

KASPERSKY CRIMEWARE INTELLIGENCE REPORTING

PRODUCT TERMS AND CONDITIONS

These Product terms and conditions ("Product T&C") set out the special terms and conditions applicable to Kaspersky Crimeware Intelligence Reporting and is to be read in conjunction with the [Kaspersky Threat Intelligence Agreement](#) ("Agreement"), that apply to these Product T&C.

These Product T&C are legally binding and govern Customer's and Partner's use of Kaspersky Digital Footprint Intelligence ("Product" or "DFI"), accordingly Kaspersky advises to read them carefully.

By purchasing, accessing and/or using the Product, and/or by clicking the appropriate acceptance button if required by Kaspersky (which shall, to the maximum extent permitted by applicable law, constitute conclusive acceptance thereof), Customer or Partner accepts and agrees to be bound by these Product T&C and shall ensure that all individuals or legal bodies involved in purchasing, accepting and using the Product are aware of the terms of these Product T&C and should comply with the same.

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

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

In the event of any 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 such separate agreement shall prevail to the extent of the conflict.

1. DESCRIPTION

Kaspersky Crimeware Intelligence Reporting provides the heightened intelligence and awareness in high profile cyberespionage campaigns. In addition to using the reports to learn, detect and mitigate risks posed by new attack techniques, large campaigns or recently-developed malware, organizations leverage them for private research purposes, to detect the described threats or to further enhance their security strategy.

Kaspersky Crimeware Intelligence Reporting enables organizations to inform their defensive strategies by providing timely information on ransomware campaigns, hacktivist threats, attacks targeting financial institutions and information on crimeware tools used to attack banks, payment processing companies and their specific infrastructures.

Kaspersky Crimeware Intelligence Reporting focuses on the latest trends in cybercrime, including data breaches sold on the darkweb, financial fraud, ransomware, and ATM/PoS malware. It provides details on new crimeware variants, their distribution methods, and the types of data they target. This reporting track focuses on attacks with financial gain as their primary goal.

Kaspersky Crimeware Intelligence Reporting will provide early notification reports on new Crimeware campaigns as well as updates on active threats.

The repository of reports contains the following types of report: Crimeware reports on specific attacks, Researcher notes, Monthly APT activity report and Early warnings.

Product content, technical features and/or its format is subject to change and not all Product features are available at all times. Customer should be responsible for maintaining secure access credentials. Respectively, Kaspersky shall not be liable for misuse due to Customer's security failures.

Benefits

- Stay updated on the newest threats in the rapidly evolving landscape of cybercrime, allowing Customer to effectively safeguard its business;

- ▶ Learn about the latest crimeware tools and techniques, helping Customer to better predict and prevent potential attacks;
- ▶ Protect customers and its reputation by understanding how cybercriminals might target the organization's data or systems.

Features

- ▶ **Privileged access to** technical descriptions of cutting-edge threats during each ongoing investigation, before public release.
- ▶ **Insights into non-public high profile crimeware.** Not all high-profile threats are subject to public notification. Some, due to the victims who are impacted, the sensitivity of the data, the nature of the vulnerability-fixing process or associated law enforcement activity, are never made public. But Kaspersky reports on all of them to our customers.
- ▶ **Detailed supporting technical data access.** Detailed supporting technical data access. Includes an extended list of Indicators of Compromise (IOCs), available in standard formats and access to our YARA and Suricata rules.
- ▶ **Continuous crimeware campaign monitoring.** Access to actionable intelligence during the investigation (information on threats distribution, IOCs, C&C infrastructure).
- ▶ **Addressing technical and non-technical audiences.** Each report contains an executive summary offering C-level oriented, easy to understand information describing the relevant threat. The executive summary is followed by a detailed technical description of the threat with the related IOCs and YARA rules, giving security researchers, malware analysts, security engineers, network security analysts and APT researchers actionable data to enable a fast, accurate response to the related threat (except for sensitive information on the victims).
- ▶ **Retrospective analysis.** Access to all previously issued private reports is provided during your subscription.
- ▶ **Threat actor profiles** with summarized information on the specific threat actor, including suspected country of origin and main activity, malware families used, industries and geographies targeted, and descriptions of all TTPs used, with their mapping to the MITRE ATT&CK Framework.
- ▶ **MITRE ATT&CK Framework.** All TTPs described in the reports are mapped to the MITRE ATT&CK Framework, enabling improved detection and response through developing and prioritizing the corresponding security monitoring use cases, performing gap analyses and testing current defenses against relevant TTPs.

