

How we combat cybercrime

GRI 3-3

As we scale security, we develop global cooperation with law enforcement agencies and the professional community, enhancing our expertise and helping improve anti-cybercrime legislation.

We cultivate international cooperation to combat digital offenses

Modern cybercrime knows no boundaries. No single country or organization can cope with this threat alone. A unified effort is required to fight it. That's why we actively cooperate with international organizations, government bodies and law enforcement agencies, helping protect people and companies from cyberthreats.

Kaspersky brings transparency and accountability to this cooperation. Our internal policies establish a clear procedure for handling requests from law enforcement and government bodies. Each request undergoes a legal review according to established criteria and, if necessary, may be rejected or challenged. Moreover, we never provide access to our infrastructure or systems storing user data.

Key documents

- Kaspersky's internal policy governing how law enforcement requests are to be handled (approved in September 2021 by the Company's top managers)
- [Agreement with INTERPOL](#) on jointly combating cybercrime under the Gateway project
- [Agreement with AFRIPOL](#) on cooperation in preventing and combating cybercrime
- Memorandums of cooperation with various cybersecurity agencies and law enforcement agencies

We conduct joint operations with INTERPOL and AFRIPOL

Kaspersky has been cooperating with INTERPOL in the fight against cybercrime since 2014. In 2019, we also signed an agreement to join the Gateway project.

The support we provide to law enforcement organizations includes:

- exchange of expert information on the latest types of malware and cyberattack methods
- participating in joint operations around the world to identify and combat cybercrime
- cybersecurity training and consulting for INTERPOL and other law enforcement agencies

In 2024, we also formalized our collaboration with AFRIPOL by signing a five-year agreement to combat cybercrime in Africa.

Results of joint operations



During the reporting period, Kaspersky announced the results of seven joint operations with INTERPOL and AFRIPOL, which resulted in the arrest of over 2,600 suspected criminals.

Operation [Synergia](#)

September – November 2023

- More than 50 INTERPOL member states helped identify and block infrastructure used for phishing, malware distribution, and ransomware attacks.
- 31 people were detained.
- 26 arrests in Europe, where most of the servers were taken down.
- Hong Kong police took down 153 servers, Singapore police — 86 servers.
- Authorities in South Sudan and Zimbabwe took down the largest number of servers on the African continent and arrested four people.

Operation [Synergia II](#)

April – August 2024

This operation targeted spear phishing, ransomware and stealers¹ around the world. The affected countries were mainly in Europe, Africa and the Asia-Pacific region.

- More than 100 suspects were identified, 41 of whom were arrested.
- Around 30,000 suspicious IP addresses and servers were detected (more than 75% were blocked).
- 59 servers and 43 electronic devices were seized.

Operation [Red Card](#)

March 2025

This operation was carried out as part of AFJOC³, an INTERPOL project to combat cybercrime in Africa, and brought together law enforcement agencies from seven countries (Benin, Côte d'Ivoire, Nigeria, Rwanda, South Africa, Togo and Zambia). Criminals victimized more than 5,000 people.

- There were 306 arrests in the region.
- Approximately 2,000 devices were seized.

Operation [Serengeti 2.0](#)

June – August 2025

This operation brought together law enforcement agencies from 18 African countries and the UK to combat ransomware, BEC attacks and online scams. About 88,000 people fell victim to the attackers.

- More than 1,200 suspects were detained.
- 11,432 malicious infrastructure objects were neutralized.
- \$97.4 million in damages were recovered.

During this operation, experts from our Threat Research Center provided findings on a cryptocurrency investment scam that led 65,000 people to lose \$300 million. As a result, Zambian authorities arrested 15 individuals.

Operation against [Grandoreiro](#)

March 2024

We assisted an INTERPOL-coordinated action that led to the arrest of five administrators who ran the Grandoreiro banking trojan, which targeted over 900 financial institutions in more than 40 countries in North and Latin America, as well as Europe. The banking trojan operators are believed to have defrauded victims of more than €3.5 million

Operation [Serengeti](#)

September – October 2024

An operation to combat ransomware, BEC attacks² perpetrated via corporate email, and other crimes, which caused damage totaling \$193 million. More than 35,000 people were identified as victims of these malicious activities.

- More than 1,000 suspects were detained.
- 134,089 malicious infrastructure objects were neutralized

Operation [Secure](#)

January – April 2025

An operation to detect and block malicious activity involving infostealing malware in the Asia-Pacific region.

- Law enforcement agencies from 26 participating countries and INTERPOL private sector partners joined the operation.
- More than 30 suspects were detained (including 18 in Vietnam).
- More than 20,000 illegitimate IP addresses and domains were blocked.
- More than 40 servers were seized.
- More than 216,000 victims were warned to take immediate protective measures.

