



サイバー攻撃から身を守る方法を
知り、組織に影響する脅威の状況
を解明

Kaspersky Threat Intelligence Portal で脅威の状況を 解明

kaspersky bring on
the future



Kaspersky Threat Intelligence Portal



Kaspersky Threat Intelligence Portal

[Threat Landscape] セクションで、ユーザー固有の脅威の状況を評価することができます。このセクションは、特定の業界や地域を標的とする攻撃者に関する情報の提供に特化して設計されており、検知技術とグローバルな脅威インテリジェンスの統合も行います。これにより、想定される攻撃者が関連する脅威、戦術、テクニック、手順 (TTP) に関する、包括的で最新のコンテキストを得ることができます。

Kaspersky Threat Intelligence Portalで解明される、組織に影響する 脅威の状況

世界的な脅威の状況は常に変化しており、新しい攻撃手法が毎日のように登場し、既知の攻撃手法もより巧妙化が進んでいます。今日、情報セキュリティチームにとってますます重要になっているのは、即座に対応が要求される脅威の効果的な優先順位付けです。しかし、自社のビジネス、業界、地域にとって関連性が特に高い脅威には、どのように注力すべきでしょうか？

[Threat Landscape] セクションから得られる、**脅威に関する情報**は次の通りです：



地理的な情報



業界



脅威の種別



脅威アクター



テクニック、戦術、手順 (TTP)



攻撃者が使用する悪意のあるソフトウェア



関係するセキュリティ侵害インジケータ (IoC)

脅威インテリジェンスデータの収集には、Kasperskyが25年以上にわたってサイバー犯罪対策に使用してきた**各種のエキスパートシステムがリアルタイムで使用されています**。Kaspersky Security Networkはその代表的なシステムの1つで、世界中の何百万人ものユーザーから匿名データを同意を得た上で収集し、1日あたり何百万ものファイルを自動処理します。他にも、Webクローラー、ボットファーム、スパムトラップ、ハニーポット、センサー、パッシブDNS、オープンウェブおよびダークウェブの情報源、パートナーなどからも情報を収集しています。当社はこの四半世紀にわたってこのデータを使用しており、独立系機関によるテストや外部評価で常に最高点を獲得しています。収集されたデータは、Kasperskyの脅威リサーチチームによって慎重に分析され、サンドボックス、ヒューリスティックエンジン、類似性チェックツールなどの最新自動システムで処理され、検証済みの最新情報となります。

[詳細はこちら](#)

仕組み

Kaspersky Threat Intelligenceの情報源

KSN
テレメトリ

センサー

Webクローラー

ボットファーム

Spam /
IoTトラップ

パッシブDNS

パートナー
とOSINT



分析対象：

400,000
件以上の

悪意のあるファイルサンプル
(毎日)



Kaspersky
Threat Intelligence
Portal



アクターの
プロフィール

- 名前 / エイリアス
- 説明
- 国 / 業界
- TTP
- ソフトウェア / レポート



ソフトウェアの
プロフィール

- 名前 / エイリアス
- 説明
- アクター
- TTP
- SIGMARルール



Kaspersky Threat Intelligence
Reporting (APT、Crimeware、ICS)

