



Know how to defend against  
your enemies — uncover  
the true threat landscape  
of your organization

# Threat Landscape on Kaspersky Threat Intelligence Portal

**kaspersky** bring on  
the future





## Kaspersky Threat Intelligence Portal



### Kaspersky Threat Intelligence Portal

Users have a unique opportunity to assess their threat landscape in the **Threat Landscape** section, which is specifically designed to provide information about attackers targeting a specific industry and region and combines detection technologies with global threat intelligence. This provides complete and up-to-date context about threats associated with your potential adversaries, their tactics, techniques and procedures (TTPs).

# Threat Landscape for your organization on Kaspersky Threat Intelligence Portal

The global threat landscape is constantly evolving, with new attack methods emerging every day, and known methods becoming more sophisticated. Today, it is increasingly important for information security teams to be able to effectively prioritize the threats that need to be responded quickly. But how to focus on the threats that are most relevant to your business, industry and region?

Threat Landscape provides **information**  
**on the threats** associated with:



geography



industry



threat types



threat actors



their techniques, tactics and procedures (TTPs)



malicious software they use



relevant indicators of compromise (IoCs)

Threat intelligence data is being collected **in real time using a variety of expert systems** that Kaspersky has been using to fight cybercrime for over 25 years: Kaspersky Security Network, which receives anonymous data from millions of users worldwide, auto-processing of millions of files per day, web crawlers, bot farms, spam traps, honeypots, sensors, passive DNS, open and dark web sources and partners. We've been using this data ourselves for the last quarter century, giving us the highest scores in independent tests and external reviews. The obtained data is carefully analyzed by Kaspersky threat research teams and processed by modern automated systems such as sandboxes, heuristic engines, and similarity tools, turning it into guaranteed verified and up-to-date information.

[Learn more](#)



## How it works



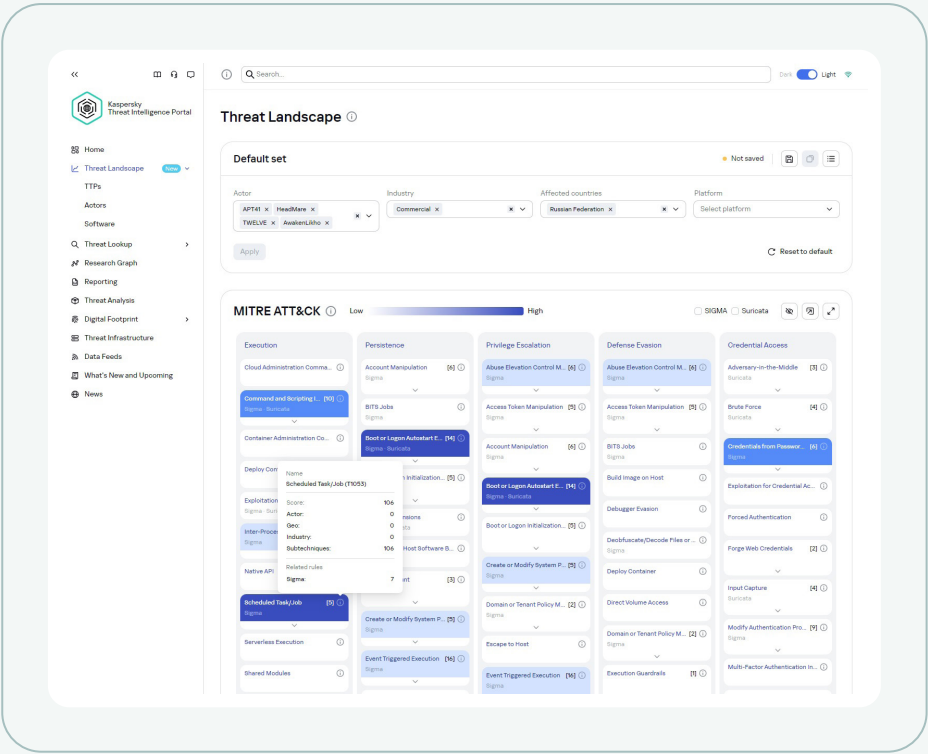
We process **hundreds of thousands of malicious file samples daily**, extracting their geolocation and industry data, then Kaspersky internal systems extract associated TTPs and attribute the files to already known cybercriminal groups and malware. Threat Landscape section is also based on a stream of real incidents data from around the world, which we receive from our expert research teams.