¹ A stealer is a malicious program that silently collects large amounts of confidential information from infected devices, such as logins, passwords and payment card details.

² In a BEC (Business Email Compromise) attack, criminals initiate correspondence with a company employee in order to gain their trust and convince them to take actions that are harmful to the interests of the company or its clients.

³ African Joint Operations against Cybercrime.

We expand our partner ecosystem

Together with INTERPOL, Kaspersky provided cybersecurity for major events.

- 2024 Summer Olympics in Paris — Our experts [helped](#) detect phishing attacks and other fraudulent activity. We provided cyberthreat intelligence to INTERPOL as part of Project [Stadia](#), INTERPOL's initiative to protect major international events.
- Singapore Grand Prix, as part of the 2025 Formula One World Championship — We [provided](#) cyberthreat intelligence to protect participants from digital risks.

In addition to INTERPOL and AFRIPOL, our partners in combating cybercrime include:

- [No More Ransom](#) (jointly with Europol) — Over nine years of work, this alliance has helped more than 6 million users recover their data without paying ransom
- Coalition Against Stalkerware
- Geneva Dialogue
- Paris Call for Trust and Security in Cyberspace
- Council of Europe
- World Internet Conference (member of the High Level Advisory Council)
- International Telecommunication Union
- International Organization for Standardization (ISO)
- Smart Africa Alliance and many other organizations



In 2025, the Company became a member of the International Telecommunication Union's Telecommunication Development Sector (ITU-D) and actively participated in global cybersecurity forums.

We research targeted attacks and advanced threats

According to our Kaspersky [Managed Detection and Response \(MDR\) report](#), in 2025, advanced targeted attacks (APTs) were detected in 25% of companies and

accounted for 43% of all high-severity incidents. APTs were detected in all sectors except telecommunications, with IT and the public sector being the hardest hit.

In 2025, we [identified](#) and helped fix a critical zero-day vulnerability in Google Chrome (CVE-2025-2783) used in Operation ForumTroll, a series of sophisticated cyberattacks against Russian organizations. During the research, experts from Kaspersky GReAT discovered for the first time that spyware created by the Italian company Memento Labs (formerly HackingTeam) was being used in real-world attacks.

Additionally, Kaspersky GReAT experts [discovered](#) a new PassiveNeuron cyberespionage campaign targeting Windows Server systems in government, financial, and industrial organizations in Asia, Africa and Latin America (from December 2024 to August 2025).

Moreover, the number of APTs has increased significantly —

by **74%**
compared to 2023

Key trends in cyberthreat landscape

Phishing and spam campaigns

In 2024–2025, we blocked more than 1.4 billion clicks on phishing and scam links worldwide. Attackers prolifically create fake pages impersonating major brands in order to steal users' credentials and money.

Threats in the financial sector and sophisticated attacks

In 2025, the financial sector faced multi-layered threats: attacks on users' smartphones with banking Trojans as well as NFC-relay attacks, attacks through instant messaging apps and telephone fraud and supply chain attacks.

Increased financially-motivated crime

In 2025, the number of unique financial-sector users encountering ransomware increased by 35.7% compared to 2023¹.

Automated attacks and the use of AI

Attackers actively use machine learning and automation to spread malware more efficiently and evade detection by security solutions.

Threats to mobile devices

The number of Trojan banker attacks on Android smartphones increased by 56% in 2025 compared to 2024.

Supply chain attacks

Almost 19,500 malicious packages were found in open-source projects by the end of 2025, representing a 37% increase compared to the end of 2024.

We help develop legislation

With our extensive expertise in critical infrastructure protection, cybercrime, and data protection, we regularly participate in working groups and public consultations to develop international and national regulations aimed at ensuring global cybersecurity.

Kaspersky was an active participant in the development of the UN Convention against Cybercrime, the first-ever universal international treaty on information security, adopted in December 2024. In October 2025, Eugene Kaspersky spoke at a panel discussion on global cooperation in cybersecurity capacity-building programs, which was held as part of the convention signing ceremony in Hanoi.

We also presented our proposals during discussions of the UN Global Digital Compact (adopted in September 2024), focusing on improving digital literacy, training specialists, the safe use of AI and countering stalkerware.

We help develop standards

Kaspersky contributes to the development of international and national standards related to cybersecurity and the secure development of digital solutions.

During the reporting period, Kaspersky experts helped develop an ISO international standard for the Internet of Things.

It describes the key factors that contribute to the reliability and trust of IoT devices and establishes the basis for more secure and sustainable development of IoT ecosystems.

