kaspersky

「Kaspersky Cloud Sandbox / Cloud Threat Attribution Engine」のご紹介

～追加リソース不要のサンドボックス・属性分析サービス～

2023年01月06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

V1.0

Cloud Sandboxのご紹介

Kaspersky Cloud Sandbox とは

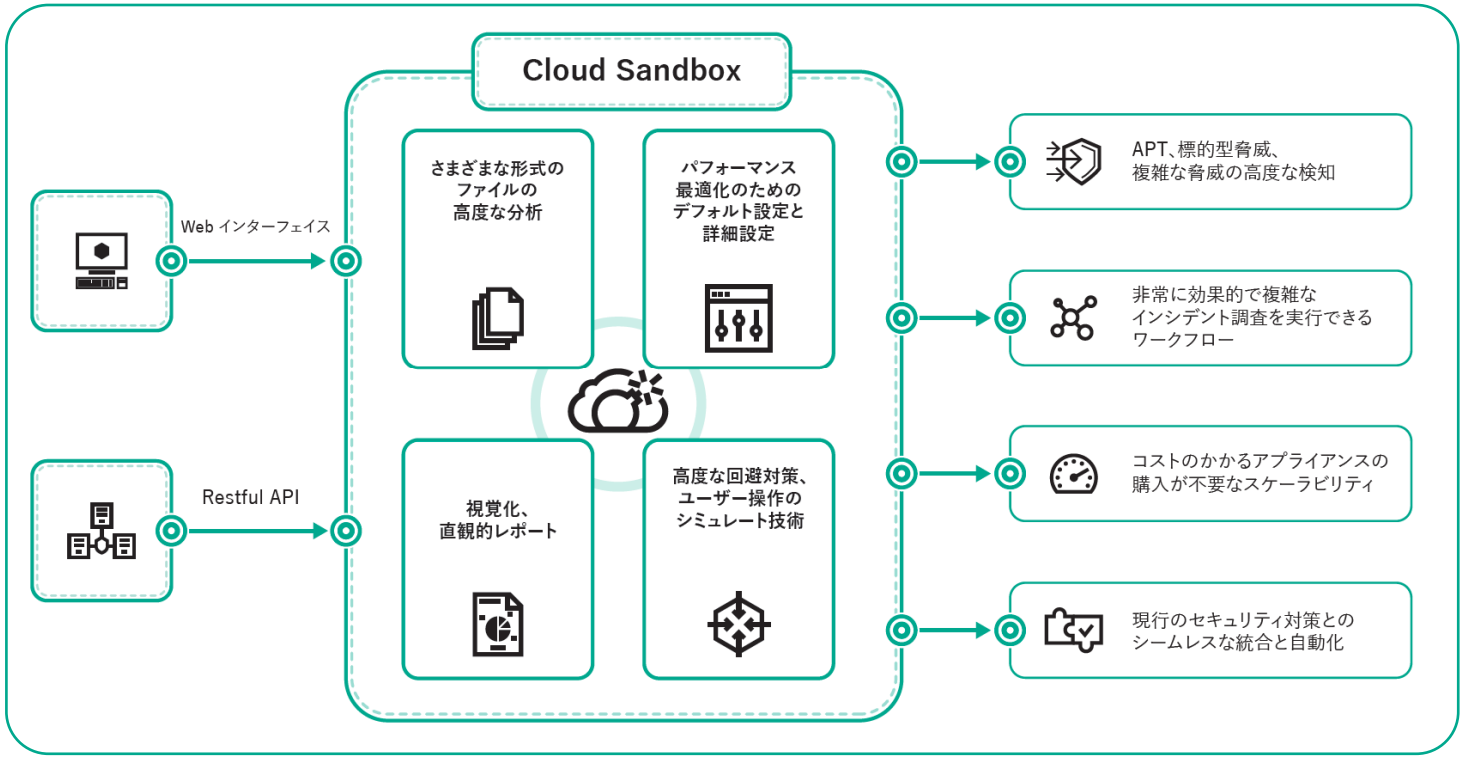
Kaspersky Cloud Sandbox

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

・カスペルスキーがクラウド上に提供するサンドボックスを使用したオブジェクト解析サービスです。

・クラウドベースの為、サンドボックス用の機器の購入が不要でメンテナンスにかかるランニングコストを削減することが可能です。

・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しています。



