

KASPERSKY ASK THE ANALYST SERVICE

PRODUCT TERMS AND CONDITIONS

These Product terms and conditions ("Product T&C") set forth the special terms and conditions applicable to the Kaspersky Ask the Analyst Service. They are to be read in conjunction with the [Kaspersky Threat Intelligence Agreement](#) ("Agreement"), which also applies to the Product T&C.

These Product T&C are legally binding and govern the use of Kaspersky Ask the Analyst Service ("Service" or "Product") by customers and partners. Accordingly, Kaspersky advises reading them carefully.

By purchasing, accessing and/or using the Product, and/or by clicking the acceptance button, if required by Kaspersky the Customer or Partner ("You") agrees to these Product T&C. The Customer or Partner shall ensure that all individuals or legal bodies involved in purchasing, accepting or using the Product are aware of these terms comply with them.

By accepting the Product T&C on behalf of the Customer or Partner, You represent and warrant that:

- (i) You have the full legal authority to bind the Customer or Partner to the Product T&C;
- (ii) You have read and understand the Product T&C;
- (iii) You agree, to these Product T&C on behalf of the Customer or Partner.

In the event of a conflict between the provisions of these Product T&C and any separate agreement entered into between Kaspersky and the Customer or Partner, the terms of the separate agreement shall prevail.

1. DESCRIPTION

It is unreasonable to expect Customers' experts to fight the war against sophisticated threats alone; they must call on expert third-party assistance. External expertise can illuminate the likely paths of complex attacks and advanced persistent threats (APTs) and provide actionable advice on effective way to eliminate them.

The Ask the Analyst service is commonly used for the following:

- Clarify any details in previously published threat intelligence reports;
- Get additional intelligence for already provided IoCs;
- Obtain details on vulnerabilities and recommendations on how to protect against their exploitation;
- Get additional details on the specific Dark Web activities;
- Get an overview of the malware family, including its behaviour, potential impact, and related activity observed by Kaspersky;
- Effectively prioritize alerts and incidents with the detailed contextual information and IoCs categorization provided in short reports;
- Request assistance in identifying whether the unusual activity detected relates to an APT or a crimeware actor;
- Submit malware files for comprehensive analysis to understand the behaviour and functionality of the sample(s) provided;
- Description of a malware family or a vulnerability including ICS-related information;
- ICS-specific information, such as threat statistics for a region or industry;
- Information about ICS regulations or standards.

The Service allows customers to direct questions to a selected group of Kaspersky researchers. It is offered on a case-by-case basis to customers who require additional capabilities to complement their existing cybersecurity environment.

The Service aims to facilitate communication among experts and empower customers with Kaspersky knowledge and resources.

Benefits

- ▶ **Augment expertise.** Get on-demand access to industry experts eliminating the need to search for and hire hard-to-find full-time specialists.
- ▶ **Accelerate investigations.** Effectively scope and prioritize incidents based on detailed, tailored contextual information.
- ▶ **Respond quickly.** Use Kaspersky's guidance to respond quickly to threats and vulnerabilities by blocking attacks via known vectors.

Each customer's request for Service will be processed through [Customer Company Account](#).

Customers can send the following types of data to Kaspersky for analysis:

- **Request for additional information** - request about a Kaspersky Intelligence Report or particular ongoing research.
- **Files** - Kaspersky will provide an in-depth analysis of the corresponding sample.
- **Hash sums of files, and Malware Family names** - Kaspersky will search the available malware samples for a file with the provided hash. If the file is found, Kaspersky will analyze it. If there are no known samples with this hash sum, further analysis will be impossible. Kaspersky will provide a report on the malware family corresponding to the provided hashes or the malware name.
- **Suspicious URLs, IP addresses or domains** - Kaspersky will check its knowledge base and known indicators of compromise, as well as passive DNS records, for suspicious URLs, IP addresses or domains. A report will be provided with information on findings.
- **Vulnerability** - request for information about a specific vulnerability – including its criticality and how Kaspersky products protect against exploitation.
- **Darkweb intelligence request** - Kaspersky will provide tailored information regarding specific Darknet activity.
- **ICS-related Requests** – a variety of requests including those about ICS threats and vulnerabilities, malware found in the ICS network, ICS cybersecurity standards and regulations, and tailored ICS threat landscape statistics and trends.

