kaspersky

「Kaspersky Threat Lookup」のご紹介
～セキュリティ体制を強化するインテリジェンスサービスの提供～

2023年09月22日
株式会社カスペルスキー
セールスエンジニアリング本部

V1.1

Kaspersky Threat Lookup: サービス概要

Kaspersky Threat Lookup

・検索対象を基にカスペルスキーの脅威情報データベースに格納された脅威情報を確認するためのセキュリティ情報検索エンジン

・脅威判定（悪意性の有無）だけではなく、効率良く次のアクションを決定するための詳細情報を提供

＜提供する詳細情報一例＞

-リダイレクト元・先　/　ドメインにアクセスするオブジェクト情報

-ファイルパス（潜伏先）

-オブジェクトのダウンロード元 / オブジェクトがダウンロード・実行するオブジェクト

・ダーク/ディープwebで確認された悪用される可能性のある情報を検索する「Dark web Search」、検索キーワードに関連する有益な記事リンクを提供する「Social web Search」を提供

kaspersky

Kaspersky Threat Lookup とは

Kaspersky Threat Lookup

・URLやIPアドレスなどの分析対象を基にカスペルスキーの脅威情報データベースに格納された脅威の兆候やファイル属性、地理位置情報データといった詳細情報を確認可能なセキュリティ情報検索エンジン

・Threat Lookupは以下5つのサービスで構成

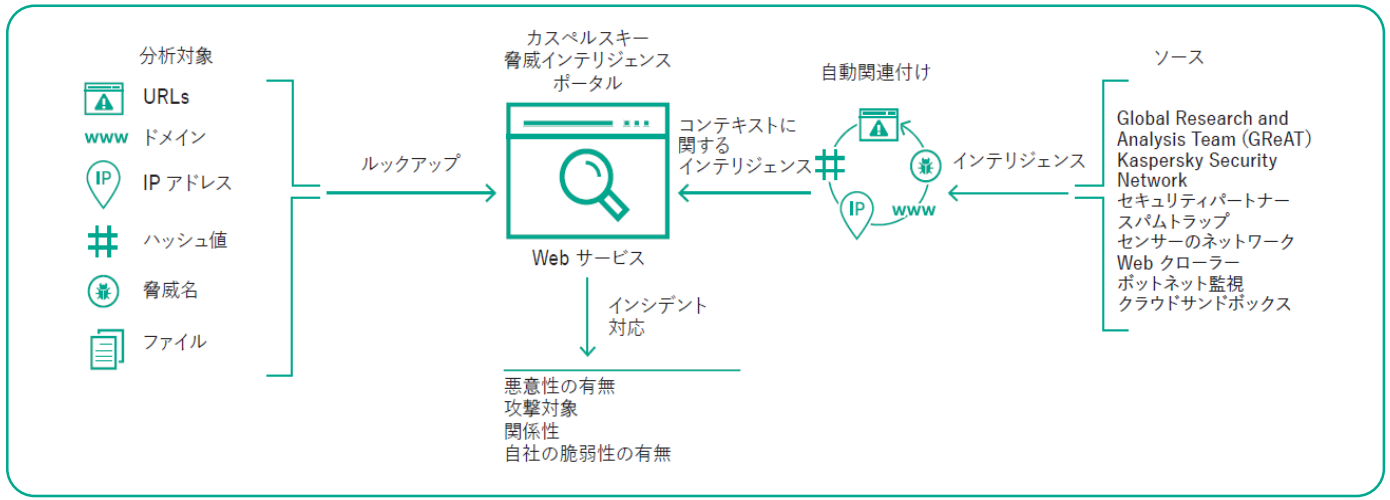
-特定のIPアドレス、ドメイン、URL、オブジェクトに関する脅威の検索を行う「**Threat Lookup**」、

