kaspersky

カスペルスキーの脅威インテリジェンスサービスのご紹介

2025年07月09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

V1.2

Kaspersky Threat Intelligene Portal とは？

kaspersky

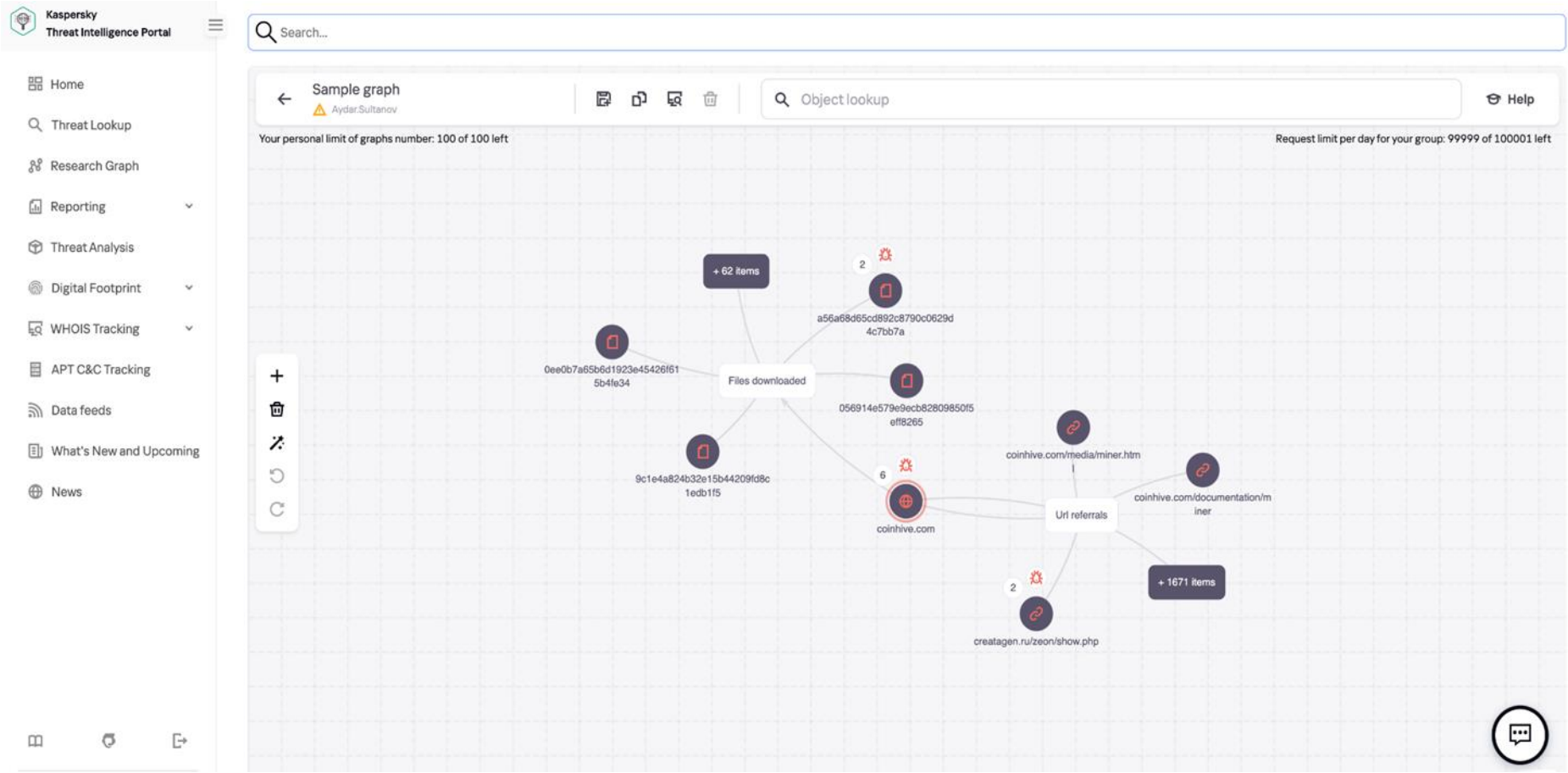
カスペルスキーが提供する各種脅威インテリジェンスサービスを単一のインターフェースから利用可能なクラウドサービス

Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ Research Graph

kaspersky

・ファイル、IPアドレス、URL、ドメイン、ハッシュ、攻撃者グループなど複数の脅威要素の関係性をグラフィカルに可視化
複雑な脅威の構造を直観的に把握

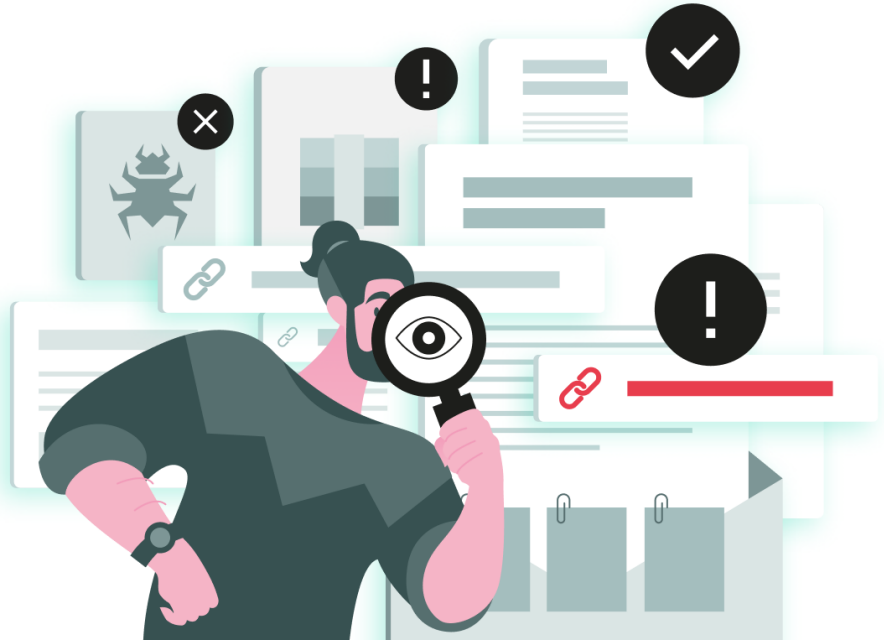


Copyright © 2025 Kaspersky Lab. All rights reserved.

