

How we protect from malware

To protect users from cyberthreats, we develop technological solutions and conduct educational activities, helping people and businesses better understand digital risks and how to protect themselves from them.

Why this matters

As technology evolves, the number of cyberthreats also grows. In 2025, Kaspersky solutions detected an average of 500,000 new malicious files daily, a 7% increase from 2024. These figures clearly illustrate the scale of the threats facing users and organizations.

Experts note that cyberattacks are becoming increasingly sophisticated, with attackers exploiting software vulnerabilities, stolen credentials, increasingly targeting supply chains, and using AI-based tools. In these circumstances, incorrect approach to cybersecurity can lead to extended business downtime and serious financial losses. For private users, it can result in the loss of data and funds.

Main types of cyberthreats

Our solutions protect users and organizations from a wide range of cyberthreats. These include, for example, various types of malware: [viruses](#), [worms](#), [Trojans](#).

Malware can also be classified according to its purposes. For example:

- **Spyware** can track the victim's location, record their screen, and monitor the victim's activity in instant messengers and browsers, as well as record the victim's surroundings using a camera and microphone.
- **Infostealers (password stealers)** can collect and send large amounts of confidential information from infected devices to attackers, such as user's logins and passwords, payment card data, and cryptocurrency wallets.

- **Ransomware** encrypts data on a private or corporate device and then demands a ransom for decryption. Wipers are another type of malware that permanently destroys data, making it impossible to recover from the attack.

Cyberthreats can also be classified according to how they are distributed:

- **Web threats** are malicious software that infects devices via the internet.
- **Local threats** are distributed via removable USB drives, CDs and DVDs or disguised installers.

In 2025, [web threats](#) were detected on the devices of 27% of users globally, and local threats were detected on the devices of 33% of users globally. Windows remains attackers' primary target: 48% of users were targeted by different types of threats throughout 2025. For macOS, this figure was 29%.

Globally, compared to 2024, in 2025, detections of password stealers increased by 59%, spyware by 51%, and backdoors by 6%.

Individual users and businesses can also fall victim to [phishing](#), scams, phone fraud and [DoS attacks](#).



Alexander Liskin

Head of Cyber Threat Research at Kaspersky

"Vulnerabilities remain the most popular way for attackers to penetrate corporate networks, followed by the use of stolen credentials. Hence the increase in both password stealers and spyware we have seen this year. Supply chain attacks are also common, including attacks on open source software. This year, the number of such attacks increased significantly, and we even saw the first widespread NPM worm, Shai-Hulud."

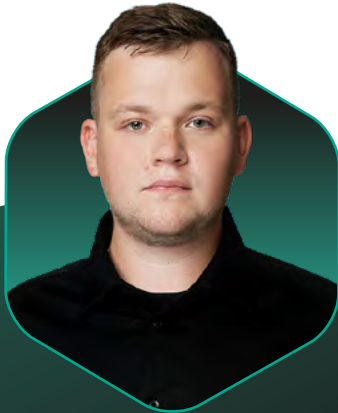
We are responding to the rise in mobile threats

Attackers are increasingly targeting data on smartphones. In 2025, Kaspersky solutions blocked a [worldwide total](#) of 14 million attacks involving malware, adware or unwanted mobile software.

Adware remains the most widespread mobile threat, accounting for 62% of all detections in 2025. Over 815 thousand new unique installation packages including 255 thousand mobile banking Trojans were observed in 2025, showing a decrease compared to the previous year. We observed a massive surge in activity from Mamont banking Trojans.

During the reporting period, new complex mobile threats were also identified: [SparkCat](#) and [SparkKitty](#) for iOS and Android, as well as [LunaSpy](#) for Android disguise themselves as legitimate applications - these malware programs stole user data, including passwords and cryptowallet seed phrases. For example, SparkCat malware is spreading through both infected legitimate apps and lures – messengers, AI assistants, food delivery, crypto-related apps, and primarily targets users in the UAE and countries in Europe and Asia. It scans image galleries for keywords in multiple languages, including Chinese, Japanese, Korean, English, Czech, French, Italian, Polish, and Portuguese.