-WHOIS情報検索、ドメインのあいまい検索を行う 「**WHOIS Lookup**」、

-設定した検索条件を基にドメイン情報を収集する「**WHOIS Hunting**」

-ダークweb/ディープwebで確認された攻撃の計画、脆弱性、データ侵害などの情報を検索する「**Dark web Search**」、

-キーワードに関連するセキュリティニュースポータルやフォーラムに公開された記事リンクを提供する「**Social web Search**」



kaspersky

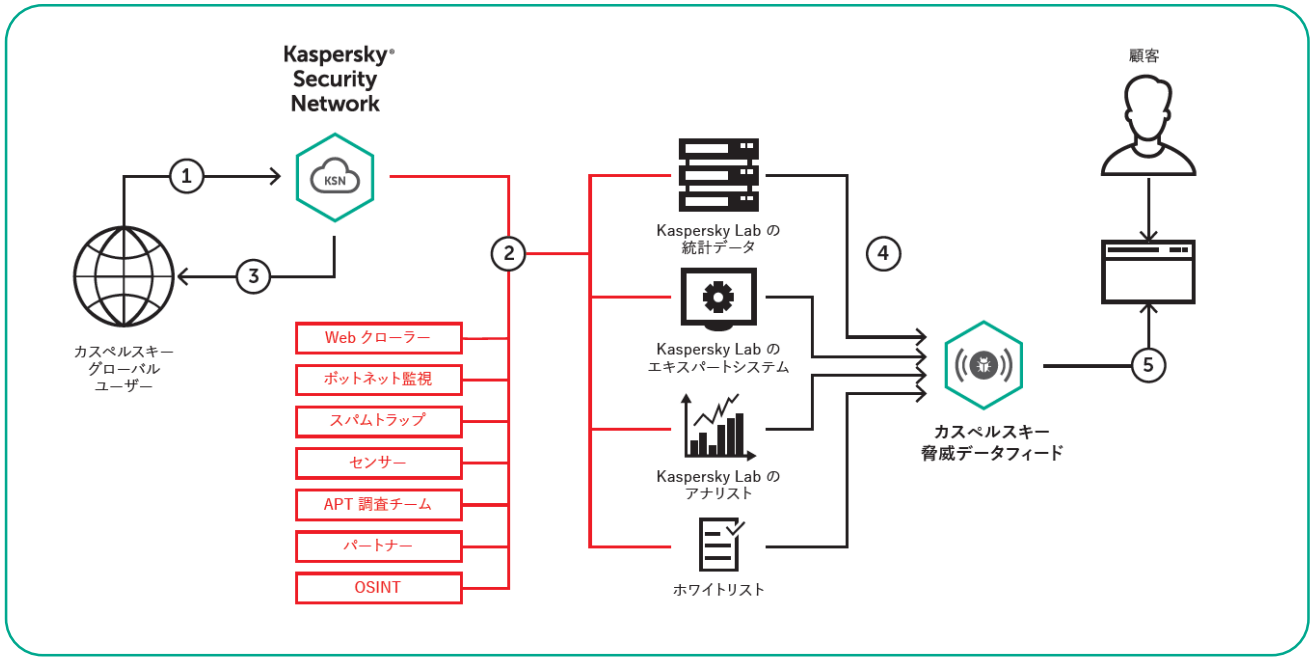
脅威インテリジェンスのソース

Kaspersky Threat Lookup

高品質なサービスを提供するための取り組み

・脅威インテリジェンスは、Kaspersky Security Network（KSN）、独自のウェブクローラー、ボットネット監視サービス（ボットネットとそのターゲットおよび活動を 24 時間 365 日監視）、スパムトラップ、リサーチチーム、パートナー及び当社が収集した悪意あるオブジェクトに関するその他の過去データなど、信頼性の高い各種のソースから収集

・収集された情報は、統計分析や 当社のサンドボックス・ヒューリスティックエンジン・マシンラーニングといったエキスパートシステム、アナリストによる検証、ホワイトリストなど、さまざまな技術を用いて、「リアルタイム」で分析