Details and Service Level Agreement (SLA) about each type of requests

Additional information

When requesting additional context and/or information about a Kaspersky report, the Customer should include the name of the report and a list of questions. These questions may request more in-depth information about specific analyses or indicators outlined in the report. They may also discuss observations from the Customer and their relation to the activity outlined in the report.

Kaspersky will not count requests that result in minimal effort on their part or that require additional information not clear in the report.

- ▶ Kaspersky reserves the right to provide the Service eight **(8) hours** a day, five **(5) Business days** per week with a response time of forty-eight **(48) hours**.

Comprehensive Malware Analysis

When requesting malware analysis, customers may send suspicious samples, URLs, domains, IP addresses, and hashes. The malware analysis workflow is as follows:

1. Registration of Request for Analysis.

The request is registered and relayed to the Kaspersky virus analyst team.

The request should contain the following information:

- Any context related to the provided malware sample;
- A password-protected archive containing the malicious file (each request should contain only one malware sample);
- MD5 sums of the attached archive and of each file contained within.

2. Initial Analysis and Complexity Level Evaluation.

At this stage a Kaspersky virus analyst will:

- Evaluate the complexity of the request;
- Perform an initial analysis of the provided data (searching for files by hash, or searching for information about IP addresses, domains, or URLs);

Then, the request is forwarded to the Kaspersky Global Emergency Response Team (GERT) team for a deep analysis.

3. Deep Analysis.

A GERT team member performs a deep analysis of the sample.

4. Final Report Preparation.

The time required to deliver the final report depends on its complexity, and can take between up to ten **(10) Business days**.

At this stage, an analyst prepares a final report with detailed information about the analysis findings.

The report includes the following information:

- Sample properties: a description of the sample and detection name based on its malware classification (in case if it's malicious).
- Malware activity: a description of the malware activity on the infected machine.
- Incident Response: suggestions for initial incident response actions.

- ▶ Kaspersky determines the complexity level of each request according to the table below.
- ▶ The complexity level of any request can be adjusted during the analysis.
- ▶ The Final report includes the Initial response and the analysis duration according to the Table of Complexity, stated below.
- ▶ Each submitted request covers the analysis of one **(1) file only**. Any additional files must be submitted as separate requests.
- ▶ Independent files contained within an archive (e.g., ZIP, RAR, or similar) are considered distinct objects and are treated and billed as individual requests.
- ▶ Any related files that are dropped, created, or downloaded by the analyzed object may increase the complexity and duration of the analysis process.
- ▶ In the event that additional or unrelated objects are identified during the analysis process, Kaspersky reserves the right to suspend the work until costs are recalculated and approved by the Customer.
- ▶ Kaspersky may process no more than two **(2) requests** concurrently per customer, unless otherwise agreed upon in writing.

Malware family report

When requesting a malware family report, customers should provide either the name of the malware family or the detection name associated with the samples.

- A single request for a description of a specific malware family or detection name description can provide more detailed context for better detection and response capabilities on the Customer's side.
- A request for additional context can include up to fifteen **(15)** IoCs or observables to help prioritize alerts/incidents that include these objects.

- ▶ Malware Family description – five **(5) Business days** per family.
- ▶ Additional context for a threat (related hashes, URLs, CnCs, etc.) – three **(3) Business days**.

Vulnerability information

A single request about a particular vulnerability must contain no more than five **(5) vulnerabilities** linked by a clearly defined context (e.g., related to the same attack). Otherwise, a request may not be completed and in this case will not account this request against the number of requests, purchased by Customer

Kaspersky may not be able to provide details of vulnerability and how Kaspersky protects against its exploitation (e.g., in case of rare software which we will not be able to check). In that case request will not be completed and will not be counted in the number of requests purchased by Customer.

- ▶ Malware Family description – five **(5) Business days** per family
- ▶ Additional context for a threat (related hashes, URLs, CnCs, etc.) – three **(3) Business days**
- ▶ Provide information on specific vulnerabilities: how critical the vulnerability is, how our products protect from the exploitation – five **(5) Business days**

Darkweb intelligence

Due to the nature of Darknet data, Kaspersky cannot guarantee that specific information will be found. If certain information is not found, Kaspersky will not count such a request toward the number of requests purchased by the Customer.