機能紹介 ｜ Threat Landscape

kaspersky

・弊社の脅威インテリジェンスサービスとMITRE ATT&CKフレームワークを連携させ、業界・地域別に
脅威や攻撃者の情報を提供する対話型ツール
ダッシュボードを通じて、TTPデータを分析でき、インテリジェンスレポートやIOC、Suricata/Sigmaルールセットも
参照可能。リアルタイムデータに基づき脅威スコアが動的に更新され、フィルタ機能によりカスタマイズも容易、
フィルタセットの保存・管理機能で効率的な分析が可能

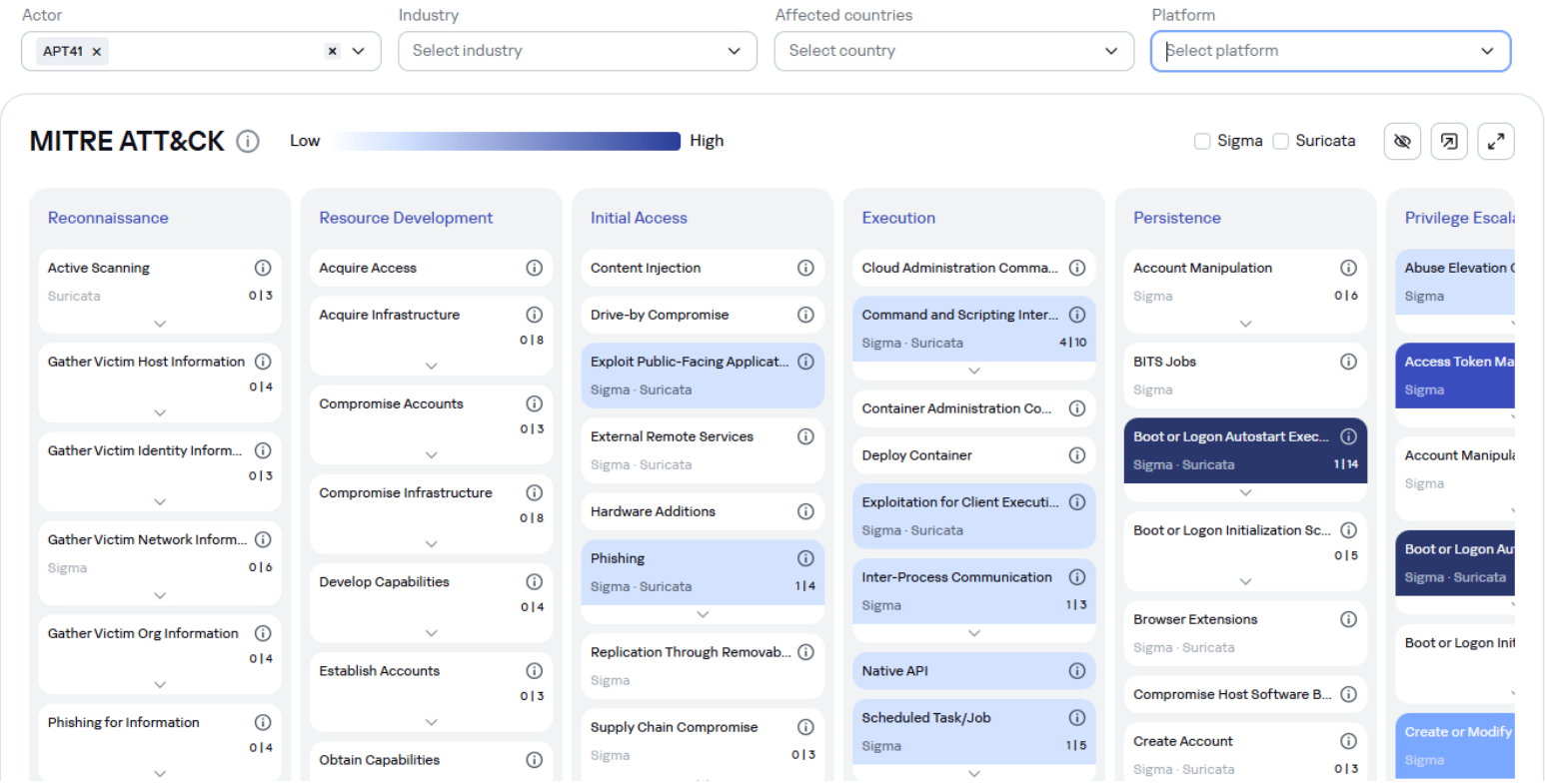


Copyright © 2025 Kaspersky Lab. All rights reserved.

Threat Landscape:ダッシュボード

kaspersky

・設定した脅威アクター名、業界、影響を受ける国、プラットフォームに関連する攻撃者の戦術・手法を一覧表示
自社に関連する攻撃を分析し、効果的な対処・防御の実現に必要な情報を提供



Copyright © 2025 Kaspersky Lab. All rights reserved.

Threat Landscape:TTPs

kaspersky

・MITRE ATT＆CKの戦術、テクニック、サブテクニックに関する詳細なデータ、一般的な攻撃手順の例の参照可能

Search by TTPs

- Reconnaissance
- Resource Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

TTPs

ID	Name	Adversary action
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Copyright © 2025 Kaspersky Lab. All rights reserved.

Threat Landscape:脅威アクター

kaspersky

・脅威アクターの概要（過去の活動・攻撃事例など）活動地域、TTPs、関連する外部記事リンクなどを参照可能
弊社レポーティングサービスご利用ユーザーは関連するレポートも閲覧可能

Actors

Search actors

ID	Name	Description	Aliases
A0176	3AM	3AM (aka ThreeAM) is a threat actor that was first discovered in August 2023 and primari...	threeam
A0098	8Base	8Base is a ransomware group that has been active since March 2022. In May - July 2023 ...	–
A0107	Agenda	Agenda or, as they call themselves, Qilin, is a ransomware group that attacks companies ...	qilin
A0159	Akira	Akira is a ransomware group discovered in March 2023 after they attacked several comp...	–
A0062	Andariel	The Andariel APT group is considered a subgroup of Lazarus APT, initially described by th...	silent ch...
A0293	Angry Likho	Angry Likho (also known as Sticky Werewolf), is an APT actor which we have been monito...	phaseshif...
A0052	Animal Farm	Animal Farm is the name given to a set of malware developed and deployed by the Gene...	atk 8 sig
A0005	APT1	APT1, also known as Comment Crew, is a cybercriminal group engaged in cyber espionag...	brownfox
A0002	APT10	APT10 is a Chinese-speaking sophisticated and persistent cyber espionage actor active ...	atk 41 br
A0068	APT3	APT 3 is also known as Gothic Panda, Pirpi, UPS Team, Buckeye, Threat Group-0110, TG-...	boron bo

APT41 APT

ID:	A0037
CVEs:	CVE-2015-1641 CVE-2017-0199 CVE-2019-0708 +10
Software:	Empire China Chopper +13
Created	Nov 22 2021
Updated	Mar 19 2025

Aliases

amoeba | axiom hacking group | barium | blackfly | brass typhoon | bronze atlas | bronze export | +11

Industries

Defense | Energy | Entertainment | Financial services | Government | Manufacturing | Technology | +1

Affected countries

NA

Afghanistan | Australia | Austria | Bangladesh | Brazil | Cambodia | China | +34

Copyright © 2025 Kaspersky Lab. All rights reserved.

