



Wissen, wie Sie sich gegen Ihre Feinde verteidigen: Erkennen Sie die spezifische Bedrohungslage für Ihr Unternehmen.

# Threat Landscape im Kaspersky Threat Intelligence Portal





## Kaspersky Threat Intelligence Portal

# Die aktuelle Bedrohungslage für Ihr Unternehmen über das Kaspersky Threat Intelligence Portal

Die globale Bedrohungslandschaft entwickelt sich ständig weiter. Jeden Tag tauchen neue Angriffsmethoden auf und bekannte Methoden werden immer raffinierter. IT-Sicherheitsteams müssen heute in der Lage sein, Bedrohungen effektiv zu priorisieren. Nur so können sie schnell reagieren. Woher wissen Sie, welche Bedrohungen für Ihr Unternehmen, Ihre Branche und Ihre Region besonders relevant sind?



### Kaspersky Threat Intelligence Portal

Im Bereich **Threat Landscape** finden Nutzer Informationen über Angreifer, die auf eine bestimmte Branche und Region abzielen. Durch die Kombination von Erkennungstechnologien mit globalen Bedrohungsdaten entsteht ein zuverlässiges Bild von der eigenen Bedrohungslage. So erhalten Sie einen vollständigen und regelmäßig aktualisierten Überblick über die Bedrohungen, Ihre potenziellen Gegner sowie deren Taktiken, Techniken und Prozeduren (TTPs).

## Im Bereich Threat Landscape finden Sie Informationen zu Bedrohungen wie:



Geographie



Industrie



Bedrohungsarten



Bedrohungsakteure



verwendete Techniken, Taktiken und Prozeduren (TTPs)



eingesetzte Schadsoftware



relevante Gefährdungsindikatoren (IoCs)

Bedrohungsdaten werden **in Echtzeit über eine Vielzahl von Expertensystemen** erfasst, die Kaspersky seit über 25 Jahren zur Bekämpfung der Cyberkriminalität einsetzt: Kaspersky Security Network sammelt anonyme Daten von Millionen von Nutzern weltweit. Dazu werden Dateien von Web-Crawlern, Bot-Farmen, Spam-Fallen, Honeypots, Sensoren, passivem DNS und Partnern sowie aus dem öffentlichen Internet und dem Darknet automatisch verarbeitet. Wir selbst nutzen diese Daten seit einem Vierteljahrhundert und erzielen damit immer wieder Bestnoten in unabhängigen Tests und externen Bewertungen. Die Threat Research Teams von Kaspersky analysieren all diese Daten sorgfältig. Dabei kommen moderne automatisierte Systeme wie Sandboxes, heuristische Engines und Ähnlichkeitstools zum Einsatz, um aus der Fülle der Daten garantiert verifizierte und stets aktuelle Informationen zu gewinnen.

Weitere Informationen



# Funktionsweise

## Kaspersky Threat Intelligence: Quellen

KSN-  
Telemetrie

Sensoren

Web-Crawler

Bot-Farmen

Spam /  
IoT-Fallen

Passives  
DNS

Partner  
und OSINT



analysieren

mehr als  
400.000

Schaddateien täglich



Kaspersky  
Threat Intelligence  
Portal



### Profile der Akteure

- Namen/ Alias
- Beschreibungen
- Länder/ Branchen
- TTPs
- Software/ Berichte



### Softwareprofile

- Namen/ Alias
- Beschreibungen
- Akteure
- TTPs
- SIGMA-Regeln



### Kaspersky Threat Intelligence Reporting (APT, Crimeware, ICS)

- YARA-, SIGMA-, Suricata-Regeln
- TTPs
- IoCs



TTPs von MITRE ATT&CK

## Threat Landscape



Filter

Branchen

Länder

Akteure

Plattformen

MITRE  
ATT&CK-Heatmap

Detaillierte  
TTP-Beschreibungen auf  
Grundlage des täglichen  
Datenstroms an Schaddateien