The Product includes, not limited to, the following information:

Repository of Reports	TYPE
	Crimeware reports on specific attacks
	Researcher notes
	Early warning
	Monthly Crimeware activity report

Crimeware reports on specific attacks includes the following information:

- ▶ **Executive summary** – a brief description of the threat, timeline, geographic distribution, and generic features.
- ▶ **Detailed description** – in-depth analysis of the threat intelligence data: kill chain overview, attack methods, exploits used, malware description, C&C infrastructure and protocols description, victims' analysis, data exfiltration analysis.
- ▶ **Conclusions and recommendations.**
- ▶ **Appendices** – Technical analysis, IOC, C&C, hashes, mapping to the MITRE ATTACK framework and any other available information.

You can also download the following separately:

- ▶ **Executive summary**
- ▶ **IoCs**
- ▶ **YARA rules** (if available)
- ▶ **Suricata rules** (if available)
- ▶ **Master YARA** – all YARA rules from all Crimeware reports
- ▶ **Master IoC** – all IoCs from all Crimeware reports

Researchers notes – brief reports that contain additional information about a specific attack, threat actor or new malware used.

Monthly Crimeware activity report – high-level information about crimeware activity that Kaspersky noticed in different regions during the previous month.

Early warnings – sneak peek at warnings on new or updated malware threats.

You can apply filters using Tags such as: Industry, Geolocation and Threat Actor.

Threat Actor profiles

Kaspersky doesn't discover crimeware attacks only – Kaspersky also monitors and attributes them to specific Threat Actors. Kaspersky collects all the information about Threat Actors in Kaspersky's database and continuously update it.

On the **Threat Actors tab** there are:

- ▶ **General information** – aliases of the threat actor, main activity information, malware families used and links to external references.
- ▶ **MITRE ATT&CK matrix** – all TTP's that the actor uses in their attacks.
- ▶ **Crimeware reports** – reports, IoCs and YARA rules related to the threat actor.

Product Options

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

License or MP License (as defined below) may be purchased for the different Subscription Periods, and allows access to the complete threat intelligence reporting database containing detailed information on each of crimeware attacks discovered by Kaspersky.

Kaspersky provides Product option(s) in accordance with the Order, Certificate and these Product T&C.

Kaspersky Intelligence Reporting Bundles

The Product is included into the following bundles, that are created to simplify access to the various Kaspersky Intelligent Reporting (APT, Crimeware, ICS).

There are few different Kaspersky Intelligence Reporting Bundles available for purchase:

Kaspersky Intelligence Reporting Bundles	Kaspersky Crimeware Intelligence Reporting	Kaspersky Crimeware Intelligence Reporting - Full Reports and IOCs	Kaspersky ICS Threat Intelligence Reporting with MRTI
Kaspersky APT & Crimeware Intelligence Reporting	+	+	-
Kaspersky APT & Crimeware & Industrial Intelligence Reporting	+	+	+

Kaspersky Threat Intelligence Bundles

The Product is included into the following Threat Intelligence Bundles, available for purchase.