Threat Landscape:ソフトウェア

kaspersky

攻撃に使用される各種ツールの情報を参照可能、攻撃シナリオ分析時のツールの特定を支援

例：ランサムウェア、RAT、OSのユーティリティツール、オープンソースソフトウェアなど

ID	Name	Aliases	Platforms affected
S0071	Qakbot	Qbot, Pinkslipbot, +1	Windows
S0072	WarzoneRAT	AveMaria, AveMariaRAT, +3	Windows
S0092	Dridex	–	Windows
S0094	WebBrowserPassView	–	Windows
S0141	Gh0st RAT	Ghost RAT, Gh0stRAT, +2	Windows
S0149	BeEF	–	Linux, macOS, +1
S0150	Maze Ransomware	ChaCha ra..., Sekhmet, +1	Windows
S0173	BITSAdmin	Backgroun...	Windows
S0182	PuTTY	PSCP, PSFTP, +1	macOS, Linux, +1
S0183	RomCom RAT	SingleCam..., SnipBot, +2	Windows

Copyright © 2025 Kaspersky Lab. All rights reserved.

Threat Landscape: 緩和策

kaspersky

セキュリティリスク低減に有益な取り組みを参照可能

Mitigations

Search by name or ID

ID	Name	Updated
M0004	Vulnerability Scanning	Dec 18 2024 12:54
M0005	User Account Control	Dec 18 2024 12:54
M0006	Update Software	Dec 18 2024 13:12
M0007	Active Directory Configuration	Dec 18 2024 13:14
M0008	Data Backup	Dec 18 2024 13:18
M0009	Privileged Account Management	Dec 20 2024 11:45
M0010	Execution Prevention	Dec 18 2024 14:28

Copyright © 2025 Kaspersky Lab. All rights reserved.

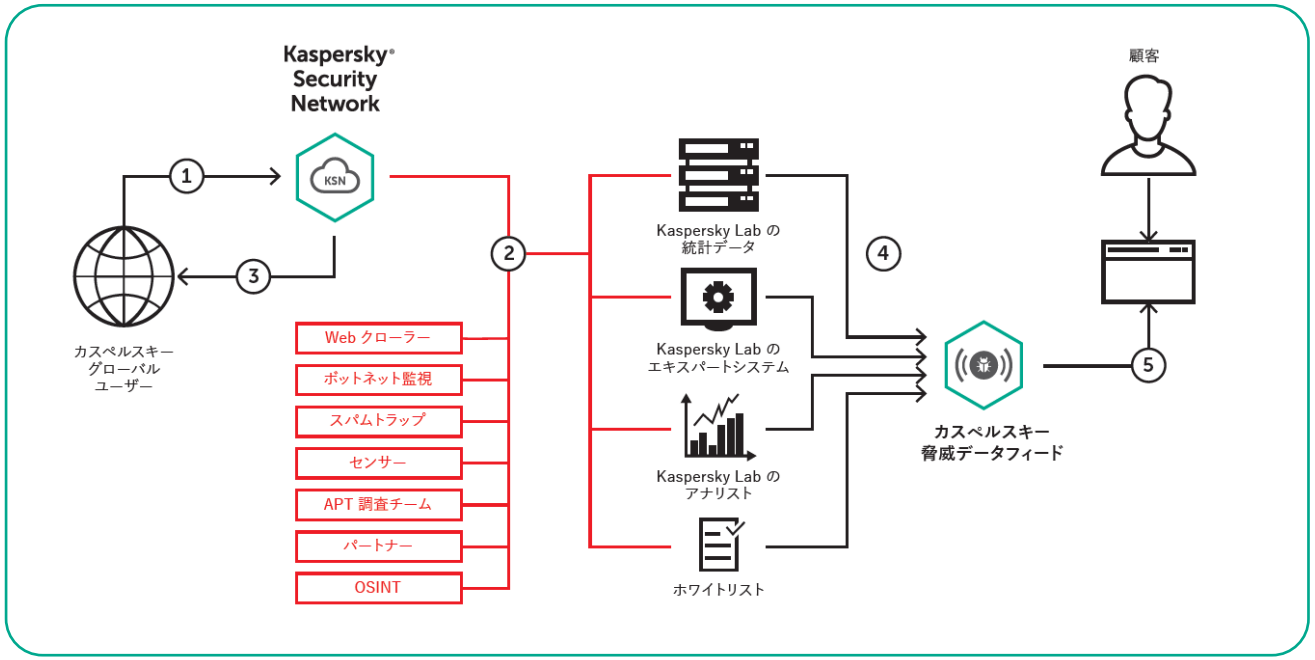
脅威インテリジェンスのソース

kaspersky

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



Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Digital Footprint Intelligence

Copyright © 2025 Kaspersky Lab. All rights reserved.

Digital Footprint Intelligence とは

kaspersky

・カスペルスキーのエキスパートがお客様リソースを調査・分析し、攻撃対象領域に存在する脆弱性・設定ミスなどの「弱点」や、サイバー空間で発見した個人情報の漏えい・お客様に対する攻撃計画などの潜在的なセキュリティリスクをアラートで報告する包括的な脅威モニタリングサービス

