

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

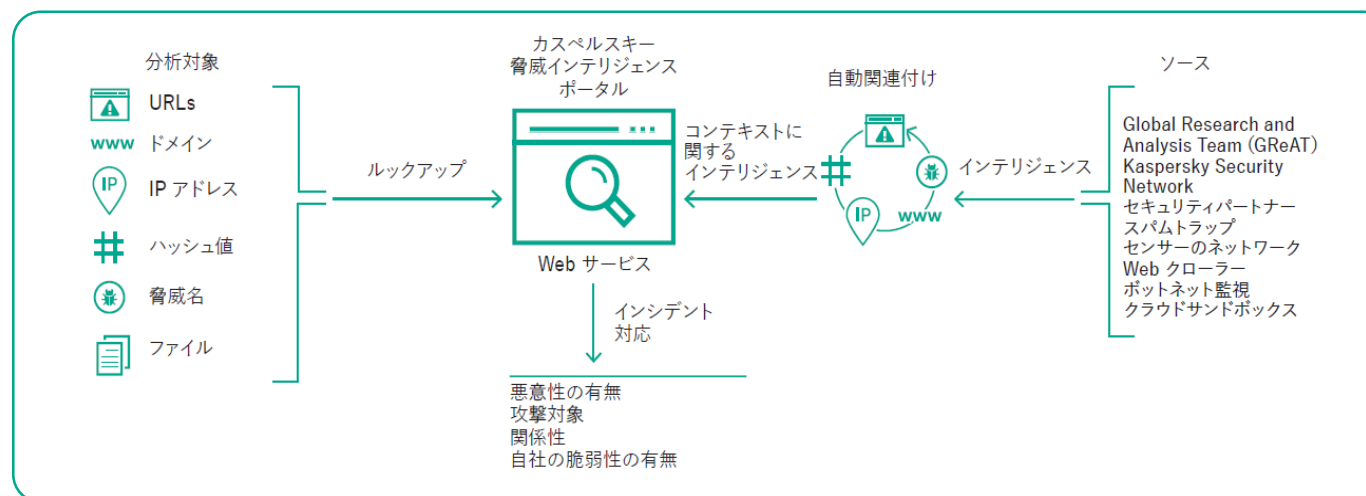
Kaspersky Threat Lookup: サービス概要



- ・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 Threat Lookup とは

- ・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」

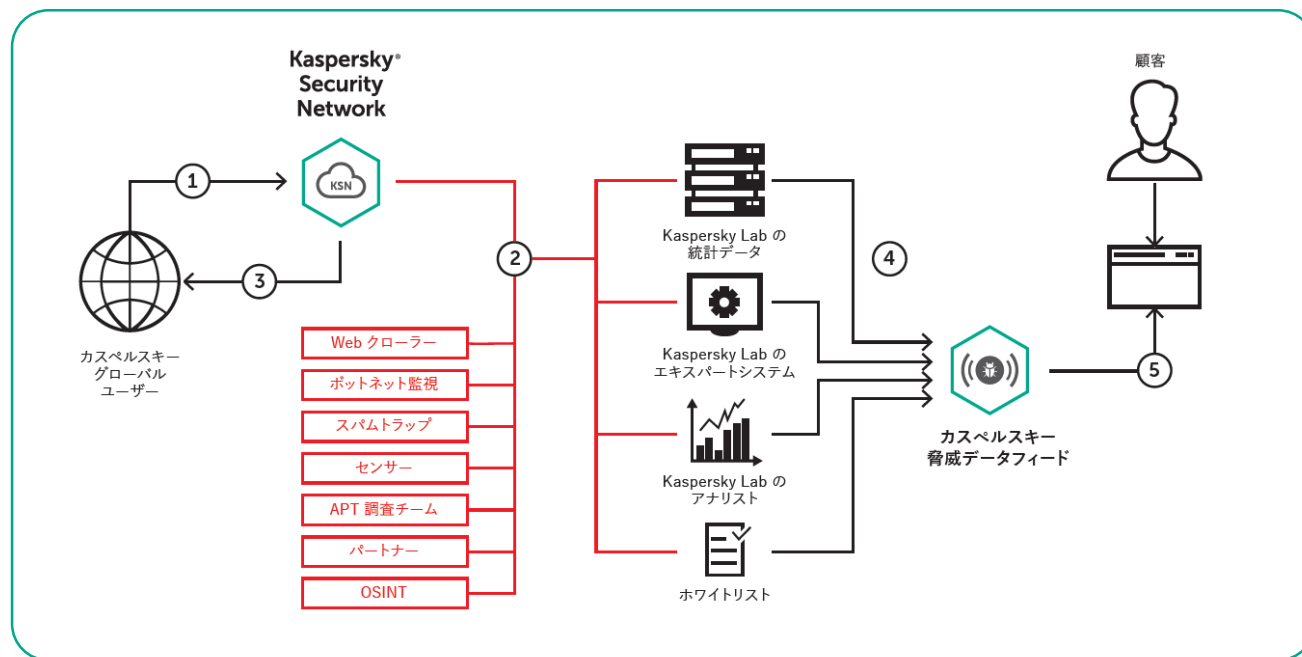




脅威インテリジェンスのソース

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





Threat Lookup:使用方法

- ・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

The screenshot displays the Kaspersky Threat Intelligence Portal interface. At the top, there is a search bar labeled "Search...". Below it, the "Recent requests" section shows a table of search results. The table has four columns: Status, Date, Type, and Request. The Status column contains various threat levels like "Adware and other", "Dangerous", "Not categorized", and "Good". The Date column shows timestamps from 30 Aug 2022 to 6 Sep 2022. The Type column lists the search criteria used, such as "Domain", "Hash", "URL", "IP", and "Search". The Request column shows redacted search queries. Red boxes highlight the Status and Type columns, with arrows pointing to them from Japanese labels: "検索結果を表示" (Show search results) and "検索対象のタイプを表示" (Show search target type). Another arrow points from the search bar to the table with the label "ハッシュ値、IPアドレス、ドメイン、URLを入力し対象を検索" (Enter hash value, IP address, domain, URL to search for target).

Status	Date	Type	Request
Adware and other	6 Sep 2022 10:47	Domain	[Redacted]
Adware and other	6 Sep 2022 10:47	Domain	[Redacted]
Dangerous	6 Sep 2022 10:46	Domain	[Redacted]
Not categorized	6 Sep 2022 10:21	Hash	[Redacted]
Good	6 Sep 2022 10:21	URL	[Redacted]
Not categorized	6 Sep 2022 10:20	IP	[Redacted]
Good	6 Sep 2022 10:20	Domain	[Redacted]