Kaspersky Threat Intelligence Bundles	Kaspersky Crimeware Intelligence Reporting	Details of the functional scope
BASIC	All reports and Actor profiles available (10 reports to download)	
ESSENTIAL	All reports and Actor profiles available (15 reports to download)	– Reports
ADVANCED	All reports and Actor profiles available (20 reports to download)	– Actors profiles
EXPERT	All reports and Actor profiles available (50 reports to download)	– IoC and Yara
MAXIMUM	All reports and Actor profiles available. Unlimited downloads	

Kaspersky Threat Intelligence Bundles Composition

PRODUCTS AND SCOPE	BASIC	ESSENTIAL	ADVANCED	EXPERT	MAXIMUM
APT Reporting — Reports — Actors profiles — IoC and Yara	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Crimeware Reporting — Reports — Actors profiles — IoC and Yara	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Threat Infrastructure Tracking	-	-	Country level	Full access	Full access
Kaspersky Threat Lookup — Access to database of threat indicators — Research graph — WHOIS Hinting Rules — 10 saved searches	1 000 requests	2 000 requests	3 000 requests	10 000 requests	50 000 requests
	per 1 year				
Threat Analysis — Cloud Sandbox — Cloud Threat Attribution Engine — Similarity	100 requests	150 requests	200 requests	1 000 requests	3 000 requests
	per 1 year for each technology				
Digital Footprint Intelligence — External perimeter analysis — Dark web monitoring — Discovery of data leaks — Threats detection	-	+	+	+	+

MSSP Bundles Composition

There are different Kaspersky Threat Intelligence Bundles – MSSP, created particularly for MP Partners in the Kaspersky price-list.

License is available for one (1) year of Subscription Period.

PRODUCTS AND SCOPE	BASIC MSSP	ESSENTIAL MSSP	ADVANCED MSSP	EXPERT MSSP	MAXIMUM MSSP
APT Reporting — Reports — Actors profiles — IoC and Yara	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Crimeware Reporting — Reports — Actors profiles — IoC and Yara	All reports and Actor profiles available				
	10 reports to download	15 reports to download	20 reports to download	50 reports to download	Unlimited downloads
Kaspersky Threat Lookup — Access to database of threat indicators — Research graph — WHOIS Hinting Rules — 10 saved searches	1 000 requests	2 000 requests	3 000 requests	10 000 requests	50 000 requests
	per 1 year				
Dark Web search — Forums — IT Forums — Messengers — Ransomware blogs — News	-	+	+	+	+
Cloud Sandbox	100 requests	150 requests	200 requests	1 000 requests	3 000 requests
	per 1 year				
Threat Analysis — Cloud Sandbox — Cloud Threat Attribution Engine — Similarity	100 requests	150 requests	200 requests	1000 requests	3000 requests
	per 1 year				
Digital Footprint Intelligence — External perimeter analysis — Dark web monitoring — Discovery of data leaks — Threats detection	-	5 End-Users	5 End-Users	5 End-Users	5 End-Users
Threat Infrastructure Tracking	-	-	Country level	Full access	Full access

Kaspersky reserves the right at any time to change the composition of the Threat Intelligence Bundles and/or its components in order to improve its value to the Customer or Partner. Actual composition of the bundles is available in the Proposal and/or in the Kaspersky's price list in effect at the time of Order placement, or by request before the Order placement.

2. DELIVERY

- 2.1. License. Kaspersky grants Customer or Partner a non-exclusive, non-transferable (not sublicenseable) limited license to access the Kaspersky threat intelligence reporting database and software allowing to get access to Crimeware Intelligence Reporting or download reports in PDF format, IOC's in openIOC format and YARA Rules in YARA format, solely for Customer's or Partner's internal business purposes, in accordance with the Order, these Product T&C, and the Agreement. The Customer or Partner acknowledges and accepts this License.
- 2.2. MP License. Kaspersky hereby grants MP Partner a non-exclusive, non-refundable, non-transferable, limited, revocable license during the Period to:

- install, integrate, execute, reproduce, display, copy for archival purposes, transmit internally, use the Product and its components on the MP Partner's server/computer system(s) for the purpose of creating, maintaining, providing and supporting MP's products and services;
- provide End-User(s) with access and the right to use the Product solely as part of MP Partner products and services managed by MP Partner in accordance with the Order, conditions of Trial use, and the Product T&C;
- permit End-User(s) to access and use the Product solely as a part of MP products and services subject to the terms of a MP End-User Agreements. MP End-user agreement means an agreement that must be executed between MP Partner and the MP End-User for the provision of MP Partner products and services which is no less restrictive and as protective of Kaspersky's rights, as stated in these Product T&C.

