）	ネットワークアクティビティは PCAP 形式でエクスポートできます。
MITRE ATT&CK matrix	エミュレーション中に記録された特定済みのすべてのアクティビティは、MITRE ATT&CK matrix の形式で表示される。

Kaspersky
Threat Analysis

Kaspersky
Threat Attribution
Engine

脅威アトリビューション

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。過剰な宣伝文句を使うまでもなく、脅威インテリジェンスには真の価値があり、脅威アトリビューションはその重要な要素です。

クラウド版とオンプレミス版をご用意しています。

アトリビューション

Kaspersky Threat Attribution Engine は、注目度の高いマルウェアの発生源や作成者と思われる人物に関する情報を提供する独自の脅威分析ツールです。独自のアルゴリズムを駆使し、APT マルウェアのサンプルおよびカスペルスキーのエキスパートが 25 年以上にわたって収集してきた業界最大規模のクリーンファイルを集積した特別なデータベースを使用して、疑わしいファイルを既知の APT 脅威、攻撃者、キャンペーンと迅速に関連付けます。

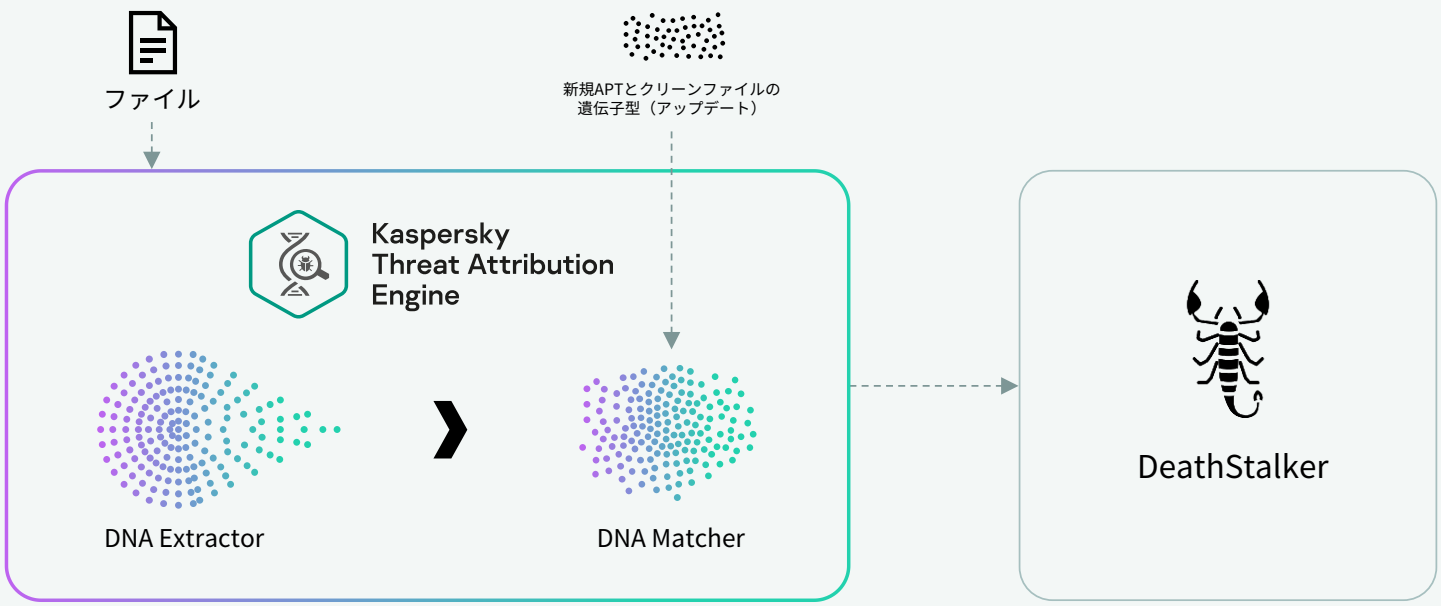
カスペルスキーは 1,100 以上の攻撃者やキャンペーンを追跡し、年間 200 以上の脅威インテリジェンスレポートを公開しています。カスペルスキーの継続的な調査は、8 万以上のファイルを含む APT コレクションをサポートしています。これを自動化されたツールと組み合わせることで、非常に正確なアトリビューションが実現します。

