Combating cybercrime

Our goal is to protect the world against cybercrime. Effectively combating cybercrime requires the joint efforts of the entire community, so we cooperate with law enforcement agencies and help improve legislation in this regard.

Key documents

- Kaspersky's internal policy governing work with requests from law enforcement agencies[1] (approved in September 2021 by the Company's senior executives);
- Agreement with INTERPOL on jointly combating cybercrime;
- Memorandums of cooperation with various cybersecurity and law enforcement agencies.

How we work with law enforcement agencies

Threat actors or hackers most commonly commit cyberattacks for financial gain. However, their motives can also be personal or political. Cybercrimes are committed by individuals and organizations that use advanced methods and are technically savvy.

Cybercrimes have serious consequences for both companies and individuals. They primarily result in financial losses, as well as a loss of trust and reputational damage. Cybercrime knows no borders, and no country or organization can tackle it alone. This task requires a comprehensive approach and joint efforts.

Law enforcement agencies often seek advice from IT companies that have a high level of expertise in cybersecurity. Kaspersky actively assists in the investigation of cybercrimes. At the same time, we take the issue of transparency in our joint work very seriously: we have a clear procedure for working with requests from law enforcement agencies, which is regulated by our own internal policy, and criteria for the legal verification of each request. If a request does not meet our criteria, we may reject or challenge it. It is important to point out that we do not provide access to our infrastructure or data.

[1] Processing Law Enforcement and Government Requests for Disclosure of Data.

Objective

Assist in investigating cybercrimes

Cybercrime knows no borders, which is why Kaspersky regularly takes part in operations and investigations conducted jointly with the global IT security community and international organizations such as INTERPOL, law enforcement agencies and national Computer Emergency Response Teams (CERT). We provide our expertise and all the technical information needed to investigate cybercrimes. We also regularly conduct trainings.

Solutions

Protect cyberspace together with INTERPOL

We began cooperating with INTERPOL in 2014 when we signed the first agreement to jointly combat cybercrime. In 2019, we concluded a new five-year agreement, which significantly expanded the scope of our interaction.

Our support for INTERPOL

- We share expert information with INTERPOL on the latest types of malware and cyberattack methods.
- We take part in joint operations around the world to identify and stop cybercrime.
- We conduct cybersecurity training programs and consult employees of INTERPOL and other law enforcement agencies.

How we assisted INTERPOL in 2022–2023:

- Our specialists assisted INTERPOL in the operations Africa Cyber Surge and Africa Cyber Surge II, which aimed to combat cybercrime in Africa.
- We organized training on “Incident Response” and “Malware Analysis” for more than 100 law enforcement representatives from different countries under the auspices of INTERPOL.
- Vitaly Kamlyuk, Head of Kaspersky’s Global Research & Analysis Team in the Asia-Pacific region, made a presentation at the INTERPOL Global Cybercrime Conference (IGCC) 2023, in which he provided an overview of the world’s largest computer worm epidemics, described the measures that have been taken to combat them, and explained what lessons the Company has learned from these events and how this experience will help us prepare for the next wave of vulnerabilities.
- Kaspersky took part in operation Synergia – spanning more than 50 INTERPOL member states – focused on the disruption of malicious infrastructure involved in phishing, malware, and ransomware attacks.

Support international cooperation

Kaspersky works closely with numerous international organizations and law enforcement agencies, takes part in joint operations, cyber threat investigations and cyber diplomacy, and promotes the development of an open and secure internet.

33
international and Russian cyberspace defense partners

>10
memorandums of understanding signed with international organizations and government agencies

>60
organizations involved in the exchange of new malware samples

For example, as part of the No More Ransom Project, created together with Europol and other partners, we are helping ransomware victims in 30 countries recover their encrypted data without paying ransom. Over its seven years of operation, this project has helped roughly 2 million users recover their data worldwide.

Our partners in combating cybercrime and promoting the sustainable development of the digital space

- INTERPOL
- No More Ransom initiative
- Coalition Against Stalkerware
- Geneva Dialogue
- Paris Call for Trust and Security in Cyberspace
- Council of Europe
- Cybermalveillance.gouv.fr (GIP ACYMA) (France)
- Renaissance Numérique (France)
- World internet Conference (as a member of the High-Level Advisory Committee)
- China Industrial Control System CERT (industry partner)
- Industry IoT Consortium (United States)
- International Telecommunication Union
- International Organization for Standardization (ISO)
- Alliance for the Protection of Children in the Digital Environment (Russia)
- ANO Digital Economy (Russia) and many others

We also readily share our cybersecurity expertise by speaking at major conferences and events such as the RSA Conference and Virus Bulletin, publishing information on our own blogs and hosting free webinars on cybersecurity. In addition, in 2023, we expanded the free service features on the Kaspersky Threat Intelligence portal, which helps find information about cyberthreats in real time.