Please note the following:

- Communication with cybercriminals is outside the scope of the Service.
- Purchase of any data samples offered on the Darknet resources is outside the scope of the Service.
- Deploying a cybercounterattack or conducting any other offensive actions (including providing recommendations for offensive activities) is also outside the scope of the Service.

- ▶ An initial response with the current status will be provided with five **(5) Business days**.
- ▶ Additional information may be requested at this stage.
- ▶ A report with the results (if possible) will be provided with ten **(10) Business days**.

ICS Related Requests

There are several options covering a variety of ICS-related Requests such as:

- Additional information on published ICS Threat Intelligence Reports as well as on any other ICS-related attacks of interest.
- ICS Vulnerability: Request for information about specific vulnerabilities in a particular ICS product to determine the presence of vulnerabilities in the product, their criticality, the necessity of updates, and effective alternative mitigation measures.
- ICS threat statistics for a given period, geographical region, country, or industry.
- Malware analysis - Information on malware samples discovered in ICS (see the "Comprehensive Malware Analysis" section).
- Information on industry-specific regulations, standards, and best practices.

- ▶ An initial response with a request evaluation will be provided with two **(2) Business days**
- ▶ Additional information may be requested at this stage.
- ▶ A report with the results (if possible) will be provided with ten **(10) Business days**

Table of Complexity Level

Complexity Level	Description	Duration (Business days)	Number of requests to charge
1	1. Standalone executable or library file 2. Not packed or packed by a well-known packer 3. No additional files are created	2	1
2	1. A file or a set of linked files (e.g., executables and libraries) 2. Packed with an unknown or customized packer 3. Anti-emulation and anti-debug techniques 4. It may download additional files, but analyzing them is not required	5	2
3	1. A set of linked files (executables and libraries) 2. Packed with an unknown or customized packer 3. Anti-emulation and anti-debug techniques 4. Creates or downloads additional files on the system	10	3

Product Options

The type and price of the Product are indicated in the Proposal, and/or in the Kaspersky's price list in effect at the time the Order is placed. The Customer or Partner declares to know and accept this price list; which shall supersede all previous price lists.

Number of the requests and Subscription Period are stated in the Order and the related Certificate.

Kaspersky will provide the Product option(s) in accordance with the Order, Certificate and these Product T&Cs.

2. PROVISION

- 2.1.** Service Delivery. The Service is available during the Subscription Period after the Order is placed and Customer provides the request and all the required details and/or files to be analyzed.

Requests can be submitted via the [Customer Company Account](#) during the Period.

The Customer can choose a separate category for each request type.

Kaspersky will provide a complete answer for each request. If necessary and agreed upon by the Parties, a conference call and/or screen sharing can be established. Once Kaspersky accepts an inquiry, it will inform the Customer of the estimated time it will take to fulfill the request.

- 2.2.** Based on the Direct agreements, Partners are authorized by Kaspersky to:

- i) resell the Product to End-User(s);
- ii) provide Kaspersky with the details and/or files of the End-User(s) that are required for analysis;
- iii) permit End-User(s) to use the Product solely as a part of Partner products and services subject to the terms of a Partner and End-User Agreement, where Partner and End-user agreement is an agreement that must be executed between a Partner and an End-User for the provision of Partner products and services. This agreement must be no less restrictive and must offer the same level of protection for Kaspersky's rights, as stated in these Product T&Cs.

Partners shall guarantee, that they are authorized by the End-User(s) and have all the necessary agreements with the End-User(s) in accordance with applicable local law, and have all the necessary rights and permissions to use the Service on the End-User(s)'s behalf.

- 2.3.** Trial Use. The Service is available for Trial Use, and is limited to one (1) request during the trial period.

- 2.4.** Term. The Product T&Cs shall commence on (i) the Effective Date, or (ii) the date on which the Customer or Partner accepts these Product T&Cs, by clicking the appropriate button, if required by Kaspersky. The Product T&C will no longer be applicable as soon as the initial Period expires, unless it is extended or renewed by a new Order, or otherwise agreed upon in writing by the Parties, including via email.