kaspersky

解析方法

Kaspersky®
Cloud Sandbox

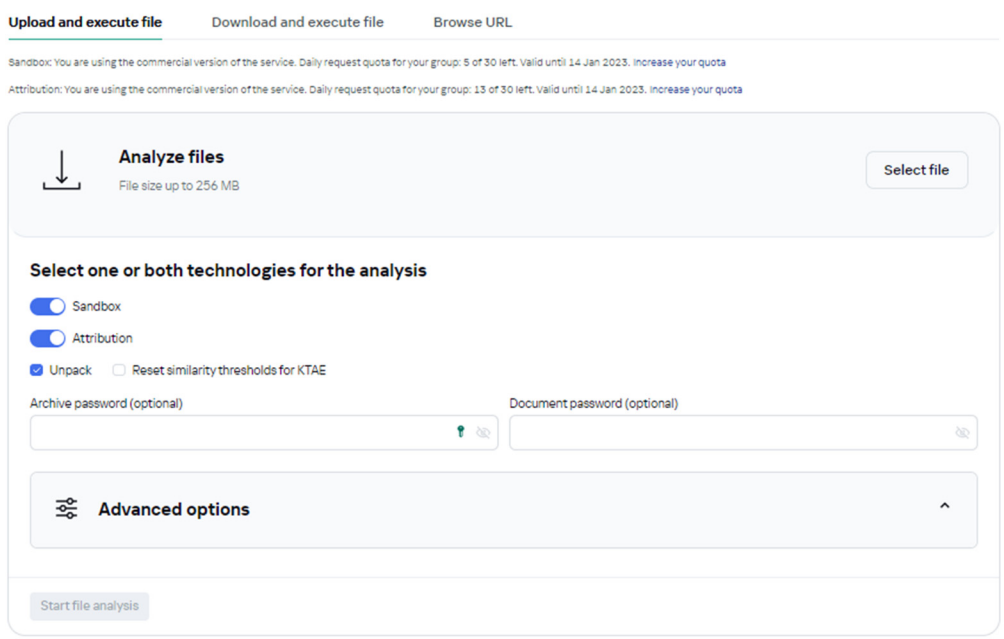
さまざまなファイルを解析するための柔軟な設定

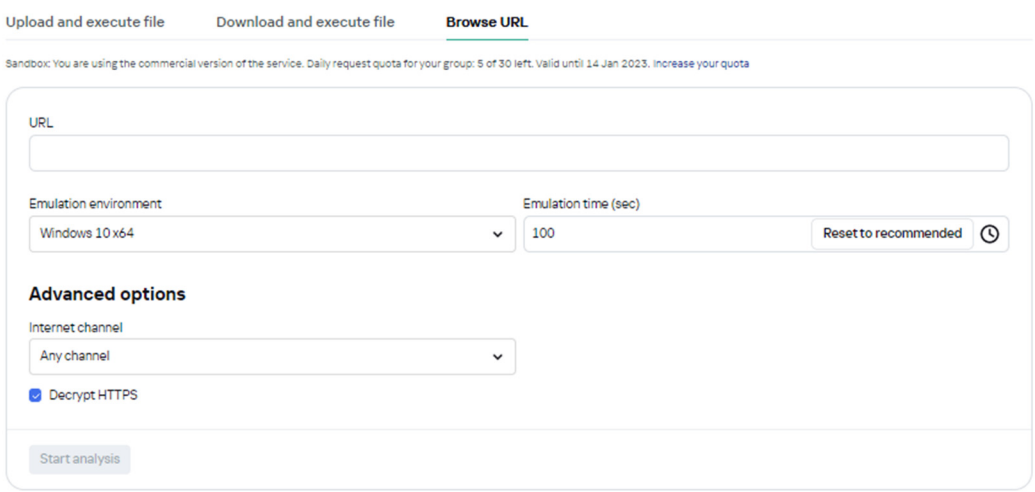
・以下の3パターンの解析が可能です。

①解析したいファイルをドラッグ＆ドロップでアップロード

②解析したいファイルがダウンロードされるURL

③アクセスした際の挙動を解析したいURL





kaspersky

解析方法

Kaspersky®
Cloud Sandbox

さまざまなファイルを解析するための柔軟な設定

・オプションを設定することで、オブジェクト解析をさまざまな条件で実施することが可能です。

①ファイル実行環境

Windows XP / Windows 7 / Windows 7 x64 / Windows 10 x64 / Android x86 / Android ARM