In 2022–2023, Kaspersky expanded cooperation with international and national organizations as part of its efforts to combat cybercrime. The Company signed several important agreements, including cooperation agreements with national cybersecurity centers and memorandums of cooperation with Korea University, the UAE Cybersecurity Council and the Italian Ministry of Education.

At the 2022 World internet Conference in China, Kaspersky received the World Leading Technology award for developing the Kaspersky Automotive Secure Gateway solution, and CEO Eugene Kaspersky was awarded the title of Special Contributor for his services in promoting global cybersecurity cooperation.

In 2023, Kaspersky received an award from the Alliance of Public Private Cybercrime Stakeholders (founded under the auspices of the Singapore Police Force) for its contribution to creating a cyber-resilient world.

In addition, we have helped generate feedback and proposals for the draft Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, which is being developed under the auspices of the United Nations (UN). We also submitted our proposals as part of the UN Global Digital Compact initiative, with a focus on improving digital literacy.

In 2022–2023, our experts took part in numerous forums and conferences on cybersecurity, including:

- UN Open-Ended Working Group on ICT (as part of an informal dialogue under the auspices of the Working Group chair);
- Fifth intersessional consultation of the UN Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes;
- African internet Governance Forum;
- Session on digital security as part of the UN Global Digital Compact initiative;
- Working groups of the Geneva Dialogue;
- INTERPOL Global Cybercrime Conference;
- UN Internet Governance Forum;
- Business 20 (B20) format as part of the G20.

In addition, we work with more than 60 other IT companies around the world by exchanging malware samples.

Objective

Improve the legislative framework

Today's technological challenges require a more flexible and adaptive legislation. Threat actors are constantly refining their techniques, so laws must be able to effectively respond to new threats. In addition, improved legislation helps standardize legal mechanisms worldwide, which allows for the more efficient exchange of information and extradition of criminals.

Solutions

Improve legislation to combat cybercrime

Kaspersky regularly takes part in drafting legislation, policies and other documents that aim to ensure cybersecurity around the world. Our experts share their knowledge and experience in protecting critical infrastructure, combating cybercrime, protecting data and other related topics. As numerous countries tighten their cybersecurity regulation, we are receiving more and more requests from national, regional and international organizations to provide expert assistance. Some of this expert content is available on our cybersecurity policy blog.

We consistently provide stakeholders with information regarding cybersecurity and cybercrime matters at the United Nations level. Since 2020, we have been actively participating in the UN informal dialogue under the auspices of the chair of the Group on developments in the field of information and telecommunications (ICTs), where discussions are held about various cybersecurity issues, measures to boost trust in cyberspace and the development of expertise. During the reporting period, the Company took part in two meetings at which it presented its proposals on the use of AI with an emphasis on cybersecurity, as well as comments on the annual OEWG report.

Our contribution to combating international cybercrime

Participation in the Africa Cyber Surge operation

The information security sector in Africa is less advanced compared to other regions, rendering its countries more susceptible to cyberattacks. To help INTERPOL combat cybercrime in Africa, Kaspersky provided the international organization with threat intelligence during the Africa Cyber Surge operation.

The first part took place from July-November 2022, and included a series of measures to gather intelligence against the hackers, while the second – Africa Cyber Surge II – began in April 2023 and lasted four months, encompassing 25 African countries. Along with other INTERPOL partners, Kaspersky provided the agency with indicators of compromise (IoC), including information about malicious servers, phishing links and domains, and fraudulent IP addresses.

What was the result?

With Kaspersky's assistance, investigators managed to detect compromised infrastructure and apprehend threat actors suspected of committing cybercrimes in Africa. The operation resulted in the arrest of 14 individuals and revealed network infrastructure that was used to cause more than US$40 milllion in financial losses.