- YARA、SIGMA、Suricataルール
- TTP
- IoC



MITRE ATT&CKのTTP

Threat Landscape



フィルター

業界

国

アクター

プラットフォ
ーム

MITRE ATT&CKヒート
マップ

毎日提供される悪意のあるサ
ンプルデータストリームに基
づくTTPの詳細な説明

トップ10統計

- TTP
- 脆弱性
- アクター
- ソフトウェア
- 業界

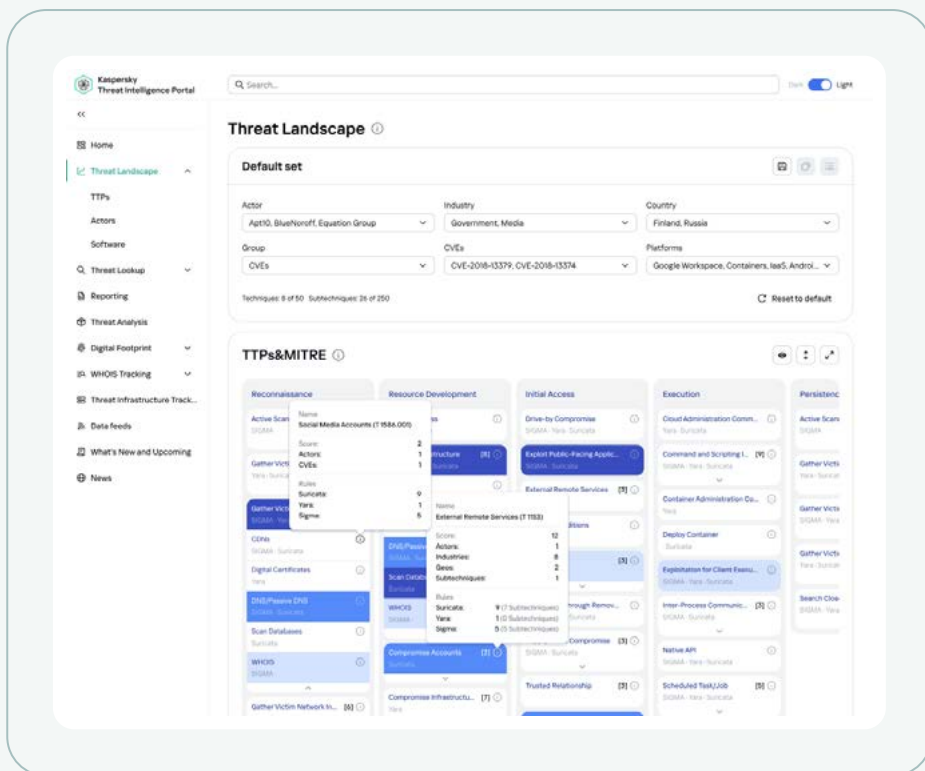
緩和策

当社は毎日、数十万もの悪意のあるファイルサンプルを処理し、その地理的情報と業界データを抽出しています。その後、Kasperskyの社内システムが関連するTTPを抽出し、既知のサイバー犯罪グループやマルウェアにファイルを属性付けします。[Threat Landscape] セクションもまた、世界中のKasperskyのエキスペートリサーチチームから寄せられる実際のインシデントデータの集積に基づいています。

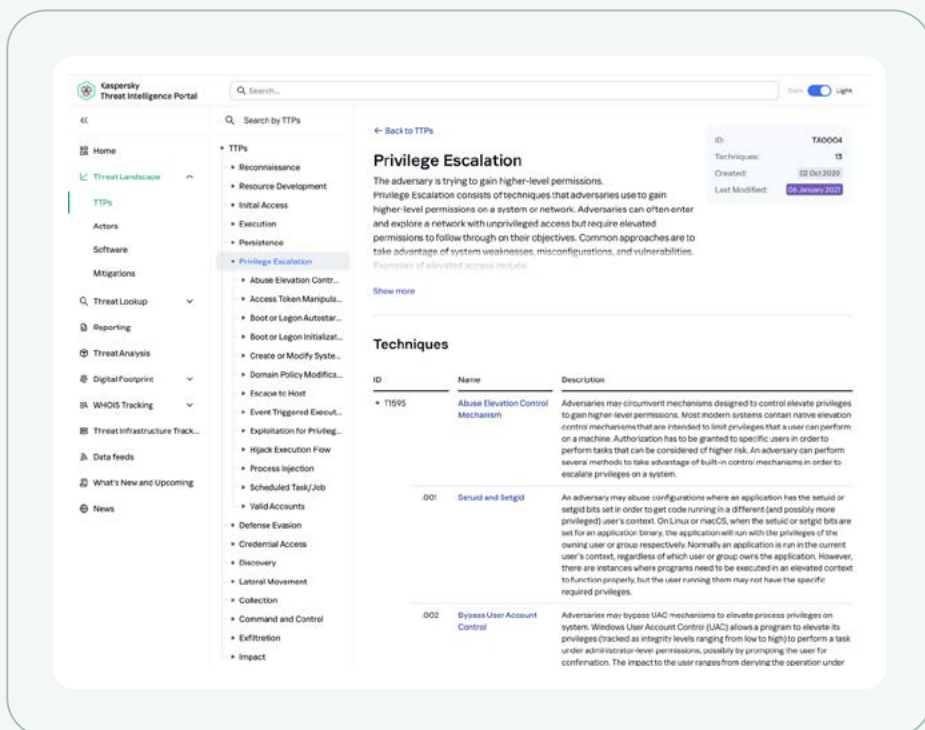
フィルターの適用により、Kaspersky Threat Intelligence Portalユーザーは、MITRE ATT&CKフレームワークに準拠した独自の脅威の状況の把握し、想定される敵対者に関する最新情報を入手することができます。入手可能な情報は次の通りです：攻撃に使用される可能性が高いテクニック、戦術、手順、それらを使用するアクター、マルウェア、およびTTPの詳細な説明、攻撃の詳細な説明を含むレポートです。最終的には、アクターのテクニックが成功裏に実行されるのを防止するための特定の推奨事項に基づいて、緩和策を講じることができます。