Not categorized	30 Aug 2022 16:18	Search	[Redacted]

検索結果:URL

Report for domain
staticset.com

判定
Dangerous

Open in research graph Copy request Export results

Overview

IPv4 count 40
File count ≈ 100
URL count ≈ 10
Hits ≈ 10,000

Created 3 Oct 2017
Expires 3 Oct 2022
Domain staticset.com

Registration organization
Privacy service provided by Withheld for Privacy ehf
Name NAMECHEAP INC

Geography

検知の多い地域

Anti-Virus Statistics

検知の時間推移

WHOIS

Domain name staticset.com
Domain status clientTransferProhibited
Created 3 Oct 2017
Updated 3 Aug 2020
Paid until 3 Oct 2022

Registrar info NAMECHEAP INC
IANA ID 1068
Email abuse@namecheap.com
Registrar servers dns2.registrar-servers.com

Contacts
Name Redacted for Privacy
Organization Privacy service provided by Withheld for Privacy ehf
Address IS, Capital Region
Phone/Fax
Email

DNS resolutions for domain

Status Threat score Hits (-) IP First resolved Last resolved Peak date Daily peak

Not trusted 68 100 168.100.9.112 29 Jul 2022 05:37 6 Sep 2022 10 Aug 2022 10

Not categorized 44 10 1.1.1.1 26 Sep 2018 26 Sep 2018 26 Sep 2018 10

Not categorized 38 1,000 164.92.221.133 2 Jan 2022 12:19 28 Jul 2022 28 Feb 2022 10

Not categorized - 1,000,000 146.185.175.64 8 Oct 2017 19:19 28 Nov 2018 28 Aug 2018 10,000

Files downloaded from requested domain

Status Hits (-) File MD5 First seen Last seen URL Detection name

Malware 10 208F0E29ED8A609959040A046DE33BD 19 Nov 2019 22:41 19 Nov 2019 22:41 HEUR:Trojan.Script.Generic

Malware 10 72613693FB315041E04D651101D24 24 Nov 2019 23:44 24 Nov 2019 23:44 HEUR:Trojan.Script.Generic

Malware 10 4819710AA5C1D85FBE99561CADC0FEE 10 Mar 2019 22:46 13 Mar 2019 15:26 HEUR:Trojan.Script.Generic

ドメインにアクセスする
オブジェクト(マルウェア)