- 2.5.** Compensation. The Service fee, payment procedure, and details shall be stipulated in the Order or Direct agreement. Kaspersky's obligations hereunder shall be subject to, and conditioned upon, the Customer's or Partner's confirmation that they have fully accepted and acknowledged the payment terms for the Product and that Kaspersky has received a valid Order for these Products. The Customer or Partner agrees to pay the fee in full, including all applicable taxes. Unless otherwise agreed upon in writing, all amounts are exclusive of value-added tax, sales tax, or other applicable taxes, which shall be paid by the Customer or Partner in addition to the service fees. If payment is not received within ten (10) Business days of the due date, Kaspersky may suspend the Subscription until full payment is received, without prejudice to any other rights or remedies available. Kaspersky may charge interest on overdue amounts at a rate of 15% per annum or the maximum rate permitted by applicable law, calculated from the due date until payment is received.

- 2.6.** Cooperation. The Customer shall provide any information reasonably required by Kaspersky to enable Kaspersky to fulfil its obligations under the Product T&Cs. Kaspersky will not be liable therefor if the required information is not provided to Kaspersky by the Customer or is inaccurate, and/or inadequate for the provision of the Product.

- 2.7.** Technical Support. During the purchased Period, Kaspersky will provide the Customer or Partner with Technical Support, which includes addressing of Customer or Partner problems related to the Product's use provided that it is used properly according to its intended use and in compliance with the documentation and technical specifications, and these Product T&C.

Depending on the nature of the request, Kaspersky Technical Support/Customer Service specialists make commercially reasonable efforts to provide quality support.

Responses within a fixed time period can only be offered as part of [paid services](#).

Customers can contact Kaspersky via [the contact page](#) or use "Contact support" button in Kaspersky TIP, if the need technical support.

2.7.1. Standard Support does not include the following:

- Development of new Product functionality at the request of a User;
- Performance improvement and configuration of user devices;
- Onsite Support and Remote Support sessions (can be purchased as an additional service through Kaspersky Professional Services);
- Assisting users via phone or via web chat while collecting data for analysis and/or applying recommendations;
- Consultations regarding third-party applications and/or operating systems;
- Use of third-party patches to fix vulnerabilities in operating systems and applications
- Integration of Kaspersky software with third-party software (can be purchased as an additional service through Kaspersky Professional Services);
- Software configuration and performance checks by Technical Support/Customer Service specialists as well as advice on network security configuration (can be purchased as an additional service through Kaspersky Professional Services);
- Software training;
- Demonstration, deployment, and configuration of Software (can be purchased as an additional service through Kaspersky Professional Services);
- Analysis and provision of a formal opinion on the causes of a technical error;
- Analysis and investigation of incidents resulting from malware infection (can be purchased as an additional service through Kaspersky Incident Response).

2.7.2. Kaspersky does not provide Support in the following cases:

- Hardware and/or platform-specific software does not meet the minimum system requirements for the Product;
- The Product version is no longer supported (support renewal can be bought upon request).

2.7.3. While Kaspersky makes reasonable efforts to ensure successful installation, stable operation of the Product, and problem resolution, these outcomes cannot be guaranteed in the following cases:

- Software interruptions are caused by hardware issues.
- Software interruptions are caused by incompatible versions of platform-specific software.
- The User is unable or refuses to provide Kaspersky Technical Support/Customer Service specialists with the information that is required to reproduce, analyze, and fix the specific problem.
- The problem arose due to incorrect use or disregard of instructions provided by Kaspersky Technical Support/Customer Service specialists or Kaspersky documentation.

2.7.4. Kaspersky provides Support under the following conditions:

- All commercial and trial versions are supported regardless of the license status.
- A valid license is required for support of all commercial versions of Product.

Some services that are not included in Standard Support may be offered as part of [paid services](#).