主な機能

MITRE ATT&CKヒートマップを使用して、組織に固有の脅威の状況をリアルタイムで構築します。フィルターを適用することで、ユーザーは、当社のシステムとエキスパートが継続的な調査を通じて入手した過去24時間分の更新情報など、最新のデータにアクセスできます。国際的な組織のレイヤーを保存することができます。



Kasperskyのエキスパートシステムに基づく、攻撃者のテクニク、戦術、手順に関するリアルタイムの最新情報。



[Mitigation] セクションでは、セキュリティギャップを回避するための組織の**予防措置**および**保護措置**について詳細な説明を参照することができます。

The screenshot displays the 'Application Developer Guidance' mitigation page in the Kaspersky Threat Intelligence Portal. The page provides detailed information for developers to avoid introducing security weaknesses. It includes a search bar, a list of mitigations, and a table of techniques addressed by the mitigation.

ID	Name	Description
70522	Exploitation for Cobalt...	Adversaries may modify access tokens to operate under a different user or system security context to perform actions and bypass access controls. Windows uses access...
70564	Hide Artifacts, Resour...	Configure applications to use the application bundle structure which leverages the Resource folder location
70574	Inject Execution Flow	When possible, include their values in manifest files to help prevent side-loading of malicious libraries
002	URL Side Loading	When possible, include their values in manifest files to help prevent side-loading of malicious libraries
70559	Inject Process Common...	Enable the hardened runtime capability when developing applications. Do not include the com.apple.security.get-task-allow entitlement with the value set to any vari...
70647	Pin File Modification	Ensure applications are using Apple's developer guidance which enables hardened runtime
70618	Secure Open (Developer)	Application developers updating to public code repositories should be careful for avoiding publishing sensitive information such as credentials and API keys
70578	Domain Policy Modifi...	Ensure that applications do not store sensitive data or credentials insecurely (e.g. plaintext credentials in code, published credentials in repositories, or credentials in pu...
70626	Escape to Host	Applications may require administrative permission. Developers should be cautioned against using this higher degree of access to avoid being flagged as a potent...
70587	Event Triggered Execu...	Application developers could be encouraged to avoid placing sensitive data in notification text
70582	Application for Plug...	Application developers can apply the [LSA_S3(20)] property to sensitive screens within their apps to make it more difficult for the screen contents to be captured
70625	Inject Execution Flow	Developers should use Android App Links and iOS Universal Links to provide a secure binding between URIs and applications, preventing malicious applications from int...
70574	Process Injection	Application developers should be cautious when selecting third party libraries to integrate into their application