サブドメインの状況

リダイレクト元

リダイレクト先

DataFeed登録情報

類似ドメイン

スパム情報



検索結果:ハッシュ値

Report for MD5 hash
de[redacted]ic16
Malware

判定

Open in research graph Copy request Export results

Overview

Hits ~ 1,000
Format exe X32
Size 399.00 KB (408576 B)
Signed by —
First seen 25 Jan 2022 01:03
SHA-1 3AA454C723B33B92B127DEAB275C982391571D9F
SHA-256 087B99AD356F2Z3D93D3ECC23C1FA2CD098C5CB0689DC4D668BC50879305FF0
Categories general

一般情報

Statistics

検知の多い地域

Detection Statistics
検知の時間推移

Detection names

25 Jan 2022 18:15 Backdoor.Win32.Blakken.sbs
25 Jan 2022 18:15 PDM:Trojan.Win32.Bazon.a
25 Jan 2022 18:15 PDM:Trojan.Win32.Generic
28 Aug 2022 14:24 HEUR:Trojan-PSW.MSIL.Agenla.gen
25 Jan 2022 18:15 PDM:Trojan.MSIL.Agent.sbs

検知オブジェクト名

File signatures and certificates

No data found

ファイルのシグネチャと証明書情報

Container signatures and certificates

No data found

コンテナシグネチャと証明書

File names

Download data

Hits (-) File Name
1,000 signed invoice.exe
10 quc17867.exe
10 signed invoice.r00

ファイル名

File paths

Download data

Hits (-) Path Location
10 content.outlook\q7bo5bco InternetCache
10 content.outlook\ay5k4pnr InternetCache
10 gfi\mailessentials\temp\arunpck ProgramFiles
10 gfi\mailessentials\emailsecurity\temp\trp00007906 ProgramFiles
10 gfi\mailessentials\emailsecurity\temp\trp00004e24 ProgramFiles
10 martau\total uninstall 7\backup ProgramData

ファイルパス(潜伏先)

File downloaded from URLs and domains

No data found

オブジェクトのダウンロード元

File downloaded the following objects

No data found

オブジェクトがダウンロードしたオブジェクト

File accessed the following URLs

Download data

Status URL Last accessed Domain IP count
Malware christophergallaghermusic.com/jy937nfopc8lh=5dvf0 25 Jan 2022 09:17 christophergallaghermusic.com
Malware christophergallaghermusic.com/jy937nfopc8lh=5dvf0 25 Jan 2022 09:17 christophergallaghermusic.com
Malware refer-to-online.com/jy937nfopc8lh=%2097kktb2\vd67v... 25 Jan 2022 09:17 refer-to-online.com
Malware lesbianparadise.com/jy937nfopc8lh=(mubj)myduelobkuud... 25 Jan 2022 09:17 lesbianparadise.com

オブジェクトがアクセスする先

File started the following objects

No data found

オブジェクトが実行したオブジェクト

File was started by the following objects

No data found

オブジェクトを実行したオブジェクト

File was downloaded by the following objects

No data found

オブジェクトをダウンロードしたオブジェクト

File was unpacked from the following objects

Download data

Status Parent MD5 Child MD5 Parent size Parent type Parent detection name Level
Malware 7D44... 7D44... 382,922 B rar HEUR:Trojan-PSW.MSIL.Agenla.gen 0
Malware 886687... 886687... 382,922 B rar HEUR:Trojan-PSW.MSIL.Agenla.gen 0
Malware 32E53BF8D8FAD7A23707B6F6358A772... DE5211E24C66A4A8E88D96A7A64AD0... 382,922 B rar HEUR:Trojan-PSW.MSIL.Agenla.gen 0

オブジェクトを解凍したオブジェクト

File contains the following objects

No data found

オブジェクトが含まれるオブジェクト


New


新たな脅威カテゴリの追加

- ・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

Daily request quota for your group: 97 of 100 left

Report for IP address

 XXX.XXX.XXX.XXX

 Dangerous

[Open in research graph](#) [Copy request](#) [Export results](#)

Overview

Hits	≈ 10	Owner name	—	Created	12 Nov 2009
First seen	23 Jul 2021 08:03	Owner ID	None	Updated	12 Nov 2009
Threat score	100				