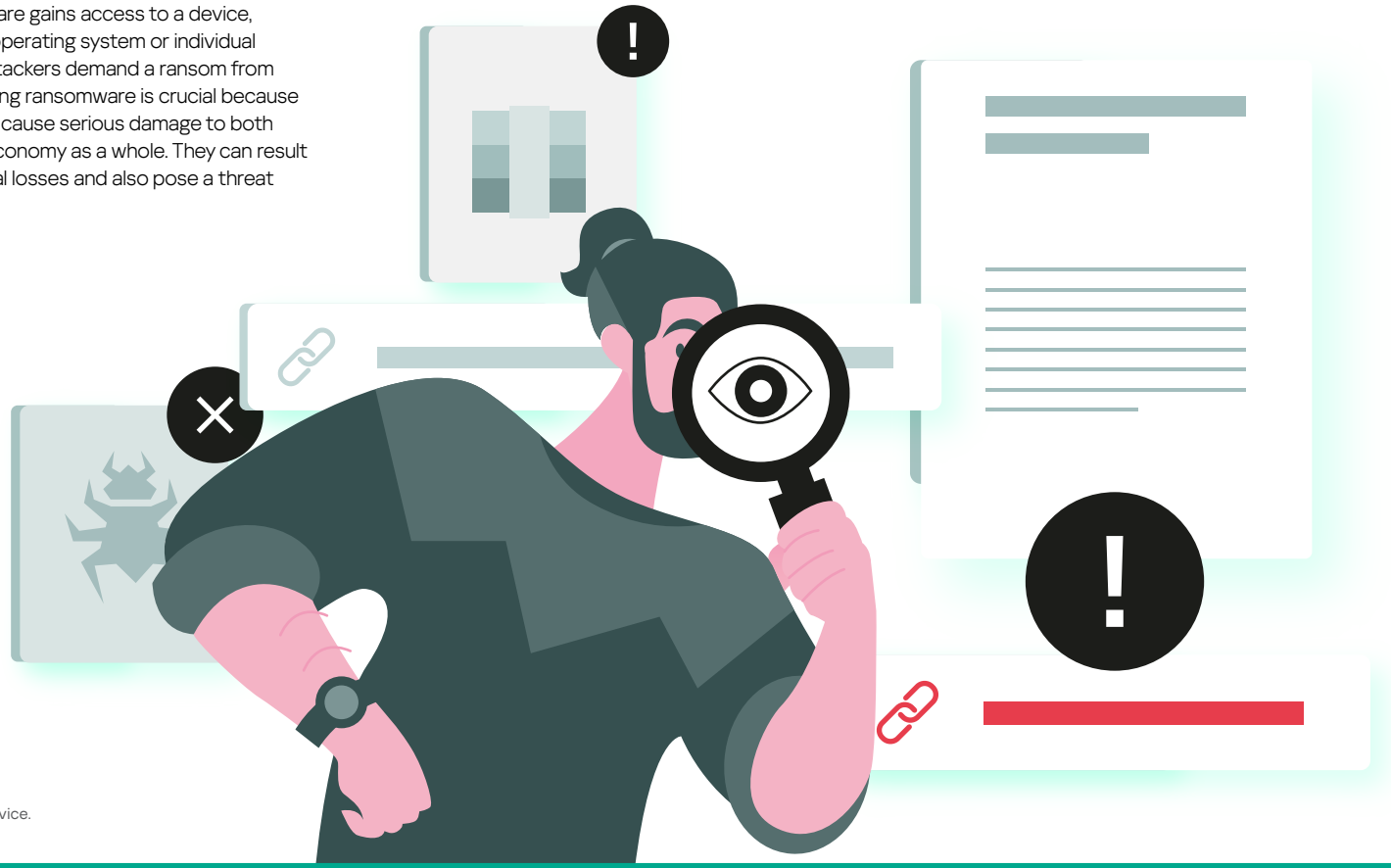
"The Africa Cyber Surge II operation has led to the strengthening of cybercrime departments in member countries as well as the solidification of partnerships with crucial stakeholders, such as computer emergency response teams and internet service providers. This will further contribute to reducing the global impact of cybercrime and protecting communities in the region".

Jurgen Stock,
Secretary General of INTERPOL

Objective

Protect users against ransomware

Ransomware programs are called encryptors because their malicious software gains access to a device, encrypts the entire operating system or individual files, and then the attackers demand a ransom from the victims. Combating ransomware is crucial because ransomware attacks cause serious damage to both individuals and the economy as a whole. They can result in substantial financial losses and also pose a threat to public security.



[1] Ransomware-as-a-Service.

Solutions

We reveal attack patterns, analyze the hackers' tools and update our own decryption utilities as part of the No More Ransom initiative.