Modifications of known mobile malware families also appeared. For example, updated versions of the banking [Necro](#) Trojan and the infamous [Triada](#) Trojan, which can modify cryptocurrency wallet addresses during transfer attempts, replace links in browsers, send arbitrary text messages and intercept replies, and steal login credentials for messaging and social media apps. These facts show how quickly mobile threats are evolving.



Dmitry Galov

Head of Kaspersky GReAT in Russia and the CIS

"Lately attackers actively spread mobile malware through instant messaging apps, disguised as photographs, delivery trackers, support apps for telecom operators, medical assistance services, and more."

To protect smartphones from cyberthreats, we recommend that smartphone owners download apps only from official sources and use our reliable protection solutions: [Kaspersky for Android](#) and [Kaspersky for iOS](#).

We protect against ransomware

Risks for businesses and individuals

Ransomware is one of the most dangerous types of cyberthreats to organizations. Ransomware programs are called cryptors because they gain access to a device, encrypt data, and then the attackers demand a ransom from the victims.

Such attacks can cripple companies of all sizes, from large corporations to small businesses, and cause damage in [all regions](#). For example, in 2025 Latin America had the highest share of organizations with ransomware attacks detected (8.13%), followed by the Asia-Pacific region (7.89%), Africa (7.62%), Middle East (7.27%), the Commonwealth of Independent States (CIS, 5.91%) and Europe (3.82%).

A successful attack costs a business far more than the ransom. The downtime, supply chain disruptions, reputational damage and subsequent recovery costs can all be many times greater than the direct payments to the attackers.

Together with VDC Research, we calculated the potential losses to industrial companies globally from downtime due to ransomware attacks in the first three quarters of 2025. We estimate that they could have exceeded [\\$18 billion](#) – and this is only the potential damage caused by the halt of production.

\$18 billion

is the potential global cost of ransomware attacks on organizations in the manufacturing sector globally in just the first 9 months of 2025

14 million attacks

involving malware, adware or unwated mobile software blocked by Kaspersky solutions in 2025

New ransomware tactics

In 2024–2025, we noted several alarming [trends](#) related to cryptors:

- **active use of AI** in the creation of malware
- **prevalence of the Raas** (Ransomware as a Service) model, where individual groups develop cryptors and rent them out to other hackers for a share of the ransom
- **shifting attacks to non-standard penetration points**. Instead of sending phishing emails or searching for vulnerabilities in a web server, attackers are now looking for non-trivial entry points: webcams, IoT devices, and other poorly protected equipment
- **increased average ransom amount** even as threat actors' total income decreases. For example, in 2024, the average ransom size [increased](#) by approximately 50% compared to the previous year, reaching \$4 million¹.



Our solutions

Kaspersky helps its customers protect themselves from the increasingly complex cyberthreat landscape.

We have developed various cybersecurity solutions and [recommendations](#) for organizations to help reduce the cyber risks of attacks and minimize damage.

We have also developed products that demonstrate high effectiveness against various types of malware. Independent tests confirm that users are [effectively](#) protected by Kaspersky Security for Business, Kaspersky Small Office Security, and Kaspersky consumer suite: [Kaspersky Standard](#), [Kaspersky Plus](#), and [Kaspersky Premium](#).

During the reporting period, [Kaspersky Standard](#) received the Top-Rated Product award for 2024 from the independent lab AV-Comparatives, scoring a total of 100 points out of a possible 105. Kaspersky has been awarded this title six times already, and in 2023 the solution was recognized as Product of the Year for the seventh time.

In 2025, [Kaspersky Premium](#) for Windows received an "Approved" certificate of quality based on annual anti-phishing testing by AV-Comparatives. It detected 93% of all phishing links and successfully passed the false positive check.

[Kaspersky Security for Business](#) achieved 100% protection in AV-Comparatives' tests of protection against unauthorized use of credentials, passing all 15 tests. Kaspersky EDR Expert was highly rated for achieving a 100% cumulative Active Response rate in the Endpoint Prevention and Response Test and was certified and awarded Strategic Leader status for the third consecutive year.