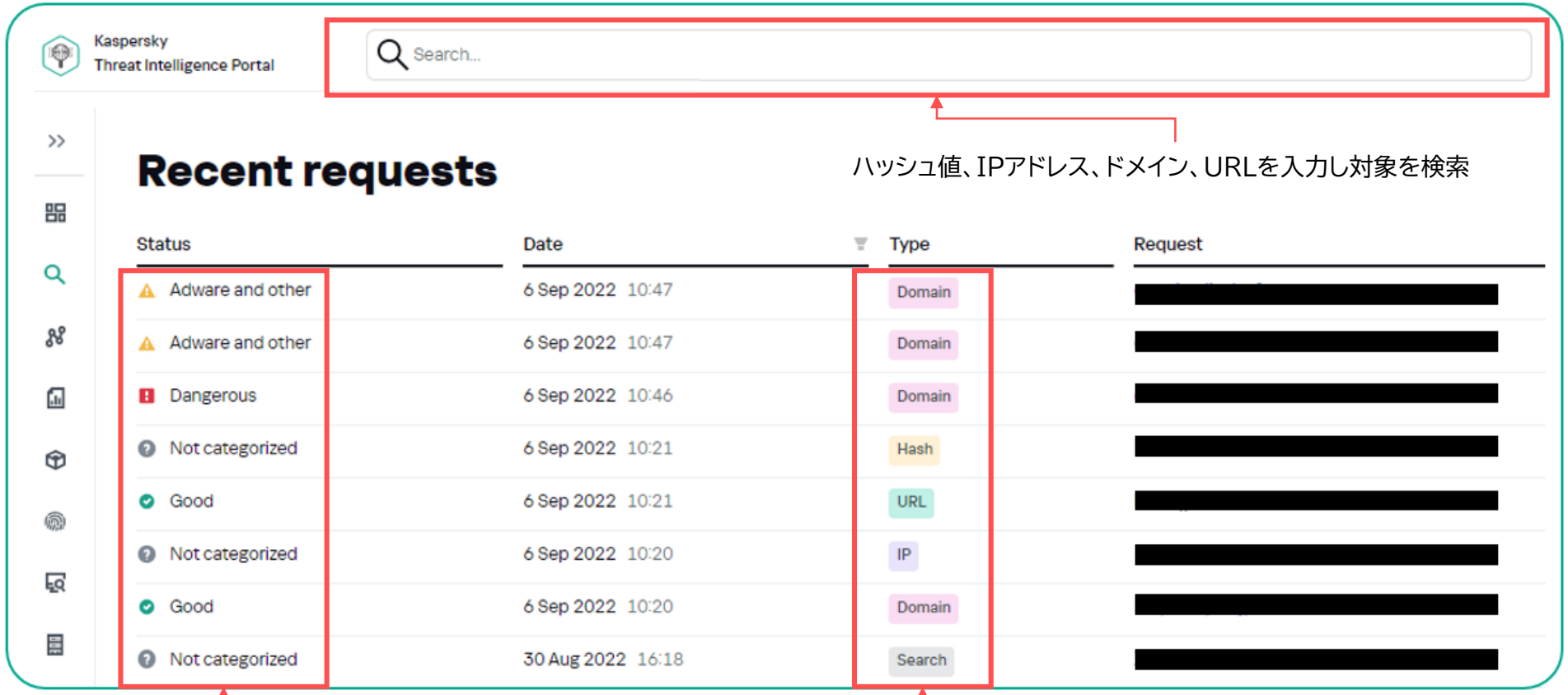


kaspersky

Threat Lookup：使用方法

Kaspersky Threat Lookup

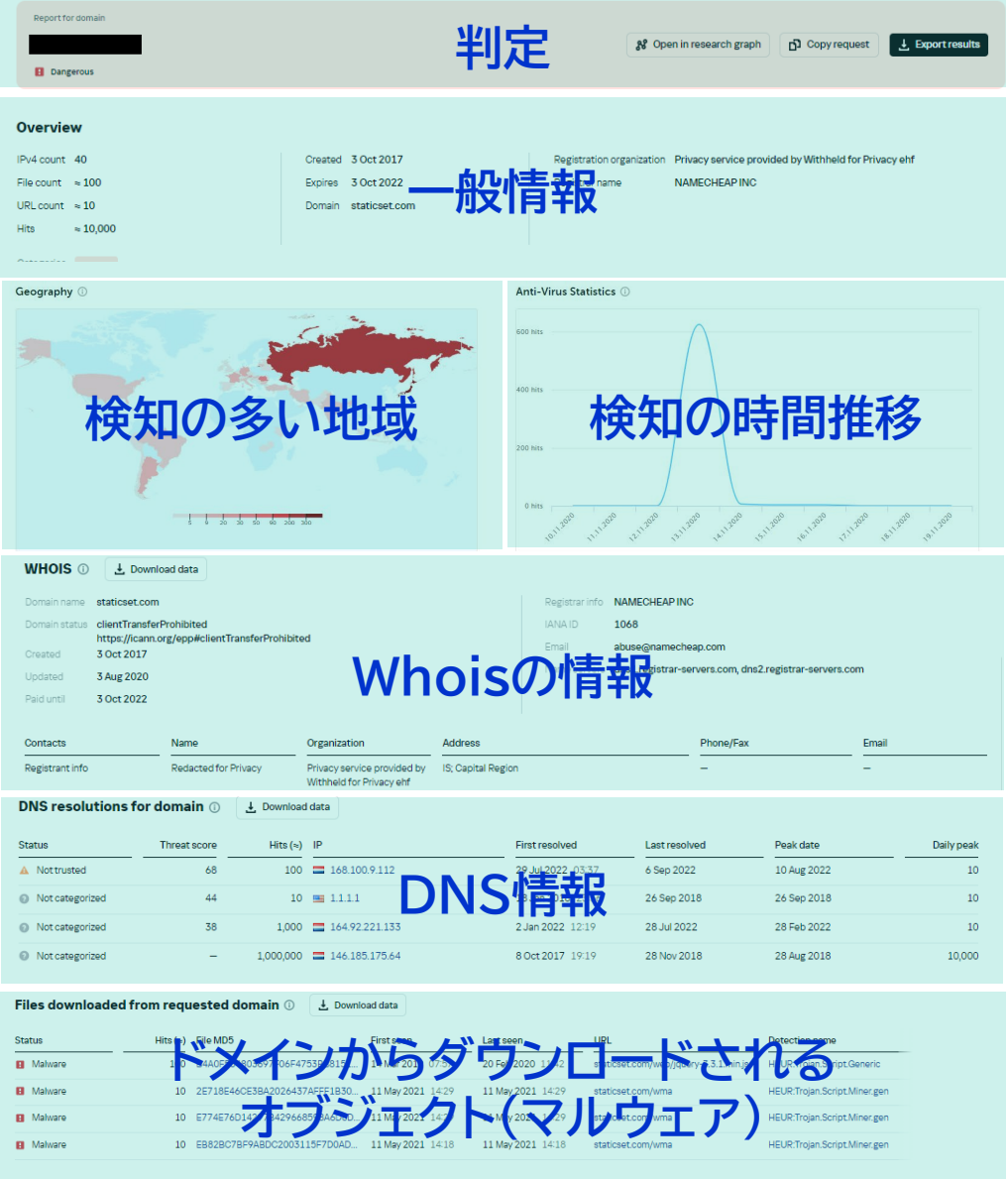
・検索タブに対象の情報（オブジェクトハッシュ値、IPアドレス、ドメイン、URL）をキーに脅威判定（悪意性の有無）や統計的データ、ふるまいデータといった詳細情報の確認が可能