この製品は、類似サンプルの比較に独自のアプローチをとりながら、誤検知をほぼゼロに抑えます。どのような新しい攻撃でも、既知の APT マルウェア、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、リスクの高い脅威を深刻度の低いインシデントの中から見つけ出し、攻撃者がシステムに足場を築けないようにタイムリーに保護対策を講じることができます。Kaspersky Threat Attribution Engine をセキュアなエアギャップ環境に導入すると、処理された情報や送信されたオブジェクトに第三者がアクセスできなくなります。

使用すべき理由

攻撃者に関する知識に基づいて、あるファイルを特定の攻撃者に関連付けることで、この攻撃者にとってサイバーキルチェーン全体でこのサンプルがどのような位置づけなのかを知ることができます。その結果、他の IoC/IoA を探すべき場所についての知識を得られるため、特定のファイルだけをブロックして攻撃全体を見逃すことがなくなります。

Kaspersky Threat Attribution Engine 運用スキームの概要



製品の特徴

数千もの APT アクター、サンプル、より広範な脅威に関するデータを集めたリポジトリへの即時アクセスを（アンチウイルスエンジンを介して）提供

カスペルスキーのエキスパートが調査した、注目度の高いキャンペーン（400 件以上）に関する独自のインサイト

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または手動で実行

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」させることが可能

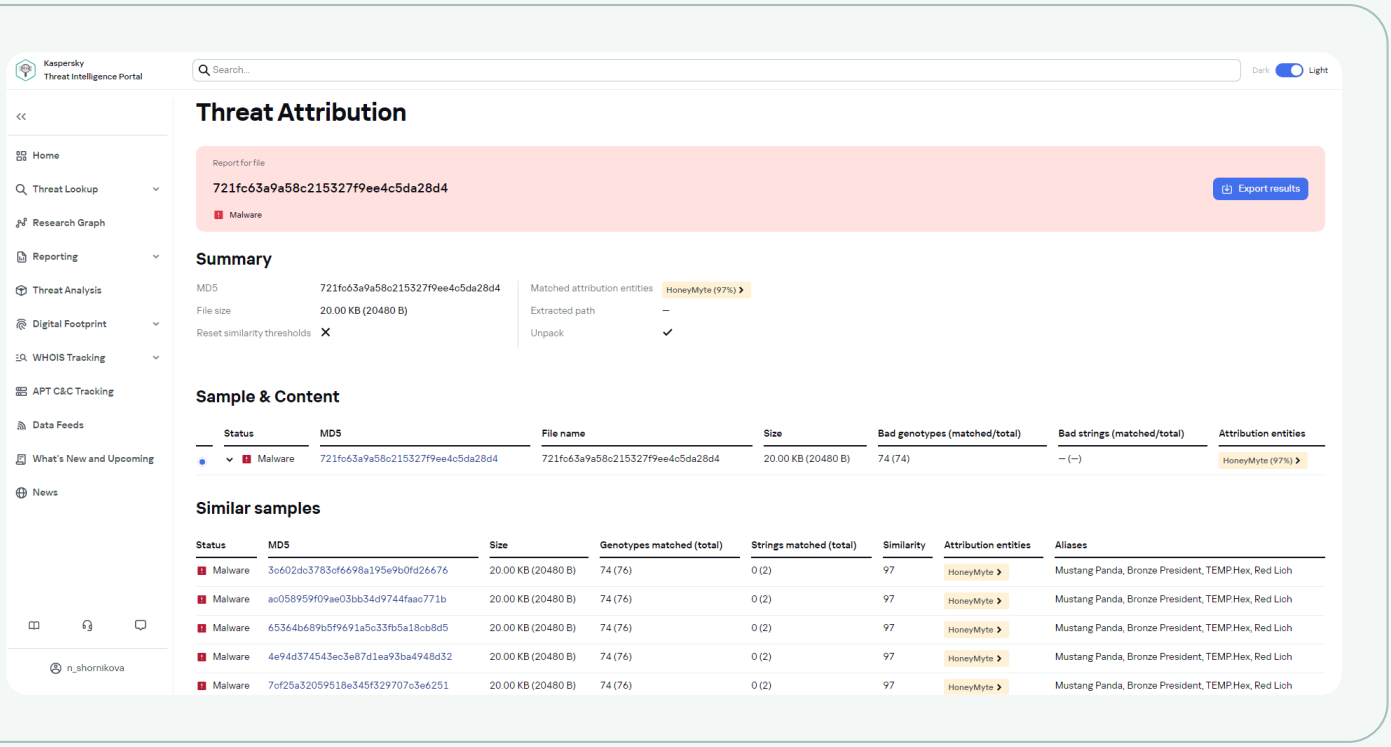
手動のサンプルアップロードと、自動化されたワークフローとの連携を可能にする強化された REST API