ネットワーク境界の調査

- 外部から悪用可能なサービス
- サービスのフィンガープリント
- 存在する脆弱性
- エクスプロイト分析
- リスク分析とリスクレベル

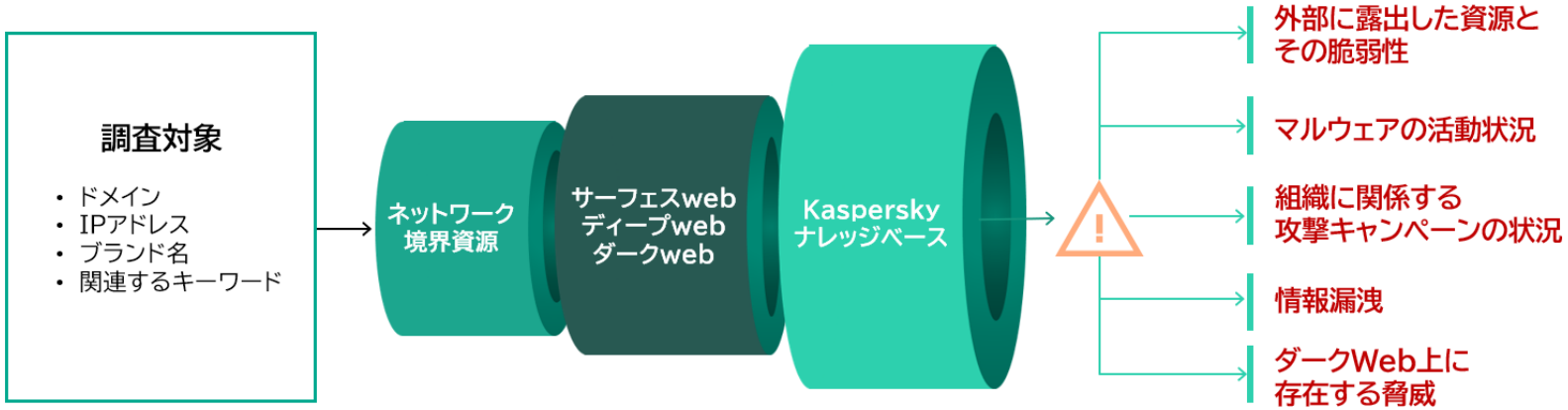
サイバー空間調査

✓ サーフェスweb
✓ ディープweb
✓ ダークweb

- サイバー犯罪者の活動
- 漏洩したデータと認証情報
- 悪意あるインサイダー
- 関係者のソーシャルメディア活動
- メタデータからの漏洩

Kaspersky エキスパートによる分析

- マルウェアコレクション
- ボットネットとフィッシングの追跡
- APTリサーチデータ
- シンクホールとマルウェアホスト
- 脅威インテリジェンスデータベース



Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky APT Intelligence Reporting

Copyright © 2025 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting とは

kaspersky

- グローバル調査分析チーム「GReAT」が現在調査中の最先端の脅威に関するレポート
  - ✓ 一般には公開されない攻撃事案に対するレポート
  - ✓ 調査の進捗、攻撃者グループの戦術や技術の変化に応じたレポートのアップデートとメールによるアラート
  - ✓ 地域毎・業種毎・攻撃者グループ毎の検索タグと全文検索

- 経営層や管理職からセキュリティ専門技術者までを対象とした読みやすく実戦的なレポート内容
  - ✓ 攻撃の概要（Executive Summary）
  - ✓ 技術的詳細（Technical Details）
  - ✓ 攻撃の戦術、技術および手法（TTPs）とMITRE ATT&CKマッピング
  - ✓ 攻撃者の属性情報（Attribution）

- 脅威ハンティングに使用できる機械読取可能なIoCを提供（openIOC、YARA）

- 脅威アクター（攻撃者グループ）のプロファイル情報

Copyright © 2025 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting：レポートサンプル

kaspersky

■Executive Summary：C-レベル（意思決定者）向けレポート

経営層・リーダーがセキュリティに関する適切な意思決定・投資判断のインプットとして活用できるよう、
攻撃の概要を要約したレポートを提供

TLP: AMBER

kaspersky

BlueNoroff employs new tools in recent activity

Report Id: 20190802
Version: 1.0 (5.August.2019)

Executive Summary

We recently tracked new BlueNoroff activity following the previously reported[12] campaigns. In particular, we found an bank in Myanmar compromised by this actor. We promptly contacted them, sharing the IOCs we had found.

This collaboration allowed us to learn valuable information on how they move laterally to access high valuable hosts, such as ones owned by the bank´s system engineers interacting with SWIFT. They used a public login credential dumper and homemade Powershell scripts for lateral movement.

BlueNoroff also starts to employ new malware with an uncommon structure, probably to slow down its analysis. Depending on the command line parameters, this malware can run as passive backdoor, active backdoor and tunneling tool. We assess that the actor runs this tool in different modes depending on the situation.

Moreover, we found another type of Powershell script used by this group when they attacked a victim in Turkey. This Powershell has similar functionalities with the ones previously used, but

This report in a nutshell:

- The actor utilized a Google Docs look-alike app, hosted on PaaS platforms for initial compromise;
- The open-source 'Ares RAT' was used as a payload in the attacks;
- The waves of attacks have been ongoing for more than a year, and most likely are originating from

Techniques, Tactics and Procedures specific for this campaign:

Infrastructure

Link shorteners; Cloud storage; VPS

Infection vector

Spear phishing emails with attachments; Spear phishing emails with urls redirecting to fake Google Docs apps

Implants

Copyright © 2025 Kaspersky Lab. All rights reserved.

APT Intelligence Reporting：レポートサンプル

kaspersky

■Full Report：SOC担当者、セキュリティ専門技術者向けレポート

攻撃の詳細（攻撃の背景、ペイロードをダウンロードさせるために攻撃者が使用する手法やツールなど）、
攻撃者のリソース、IoC、Yaraルールを提供

Technical Details

Initial Infection

The campaigns discussed in this report began with spear phishing emails. While many of the initial emails were not obtainable by us, using our statistical data and telemetry we were able to reconstruct what we believe is the entire infection chain. Moreover, the actor's heavy usage of public services such as URL shorteners allowed us to get a broad view of their operational activity. We divide this activity into two different campaigns based on how the initial access was obtained. The first campaign began in December 2017 and was completed around August 2018, while the second one began around October 2018 and still goes on.

Google Drive URL: https://drive[.]google[.]com/file/d/[redacted]

Google Drive URL: https://drive[.]google[.]com/file/d/[redacted]

Google Drive URL: https://drive[.]google[.]com/file/d/[redacted]
B0lad
Owner: [redacted]@gmail.com
Filename: Wedding Invitation.pdf
Created Time: 2018-01-08 06:58:34
Modified Time: 2018-01-0806:58:42
MD5: 3919a78[redacted]c44cb5ab

Data Exfiltration

The purpose of the attacks appears to be pure data theft. Sometimes after a successful compromise, the malware will receive the following set of commands:

- List current catalogue with `dir`
- Download "o.txt" from the C2 (i.e. - http://[redacted]/static/x/o.txt)
- Rename "o.txt" to "o.bat" and execute it

The code contained in o.txt[6] will then download the following additional files from Dropbox.

Original EXE Name	Name of Downloaded EXE	Hash
7za.exe[7]	tmp.exe	5E0CFB5F[redacted]C9B1
rclone.exe[8]	system.exe	59B363E5[redacted]6ED8
rclone.conf	rclone.conf	F68D250C[redacted]AF8E

Next, it will look for all files with the following file types on the victim's file system:

- Documents - files with extension .doc, .docx, .odt, .pdf
- Spreadsheets - files with extension .xls, .xls, .ots
- Presentations - files with extension .ppt, .ppsx, .pptx, .odp

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Crimeware Intelligence Reporting

Copyright © 2025 Kaspersky Lab. All rights reserved.