Having applied filters, Kaspersky Threat Intelligence Portal users are able to create their own threat landscape **in alignment with MITRE ATT&CK framework** obtaining the most up-to-date information about their potential adversaries: techniques, tactics and procedures that are most likely to be used to for attack, detailed descriptions of actors, malware and TTPs they use, reports with detailed description of the attacks, and finally get mitigations — specific recommendations that can be used to prevent a technique from being successfully executed.

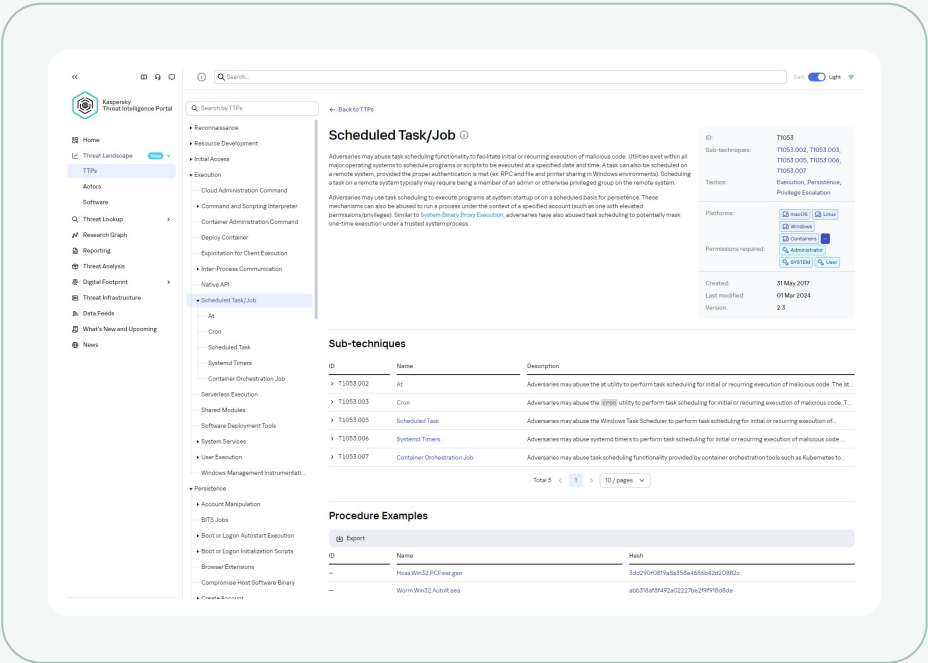


# Highlights

MITTRE ATT&CK heat map to build a **unique threat landscape** for your organization in real time. By applying filters, the user get access to the most up-to-date data, including updates over the last 24 hours, obtained by our systems and experts through continuous research. Ability to save layers for international organizations.



Live real-time information about attacker's **techniques, tactics and procedures** based on Kaspersky expert systems.



Access to the industry's most extensive repository of actor and malware profiles and with detailed descriptions compiled by Kaspersky experts.

[illegible]

Access to Sigma / Yara / Suricata-rules related to the MITRE ATT&CK techniques, tactics and procedures relevant to your organization.

Expensify Threat Intelligence Portal

Home

Threat Landscape

Actors

Software

Threat Lookup

Research Graph

Reporting

Threat Analysis

Digital Footprint

Threat Infrastructure

Data Feeds

What's New and Upcoming

News

Search by TTPs

Cloud Storage Object Discovery

Container and Resource Discovery

Debugger Evasion

Device Driver Discovery

Domain Trust Discovery

File and Directory Discovery

Group Policy Discovery

Log Enumeration

Network Device Discovery

Network Share Discovery

Network Sniffing

Perimeter Policy Discovery

Peripheral Device Discovery

Permission Groups Discovery

Process Discovery

Query Registry

Remote System Discovery

Software Discovery

System Information Discovery

System Location Discovery

System Network Configuration Discov...

System Network Connections Discov...

System Owner/User Discovery

System Service Discovery

System Time Discovery

Virtualization/Sandbox Evasion

Lateral Movement

Collection

Command and Control

Exfiltration

Various utilities and commands may require this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `id` and `who`. On macOS the `dscl /localhost read /Users/$(whoami) user` command can also be used to enumerate user accounts. Environment variables, such as `USER` and `USERNAME`, may also be used to access this information.