During the reporting period, Kaspersky:

- Discovered an attack using zero-day vulnerability in the Microsoft Common Log File System (CLFS). Our Behavioral Detection Engine and Exploit Prevention components detected attempts to execute elevation-of-privilege exploits on Windows servers belonging to SMBs in the Middle East, North America and Asia.
- Updated decryption tool for victims of Conti ransomware. Kaspersky updated the publicly available decryption tool on the Noransom portal to a version that was used to attack commercial companies and government agencies.
- Analyzed the Lockbit 3 builder. Lockbit is one of the most common types of ransomware. It is distributed among partners using the RaaS[1] model, offering participants up to 80 percent of the ransom amount. In September 2022, the Lockbit 3 builder was leaked, allowing any user to construct their own version of the ransomware. Kaspersky's global cyber incident response team analyzed the builder to understand the ransomware design methodology and find opportunities for additional analysis. This tool allowed anyone to create their own version of ransomware.

Objective

Investigate targeted attacks and advanced threats

Unlike mass attacks, targeted attacks can attempt to infect the network of a specific company or organization, or even a single server in the network infrastructure. Advanced threats are considered the most dangerous: hackers use a set of sophisticated tools and tactics to carry out targeted attacks in a highly covert manner. With the escalation of geopolitical conflicts, such threats are becoming even more dangerous.

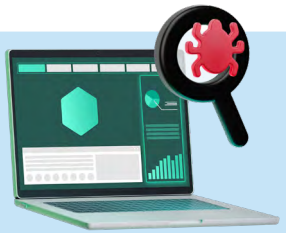
Solutions

Experts from Kaspersky's Global Research & Analysis Team (GReAT) and the Kaspersky Cyber Threat Intelligence team closely monitor numerous advanced persistent threat groups, analyze current trends and predict how the cyberthreat landscape will further develop in order to stay one step ahead of hackers and ensure the security of Kaspersky customers.

Examples of cyber-groups that have been monitored and their attacks:

- **Analysis of threats from the Cuba Ransomware group.** In 2023, Kaspersky released the results of an investigation into a new cyber incident involving the Cuba group. This ransomware group has attacked numerous companies around the world, including retail, logistics, financial and government agencies and industrial enterprises in North America, Europe, Oceania and Asia. Our experts analyzed the infamous cyber-group's history, as well as its techniques, tactics and procedures.
- **Andariel's mistakes and a new malware family.** Kaspersky experts uncovered a new form of malware – a remote access Trojan called EarlyRat – in the arsenal of the Andariel cyber group, which is part of Lazarus. The malware can reach a device through a vulnerability found using the Log4j exploit, or via links in phishing documents.
- **A new APT group called GoldenJackal**. This group has been active since 2019 and usually attacks government and diplomatic organizations in the Middle East and South Asia. Kaspersky experts began monitoring the group in mid-2020. Its main distinction is a specific set of malicious implants that are distributed through removable drives and are used to control target computers, extract data, steal records, collect information about the victim's local system and online activities, and also create and send screenshots.
- **The cyber group ToddyCat is stepping up the complexity of its cyber espionage campaigns**. Kaspersky experts discovered a new set of malicious tools and programs used to steal and exfiltrate data, as well as the methods this active group uses to navigate infrastructure and conduct espionage operations.

Results of efforts to combat cybercrime



From November 2022 to October 2023[1], our Web Anti-Virus detected

112,922,612

unique malicious objects.

During this period, Kaspersky's solutions:

- Blocked 437,414,681 malware-class attacks launched from online resources across the globe;
- Found 106,357,530 unique malicious URLs;
- Prevented ransomware attacks on the computers of 193,662 unique users;
- Blocked miners from infecting 1,140,573 unique users;
- Prevented the launch of malware designed to steal money via online access to bank accounts on the devices of 325,225 users.

These results were achieved with contributions from four of our units: Anti-Malware Research (AMR), the Industrial Control Systems Cyber Emergency Response Team (ICS CERT), Special Cyber Forces and the Global Research & Analysis Team (GReAT).

Our plans for 2024

- Take part in creating a legal framework to combat cybercrime.
- Provide training and advanced training on cybersecurity for parties involved in cyberspace.
- Collaborate and partner with government agencies to share information on cyberthreats.
- Regularly update software and technology to ensure reliable protection against the latest threats.

[1] See Kaspersky's report https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2023/11/28102415/KSB_statistics_2023_en.pdf.