TOP-10-Statistik

- TTPs
- Schwachstellen
- Akteure
- Software
- Branchen

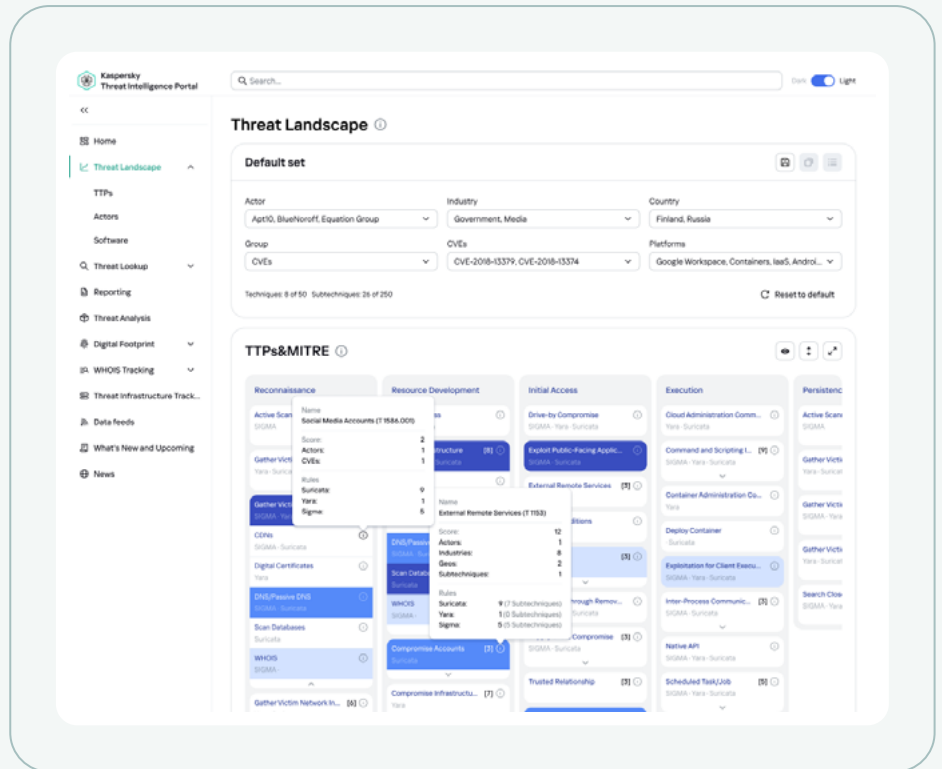
Abwehr-  
maßnahmen

Wir verarbeiten **täglich Hunderttausende von Schaddatei-Samples** und ermitteln deren Geolokalisierungs- und Branchendaten. Anschließend extrahieren unsere proprietären Systeme die zugehörigen TTPs und ordnen die Dateien bereits bekannten Cybercrime-Gruppen und Malware zu. Der Bereich Threat Landscape stützt sich ebenfalls auf einen Strom von Daten über reale Vorfälle aus der ganzen Welt, die wir von unseren Forschungsteams erhalten.

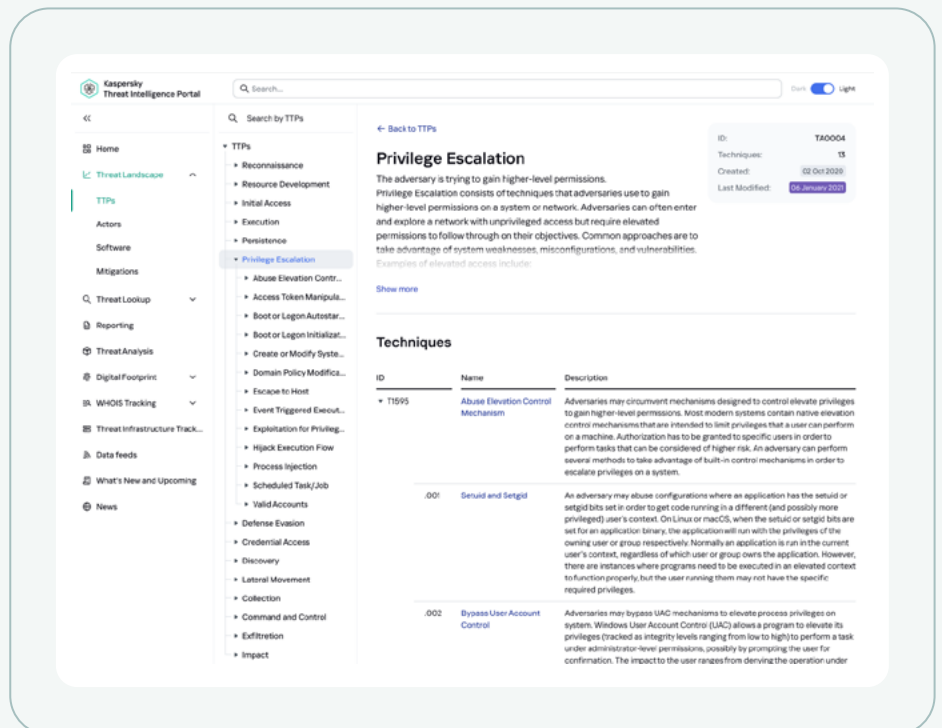
Über eine Filterfunktion können die Nutzer des Kaspersky Threat Intelligence Portals ihre eigene Bedrohungslage **gemäß dem MITREATT&CK-Framework** ermitteln und erhalten so brandaktuelle und detaillierte Informationen über ihre potenziellen Gegner: deren bevorzugte Techniken, Taktiken und Vorgehensweisen, detaillierte Beschreibungen der eingesetzten Malware, Berichte mit detaillierten Beschreibungen des wahrscheinlichen Angriffsverlaufs. All dies mündet schließlich in Empfehlungen zur Eindämmung, mit denen sich die erfolgreiche Umsetzung einer Angriffstechnik verhindern lässt.