Permissions required

Created: 31 May 2017

Last modified: 29 Sep 2023

Version: 1.0

Procedure Examples

Export

ID	Name	Hash
ATT05_DEV	License	629d5a445f4d5a0b0a4d4f050a0705
ATT07_DEV	Software	576d1d776f55522034c40709b6d3b8
ATT09_DEV	StrongPity	4e9f9a703006c075a080a0a000a0
Backdoor/Win64/Supershell/ty		23f019a03230a425f9a0a0a000a0
Backdoor/Win64/Supershell/ty		8d5d179a0a0a0a0a0a0a0a0a0a0a
HEUR/Backdoor/Win64/Supershell/pef		a7b99f9077f0a0a0a0a0a0a0a0a0
Backdoor/Win64/Supershell/ah		67b035c3a0a070a0a0a0a0a0a0a0
HEUR/Backdoor/Win64/Supershell/ee		50273f5a0a0a0a0a0a0a0a0a0a0a
HEUR/Backdoor/Win64/Supershell/ee		01773a0a0a0a0a0a0a0a0a0a0a0a
HEUR/Backdoor/Win64/Supershell/pef		b3f7f4a0a0a0a0a0a0a0a0a0a0a0

Total 10000 < 1 2 3 4 5 > 1000 > 10 / pages >

Rules

Sigma	Suricata	ID	Title	Description	Severity
		a23a4b4b-00a4-433b-9a0a-67a0a033a0a	System Owner/User Discovery via PowerShell	System Owner/User Discovery via PowerShell	Medium
		7a0a0a0a-0a0a-4a0a-8a0a-0a0a0a0a0a0a	System Owner/User Discovery via Suspicious Comm...	System Owner/User Discovery via Suspicious Comm...	Low
		ae0a0a0a-0a0a-4a0a-8a0a-0a0a0a0a0a0a	System Owner/User Discovery via Standard Windows U...	System Owner/User Discovery via Standard Windows U...	Low
		100a0a0a-0a0a-4a0a-8a0a-0a0a0a0a0a0a	Anomaly Parent Process whom are	Anomaly Parent Process whom are	Medium

Total 4 < 1 > 10 / pages >

TOP-10 statistics on the industries, actors, TTPs, vulnerabilities and software.

Expensify Threat Intelligence Portal

Home

Threat Landscape

Actors

Software

Threat Lookup

Research Graph

Reporting

Threat Analysis

Digital Footprint

Threat Infrastructure

Data Feeds

What's New and Upcoming

News

Top Techniques

Popularity

Scoring

11247

11248

11249

11250

11251

Attacks by industry

Agriculture

Health

Manufacturing

Education

Technology

Government

Sigma, Suricata, Reports

45

Sigma

Suricata

Reports

10

15

20

Top Software

Chief

Ngrok

Mindatc

Plugi

Top Tactics

Reconnaissance

Initial access





The ever-evolving world of cyber threats today contains a wealth of **Threat Intelligence data** available through a variety of products and services. By understanding their own threat landscape, organizations are able to take strategically reasonable steps to proactively defend against relevant attacks.

## Benefits of use

### Proactive defense approach

Understand the most likely for the organization attack vectors in order to build an effective defense strategy

### Attack surface monitoring

Identify security gaps before attackers exploit them

### Focus on relevant threats

Ability to focus on the threats that are most likely to affect your business, industry and region

### Strategic planning

Use threat landscape information for planning investments and development of protection tools / methods

### Improving the information security departments efficiency

Increase staff efficiency and reduce staff costs through access to information on relevant threats and global trends

### Treat awareness

Awareness of the latest threats and their global trends for effective defense



If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself, but not your enemy, for every victory gained you will also suffer defeat. If you know neither the enemy nor yourself, you will succumb in every battle

## Sun Tzu

from The Art of War

## Kaspersky Threat Intelligence

Kaspersky Threat Intelligence provide access to a variety of information gathered by our world-class analysts and researchers. This data will help any organization **effectively counter today's cyber threats**.

Our company owns deep knowledge, extensive experience in cyber threat research and unique insights into all aspects of cybersecurity. This has made Kaspersky a trusted partner of law enforcement and government organizations around the world, including Interpol and various CERT units. Kaspersky Threat Intelligence provides up-to-date tactical, operational and strategic threat intelligence.





# Kaspersky Threat Intelligence

[Learn more](#)

[www.kaspersky.com](https://www.kaspersky.com)

© 2024 AO Kaspersky Lab.  
Registered trademarks and service marks  
are the property of their respective owners.

[#kaspersky](#)  
[#bringonthefuture](#)