②インターネットチャネル

Tor / Tarpit（インターネットにアクセスせず実行） / AU / BR / DE / EG / JP / KR / RU / US

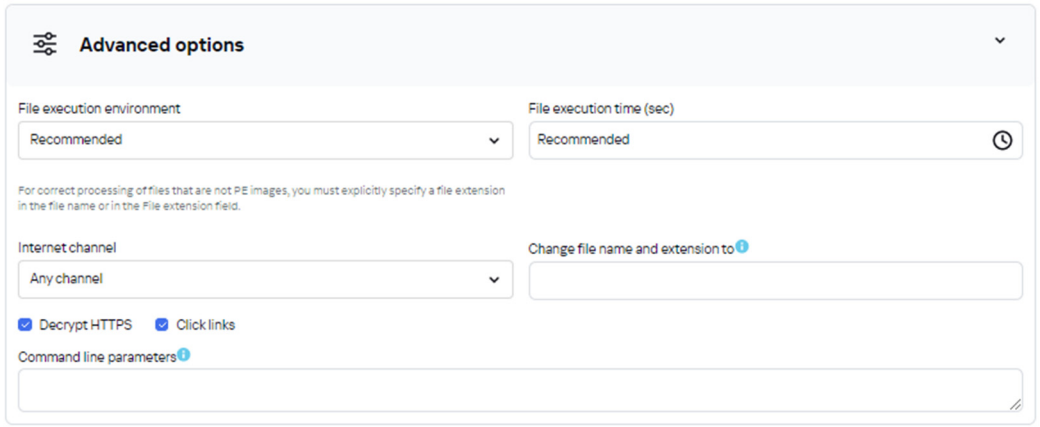
③その他オプション

-HTTPS複号

-ドキュメント内のリンク追跡

-特定のパラメータを使用したオブジェクト実行

-解析時間（30～500秒）



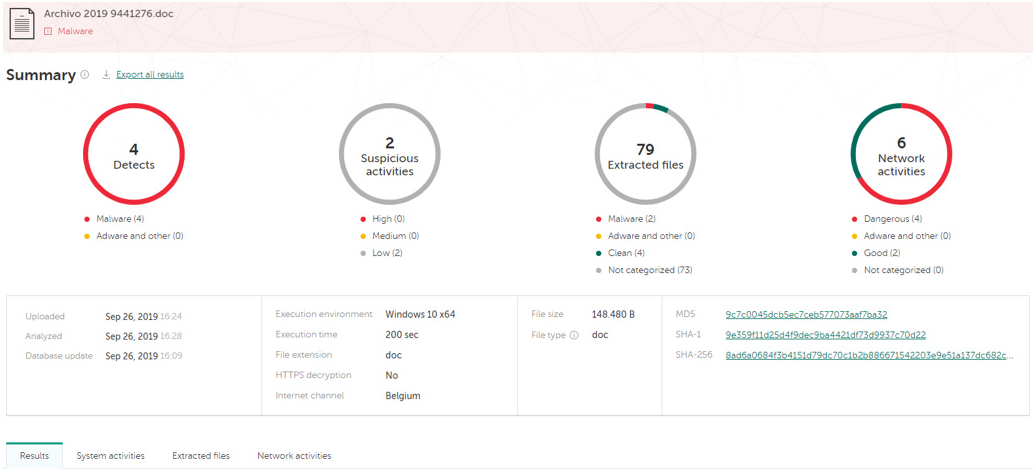
kaspersky

解析結果

Kaspersky®
Cloud Sandbox

・対象のオブジェクト解析後、ファイルの実行結果と分析結果が以下のカテゴリごとに表示されます。

項目	説明
サマリ	実行タスクの詳細（ファイル実行時に検知したアイテム・アクティビティ・抽出ファイルのサマリ）
検知	検知された脅威、適用されたネットワークルール、疑わしい活動
静的分析結果	オブジェクトの静的分析結果 （Androidのサンドボックス環境で解析した場合のみ表示）
システムアクティビティ	ファイル実行中に読み込まれたPEイメージおよび登録された様々な動作
抽出されたファイル	実行されたファイルによってダウンロード・ドロップされたファイル
ネットワークアクティビティ	ファイル実行中に登録されたネットワーク動作



kaspersky

解析結果:「検知」カテゴリ

Kaspersky Cloud Sandbox

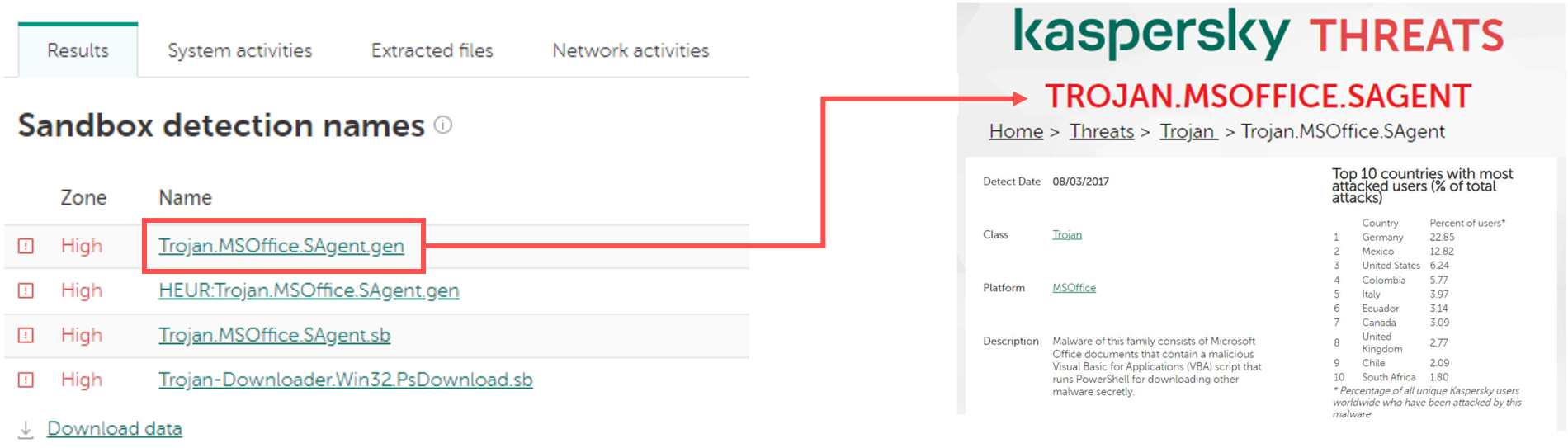
検知されたオブジェクト・ファイルの実行中に登録された動作を提供

・検知カテゴリではファイル実行中に検知や登録されたアイテム・アクティビティに関する情報を提供します。

①検知したマルウェア

-ファイル実行中に脅威として検知されたマルウェアの一覧

->マルウェア名をクリックすることで脅威に関する「検出日」や「プラットフォーム」、「攻撃の地理的分布」といった詳細情報が「Kaspersky THREATS」で確認可能



kaspersky

解析結果:「検知」カテゴリ

Kaspersky®
Cloud Sandbox

②ネットワークトリガールール

-実行されたファイルからのトラフィック分析に適用されたSNORT・Suricataルール

③ファイルのダウンロードに関する情報（「解析したいファイルがダウンロードされるURL」を指定して解析した場合のみ表示）

-ファイルダウンロードプロセス（HTTPリクエストのメソッド、ユーザーエージェント）

-ファイルのダウンロード元から送信されたWebアドレスに対するリクエスト、Webアドレスからのレスポンス

File download information

Method GET

Download request Download data

Name	Value
Host	p[redacted]t
User-Agent	Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko

Download responses Download data

Status	Categories	Protocol	URL	Response code	Response length	Response headers
Not categorized	Malware	HTTP	p[redacted]s	407	3.00 KB	Request headers – Response headers

Response headers	
Connection	keep-alive
Content-Length	3070
Content-Type	text/html;charset=utf-8
Date	Thu, 22 Dec 2022 05:41:07 GMT
Mime-Version	1.0
Proxy-Authenticate	Basic realm="restricted area"
Server	squid/5.7
X-Cache-Lookup	NONE from anon2-disp1.kaspersky-labs.com:3
X-Squid-Error	ERR_CACHE_ACCESS_DENIED 0

kaspersky

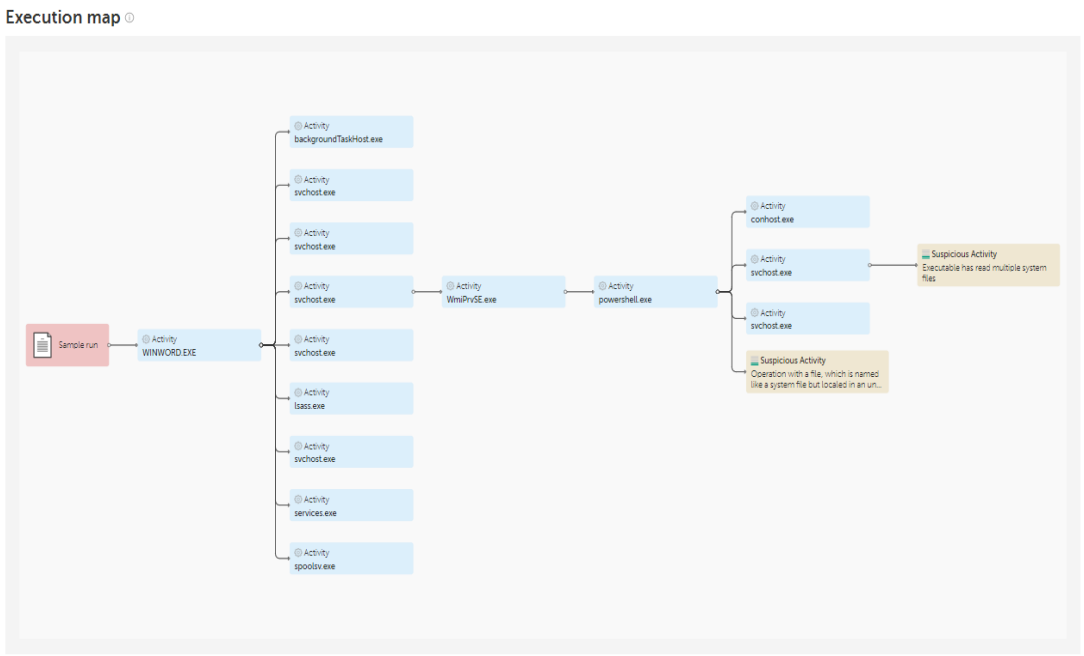
解析結果:「検知」カテゴリ

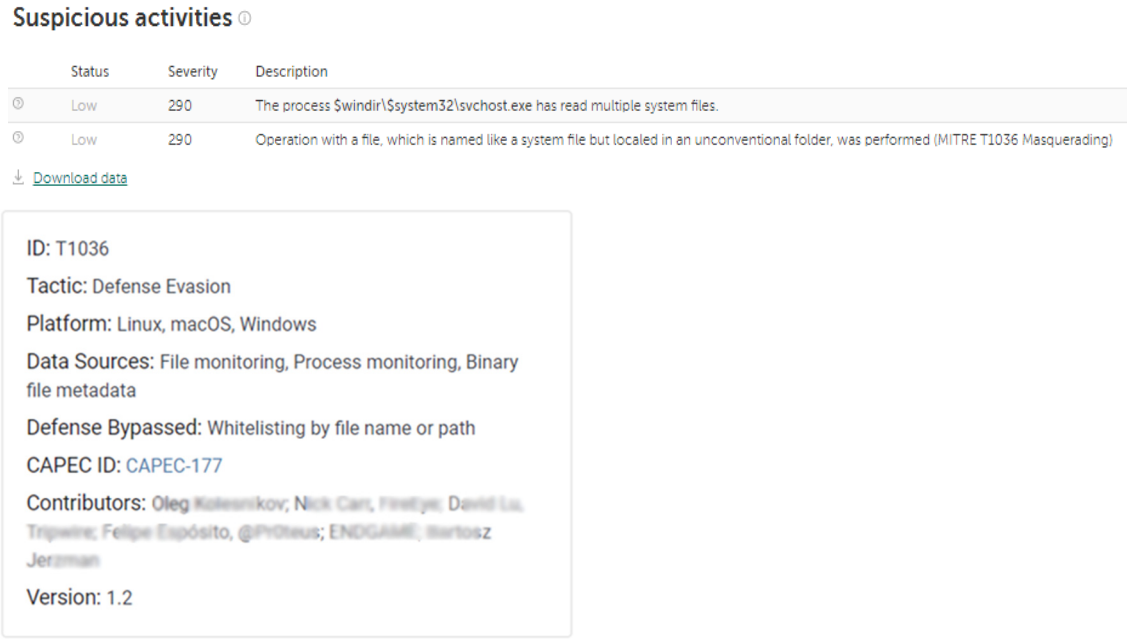
Kaspersky®
Cloud Sandbox

④Execution map

-各アクティビティのシーケンスの関係を可視化、各ツリー要素は危険レベルによって色分けされ、クリックすることで詳細情報を表示

-疑わしいアクティビティにはMITRE ATT&CK(攻撃を戦術・技術・手法の観点で分類したナレッジベース)の情報がマッピング





kaspersky

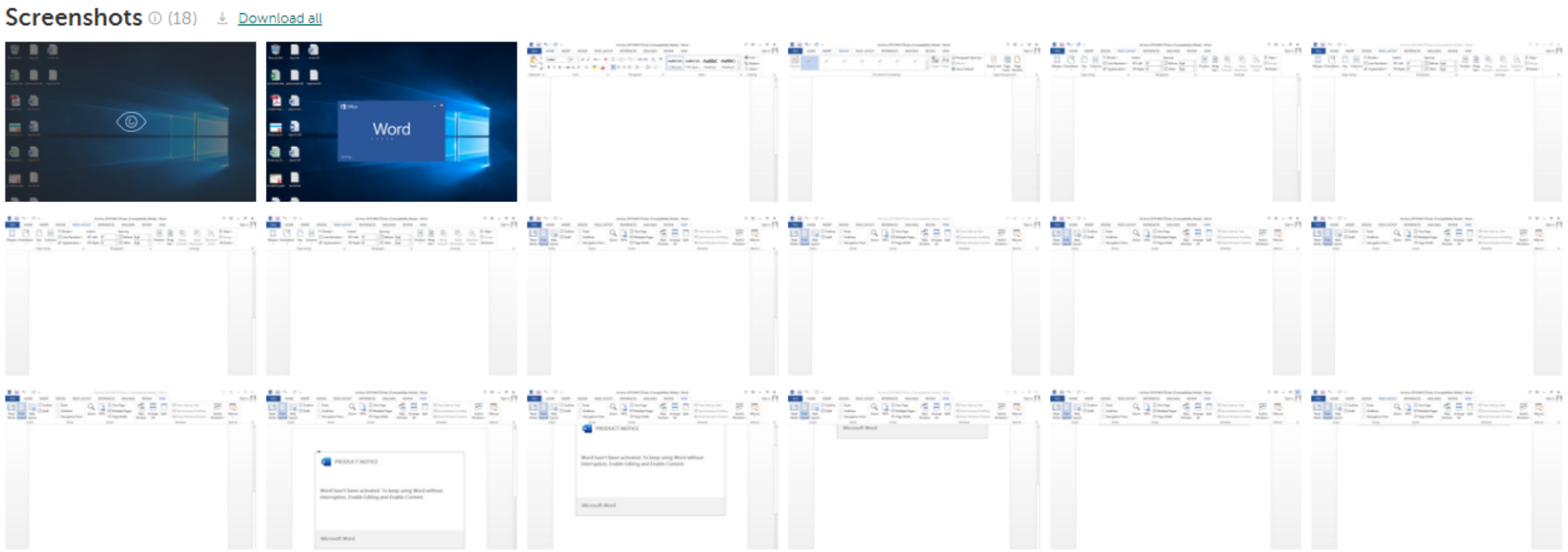
解析結果:「検知」カテゴリ

Kaspersky®
Cloud Sandbox

⑤スクリーンショット

-対象のオブジェクトを解析環境で実行した際の動作を記録した一連のスクリーンショット

->提供されたスクリーンショットはダウンロード可能



kaspersky

解析結果:「静的分析結果」カテゴリ

Kaspersky Cloud Sandbox

Androidを標的にしたマルウェアの動的解析結果

・静的分析結果カテゴリではAndroidの解析環境で実行された関する情報を提供します。

①マニフェスト

-アプリの内部構造などが記載されたxmlファイル

②モジュール、コンポーネント

-検知されたモジュールのパス、説明

-検知されたコンポーネント名、重大度、ステータス、説明

③権限

-検知されたアプリの権限ステータス、重大度、権限の値、説明