References

- Microsoft (2024, November 19). Security Considerations for Trusts. Retrieved November 21, 2023. <https://www.pwn20wnd.com/sectors/cyber-security-data-governance/highlights/operation-credential-exploit.html>
- Microsoft (2024, November 19). Filter Operations on External Trusts. Retrieved November 20, 2023. <https://www.cis-cert.gov/ncsc/ptg/143-154>
- Microsoft (2019, September 19). Contented Line Reference. Nathan Trout. Retrieved November 20, 2023. <https://www.exploit-exchange.com/2019/09/19/contented-line-reference-weak-credential-0day/>
- Microsoft (2016, August 18). Surface Border: Trends on the Main Surface. Retrieved December 1, 2023. <https://www.microsoft.com/security/blog/2016/08/18/surface-border-on-the-main-surface/>
- Mandiant (2023, January 19). Remediation and Hardening Strategies for Microsoft .NET to Default Agent. <https://www.mandiant.com/resources/microsoft-net-to-default-agent/>
- https://www.cis-cert.gov/ncsc/ptg/143-154
- https://www.exploit-exchange.com/2019/09/19/contented-line-reference-weak-credential-0day/
- https://www.pwn20wnd.com/sectors/cyber-security-data-governance/highlights/operation-credential-exploit.html
- https://www.pwn20wnd.com/sectors/cyber-security-data-governance/highlights/operation-credential-exploit.html

アクターおよびマルウェアのプロファイルを業界で最も大規模に収集したリポジトリと、Kasperskyのエクスパートがまとめた詳細な説明を参照できます。

The screenshot displays the 'Apt10' actor profile page in the Kaspersky Threat Intelligence Portal. The page provides detailed information about the actor, including a description, a world map showing incident locations, and a list of incidents.

Apt10

Aliases: Russia, China, Pakistan, Red teams, Blood pack, TeamSentry, SIDA

Industries: Manufacturing, Distribution, Software development, Legal, Healthcare

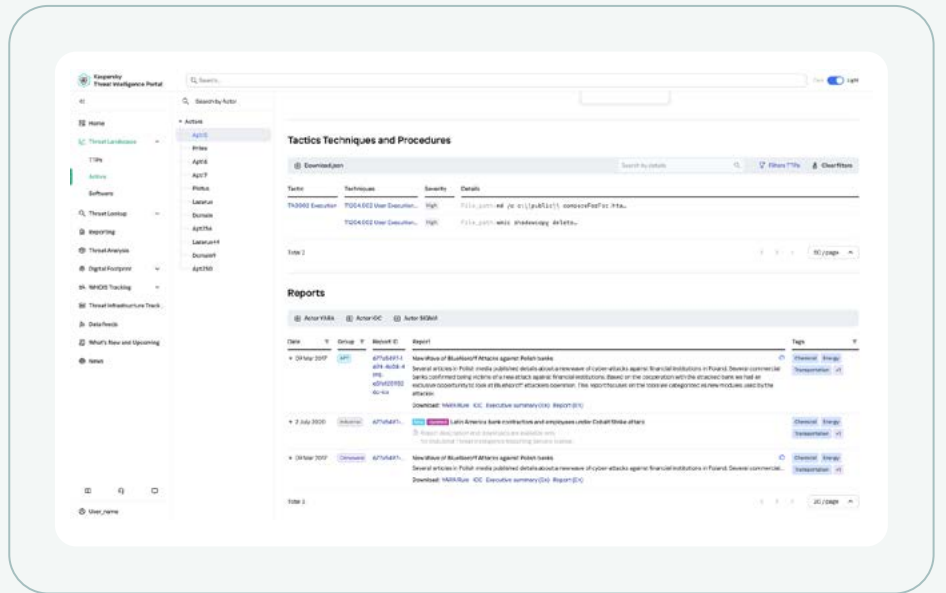
Description

APT10 is a Chinese-speaking sophisticated and persistent cyber espionage actor active at least since 2009. One of APT10's first public appearances was in a Freedom report describing the actor using Poison Ivy (PIVI) back in 2009, targeting U.S. and overseas defense contractors. At that time, the campaign codename used inside PIVI was said to be "manuscript". Based on this, some security researchers still call the group Manuscript.