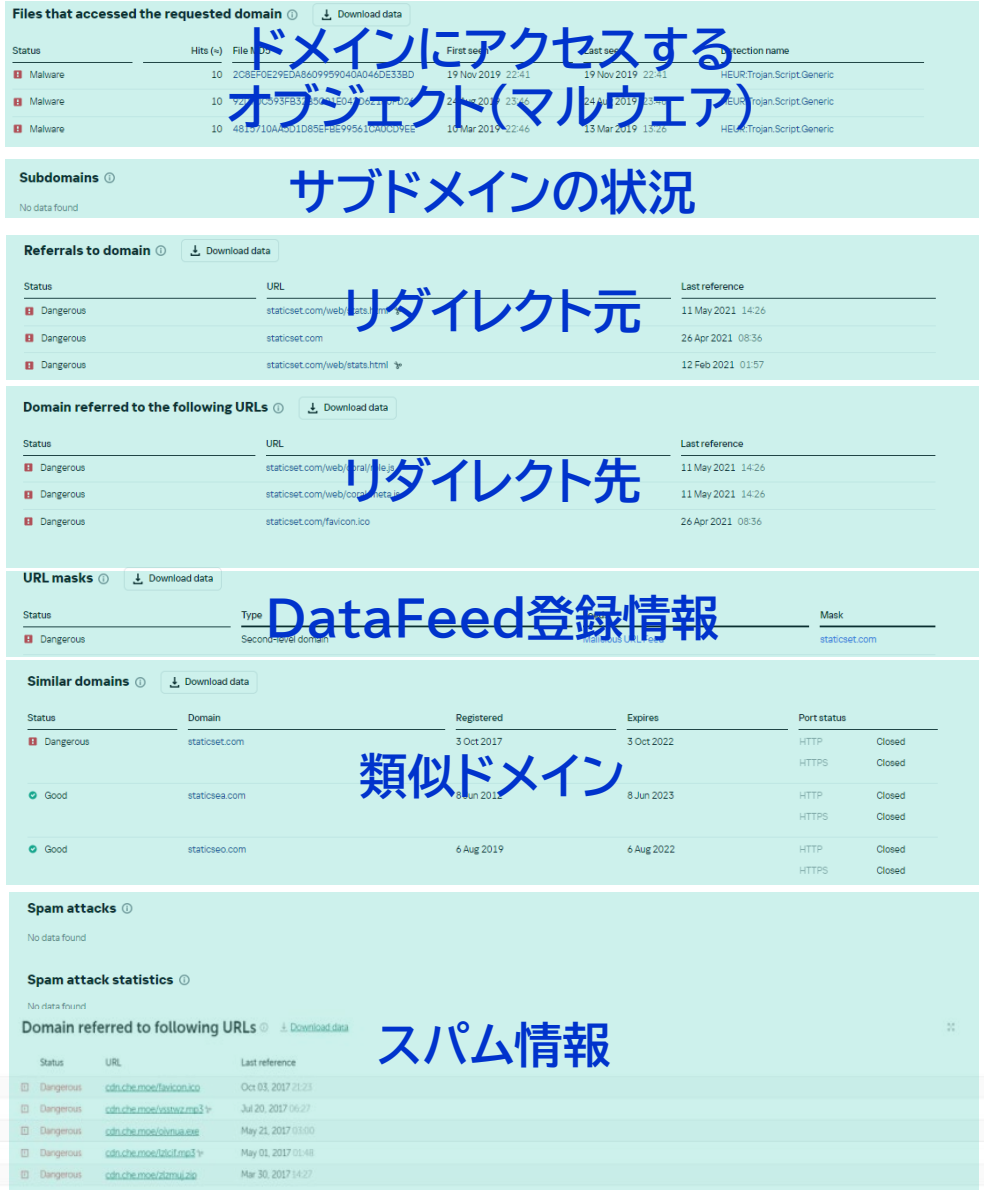


kaspersky

検索結果：URL

Kaspersky Threat Lookup

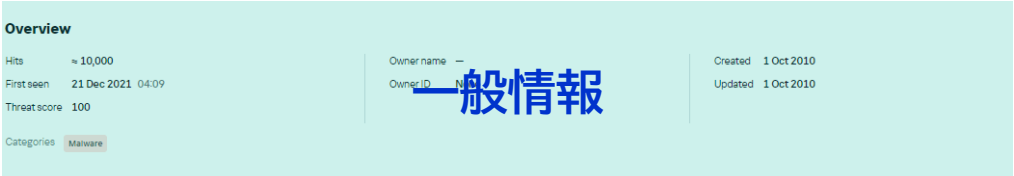


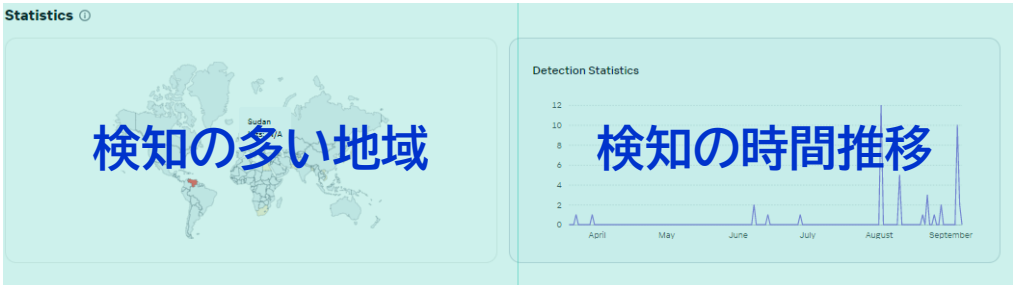


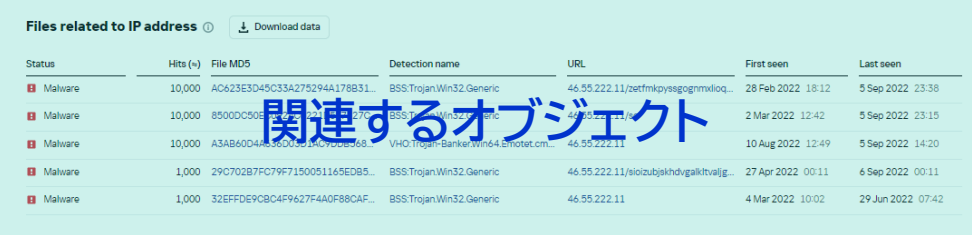
kaspersky

検索結果：IPアドレス

Kaspersky Threat Lookup



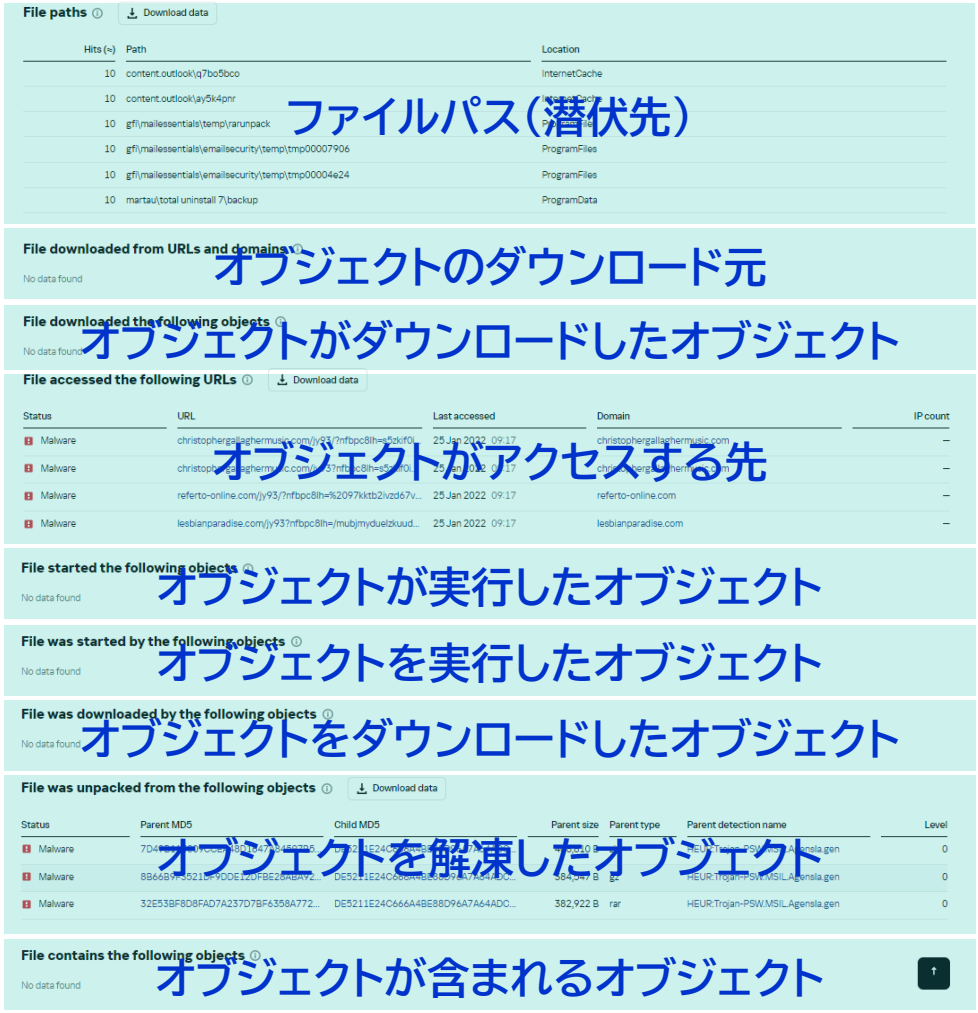




kaspersky

検索結果：ハッシュ値

Kaspersky Threat Lookup



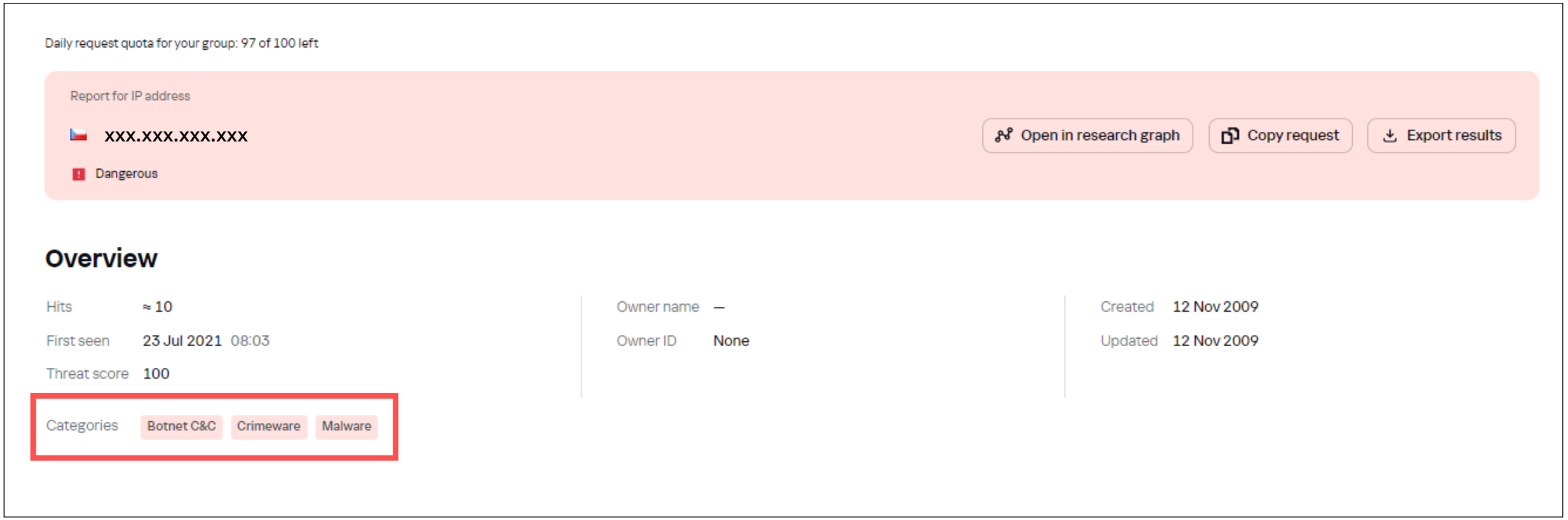