- 2.3.** Trial Use License. Kaspersky grants Customer or Partner a non-exclusive, non-transferable trial license to store, load, install, and use the Product or its components for its internal evaluation business purposes for a period of up to thirty (30) calendar days from the Effective date with no charge. Kaspersky may upon mutual written agreement (including via email), extend the Period of this Trial Use License.

Trial Use License is a time-limited and/or functionality-limited license to use the Product in accordance with these Product T&C. Trial use is available in a full format, with a limited Period, and in format of Demo use, or Pilot project mode. Parameters and limitations, Trial use format is previously agreed by Parties in written (including via email), or stated in the Proposal, or in the Order. Usage of Trial Use License indicates Customer's or Partner's acceptance of any such parameters and limitations.

Kaspersky reserves all rights to provide Pilot projects on a royalty-free and/or commercial basis. All conditions of Trial use, including but not limited to terms of subscription, functionality, scope of the extended support of Kaspersky team, etc. are previously agreed by Parties in written including via email.

Demo use can be limited by functionality, provided at the time of Customer's or Partner's access.

- 2.4.** Delivery. Kaspersky provides the Customer or MP Partner with digital certificate through the encrypted email to download the Product via HTTPs-based service within five (5) working days after the Order for the Product is placed. The Product is delivered in accordance with the Order, Certificate and these Product T&C.

- 2.5.** Compensation. The License fee and payment procedure and details shall be stipulated in the Order and/or in the Direct agreement. Obligations of Kaspersky hereunder shall be subject to and conditioned upon the confirmation from Customer or Partner that the payment terms for the Product have been fully accepted and acknowledged by Customer or Partner and Kaspersky received a valid Order in respect of these Product. Customer or Partner hereby agrees to pay License fee in due order. Unless otherwise agreed in writing, all amounts are exclusive of value added tax, sales tax, or other applicable taxes, which shall be payable by Customer or Partner in addition to license fees. In the event of delayed payment beyond ten (10) Business days after the due date, Kaspersky may suspend the provision of Product 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 fifteen (15) % per annum or the maximum rate permitted by applicable law, calculated from the due date until payment is received.

- 2.6.** Term. The Product T&C shall commence on (i) the Effective Date, (ii) the date of Customer or Partner acceptance of These Product T&C, by clicking the appropriate buttons if required by Kaspersky. The Product T&C becomes not applicable as soon as the Period is expired unless the initial Period is extended or renewed by a new Order, or otherwise agreed by Parties in written, including via email.

2.7. Cooperation. Customer or Partner shall provide the access to its information and property as may be reasonably required in order to permit Kaspersky to perform its obligations hereunder. Kaspersky will not be liable if information or materials provided to Kaspersky by the Customer or Partner are unavailable, inaccurate, and/or inadequate for the Product delivery. Kaspersky will use commercially reasonable efforts to work with the Customer or Partner to correct or clarify any inaccuracies in the Customer's or Partner's information or materials.

2.8. Technical Support. During the term of license purchased Kaspersky provides Customer or Partner with Technical Support, which includes resolution of Customer or Partner problems related to the Product use and being utilized properly according to its intended use and in compliance with the documentation and technical specifications, and these Product T&C.

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

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

Customer can ask Kaspersky via [the contact page](#) or use a dedicated "Contact support" button in Kaspersky TIP, if technical support is needed.

2.8.1. Standard Support does not include the following:

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

2.8.2. 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;
- Product version is no longer supported (support renewal can be bought upon request).

2.8.3. Kaspersky does not guarantee successful installation, stable Product operation, and resolution of problems in the following cases:

- Installation is performed on an infected device.
- Kaspersky Software is installed in a mixed environment together with other incompatible applications.
- 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.

2.8.4. 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](#).

2.8.5. Kaspersky guarantees the provision of Technical Support/Customer Service for the Product in accordance with these Product T&C.

