KASPERSKY LAB STUDY: CHILDREN ONLINE

#KLReport

Version 1.0
March 2015

CONTENTS

▶ MAIN FINDINGS

In early 2015, Kaspersky Lab experts carried out a study of the threats encountered in 2014 by users of the Parental Control module in the company's products. The aim was to assess the level of threats faced by children online and to identify the main sources of danger.

The main findings of the study were as follows:

- The Parental Control module, which protects against content that is potentially dangerous for children, was triggered at least once during the year on computers of 4.88% of Kaspersky Lab users that have Parental Control module on their computer;
- More than half (**59.5%**) of users encountered pornography; over a quarter (**26.6%**) landed on websites dedicated to gambling; **every fifth user** stumbled across sites featuring weapons; and almost the same number were confronted by strong language.
- On average, the Parental Control module **was triggered 127 times** per Kaspersky Lab user during the year;
- **About 65%** of computers on which the Parental Control module was triggered in 2014 were located in just ten countries;
- **Russia, India and China** were the top three countries in which users encountered potentially dangerous content;
- **China, US, Germany, UK and Russia** were the countries where the module was triggered most often by dangerous content.

▶ METHODOLOGY

The study was based on data generated when the Parental Control module was triggered by attempts to load websites that fell into one of the categories defined by Kaspersky Lab as not suitable for children. It also used data on the number of unique users who had encountered websites in one of these categories. At the time of writing the report, Kaspersky Lab security products have 14 different categories of websites that are deemed unsuitable for children[1].

Some of these categories are activated in Parental Control by default, others can be activated by parents. Only the most 'dangerous' site categories are activated by default, such as those with adult content, including pornography and violence; sites devoted to weapons, alcohol or drugs; gambling sites; anonymizing services; and sites containing obscene language.

Although all other categories of web sites can also potentially be harmful to children, for the purposes of this report Kaspersky Lab experts confined themselves to data on instances of Parental Control being triggered and the number of users encountering websites included in those categories which are blocked by default. These particular categories were selected in order to assess the scope of the threat as accurately as possible and to avoid including 'harmless' episodes of users of Kaspersky Lab products with Parental Control functionality [enabled?] surfing the Internet.

In this context, 'harmless' episodes are those in which Parental Control was triggered by attempts to load a social networking site, visit an online store, a computer games site or some other resource.

Chat services were also included in the list of 'dangerous' categories for the purposes of this study. This is primarily due to the existence and popularity of video chats that allow people to communicate using their web cameras. In most cases, such services offer anonymous communication, and this type of resource has given rise to an online phenomenon known as webcam sex tourism. Chat services can also be used as a tool for cyber-bullying, another child-threatening phenomenon that was made possible by the advent of the Internet. For technical reasons, we were unable to separate instances of the Parental Control module being triggered by video chats from the bulk of instances in which it was triggered by this website category. It should be kept in mind when viewing the data in this report that not all of the detections in the Chat category were actually caused by video chats.

[1] The list of Parental Control categories includes: "Adult Content", "Alcohol, tobacco, drugs", "Violence", "Weapons", Obscene Language", "Gambling, Lotteries, Sweepstakes", "Internet Communication Media (incl. Chats)", "E-commerce", "Recruitment", "Anonymous Internet Access", "Computer Games", "Religions, Religious Associations", "News Media".

▶ INTRODUCTION. THE FLIPSIDE OF INFORMATION AVAILABILITY

The evolution of the Internet has helped to make information universally accessible: any user, virtually anywhere on Earth can quickly gain access to virtually any data. However, this relatively unrestricted access forces us to take on new responsibility for the effect this information might have on users. Where it concerns grownups, this is hardly a critical problem, but children, who have almost the same access to online information, could be placed at risk if confronted with information or services intended for adults.

Pornography, drugs and alcohol, obscene language, weapons, cyber-bullying and undesirable communication with strangers – these are the main threats that are generally considered relevant when it comes to children on the Internet. Although these are valid concerns, the principal problem related to the security of children online is probably one of control. Children spend most of their time being supervised by their parents or the staff at their schools, but when they turn on their computers or pick up smartphones or tablets, there are far fewer options to keep children away from undesirable information.

In response to this problem various 'parental control' technology have been implemented by the developers of operating systems, search engines and security solutions. These modules aim to minimize the chances of children finding and accessing websites that fall into 'dangerous' categories. However, these modules cannot provide a complete solution to the problem – not least because, for a variety of reasons, they are not used by all the parents whose children access the Internet.

In July 2014, Kaspersky Lab carried out **a joint survey** with a research company called B2B International, in which over 11,000 respondents from 23 countries in North and South America, Europe, Africa and the Asia-Pacific region were asked questions on the IT risks encountered by users of connected devices. The dangers of online content unsuitable for children were among the issues covered by the survey. Based on the results, only 22% of parents who have children aged 16 or younger use technology-based parental control solutions; the rest either do not control their children's online activity in any way or use other methods of control (such as checking browser history, telling their children about the potential dangers of the Internet, etc.).

At the same time, the survey results show that most parents have relatively little trouble answering questions about what their children do online.