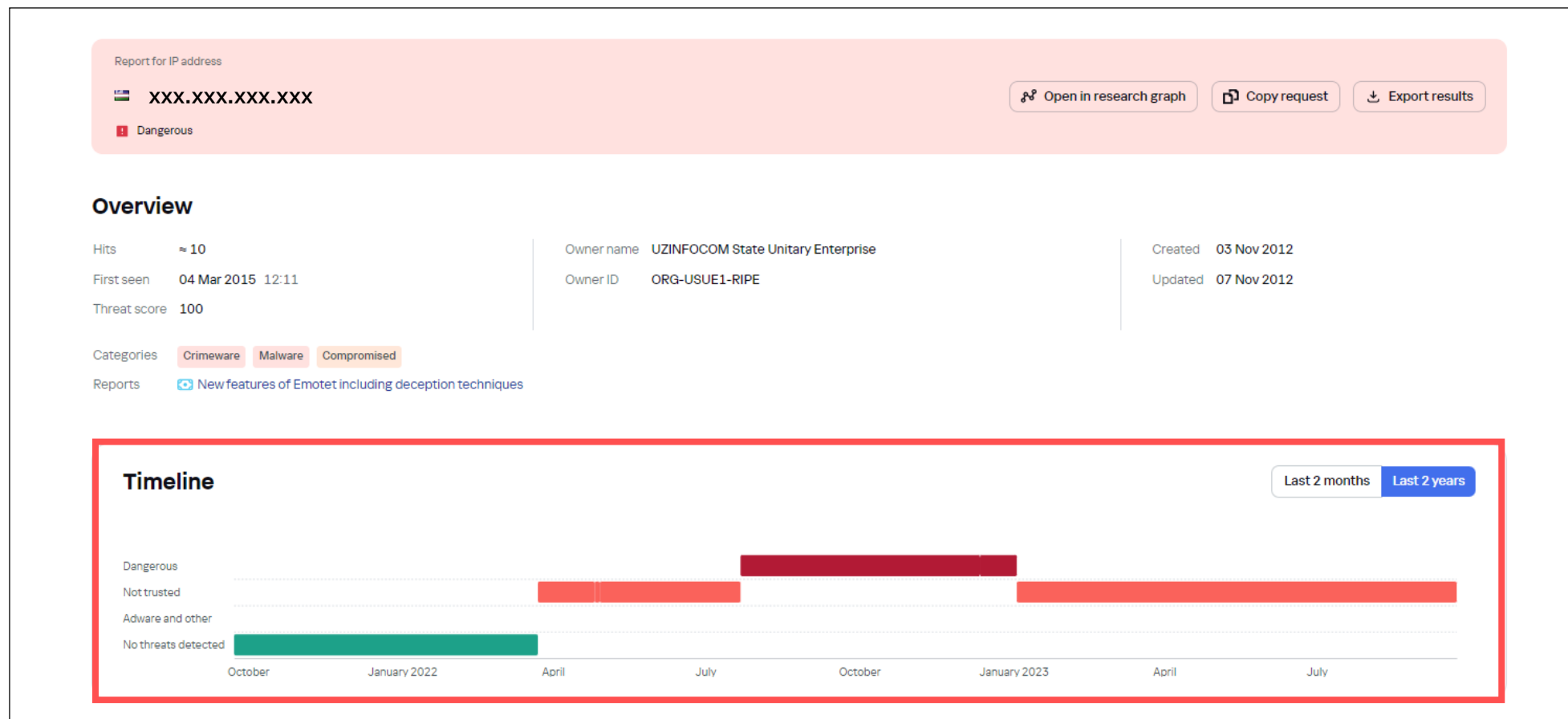
Categories

Botnet C&C Crimeware Malware

New

タイムラインの追加

- ・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





Threat Lookup:活用方法例

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？



WHOIS Lookup:使用方法

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

Request	Type	Date	Action
kaspersky	Domain	30 Nov 2021 15:02	Resend request
kaspersky	Domain	22 Nov 2021 09:40	Resend request

WHOIS Lookup

Daily request quota for your group: 72 of 100 left Increase your quota

Domain IP address

Domain

Contact

Name server

Advanced options

Information checked date (range)

Start date



End date



Creation date (range)

Start date



End date



Expiration date (range)

Start date



End date



Updated date (range)

Start date



End date



Search

Recent requests

Request	Type	Date	Action
kaspersky	Domain	30 Nov 2021 15:02	Resend request
kaspersky	Domain	22 Nov 2021 09:40	Resend request

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



WHOIS Hunting:使用方法

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

The screenshot displays the 'WHOIS Hunting' web interface. At the top, there are tabs for 'Domain' and 'IP address'. Below this, a form for creating a tracking rule is shown. A red box highlights the 'Normal 4/10 available' radio button, with an arrow pointing to it from the text '■検索の間隔を設定' (Set search interval). The form includes fields for 'Rule name', 'Domain', 'Contact', and 'Name server', along with a 'Notifications enabled' checkbox. Under 'Advanced options', there are date range selectors for 'Information checked date', 'Creation date', 'Expiration date', and 'Updated date'. A 'Create tracking rule' button is at the bottom of the form. Below the form, a 'Tracking rules' table lists existing rules. A red box highlights the 'View result' button for the 'Sample' rule, with an arrow pointing to it from the text '■設定したトラッキングの結果を表示' (Display tracking results for the configured rule).