¹ Data for the period November 2024 to October 2025 compared to November 2022 to October 2023.

We share our expertise

We are passionate about sharing our cybersecurity expertise by speaking at major events and organizing our own conferences, such as the Security Analyst Summit, with representatives from law enforcement agencies, government bodies and the academic community. We publish information about cyberthreats in our own [blog](#), threat intelligence reports, malware research, APT analysis and statistics via our securelist blog and conduct free [webinars](#) on cybersecurity.

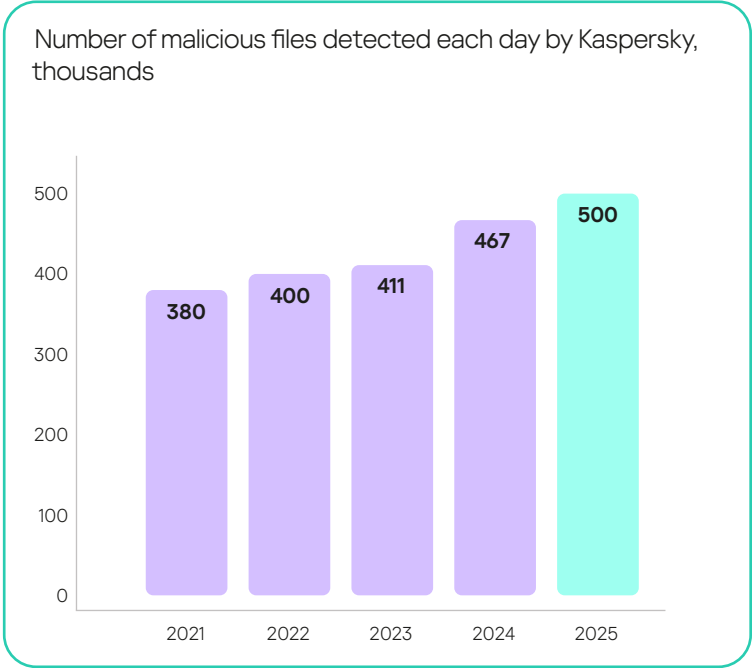
In 2024–2025, our experts participated in numerous cybersecurity forums and conferences, including:

- UN Open-Ended Working Group on Information and Communication Technologies (within an informal dialogue under the auspices of the Chair of the OEWG)
- consultations of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.
- UN Internet Governance Forum, UN Global Digital Compact
- African Cyber Defense Forum.
- Geneva Dialogue working groups
- INTERPOL expert working groups
- World Internet Conference (China)
- Cyber Security Summit (China)
- it-sa Expo&Congress (Germany)
- Singapore International Cyber Week (Singapore)

From November 2025 to March 2026, Kaspersky experts [conducted](#) the “Security Operations and Threat Hunting” online training course for around 40 law enforcement officers from 23 AFRIPOL member states.

Results of work combating threat actors

In 2025, Kaspersky's cyberthreat detection systems detected an average of 500,000 malicious files per day—7% more than in 2024¹.



- GReAT has uncovered evidence linking the HackingTeam successor, Memento Labs, to a new wave of cyberespionage attacks using Dante spyware. The discovery stems from an investigation into Operation ForumTroll, an Advanced Persistent Threat (APT) campaign that exploited a zero-day vulnerability in Google Chrome. The research was presented at the Security Analyst Summit 2025, taking place in Thailand.
- Kaspersky Threat Research expertise center has discovered a new data-stealing Trojan, SparkCat, active in AppStore and Google Play since at least March 2024. This is the first known instance of optical recognition-based malware appearing in AppStore. SparkCat uses machine learning to scan image galleries and steal screenshots containing cryptocurrency wallet recovery phrases.
- Kaspersky's Global Research and Analysis Team (GReAT) have uncovered an ongoing cyberespionage PassiveNeuron campaign, that targets Windows Server systems in government, financial and industrial organizations across Asia, Africa and Latin America. The activity has been observed since December 2024 and continued through August 2025.
- Kaspersky's Global Emergency Response Team has identified a previously unseen ransomware strain in active use, deployed in an attack following the theft of employee credentials. The ransomware, dubbed “Ymir,” employs advanced stealth and encryption methods. It also selectively targets files and attempts to evade detection.

Our plans for 2026

- Help shape the legal framework for combating cybercrime.
- Train and upskill experts, conduct training sessions on relevant cybersecurity topics.
- Collaborate with external organizations and establish partnerships with government institutions to share information on cyberthreats.
- Regularly update software and technology for reliable protection against cyberthreats.

¹ See the [Kaspersky Security Bulletin 2025](#). The statistics in the report cover the period from November 2024 to October 2025.