Kaspersky Threat Intelligence Reporting

kaspersky cybersecurity true to business

2000+

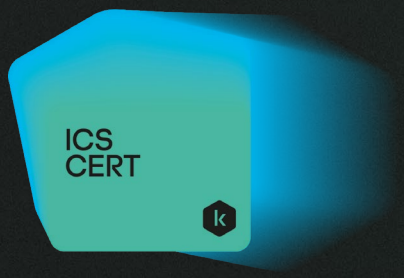
exclusive reports published to date

200+

reports released annually

100 000+

research hours invested each year



Kaspersky Threat Intelligence Reporting

Kaspersky Threat Intelligence Reporting provides organisations with expert-led insight into global cyberthreats, combining technical analysis with real-world context to support informed security decisions.

It delivers a structured view of threat actors, including their tactics, techniques and procedures (TTPs), helping teams understand how attacks are conducted and their potential impact.

Customers gain access to intelligence from ongoing Kaspersky investigations, including findings not publicly disclosed. This supports earlier awareness of emerging threats and more proactive detection and risk mitigation.

Kaspersky's Global Research and Analysis Team and Threat Research experts investigate advanced attacks, including those conducted by state-sponsored APT groups and those leveraging zero-day exploits. In turn ICS CERT is focused on the research of threats targeting industrial systems paired with analysis of potential flaws providing detailed mitigation measures.

Insights are delivered in formats designed to support both rapid response and in-depth analysis, such as:

Flash reports

Timely updates on significant findings, including zero-day attacks and supply chain compromises

Researcher notes

Early-stage research with newly identified indicators of compromise (IOCs)

Detailed reports

Comprehensive analysis, including reverse engineering and mitigation guidance

Kaspersky Threat Intelligence Reporting provides access to intelligence from ongoing investigations, offering visibility into emerging threats. Customers can also access a comprehensive archive of reports covering APT, ICS and Crimeware.

Advanced Persistent Threats (APTs)

APT Reports give your team ongoing access to Kaspersky investigations, including detailed technical data on campaigns as they are identified. This helps you understand advanced threat actor behaviour and assess potential risks, including from threats that may not be publicly disclosed.

Industrial Control Systems (ICS)

ICS Reports help you understand and manage risk in industrial environments, with in-depth intelligence on campaigns targeting industrial organisations and analysis of vulnerabilities in widely used control systems and underlying technologies.

Crimeware

Crimeware Reports help you strengthen defenses against financially motivated attacks by providing timely insight into malware campaigns affecting financial institutions. They include analysis of tools and techniques used against banks, payment processors and related infrastructure, along with guidance to support defensive strategies.

Who it's for

SOC team

Use detailed reports to analyze TTPs, expand detection capabilities and prioritise threats based on context and severity

Security engineers

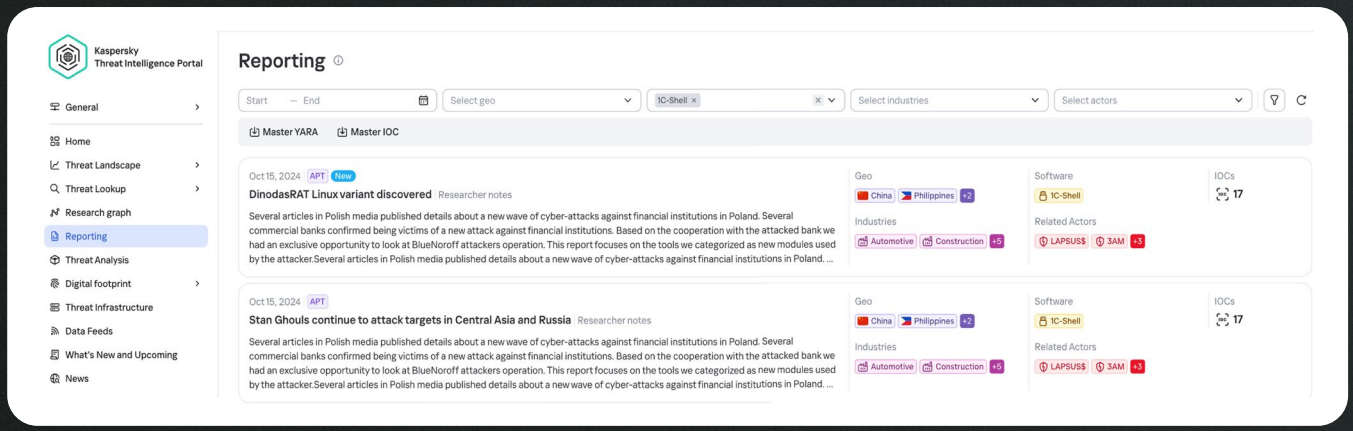
Apply threat intelligence to develop and refine detection logic and compare internal threat models with observed attack patterns

C-level executives

Use global threat intelligence to inform decisions on cybersecurity strategy and investment

Sophisticated, streamlined interface

Kaspersky Threat Intelligence Reporting is delivered through an interface supporting efficient access and analysis.



Filter reports by:

- Targeted industry
- Attributed actors
- Threat category (APT/ crimeware/ICS)
- Targeted country
- Release date
- Report type

Actionable insights

Each report provides extensive data, enabling faster, informed decision-making when time is tight.

Additional content

- Decryption routine
- Extracted configs

MITRE ATT&CK Mapping

- TTPs and how they were used in attack

IoA

- Suricata rules
- YARA rules

IoC

- Registry keys
- Services/ tasks names
- Mutexes
- Domains, IPs, URLs
- File names/ paths
- File hashes

Business value

Vital insight

Support vulnerability assessment with intelligence aligned to threats relevant to your industry and region

Relevant Intelligence

Be prepared for APT activity observed in your sector, including threats that may not yet have reached your environment

Global visibility

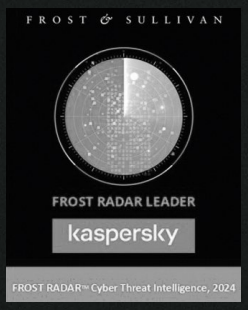
Understand commonly used TTPs worldwide and adapt your defenses to potential cross-region threats

Operational integration

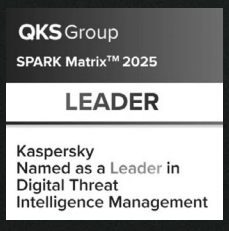
Integrate threat intelligence into your existing workflows with API support, enabling consistent and scalable use of detection data

	Kaspersky Threat Intelligence Reporting	SECURELIST by Kaspersky*	Third-party TI reporting
Source of Intelligence	KSN exclusive insights	KSN exclusive insights	Mostly public data
Indicators of compromise (IoCs)	All available	Limited set for awareness only	Depends on threats visibility
Detection logic (YARA, etc.)	Yes	No	No
MITRE TTPs	Yes	No	No
Available to threat actors	No	Yes	Yes
Minimal time between discovery and delivery	Yes	No	No
Covers unseen high-profile threat actors	Yes	Yes	Limited
Provides additional information on demand	Yes	No	No

*Official Blog from Kaspersky covering information about protection against viruses, spyware, hackers, spam & other forms of malware



Frost & Sullivan named Kaspersky a Leader in the Frost Radar™: Cyber Threat Intelligence, 2024 report.



QKS Group named Kaspersky a Leader in the 2025 SPARK Matrix™: Digital Threat Intelligence Management report

www.kaspersky.com

Consult with an expert

#kaspersky
#truetobusiness