Crimeware Intelligence Reporting とは

kaspersky

- <u>さまざまなセクターを標的とする金銭目的のサイバー犯罪に関するレポート</u>
  - ✓ 対象：主に金融機関とその大口顧客、対応する政府機関、および M&A 取引に関与する企業
  - ✓ 特定のインフラストラクチャ（ATM や POS デバイスなど）に対する攻撃情報
  - ✓ 広範で危険なマルウェアキャンペーン
  - ✓ さまざまな地域のダークウェブマーケット上でサイバー犯罪者によって使用、開発、または販売されている特定のクライムウェアツールに関する情報

- <u>レポート、IoC、YARAに加え、Sigmaルールを提供</u>

  ※ Sigmaルールとは：
  ログファイルに対する汎用的なシグネチャフォーマットで、SIEMを使用した脅威を検知するためのルールを定義。
  SigmaをサポートするSplunk、Elastice Searchなどの製品、MISPなどのOSSなど各SIEMのクエリに変換可能なため、
  SIEMに依存することなくルールを適用可能。

- <u>脅威アクター（攻撃者グループ）のプロファイル情報</u>

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky ICS Threat Intelligence Reporting

Copyright © 2025 Kaspersky Lab. All rights reserved.

ICS Threat Intelligence Reporting とは

kaspersky

- 産業制御システム(ICS)に関連するサイバー脅威に関するレポート
  - ✓ 産業組織を標的とした新たなAPT、攻撃キャンペーンおよび活発な脅威に関する最新情報
  - ✓ SCADA、PLC、リモート管理ツールなどICS関連の脆弱性情報の提供
  - ✓ 脆弱性がどのように悪用されるのかといった内容や、リスク緩和のための推奨アクションも提供

- 直近1ヵ月に発生した産業組織をターゲットにした攻撃の概要をまとめたマンスリーレポート
  - ✓ 産業組織をターゲットにした攻撃のトレンド、流行する地域の把握に活用
  - ✓ 地域ごとの統計情報

    <レポートで提供する統計情報>

    -脅威の発生源(インターネット、Email、リムーバブルデバイスなど)

    -脅威タイプ(スクリプト、悪意のあるドキュメント、トロイの木馬など)

    -分野(製造業、オイル・ガス、電力・エネルギーなど)ごとの攻撃の被害状況の詳細

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Threat DataFeeds

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Threat Data Feeds とは

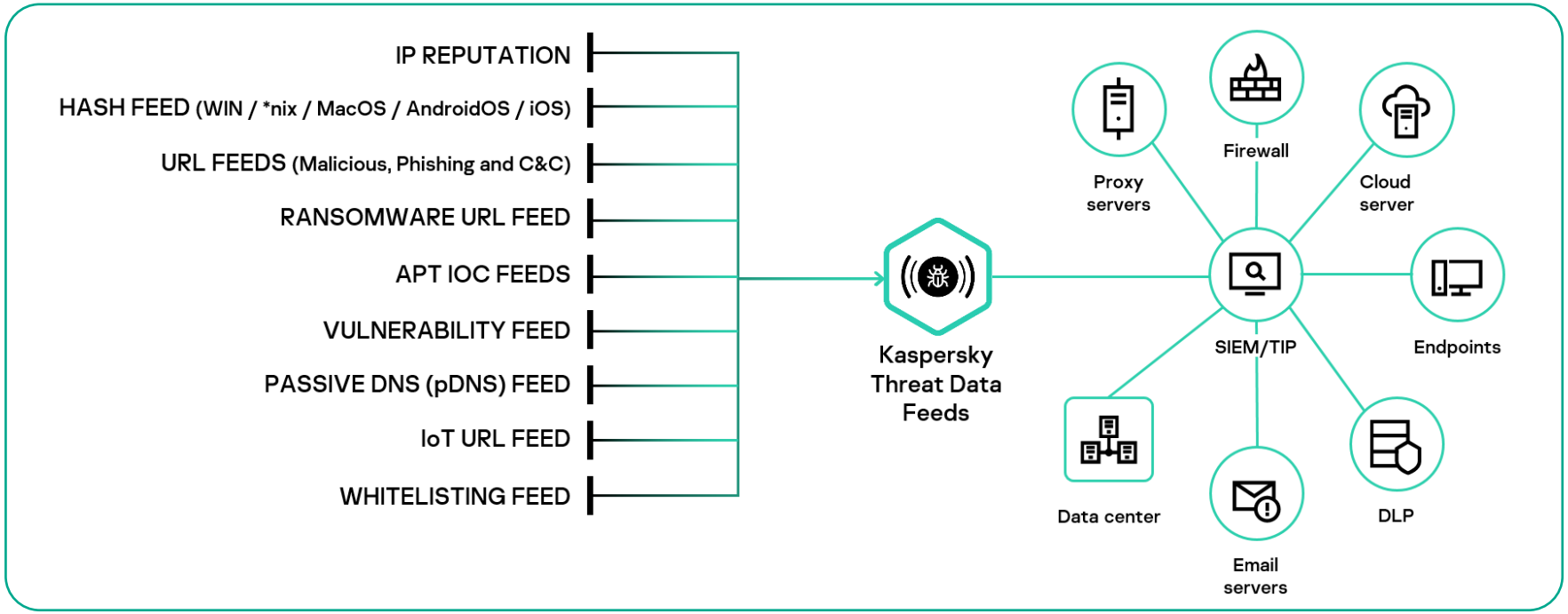
kaspersky

高品質なIoCとコンテキスト情報を提供

・脅威の早期検知や分析に必要なIoC（IPアドレス・URL・ドメイン・ハッシュ値）と実用的なコンテキスト情報をJSON形式で提供

・世界中で収集した情報を基にデータフィードをリアルタイムで自動生成、フィードリリース前に多角的なテストを実施することで誤検知を削減し、高い検知率と精度を実現

・SIEMやFW・プロキシと統合し、ログ解析や脅威の検知、リスク評価に活用することでお客様のインシデント対応能力を改善、強化



Copyright © 2025 Kaspersky Lab. All rights reserved.