- 2.7.5.** Kaspersky guarantees to provide Technical Support/Customer Service for the Product in accordance with the Product T&C.
- 2.7.6.** Kaspersky Technical Support/Customer Service specialists may ask the User to run additional Kaspersky utilities (software tools) if this is deemed necessary to handle a request.
- 2.7.7.** After processing a request and on a periodic basis, Kaspersky reserves the right to periodically ask the User for feedback on the quality of service.
- 2.7.8.** When communicating with Technical Support or Customer Service, the User must provide Kaspersky with timely responses and any information reasonably necessary to properly process the request, including information about the purchased License.

3. LIMITATIONS

- 3.1.** The Service is provided in English via the [Customer Company Account](#). Progress updates will be shared with the Customer upon request.
- 3.2.** Kaspersky may request additional information from the Customer to clarify the scope and increase the likelihood of obtaining valuable information. If necessary, Kaspersky may request additional information from the Customer, such as timeframe, targets, hashes, IOCs, and additional filenames as well as details related to the attack, to support the investigation.
- 3.3.** If Kaspersky does not have enough information to fulfil the request, or does not have an ongoing internal investigation relevant to Customer's request, or if the Customer cannot provide the necessary background information in order to conduct an inquiry, or if Darkweb research is not applicable, - Kaspersky will inform the Customer, that the request cannot be completed and will not count toward the purchased requests.
- 3.4.** The Customer's name shall never be used in any deliverable from Kaspersky.
- 3.5.** Once the response is delivered and all related questions are answered, the request is closed.
- 3.6.** Kaspersky aims to provide the Customer with timely responses as stated in the Product T&C, but does not commit to strict SLAs for the Service due to the nature of the Service.
- 3.7.** The Service is carried out on Business days, Monday through Friday, from 10:00 to 18:30 (GMT+3).

4. MISCELLANEOUS

- 4.1.** Kaspersky reserves the right at any time to improve the Product and/or its components at any time. This includes but is not limited to content, format, delivery, update details, number of records, sources of intelligence and internal manuals).
- 4.2.** If Customer or Partner violates any of their obligations their obligations under the T&Cs or Product limitations or any other legally binding document concluded between Kaspersky and the Customer or Partner related to the Product, Kaspersky may stop or suspend delivery of the Product. No refund is due in such an event.
- 4.3.** The Customer may not remove or alter any copyright notices or other proprietary notices on the Product, related documentation or materials. All rights not expressly granted herein are reserved by Kaspersky and its licensors.
- 4.4.** Kaspersky reserves the right, at any time, to modify these Product T&C by posting the modifications on its website or via email to contact information provided by the Customer or Partner, and to impose new or additional terms or conditions on the use of Product. Such

modifications will be effective immediately upon incorporation into the Product T&C. Continued use of the Product by Customer or Partner will be deemed acceptance thereof.

- 4.5.** Neither party may assign or transfer its rights or delegate its obligations under the Product T&C without the prior written consent of the other party. However, Kaspersky may assign the Product T&C to an affiliate or in the context of a merger or acquisition.
- 4.6.** Unless otherwise is stated in the agreement, the Product T&C are governed by the material laws of Germany. Any disputes arising out of or in connection with the Product T&C shall be subject to the exclusive jurisdiction of the courts in the country where the Kaspersky entity providing the services is located.
- 4.7.** If Kaspersky processes any personal data on behalf of the Customer or Partner, it shall do so in accordance with the Data Processing Addendum. This Addendum is available upon request or as set forth in the agreement.
- 4.8.** Unless the Agreement states otherwise, and to the maximum extent permitted by applicable law, Kaspersky, its affiliates, and its licensors shall not be liable for any indirect, incidental, special, consequential or punitive damages: any loss of profits or revenues, whether direct or indirect; or any loss of data, use, goodwill, or other intangible losses, resulting from the Customer's use of, or inability to use, the Product. This applies even if Kaspersky has been advised of the possibility of such damages. Kaspersky's aggregate liability of under the Product T&Cs shall not exceed the fees paid by the Customer for the Product in the twelve (12) months preceding the event that gave rise to the liability.

THESE PRODUCT T&Cs SHALL BE BINDING UPON, AND INURE TO THE BENEFIT OF, BOTH PARTIES AND THEIR RESPECTIVE SUCCESSORS AND ASSIGNS