Amazon Web Services（AWS）などのクラウドインフラへの展開をサポートするため製品を迅速に設定でき、ハードウェアへの先行投資が不要なことからコスト削減も実現

YARA ルールにエクスポートし、類似ファイルの自動検索/スキャンやサードパーティ製ソリューションとの統合が可能

STIX 2.1フォーマット（TXT および JSON フォーマットにも対応）へのエクスポートにより、セキュリティログのさらなる自動分析や、サードパーティ製ソリューション/セキュリティ管理との統合が可能

パスワード保護されたアーカイブをカスタムパスワードで解凍



独自の検索手法

Kaspersky Threat Attribution Engine は、マルウェアとアトリビューションエンティティの関連付けに、ファイル間でよく似た遺伝子型や文字列を検索する独自の手法を採り入れています。この手法では、以下の作業を行います。

サンプルの遺伝学的分析

サンプルのコードから以下の要素を抽出します。

- 遺伝子型 - バイナリコードの特徴的な部分
- 文字列 - 特徴的な文字列

分析済みのファイルを自動的に検索

以前に分析した APT サンプルの遺伝子型や文字列と類似している遺伝子型や文字列、または既にアトリビューションエンティティに関連付けられている遺伝子型や文字列を検索します。

類似の遺伝子型と文字列に基づくレポート

APT サンプルで発見された遺伝子型と文字列に基づいて、分析されたサンプルの発生源、関連するアトリビューションエンティティ、およびこのサンプルと既知の APT サンプルとの類似性に関するレポートを提供します。

Kaspersky Threat Analysis

Kaspersky Similarity

ファイルの類似性

効果的な防衛ラインを構築するために、必ずしも敵を目視で把握する必要はありません。Kaspersky Similarity により、類似の機能を持つファイルサンプルを識別することで、未知の脅威や回避型の脅威から保護することができます。

クラウド版は Kaspersky Threat Intelligence Portal から利用できます。

類似性

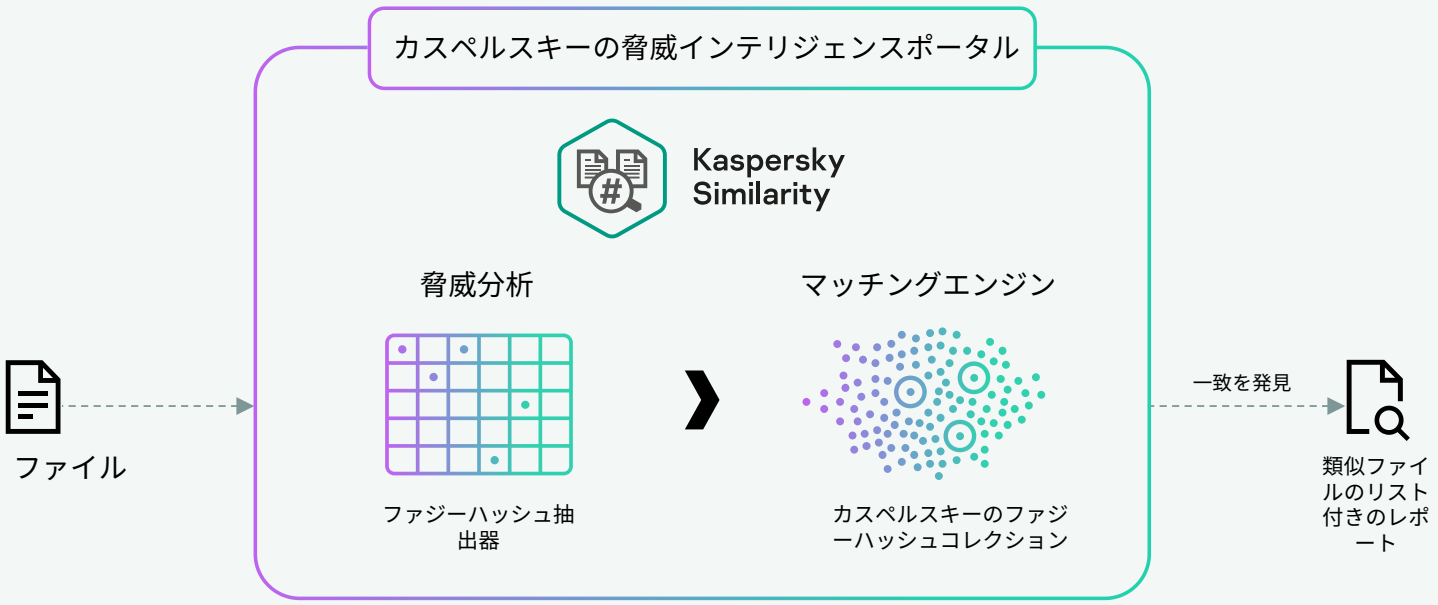
Kaspersky Similarity は、Kaspersky Research Sandbox や Kaspersky Threat Attribution Engine のユーザーが脅威インテリジェンスポータルから利用できる追加の機能で、見た目やふるまいが類似しているファイルの特定に役立ちます。