脅威データフィード構成

kaspersky

様々な脅威情報に特化した脅威データフィード

脅威データフィード名	フィードに含まれる情報
Malicious URL Feed	悪意のあるリンクやウェブサイトを含むコンテキストを持つURLマスクのセット
Phishing URL feed	フィッシング・リンクやウェブサイトを含むコンテキストを持つURLマスクのセット
Botnet C&C URL Feed	デスクトップ・ボットネットのC&Cサーバーや関連する悪意のあるオブジェクトを含むURLマスクのセット
Malicious Hash Feed	最も危険で広く普及している新興のマルウェアに対応するコンテキストを持つファイルハッシュのセット
Mobile Malicious Hash Feed	AndroidおよびiPhoneのモバイルプラットフォームに感染する悪意のあるオブジェクトを検出するために対応するコンテキストを持つファイルハッシュのセット
Mobile Botnet C&C URL Feed	モバイル・ボットネットのC&Cサーバのコンテキストを含むURLのセット
IP Reputation Feed	疑わしいホストや悪意のあるホストのさまざまなカテゴリを示すコンテキストを持つIPアドレスのセット
Ransomware URL feed	ランサムウェアのリンクやWebサイトを含むURL、ドメイン、ホストのセット
IoT URL Data Feed	IoTデバイスに感染するマルウェアのホスティングに使用されるサイトのコンテキストを含むURLセット・マルウェアのハッシュ値も提供
Vulnerability Data Feed	関連するサイバー脅威情報(脆弱なアプリケーション/エクスプロイトのハッシュ・タイムスタンプ・CVE・パッチなど)を含むセキュリティ脆弱性のセット

Copyright © 2025 Kaspersky Lab. All rights reserved.

脅威データフィード構成

kaspersky

様々な脅威情報に特化した脅威データフィード

脅威データフィード名	フィードに含まれる情報
pDNS Data Feed	実用的なコンテキストで強化された対応するIPアドレスへのドメインのDNS解決の結果を含むレコードのセット
ICS Hashes Feed	産業用制御システムのインフラストラクチャ(ICS)を攻撃するために使用される悪意のあるオブジェクトに対応するコンテキストを持つファイル・ハッシュのセット
ICS Vulnerability Feed	産業用制御システム(ICS)およびICSネットワークに統合された一般的なITシステムにおけるセキュリティ脆弱性の集合体
Suricata Rules Data Feed	APT、ボットネットC&C、ランサムウェアなどさまざまな脅威を検出するSuricata IDSルール
Cloud Access Security Broker Feed	クラウドサービスのドメインをカバーするマスクのセット
Open Source Software Threats Data Feed	脆弱性が存在するオープンソースソフトウェアのバージョン・ダウンロード元、受ける可能性のある攻撃手法のセット
Industrial OVAL Data Feed for Windows	産業用制御システムに利用されるソフトウェアに存在する脆弱性を検出するための脅威データフィード
SIGMA Rules Feed	SIEMシステム用シグネチャフォーマット:SIGMAで記述された脅威を検出するためのルールセット
Network Security Threat Data Feeds	ファイアウォール(Check point/FortiGate/PaloAlto/Cisco)とAPIで簡単に連携可能なURL・IPアドレスのセット(フィード内容はIP Repuration / Malicious URL / Phishing URL / Botnet C&Cと同様)

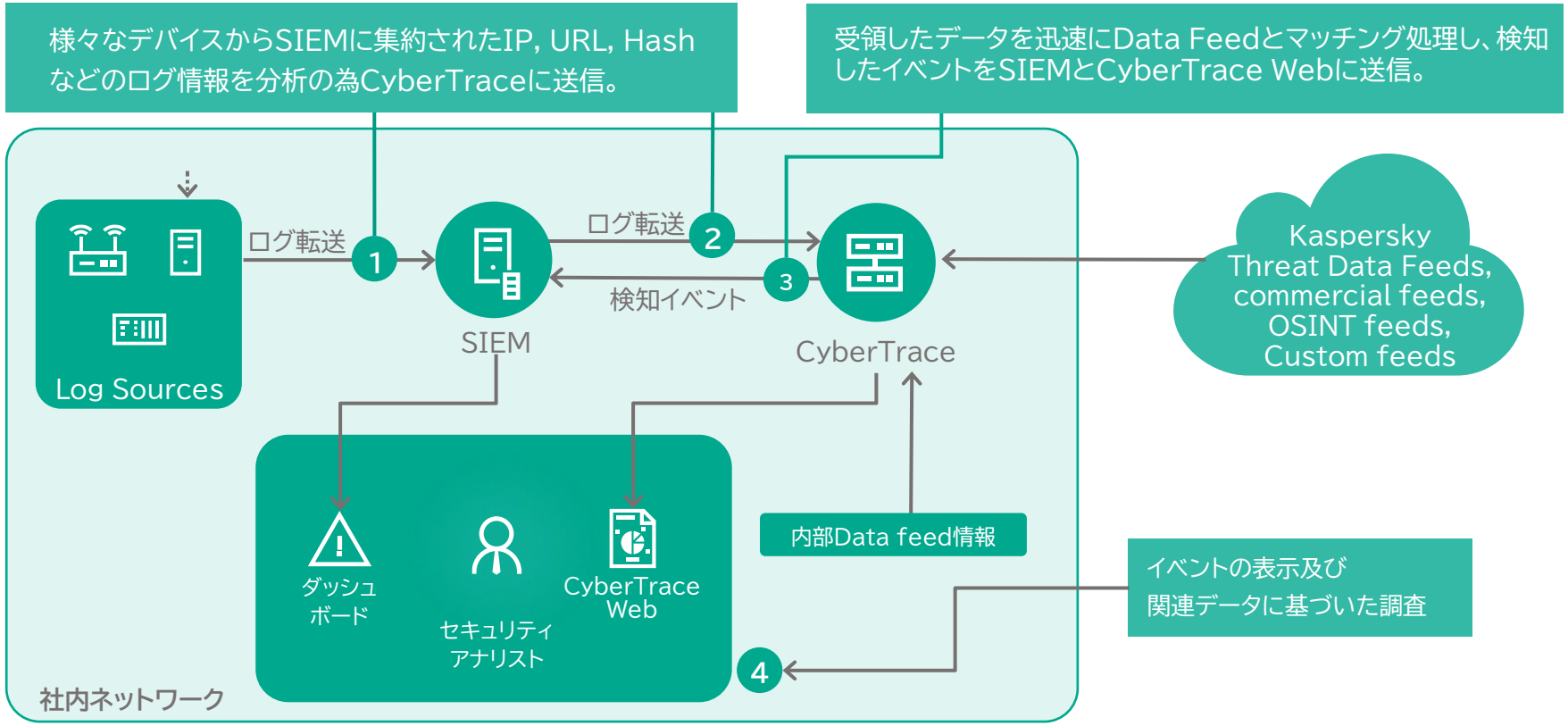
Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky CyberTrace とは

kaspersky

・SIEMに集約された各ログと脅威データフィードの自動照合用ソリューション

・CyberTrace内部で照合を行い、脅威を検知したイベントのみSIEMにアラート通知する為、SIEMの負荷を増やすことなく導入が可能



Copyright © 2025 Kaspersky Lab. All rights reserved.