kaspersky

New 新たな脅威カテゴリの追加

Kaspersky Threat Lookup

・検索結果：「脅威カテゴリ」にDDoS、侵入、クライムウェア（金銭を目的とした サイバー攻撃）、総当たり攻撃、ネットワークスキャナーなど新たな脅威カテゴリを追加

->検索したインジケーターがどのような目的で使用されたかを把握し、インシデント対応を最適化

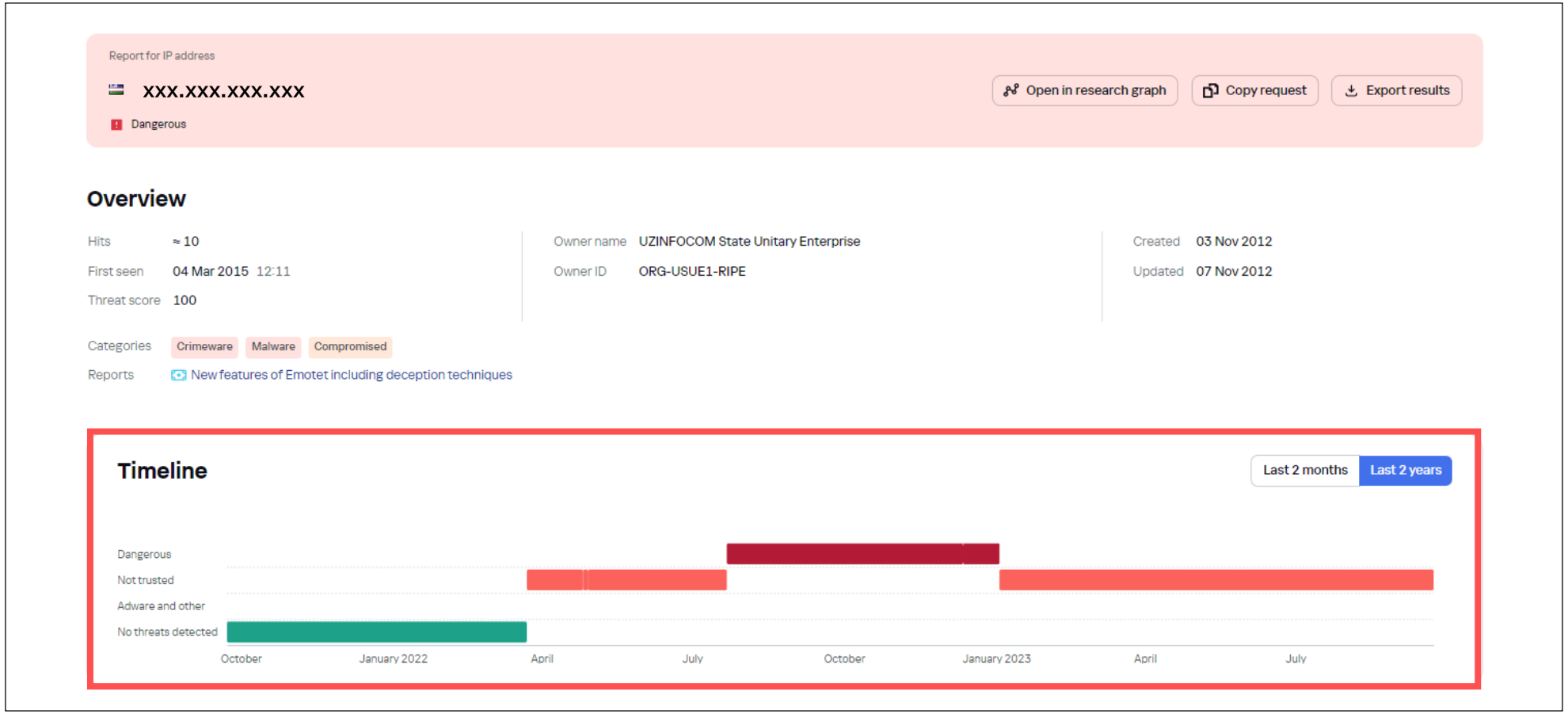


kaspersky

New タイムラインの追加

Kaspersky Threat Lookup

・検索結果：「脅威カテゴリ」にタイムラインを追加（IPアドレス/Webアドレス/ドメイン検索結果のみ）
検索対象に対する判定結果の遷移を可視化し、インジケーターがどのように攻撃に利用されてきたかを把握