④Android App Bundle

-Android App Bundle(Google PlayがAPKの生成と署名を行ったアプリのコンパイル済みコードとリソースをすべて含むアップロード形式)のファイルタイプ、パス、サイズおよびMD5ハッシュ値

-Android App Bundleの画像

kaspersky

解析結果:「システムアクティビティ」カテゴリ

Kaspersky®
Cloud Sandbox

・システムアクティビティカテゴリでは、ファイル実行中に読み込まれたPEイメージおよび登録された様々な動作に関する情報を提供します。

①PEイメージ

-ファイル実行中に読み込まれたPEイメージのファイルパスとファイルサイズ

②ファイル操作、レジストリ・プロセス・同期オブジェクトに関するオペレーション

-ファイル実行中に登録されたファイル・レジストリの操作、ファイルと様々なプロセスの通信

-作成された同期オブジェクトの操作

Results | **System activities** | Extracted files | Network activities

Loaded PE Images ⓘ Download data

Path	Size
$programfiles\Internet Explorer\iexplore.exe	64.00 KB (65536 B)
$programfiles\Internet Explorer\iexplore.exe	664.00 KB (679936 B)

File operations ⓘ Download data

Operation	Name	Size
File read	C:\Users\desktop.ini	174.00 B (174 B)
File read	$user\Searches\desktop.ini	524.00 B (524 B)

Process operations ⓘ Download data

Interaction type	Process name
Process started	$programfiles\Internet Explorer\iexplore.exe

Registry operations ⓘ Download data

Operation	Details
Registry key created	Key \REGISTRY\USER\$usersid\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
Registry key created	Key \REGISTRY\USER\$usersid\Software\Microsoft\windows\CurrentVersion\Internet Settings\Connections