類似ファイルは、カスペルスキーのエキスパートによって考案された、50種類以上の類似性ハッシュのタイプを活用する最先端技術により、元のファイルに対して検索・計算されます。これにより、精度と信頼性の高い類似性結果が保証されます。

使用すべき理由

類似の（回避型などの）マルウェアを見つけ、インフラ内でそれを探すことで、攻撃者によるサンプルのささいな変更をセキュリティレーダーの監視下に留めます。この技術はアトリビューションと違い、関連付けがされていない類似マルウェアファイルも見つけることができます。

Kaspersky Similarity 運用スキームの概要



類似性レポート

それぞれのファイルは特定のフォーマットを持ち、使用されるパッカー、セクション、文字列、インポートテーブルなどもそれぞれ違います。カスペルスキーのエキスパートは、こうした属性に基づいて異なるファイル間の類似性を判断するためのハッシュセットを作成しました。Kaspersky Similarity では、ユーザーが疑わしいファイルを提出し、そのファジーハッシュを抽出して、カスペルスキーの脅威データベースに存在するファイルのファジーハッシュと比較することができます。一致したものがあれば、カスペルスキーが把握済みの類似した悪意のある主なファイルのハッシュのリストが生成され、類似性のスコアでソートされます。このレポートには、それぞれの類似ファイルのメタデータによる追加コンテキストが含まれています。

- 類似性の信頼度
- ファイルのステータス（マルウェア、アドウェアなど）
- 脅威の名称
- 最初と最後の検知のタイムスタンプ
- ヒット数（検知数）
- ファイルハッシュ
- ファイルの種類
- ファイルのサイズ