kaspersky

Threat Lookup：活用方法例

Kaspersky Threat Lookup

詳細情報を基に効果の高いインシデント調査を実施

① アンチマルウェア製品が検知したURLを検索

-「DNS情報」に表示された悪意あるIPアドレスとの通信が発生していないか？

-「ドメインからダウンロードされるオブジェクト」に表示されたファイルがダウンロードされていないか？（感染の有無の確認）

-「リダイレクト元」「リダイレクト先」のURLからリダイレクトされた端末や感染経路、感染原因を確認

② 端末と通信する不審なIPアドレスを検索

-「関連するオブジェクト」に表示されたURLにアクセスしていないか？

URLからダウンロードされる可能性がある悪意あるファイルが対象の端末にダウンロードされていないか？

→ハッシュ値をクリックして悪意あるオブジェクトの詳細から潜伏先のファイルパスを確認

ダウンロードされていた場合、オブジェクトが行う通信やダウンロードを試みるオブジェクト情報を確認

-「スパム情報」の詳細からスパム攻撃の可能性や狙われるデータのタイプを確認

③ 端末にダウンロードされた不審なオブジェクトを検索

-「オブジェクトが実行したオブジェクト」などの関連するマルウェア情報を確認し、感染の有無や攻撃がどこまで進行しているか確認

-その他端末が「オブジェクトのダウンロード元」に表示されたURLにアクセスしていないか？

kaspersky

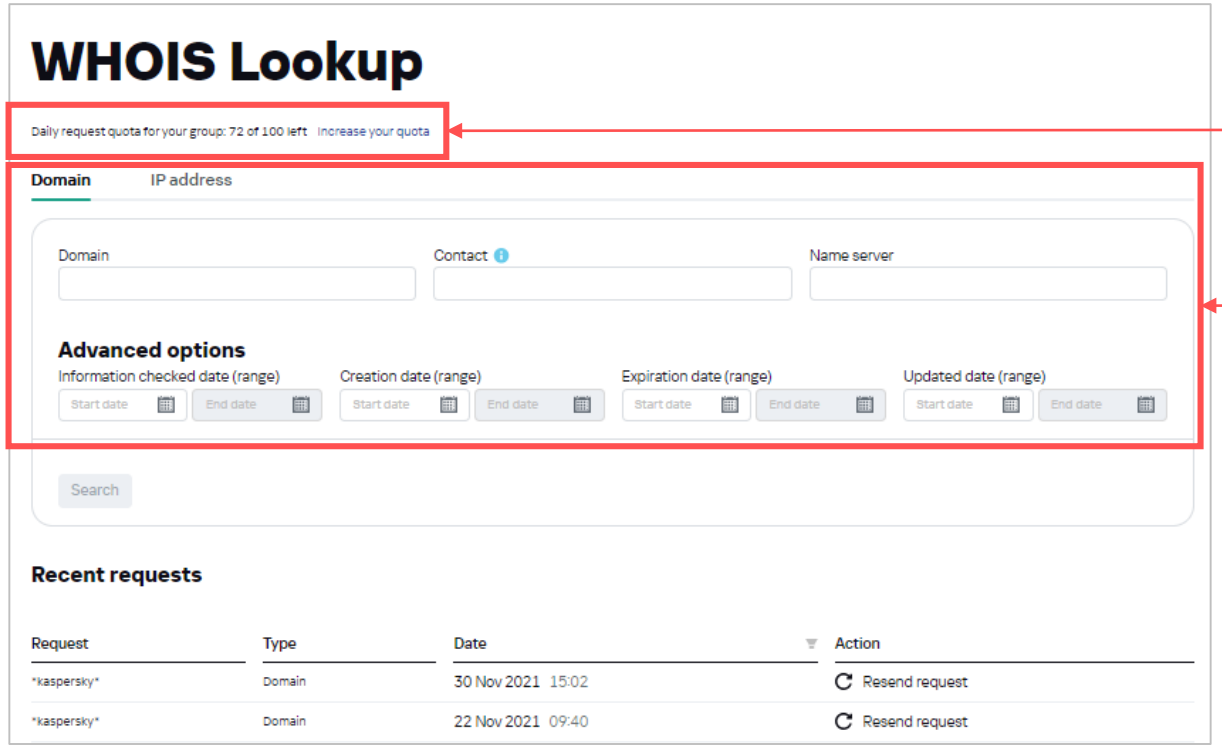
WHOIS Lookup：使用方法

Kaspersky Threat Lookup

WHOISの検索だけでなく、ワイルドカードを使用したドメインのあいまい検索が可能

「特定のキーワードに関連する脅威情報の検索」を目的とするサービスのThreat Lookup では、 明確な情報をキーに検索する必要がありますが、WHOIS LookupではWHOIS情報とワイルドカードを組み合わせた文字列をキーにあいまい検索が可能