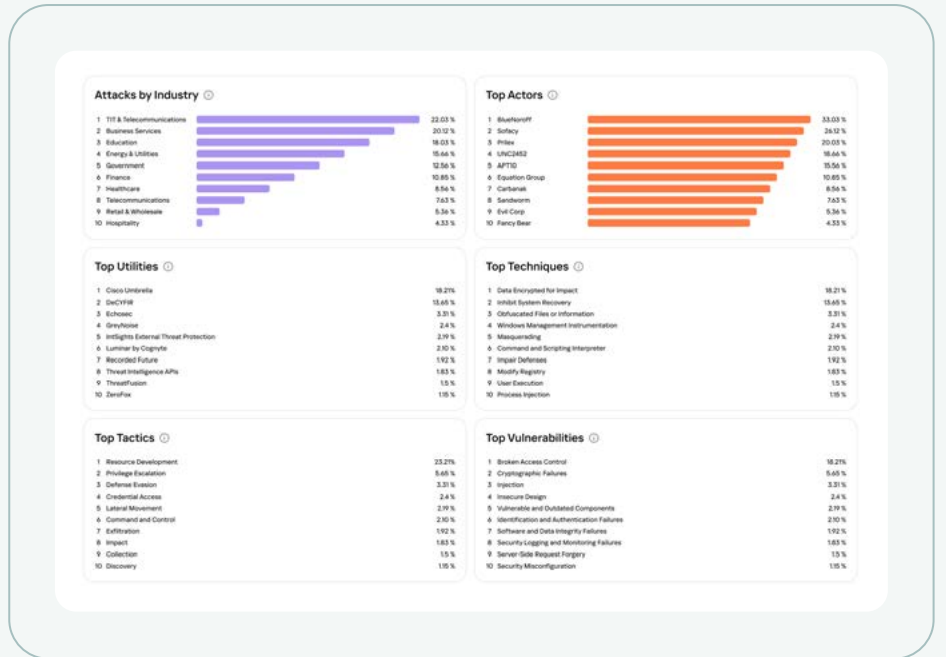
Incidents

- Russia
- Malaysia
- Andhra
- Iran/Georgia

MITRE ATT&CKのテクニック、戦術、手順に関連するSigma/Yara/Suricataのルールにアクセスし、組織に影響する脅威を検知します。



トップ10の統計情報を、業界、アクター、TTP、脆弱性、ソフトウェアについて表示。





日々進化し続けるサイバー脅威の世界には、多数の製品やサービスを通じて取得可能な脅威インテリジェンスデータが潤沢に存在しています。組織は、自らの脅威の状況を理解することで、関連する攻撃に対して戦略面で合理的な対策を講じ、事前に防御することが可能になります。

使用するメリット

予防的な防御アプローチ

組織に対する最も可能性の高い攻撃経路を理解し、効果的な防御戦略を策定します

攻撃対象領域の監視

攻撃者が脆弱性を悪用する前に、セキュリティ上のギャップを特定します

組織に関連する脅威に専念する

ビジネス、業界、地域に最も大きな影響を与える可能性が高い脅威に集中的に対処することができます

戦略的な計画

脅威の状況に関する情報を、投資計画や保護ツール/方法の開発に使用します

情報セキュリティ部門の効率性の向上

関連する脅威や世界的な傾向に関する情報へのアクセスにより、スタッフの作業効率を向上させ、人件費を削減します

脅威の正しい認識に基づいた防衛策

最新の脅威とその世界的な動向を認識し、効果的な防衛策を講じることができます



「彼を知り己を知らば、百戦殆うからず。彼を知らずして己を知らば、一勝一負す。彼を知らず己を知らざれば、戦う毎に必ず殆うし」

孫子

『孫子の兵法 謀攻編』より引用

Kaspersky Threat Intelligence

Kaspersky Threat Intelligenceは、世界トップクラスのアナリストやリサーチャーが収集した幅広い情報へのアクセスを提供します。このデータを活用することで、あらゆる組織が今日のサイバー脅威に効果的に対抗できるようになります。

当社は、サイバー脅威の研究における深い知識と豊富な経験、そしてサイバーセキュリティのあらゆる側面に対する独自の分析力を備えています。これにより、Kasperskyはインターポールや各種のCERT機関をはじめ、世界中の法執行機関や政府組織から信頼されるパートナーとなっています。Kaspersky Threat Intelligenceをご利用になることで、最新の戦術的、運用的、戦略的な脅威インテリジェンスを活用できるようになります。



Kaspersky Threat Intelligence

[詳細はこちら](#)

www.kaspersky.co.jp

© 2024 AO Kaspersky Lab.登録商標およびサービスマークは、各所有者の財産です。

#kaspersky
#bringonthefuture