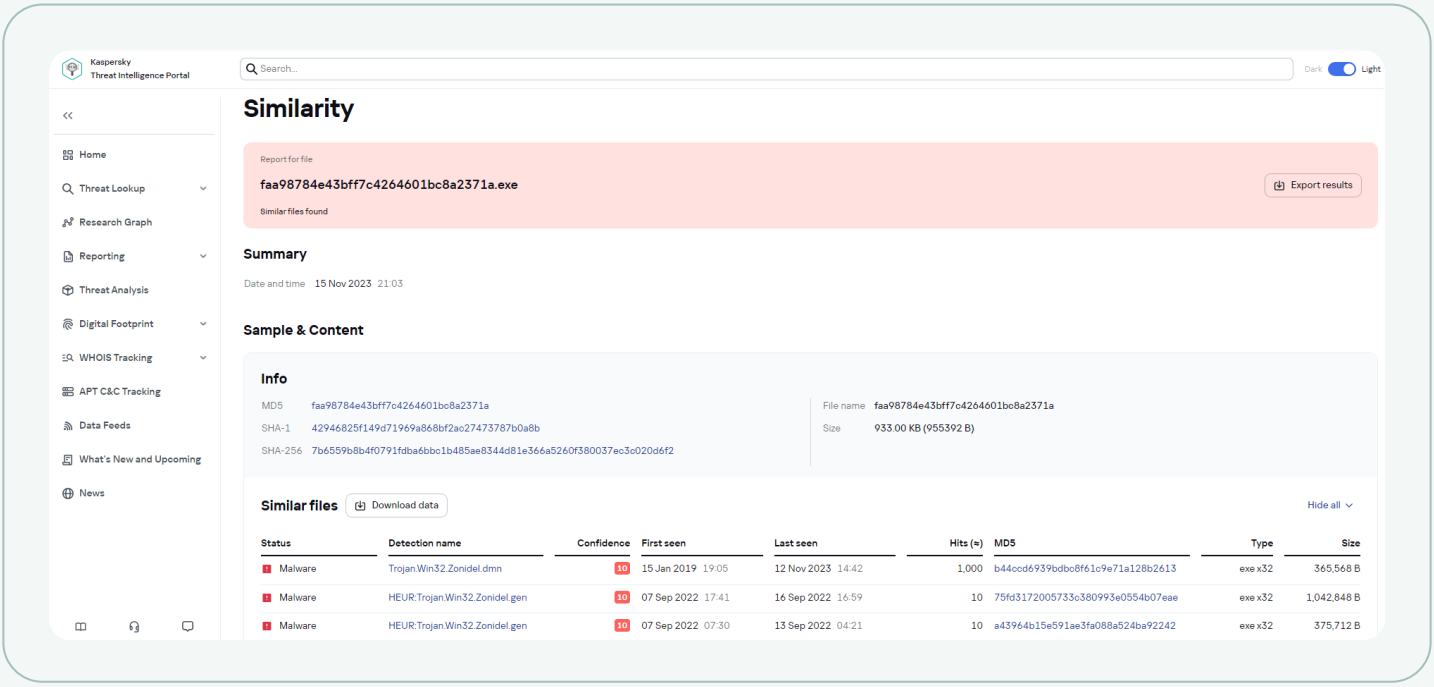
機能の特徴

過去 25 年以上にわたって収集された悪質なファイルとクリーンなファイルの業界最大級のデータベースを活用し、最大限のカバー率で比較精度を最大限に高めます。

手動のサンプルアップロードと、自動化されたワークフローとの連携を可能にする強化された REST API

Kaspersky Research Sandbox および Kaspersky Threat Attribution のユーザーに対し、両技術の効果を高め、分析対象ファイルに関する包括的な情報を提供するために無料で提供されています。

カスペルスキーのエキスパートにより、新たな脅威を探索するために既に幅広く使用されており、第三者機関によるテストで常に上位にランクインしているカスペルスキー製品の脅威防御性能をより一層高めています。



Kaspersky Threat Analysis ユースケース

Kaspersky Threat Analysis は、未知の脅威を検知するための成熟したツールを提供しており、以下のシナリオに幅広く適用できます。

インシデント対応

回避型の脅威の発見

疑わしいファイルの静的/動的分析

新種のマルウェアと特定の攻撃者との関係を明らかにし、攻撃の次のステップを予想

脅威ハンティング

レポートを通じて受信した IoC のインフラストラクチャ内でのスキャン

一般的なクリーンファイルに加えられた可能性がある悪意のある変更の発見

未知の悪意のあるファイルと既知の悪意のあるファイルで共通する IoC の特定

マルウェア解析

未知の脅威の分析

難読化されたファイルのリバースエンジニアリングに役立つ関連マルウェアの検索

Kaspersky Threat Analysis は、相互接続されたコンポーネントを実装した柔軟な調査ツールです。不審なオブジェクトを包括的かつ多層的に評価し、高度な攻撃を特定、分類します。SOC チーム、セキュリティ研究者、マルウェアアナリストは既存または新たなマルウェア関連の脅威に関する最新情報を入手できるため、重要な脅威の優先順位を速やかに見極めて迅速に対処し、より効果的に修復できるようになります。

Kaspersky Threat Analysis

詳細

www.kaspersky.co.jp

#kaspersky
#bringonthefuture