# Wichtigste Vorteile

MITRE ATT&CK-Heatmap als **Echtzeit-Überblick über die einzigartige Bedrohungslage** für Ihr Unternehmen. Nach dem Filtern der Ansicht erhält der Benutzer Zugang zu den aktuellsten Daten der letzten 24 Stunden, die von unseren Systemen und Experten durch kontinuierliche Forschung zusammengetragen wurden. Es besteht die Möglichkeit, Layer für internationale Organisationen zu speichern.



Live-Informationen in Echtzeit zu **Techniken, Taktiken und Vorgehensweisen** von Angreifern auf Basis von Kaspersky-Expertensystemen.





Im Bereich Mitigation finden Sie **detaillierte Hinweise** zu Präventiv- und **Schutzmaßnahmen, die Unternehmen ergreifen können**, um Sicherheitslücken zu schließen.

The screenshot displays the 'Application Developer Guidance' page in the Kaspersky Threat Intelligence Portal. The page is titled 'Application Developer Guidance' and includes a sub-header 'Techniques Addressed by Mitigation'. A table lists various techniques with their IDs and descriptions:

ID	Name	Description
T022	Exploitation for Credentials	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...
T064	Hide Artifacts: Resource	Configure applications to use the application bundle structure which leverages the Resource folder location
T074	High Execution Flow	When possible, include hash values in manifest files to help prevent side-loading of malicious binaries
002	OS: Side Loading	When possible, include hash values in manifest files to help prevent side-loading of malicious binaries
T059	User Process Communi...	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...
T047	Privat File Modification	Ensure applications are using Apple's developer guidance which enables hardened runtime
T019	Search Open Websites	Application developers uploading to public code repositories should be careful to avoid publishing sensitive information such as credentials and API keys
T078	Domain Policy Modifica...	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...
T026	Escape to Host	Applications very rarely require administrator permission. Developers should be cautioned against using this higher degree of access to avoid being flagged as a potent...
T087	Event Triggered Executi...	Application developers could be encouraged to avoid placing sensitive data in notification text
T093	Exploitation for Privileg...	Application developers can apply the [LAL_SECURE] property to sensitive screens within their apps to make a more difficult for the screen contents to be captured
T025	High 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...
T074	Process Injection	Application developers should be cautious when selecting third party binaries to integrate into their application

References:

- Microsoft. (2024, November 19). Security Considerations for Trusts. Retrieved November 20, 2023. <https://www.pent.io.uk/news/cyber-security-data/privacy/insights/operation-cloud-trusts.html>
- Microsoft. (2024, November 19). Filter Quarantining on Internet Trusts. Retrieved November 20, 2023. <https://www.cis-cert.gov/ocsp/ocsp/1417-024>
- Microsoft. (2022, September 15). Command-Line Reference - Hashbin Trust. Retrieved November 20, 2023. <https://www.kaspersky.com/resources/whitepapers/whitepapers-media-highlight/whitepapers-media-highlight-2022-09-15>
- Wardell, S. (2016, August 15). Android Badly: 'Trusts' are the Most Sensitive. Retrieved December 1, 2023. <https://www.sans.org/whitepapers/android/2016/08/15/android-badly-trusts-are-the-most-sensitive/>
- Mandiant. (2022, January 19). Remediation and Hardening Strategies for Microsoft 365 to Defend Against. <https://www.mandiant.com/resources/whitepapers/whitepapers-microsoft-365-to-defend-against/>
- https://www.kaspersky.com/resources/whitepapers/whitepapers-media-highlight/whitepapers-media-highlight-2022-09-15

Sie haben Zugriff auf das **branchenweit größte Repository mit Schadakteur- und Malware-Profilen** sowie auf detaillierte Beschreibungen, die von Kaspersky-Experten erstellt wurden.

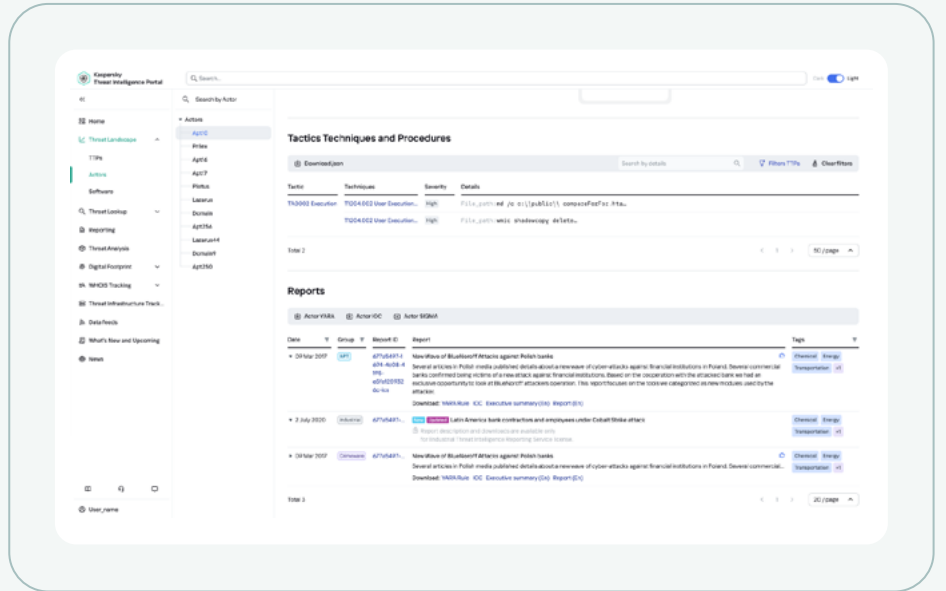
The screenshot displays the 'Apt10' profile page in the Kaspersky Threat Intelligence Portal. The profile includes a description of the group and a world map showing incident locations.

**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 FireEye report describing the actor using Poison Ivy (PIV) back in 2009, targeting U.S. and overseas defense contractors. At that time, the campaign codename used inside PIV was set to "honeybear". Based on this, some security researchers still call the group Menupass.