kaspersky

Kaspersky Threat Lookup

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Threat Lookup とは

kaspersky

・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

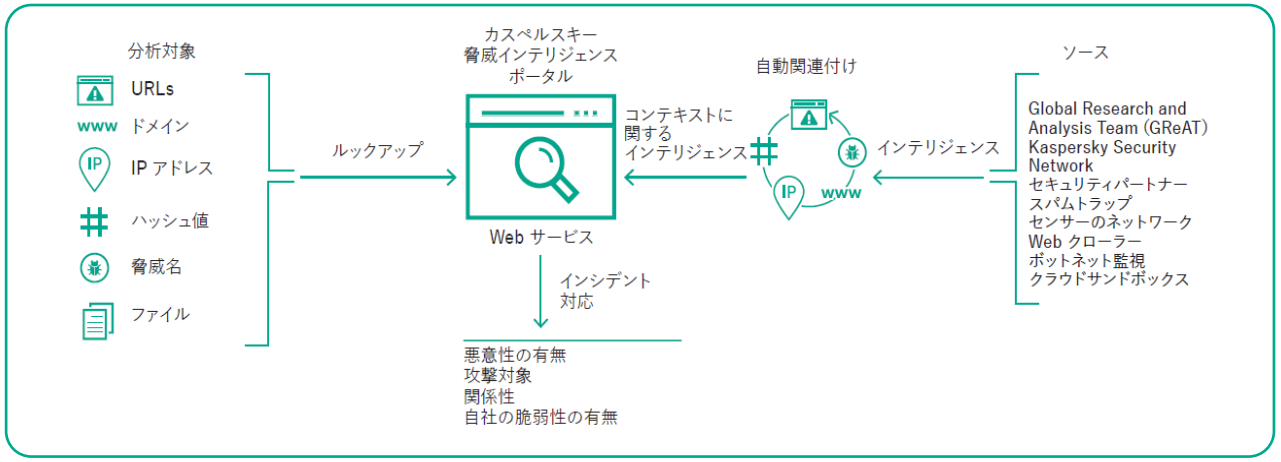
-特定のIPアドレス、ドメイン、URL、オブジェクトに関する脅威の検索を行う「Threat Lookup」

-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」



Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Cloud Sandbox

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Cloud Sandbox とは

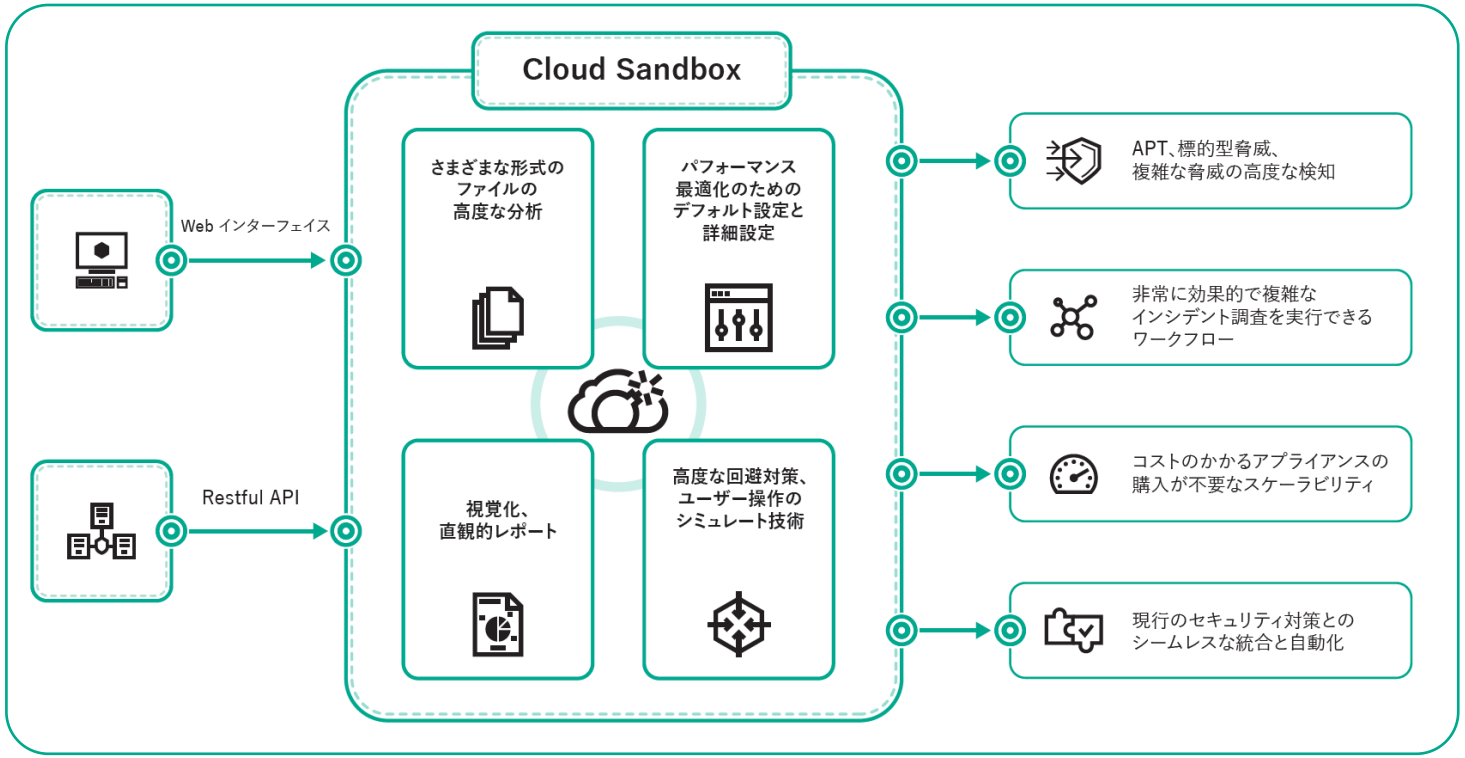
kaspersky

オブジェクトの動的解析をクラウド上のサンドボックスで実現するソリューション

・クラウド上のサンドボックスを使用したオブジェクトの動的解析サービス

・クラウドベースの為、サンドボックス用の機器の購入やメンテナンスにかかるランニングコストの削減が可能

・統計データから収集した脅威インテリジェンス、ふるまい分析、サンドボックスを回避する最新手法に対する信頼性の高い回避対策、自動クリック、文書スクロール、ダミープロセスなどのユーザ操作のシュミレート技術を組み合わせたハイブリットアプローチを採用



Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Threat Attribution Engine (Cloud)

Copyright © 2025 Kaspersky Lab. All rights reserved.