Synchronization operations ⓘ Download data

Type	Name
Event creation attempt	$Global\BFE_Notify_Event_{8f882256-26b6-4f07-bf33-8b34f282b140}
Event created	$Global\BFE_Notify_Event_{8f882256-26b6-4f07-bf33-8b34f282b140}

kaspersky

解析結果:「抽出されたファイル」カテゴリ

Kaspersky®
Cloud Sandbox

・抽出されたファイルカテゴリでは、実行されたファイルによって保存されたファイル関する情報が提供されます。

①アップロードされたオブジェクトに含まれるファイルの情報

-ファイルの危険レベル、MD5ハッシュ値、ファイル名、使用されたパッカーの名前など

②実行されたファイルによって保存されたファイル、ネットワークトラフィックから抽出されたファイル

-ファイルのステータス、MD5ハッシュ値、ファイル名、検知されたオブジェクト名など

Dropped files

Status	MD5	Detection name	File name
Malware (APT Related)	2E[redacted]B08	HEUR:Trojan-Downloader.MSOffice.DdeExec.i	Meeting-Details.docx
Not categorized	34[redacted]D32	—	index.dat
Not categorized	8E[redacted]8C2	—	OAlerts.evtx
Not categorized	99[redacted]E84	—	~WRS{05FD853F-A162-4CC3-8F
Not categorized	AF[redacted]F10	—	Meeting-Details.docx.LNK
Not categorized	C9[redacted]BD18	—	~Seting-Details.docx
Not categorized	E3[redacted]4FE	—	qmgr0.dat
Not categorized	F8[redacted]075C0	—	qmgr1.dat
Clean	5D[redacted]323A	—	~WRS{2AC8F5C5-C89C-4DA1-B

Download data

kaspersky

解析結果：「ネットワークアクティビティ」カテゴリ

Kaspersky Cloud Sandbox

動的解析中に発生した通信の詳細を提供

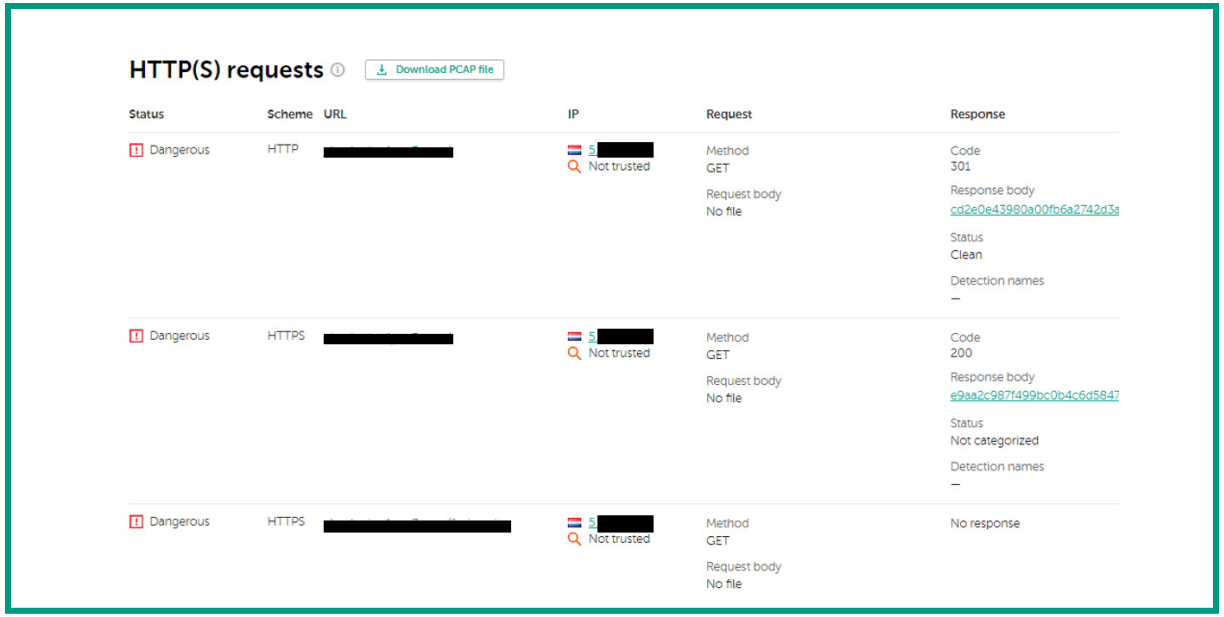
・ネットワークアクティビティでは：ファイル実行中に登録されたHTTP(S)・DNSリクエスト情報を提供します。