2.8.6. Kaspersky Technical Support/Customer Service specialists may ask the User to execute additional Kaspersky utilities (software tools) if this is deemed necessary for handling a request.

2.8.7. After processing a request and on a periodic basis, Kaspersky has the right to ask the User for feedback on the quality of service.

2.8.8. When communicating with Technical Support/Customer Service specialists, the User must provide Kaspersky with timely responses, information about the purchased License, and any information reasonably necessary to properly process the request.

3. MISCELLANEOUS

- 3.1.** Kaspersky reserves the right at any time to improve the Product and/or its components (including without limitation content, format, delivery, update details, number of records, sources of intelligence and internal manuals). Content of the Product, its features and/or its format is subject to change and not all their features are available at all times.
- 3.2.** If Customer or Partner violates any of its obligations hereof or License limitations stipulated in these Product T&C or other legally binding document concluded between Kaspersky and Customer or Partner related to the Product, Kaspersky may stop or suspend its delivery. No refund is due in such event.
- 3.3.** Unless otherwise is stated in the Agreement, and to the maximum extent permitted by applicable law, in no event shall Kaspersky, its affiliates, or licensors be liable for any indirect, incidental, special, consequential or punitive damages, or for any loss of profits or revenues, whether incurred directly or indirectly, or any loss of data, use, goodwill, or other intangible losses, resulting from Customer's use of or inability to use the Product, even if Kaspersky has been advised of the possibility of such damages. The aggregate liability of Kaspersky under these Product T&C shall not exceed the fees paid or payable by Customer for the Product in the twelve (12) months preceding the event giving rise to the liability.
- 3.4.** Customer may not remove or alter any copyright notices or other proprietary notices of the Product, related documentation or materials. All rights not expressly granted herein are reserved by Kaspersky and its licensors.
- 3.5.** Kaspersky prohibits disclosure of the information contained in the Crimeware Intelligence reports.
- 3.6.** All the information provided subject of the Product shall be properly marked according to the Traffic Light Protocol (TLP) (<https://www.us-cert.gov/tlp>), and Customer hereby agrees to honor the protocol.

For Product deliverables without a TLP but being part of the same publication, the TLP of the report is applicable to all the deliverables.

Customer or Partner shall comply with all applicable restrictions communicated pursuant to the Traffic Light Protocol (TLP), and any further handling restrictions specified in the Product or deliverables. In the event Deliverables are not marked, the TLP of the accompanying report shall apply.

- 3.7.** Kaspersky reserves the right at any time to modify (by posting on its website or via email to the contact provided by Customer/Partner) these Product T&C and to impose new or additional terms or conditions on the Product use. Such modifications will be effective immediately when incorporated into the Product T&C. Continued use of the Product by Customer or Partner will be deemed acceptance thereof.
- 3.8.** Neither party shall assign or transfer its rights nor delegate its obligations under these Product T&C without the prior written consent of the other party, save that Kaspersky may assign these Product T&C to an affiliate or in the context of a merger or acquisition without restriction.
- 3.9.** Unless otherwise is stated in the Agreement, these Product T&C are governed by the material laws of Germany. Any disputes arising out of or in connection with these Product T&C shall be subject to the exclusive jurisdiction of the courts of country where Kaspersky entity rendering the services is located.
- 3.10.** To the extent Kaspersky processes any personal data on behalf of the Customer/Partner, such processing shall be in accordance with the Data Processing Addendum, available upon request or as set forth in the Agreement.
- 3.11.** No delay or omission by either party in exercising any right under this Agreement shall operate as a waiver of that or any other right. A waiver or consent given by a party on any one occasion shall be effective only in that instance and shall not be construed as a bar or waiver of any right on any other occasion. In the event that any provision of this Agreement shall be invalid, illegal or otherwise unenforceable, the validity, legality and enforceability of the remaining provisions shall in no way be affected or impaired. This Agreement may also be amended or modified by a written instrument executed by both the Customer or Partner and Kaspersky or by Kaspersky only as stipulated in clause 3.7.

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