In 2025, Kaspersky received the Cybersecurity Leaders award in three categories. The jury noted the development of Kaspersky Container Security (KCS), a solution for protecting container environments at all stages of their lifecycle (by the end of the year, more than 30 KCS deployment projects had been completed), and Kaspersky Unified Monitoring and Analysis Platform (KUMA), a SIEM platform with the integrated AI-powered Kaspersky Investigation and Response Assistant (KIRA).

Kaspersky also received awards for its achievements in cyberthreat analytics—in its Kaspersky Threat Intelligence suite of services—and its work in providing organizations with up-to-date data on attacker techniques and tactics for building proactive defenses.

In addition, Kaspersky continues to actively participate in [No More Ransom](#), an international initiative that it helped to found. This project was created in 2016 with the aim of helping ransomware victims regain access to their encrypted data without paying money to the attackers.

Members of the alliance, including Europol, the Dutch police and cybersecurity vendors, share expertise, knowledge, and decryption tools that help recover data encrypted by ransomware.

How we closed a loophole for attackers

Our incident response experts regularly identify and address vulnerabilities exploited by ransomware.

We participate in incident investigations, helping to close vulnerabilities before they can be exploited.

In 2025, while analyzing a [MedusaLocker](#) ransomware attack on a company in Brazil, Kaspersky specialists identified a vulnerability in ThrottleStop, a legitimate utility that the virus used to gain privileged access to the system.

Result

We immediately reported the issue to the utility's developer and quickly added detection for the new exploit to our products, thereby closing another hole used by ransomware.

¹ According to a report published by Sophos, a software development company.

We provide the latest information on cyberthreats

To effectively combat cyberthreats, we provide organizations with access to the [Kaspersky Threat Intelligence](#) suite of services, which delivers up-to-date data on attackers' tactics, techniques, and procedures. The Kaspersky Threat Intelligence Portal is a single point of access to reliable threat intelligence. Users can also access a free version of the portal: [Kaspersky Open TIP](#). You can request access to this service [here](#).

>200

private cyberthreat reports published annually

>900

APT groups and operations continuously monitored by Kaspersky

We regularly share insights into cyberattacks at industry events and in the media. For example, GReAT experts analyzed the activities of the [FunkSec](#) ransomware group and published a report on its methods. They discovered that it features a unique password-based mechanism that controls its operation modes. Without a password, the malware performs basic file encryption, while providing a password activates a more aggressive data exfiltration process in addition to encryption to steal sensitive data. Notably, code analysis showed that FunkSec was actively using generative artificial intelligence to create its tools.

We improve digital literacy

Kaspersky conducts special research and surveys as well as lifestyle guides and tips to raise awareness about cyberthreats that people face in real life, often without even realizing it:

- [Scams targeting lovers or the lovelorn](#). With Valentine's Day coming up, we examined a special breed of scams aimed at lovers, married couples, and single people.
- [Is this love or stalking?](#) Kaspersky privacy experts explained how to spot red flags in digital relationships

- [Travel safely and comfortably](#). Ahead of summer we shared a guide on the best apps for travelers to help them plan a comfortable vacation trip, focusing on tips how to stay connected, find bearings in a new place or good food and get around safely.
- [Growing up online](#). In collaboration with the UAE Cyber Security Council we released a report on the online behavior of parents and children in the UAE, aiming to uncover trends, habits, and concerns associated with internet usage. One of the key findings showcased that 33% of children in the UAE play computer games that are not suitable for their age.

- [The digital illusion: millennials and the risks of online trust](#). Our research revealed a concerning stat – 70% of millennials rarely verify the authenticity of the people they engage with online, leaving them vulnerable to cyber risks such as identity fraud, misinformation, and emotional deception.

In 2024–2025, in partnership with other organizations, we released several interesting studies to the general public.

Our plans for 2026–2027

- Research various schemes and cyberthreats and provide relevant analytics in new reports
- Conduct and publish research and surveys to inform users about the various cyberthreats they may face
- Release our annual global reports on ransomware attacks, mobile threat landscape, etc.