①ネットワークセッション

-ファイル実行中に登録されたIP/TCP/UDP/DNS/TLS/FTP/IRC/POP3/SMB/SMTP/SOCKSセッション

②HTTP(S)リクエスト

-ファイルの実行中に登録されたHTTP(S)リクエスト



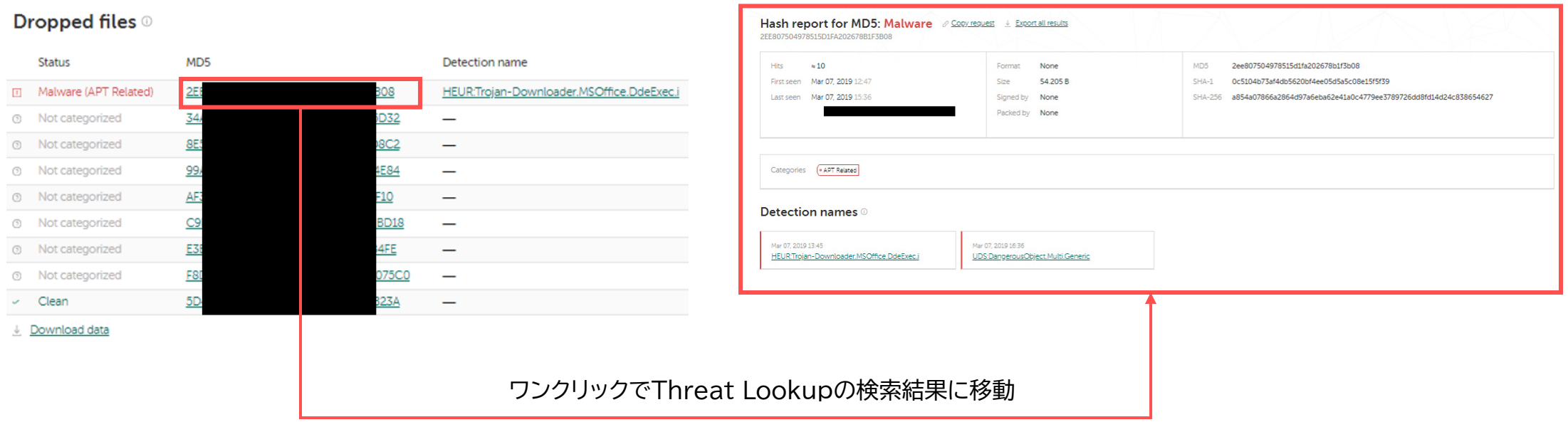
kaspersky

Kasperskyの脅威インテリジェンスサービスとの連携

Kaspersky®
Cloud Sandbox

サービス連携によるインシデントレスポンスの強化

・Threat Lookup：脅威ルックアップサービスと連携することで、検知したオブジェクト名からワンクリックで脅威情報の詳細を確認可能です。



kaspersky

Cloud Threat Attribution Engineのご紹介

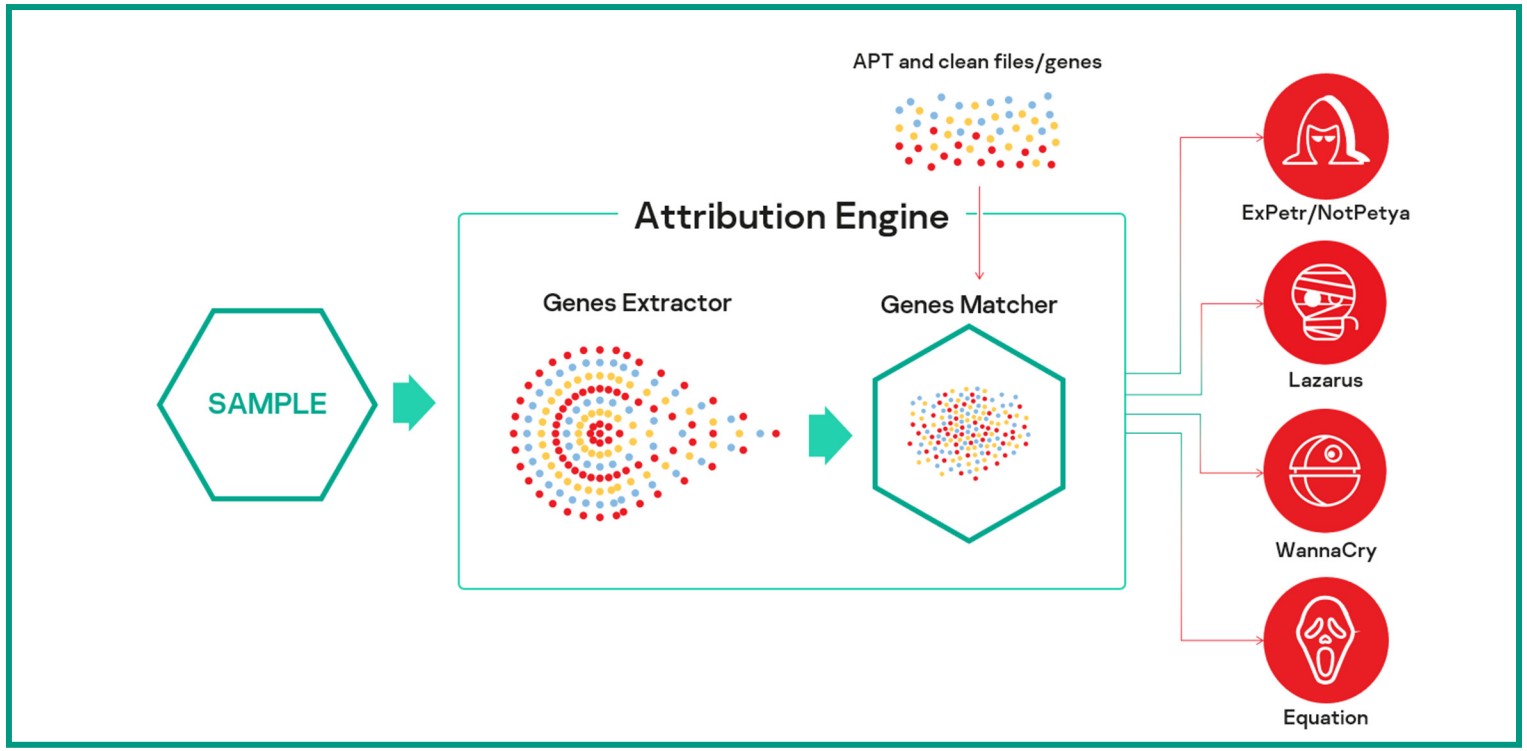
Cloud Threat Attribution Engine とは

Kaspersky Threat Attribution Engine

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です。

・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です。
＝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します。