Rule	Type	Created	Priority	Notifications	New results	Action
Sample	Domain	19 Nov 2020 07:14	Normal	-	416	View result

■設定したトラッキングの結果を表示

WHOIS Hunting:アラート通知

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

Notifications

☒ Receive email notifications

Email address for notifications

xxxxxxxxxx@xxx.com

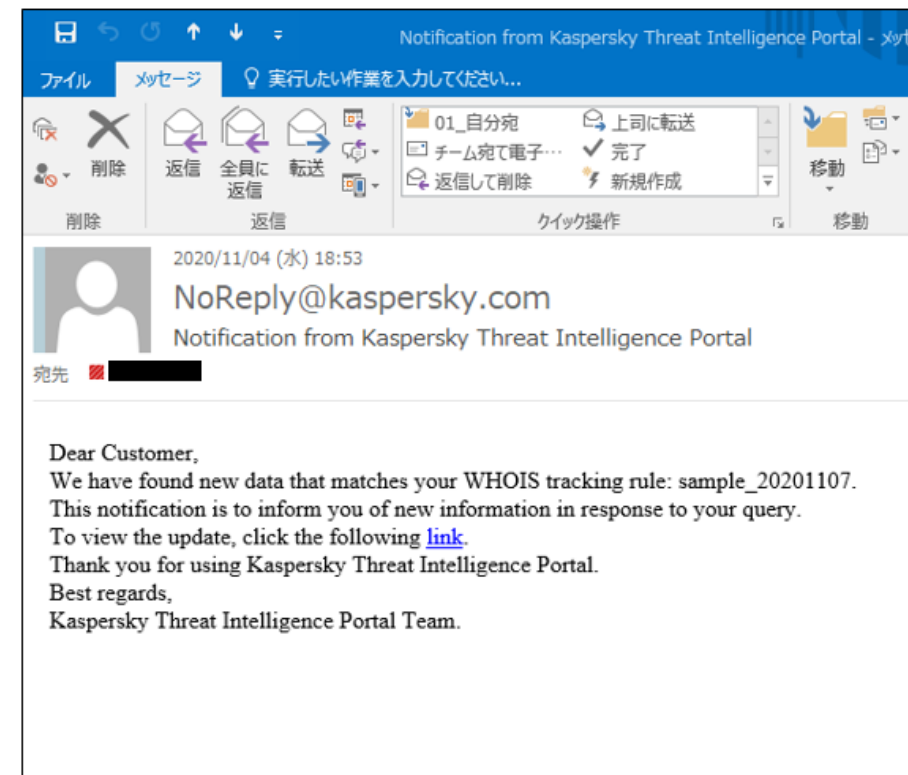
Select notifications

<input type="checkbox"/> New / updated APT Intelligence reports	<input type="checkbox"/> New Digital Footprint Intelligence threats
<input type="checkbox"/> New / updated Crimeware Threat Intelligence reports	<input type="checkbox"/> New Digital Footprint Intelligence reports
<input type="checkbox"/> New / updated ICS Intelligence reports	<input checked="" type="checkbox"/> WHOIS tracking rules

By selecting any of the check boxes above, specifying your email address, and clicking Save, you agree to receive automatic email notifications from Kaspersky Threat Intelligence Portal about the selected events. Your user name (login), full name, and email address will be processed in accordance with the Privacy Policy.

Save

<通知メール>



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

CVE-2022-41352

Threat Lookup

Lookup 0Dark web 2Surface web 0OSINT IoCs 0Reporting 8Actors 0Digital Footprint 0

Daily request quota for your group: 92 of 100 left

Forums 1Forums (archived) 1Messengers 0Ransomware blogs 0IT forums 0News 0Pastes 0

Date	Preview	Source	Category
15 Oct 2022 16:42	Almost 900 servers hacked using Zimbra zero-day flaw ...The vulnerability tracked as CVE-2022-41352 is a remote code execution flaw that allows attac	crdclub4wraumez4.onion	Forums (archived)
15 Oct 2022 16:42	Almost 900 servers hacked using Zimbra zero-day flaw ...The vulnerability tracked as CVE-2022-41352 is a remote code execution flaw that allows attac	crdclub4wraumez4.onion	Forums



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

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

The image features the Kaspersky logo in white lowercase letters, centered within a teal hexagonal shape. The background is a gradient of teal and green, with a bright green area on the left side.

kaspersky