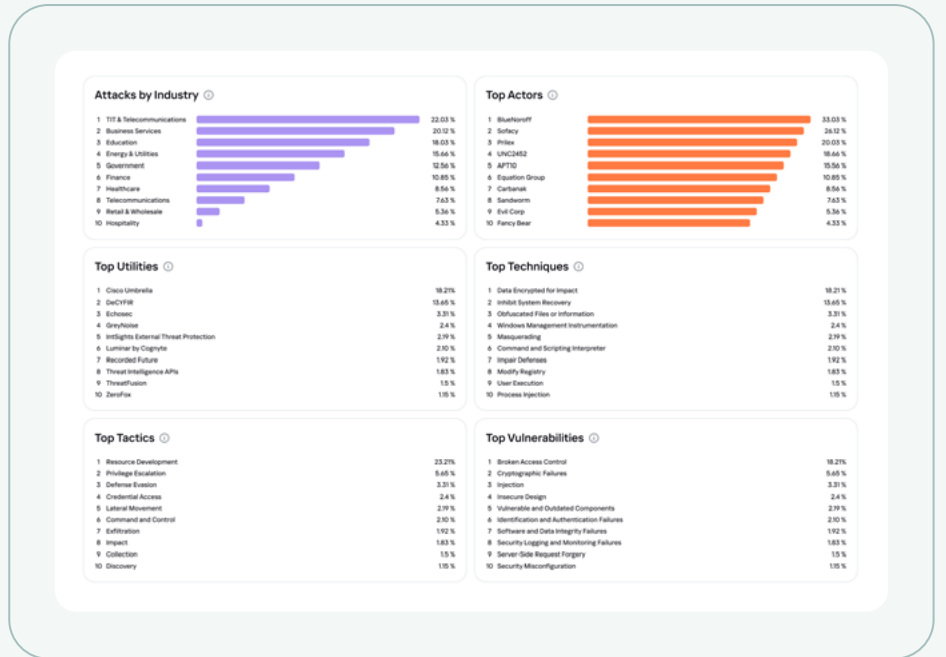
**Incidents:**

- Athens
- Montenegro
- Andros
- Singapore

Zugang zu **Sigma-/Yara-/Suricata-Regeln** in Verbindung mit den von MITRE ATT&CK identifizierten Techniken, Taktiken und Vorgehensweisen, um insbesondere die für Ihr Unternehmen relevanten Bedrohungen zu ermitteln.



**TOP-10-Statistiken** zu Branchen, Akteuren, TTPs, Schwachstellen und Software.







Da sich Cyberbedrohungen ständig weiterentwickeln, gibt es eine Fülle von **Threat Intelligence-Daten**, die über zahlreiche Produkte und Services bereitgestellt werden. Wer die eigene Bedrohungslage kennt, kann strategisch sinnvolle Schritte ergreifen, um relevante Angriffe proaktiv abzuwehren.

## Vorteile

### Proaktive Bedrohungsabwehr

Wer die wahrscheinlichsten Angriffsvektoren für sein Unternehmen kennt, kann auch eine effektive Abwehrstrategie entwickeln

### Monitoring der Angriffsfläche

Sicherheitslücken identifizieren, bevor Angreifer sie ausnutzen können

### Konzentration auf relevante Bedrohungen

Sie können sich auf die für Ihr Unternehmen, Ihre Branche und Ihre Region relevanten Bedrohungen fokussieren

### Strategische Planung

Nutzen Sie die vorhandenen Informationen über die Bedrohungslandschaft bei der Investitionsplanung und der Entwicklung von Sicherheitsmechanismen und -methoden.

### Steigerung der Effizienz von IT-Sicherheitsabteilungen

Steigerung der Personaleffizienz und Kostensenkung durch Zugang zu Informationen über relevante Bedrohungen und globale Trends

### Bewusstsein für Bedrohungen

Kenntnis aktueller Bedrohungen und globaler Trends für eine wirksame Abwehr



Wenn du dich und den Feind kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. Wenn du dich selbst kennst, doch nicht den Feind, wirst du für jeden Sieg, den du erringst, eine Niederlage erleiden. Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen.

## Sun Tzu

aus „Die Kunst des Krieges“

## Kaspersky Threat Intelligence

Kaspersky Threat Intelligence bietet Zugang zu einer Vielzahl an Informationen, die von unseren Weltklasse-Analysten und Forschern zusammengetragen werden. Diese Daten können jedem Unternehmen helfen, aktuellen **Cyberbedrohungen wirksam entgegenzutreten**.

Unser Unternehmen verfügt über fundiertes Know-how, langjährige Erfahrung in der Erforschung von Cyberbedrohungen und einzigartige Einblicke in alle Bereiche der Cybersicherheit. Dies hat Kaspersky zu einem zuverlässigen Partner von Strafverfolgungsbehörden und Regierungsorganisationen auf der ganzen Welt gemacht, darunter Interpol und verschiedene CERT-Einheiten. Kaspersky Threat Intelligence bietet Zugriff auf aktuellen taktische, operative und strategische Bedrohungsdaten.





# Kaspersky Threat Intelligence

Mehr erfahren

[www.kaspersky.de](http://www.kaspersky.de)

© 2024 AO Kaspersky Lab.  
Eingetragene Marken und Servicemarken sind Eigentum  
ihrer jeweiligen Rechtsinhaber.

#kaspersky  
#bringonthefuture