kaspersky

解析方法

Kaspersky®
Threat Attribution
Engine

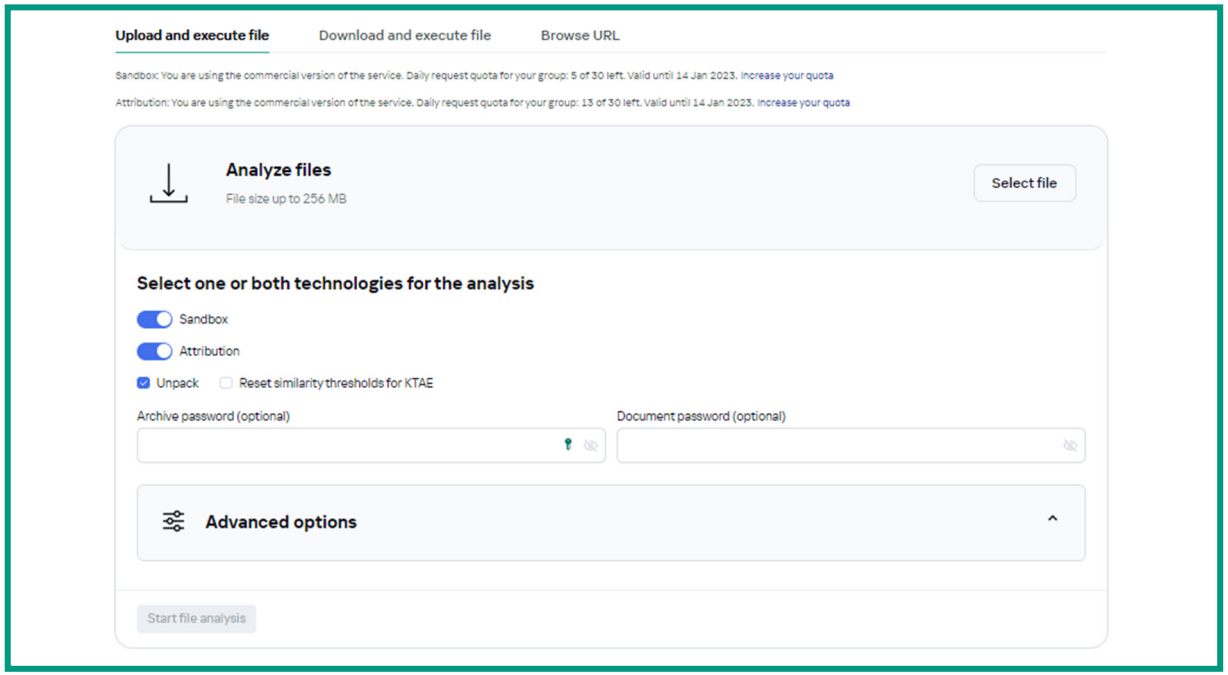
対象オブジェクトの動的解析と属性分析を一度に実施

・以下の2パターンの分析が可能です。

①分析したいファイルをドラッグ＆ドロップでアップロード

②分析したいファイルがダウンロードされるURL

・Cloud Threat Attribution EngineはCloud Sandboxとの同時解析が可能です。



kaspersky

解析結果

Kaspersky®
Threat Attribution
Engine

・対象のオブジェクト解析後、既知のAPTサンプルとの類似性に基づき、考えられるファイルの属性に関する情報を提供します。

①サマリ

-オブジェクト判定および分析結果に関する一般情報

②サンプル・コンテンツ

-抽出されたファイルのステータス、データベースと一致した遺伝子型・文字列の数、考えられる攻撃者グループ名

kaspersky

解析結果

Kaspersky®
Threat Attribution
Engine

③類似サンプル

-分析されたファイルに類似するオブジェクトのハッシュ値、考えられる攻撃者グループ、攻撃者グループの別名

④分析されたファイルと一致した遺伝子型、文字列

Similar samples

Status	MD5	Size	Genotypes matched (total)	Strings matched (total)	Similarity	Attribution entities	Aliases
Malware	595.....156a	240.00 KB (245760 B)	686 (1306)	4 (4)	99	BlueNoroff	APT38, Stardust Chollima, CTG-6459, Nickel Gladstone, T-APT-15, ATK 117
Malware	5cc.....ae58	666.00 KB (681984 B)	495 (1078)	8 (8)	99	BlueNoroff	APT38, Stardust Chollima, CTG-6459, Nickel Gladstone, T-APT-15, ATK 117
Malware	630.....3c1f	666.00 KB (681984 B)	498 (1070)	8 (9)	89	BlueNoroff	APT38, Stardust Chollima, CTG-6459, Nickel Gladstone, T-APT-15, ATK 117

Matched genotypes

Genotype	Matched	Used by
0200000fb60c028d4201898398020000	13	BlueNoroff (12), Lazarus (1)
020000420fb60c10ffc0898398020000	13	BlueNoroff (12), Lazarus (1)

Matched strings

String	Matched	Used by
4MD9U,L	10	BlueNoroff (10)
4M9]8H	10	BlueNoroff (10)

kaspersky

kaspersky