→お客様に成りすますフィッシングサイトや把握出来ていないドメイン情報等の検索が可能



1日あたりの残り検索回数が表示

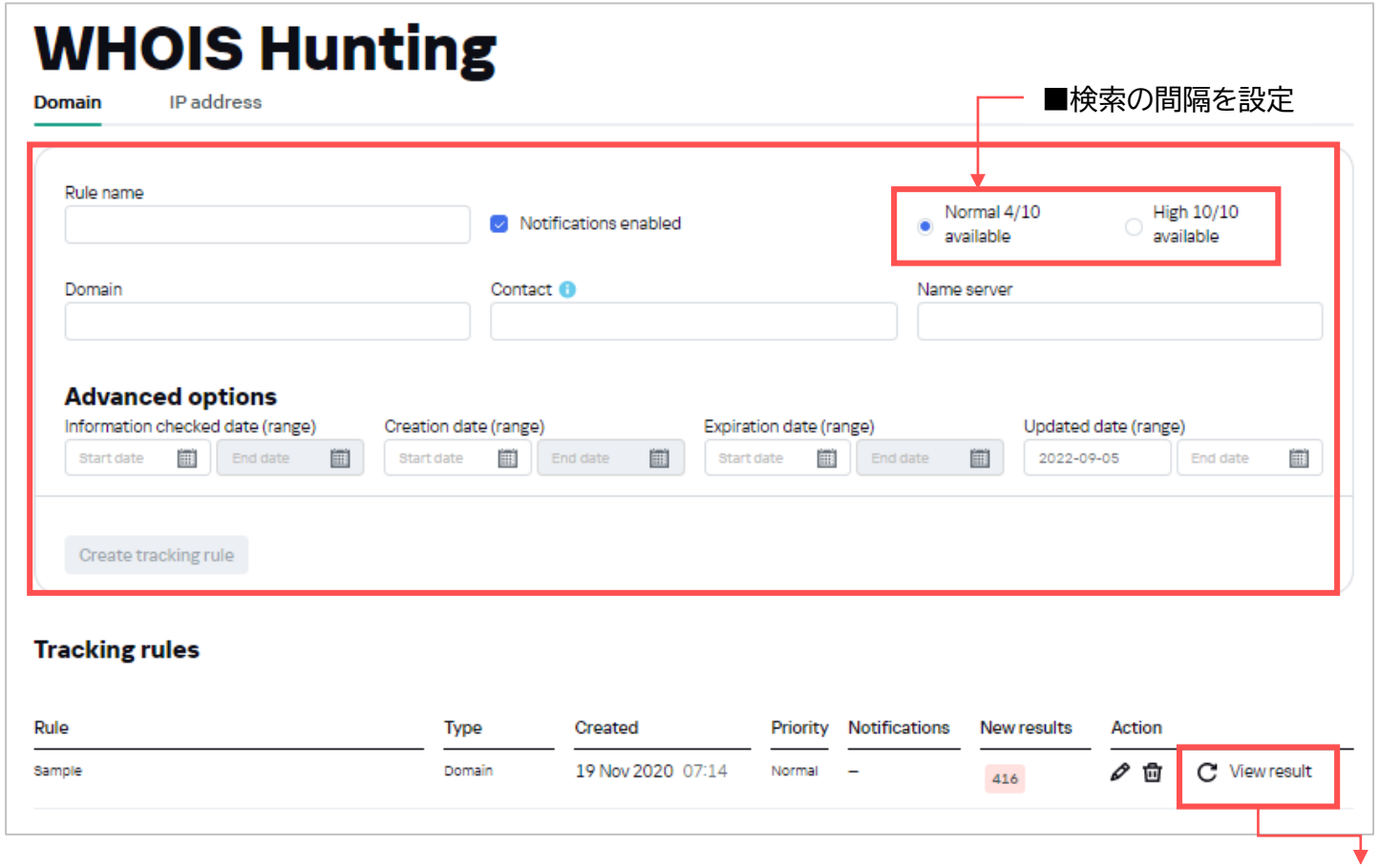
WHOIS情報を入力し対象を検索

kaspersky

WHOIS Hunting：使用方法

Kaspersky Threat Lookup

トラッキングしたいWHOIS情報を基に「トラッキングルール」を作成することで、ルールに合致するドメイン情報を収集

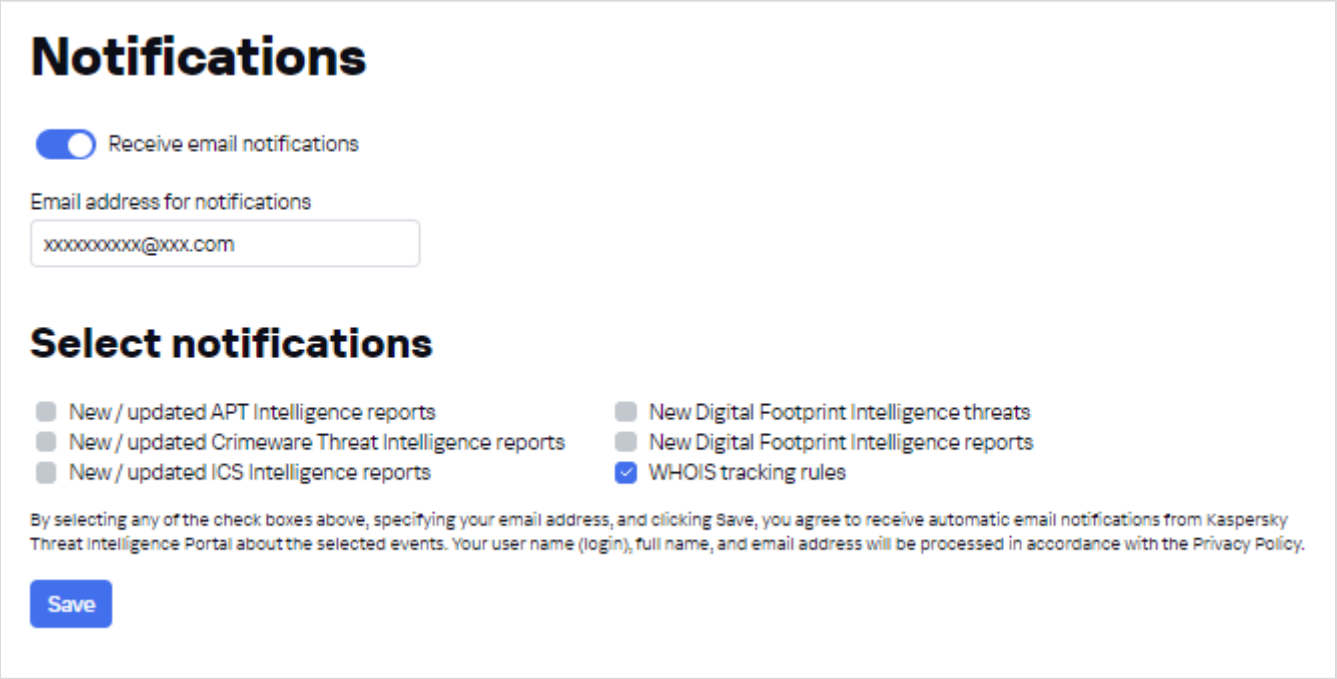


kaspersky

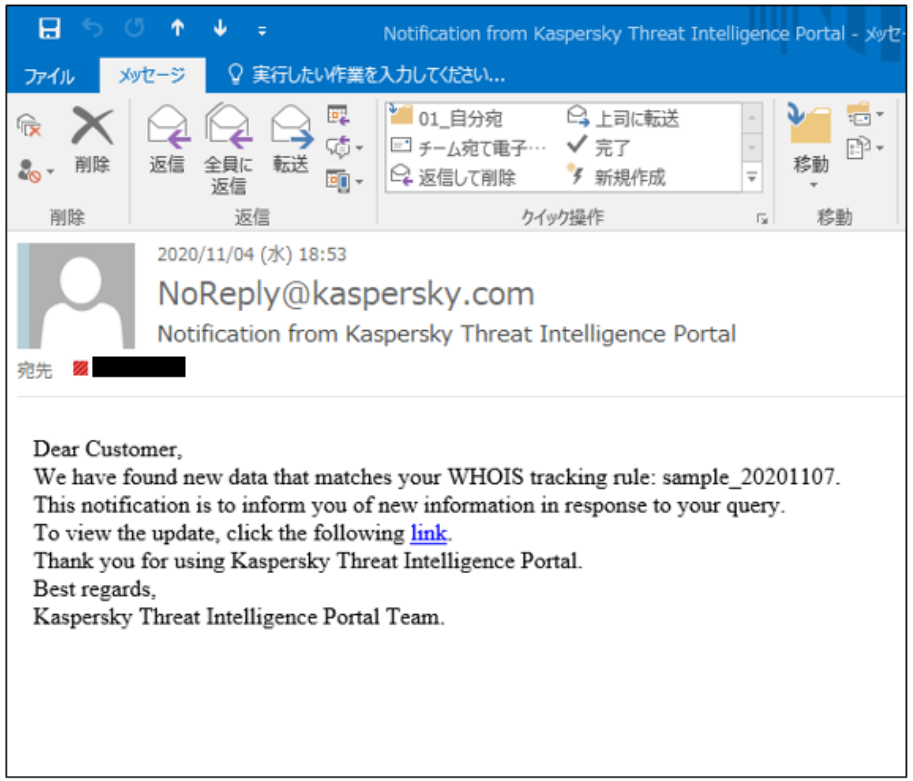
WHOIS Hunting：アラート通知

Kaspersky Threat Lookup

通知設定を有効にすることでトラッキングルールと一致する新規データが追加されたタイミングで通知メールを送付



<通知メール>



kaspersky

Dark Web Search / Surface Web Search

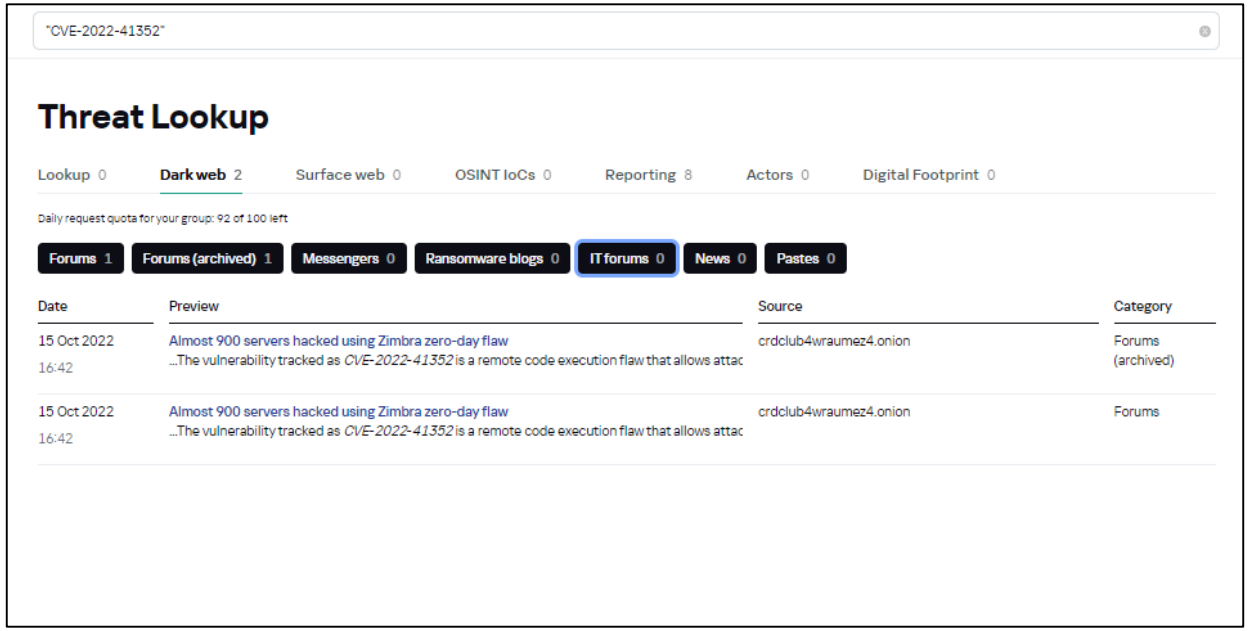
Kaspersky
Digital Footprint
Intelligence

Dark Web Search:

カスペルスキーのエキスパートが発見したダークwebやディープweb上でやり取りされるサイバー攻撃の計画や攻撃経路になり得る脆弱性に関するディスカッション、漏洩した認証情報やクレジットカード情報、個人情報などを提供するサービス

Surface Web Search:

カスペルスキーのエキスパートが選定した信頼できるセキュリティ関連の公開情報を提供するサービス



kaspersky

Dark Web Search / Surface Web Search：活用方法例

Kaspersky
Digital Footprint
Intelligence

① Dark Web Searchで特定企業名やブランド名、脆弱性をキーワードに検索

例：Kaspersky、CVE-2022-xxxx

-検索した企業に関する情報漏洩やバグハント依頼の確認

-該当の脆弱性が存在する企業の情報や悪用するツールの売買などの不正なやり取りの確認

② Surface Web Searchで脆弱性、マルウェア、サイバー攻撃に関連するキーワードを検索

例：（Log4j）、CVE-2022-xxxx、CryWiper

-世界で流行が確認されたマルウェアや脆弱性（CVE）を検索することで、カスペルスキーのエキスパートが選定したキーワードに関する記事を表示

kaspersky

kaspersky