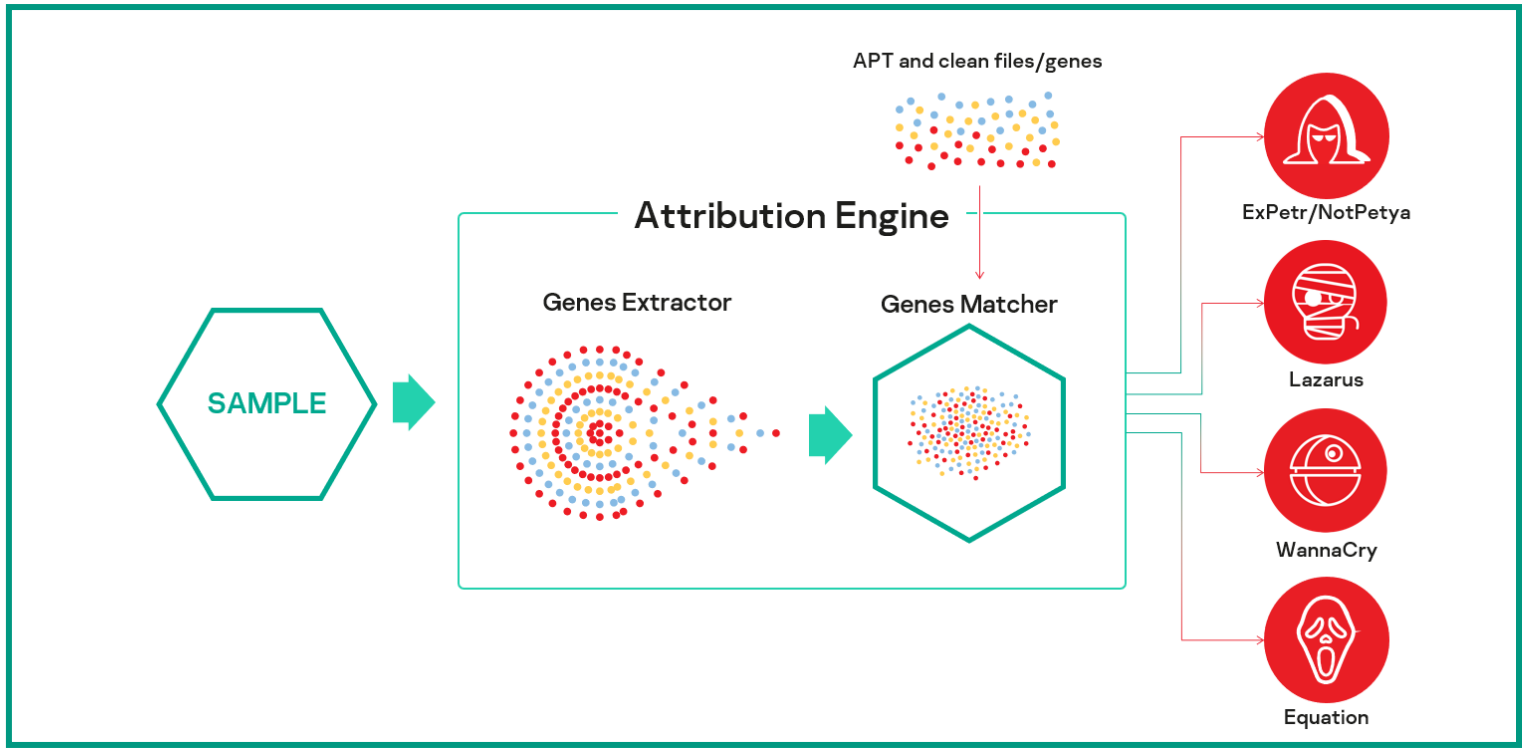
Cloud Threat Attribution Engine とは

kaspersky

コードの類似性を解析し、攻撃者を特定するための技術的証拠を示すソリューション

・サンプルから抽出された遺伝子型（16バイト長の小さなバイナリ断片）と60,000件以上のAPTマルウェアサンプルを含んだ大規模のAPTデータベースをクラウド上で比較し、攻撃者を特定するマルウェア属性分析サービス

・特許取得の類似コード比較技術に基づいた独自の製品で、OSに依存せずあらゆるファイルの解析が可能
＝攻撃の背後にいる攻撃者・攻撃グループの情報を提供し、適切かつ迅速なインシデントレスポンスを支援



Copyright © 2025 Kaspersky Lab. All rights reserved.

参考

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Ask The Analyst

kaspersky

Kasperskyのエキスパートが質問に回答

・Kasperskyのお客様のサイバーインシデント対応を支援するグローバル調査分析チーム・脅威調査チームがお客様から
いただいたサイバー攻撃に関するご質問・追加情報のリクエストに回答するサービス

<Kaspersky Ask The Analystを通じて受けられるサービス一例>

-詳細なIoC・解析の背景情報など、当社の脅威インテリジェンスレポートの追加データの提供

お客様の状況に応じ、お客様の会社で検知されたIoCとレポートに記載された活動との関連性

-検体の詳細解析

ご提供いただいた検体を解析、検体のふるまいに関する詳細な解析・目的の特定、攻撃の影響を緩和するための推奨事項

-特定のマルウェアファミリーの情報・防御に関するアドバイス、IoCの背景情報の提供

-具体的な脆弱性とその深刻度、カスペルスキー製品が脆弱性を防ぐ方法の提供

-ダークWeb調査

特定のアーティファクト（IPアドレス・ドメイン名・Eメールアドレスなど）をダークWeb上で調査、漏洩や攻撃計画の有無などを報告

Copyright © 2025 Kaspersky Lab. All rights reserved.

Kaspersky Takedown Service

kaspersky

お客様に被害を与えるWebサイト閉鎖に必要な対応をカスペルスキーが代行

・お客様になりすますフィッシングサイト・悪意のあるドメイン・タイポスクワッティングサイトの閉鎖に必要な情報収集および対応機関への依頼をカスペルスキーが代行するサービス

・各国のCERT、国際サイバー警察（INTERPOL、Europol）と連携することで、ドメインが登録された国にかかわらずサービスの提供が可能

・Webサイト閉鎖が正常に削除されるまで、作業の進捗状況を報告

・以下2つの方法でWebサイト閉鎖を依頼することが可能

＜依頼方法＞

①Kaspersky Takedown Serviceを個別契約し、カンパニーアカウントから依頼

カンパニーアカウント（カスペルスキーのテクニカルサポートにオンラインリクエストを送付可能なポータルサイト）よりWebサイト閉鎖を依頼

②Digital Footprint Intelligence（DFI）の検知結果から依頼

DFIで悪意のあるドメイン・フィッシングサイト・タイポスクワッティングが発見された場合、ポータル上に表示されたアラート通知からWebサイト閉鎖を依頼

Copyright © 2025 Kaspersky Lab. All rights reserved.

kaspersky