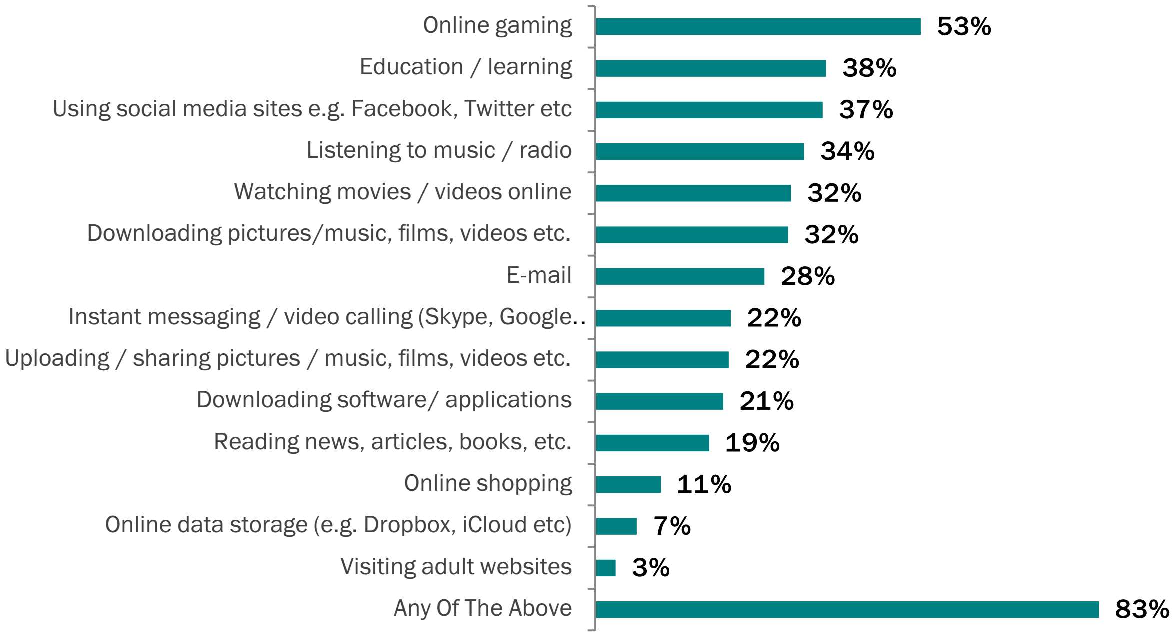

Figure 1. What children use the Internet for, according to their parents. Source: Consumer Security Risks Survey 2014: Multi-Device Threats in a Multi-Device World, conducted by Kaspersky Lab and B2B International

But how far from reality are parents' ideas about their children's online activity? Apart from legitimate and safe sites, what else do their children encounter online, and how often?

To answer this question, Kaspersky Lab experts analyzed statistics produced by the Parental Control modules running on the computers of millions of users across the globe. The results of this research are presented below.

PART 1. GENERAL TRENDS

The Parental Control module for Mac OS X and Windows is included in Kaspersky Lab's consumer security products Kaspersky Internet Security – Multi-Device and Kaspersky Total Security – Multi-Device. This study is based on information related to instances of the Parental Control module being triggered on computers on which these products are installed.

According to Kaspersky Security Network data, in 2014 the Parental Control module was triggered at least once on **4.88%** of Kaspersky Lab users' computers on which technologies designed to protect children against undesirable content are present. In 2013, this proportion was **3.45%**. In absolute figures, **4.88%** is more than 1.5 million users across the globe.

It should be noted, however, that not all of these users encountered sites from categories that are definitely dangerous. Sites in these categories – that is, "adult content", "violence", "weapons", "alcohol and narcotics", "gambling", "obscene language", "anonymous Internet access" and "chats", triggered the Parental Control module at least once during the year on computers of 68.48% of the 1.5 million affected users (about one million users globally).

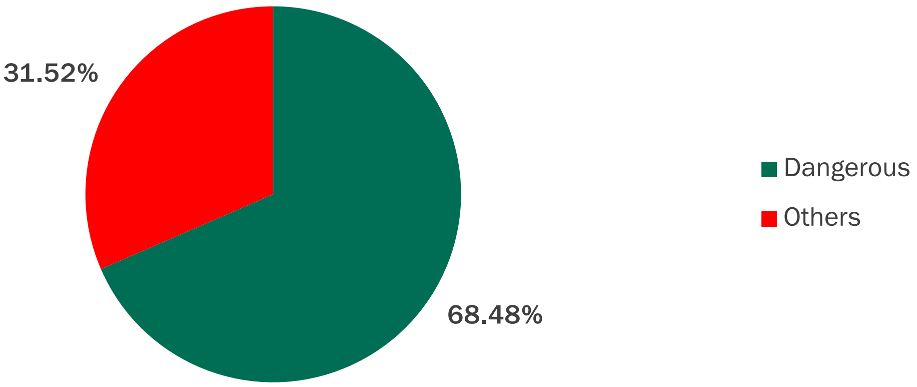

Figure 2. Proportion of users who encountered content that is definitely dangerous for children in 2014

In 2013 the number of Parent Control modules triggered last once for dangerous content was almost 82%.

In the remaining part of this report, we include only statistics from the computers of those users who had encountered, at least once during the year, websites in one or more categories that are definitely "dangerous" for children.

Dangerous Content in 2014

Below, we take a closer look at which "dangerous" site categories of had the largest number of visitors in 2014 and how these figures changed from the previous year.

The table below compares the percentages of users whose Parental Control module was triggered at least once by different site categories during the year. According to the diagram below, the most frequent alerts involved users accessing chat services (67.29%), or being taken to sites that feature pornography (59.56%), gambling (26.66%), weapons (20.29%) and obscene language (19.93%).

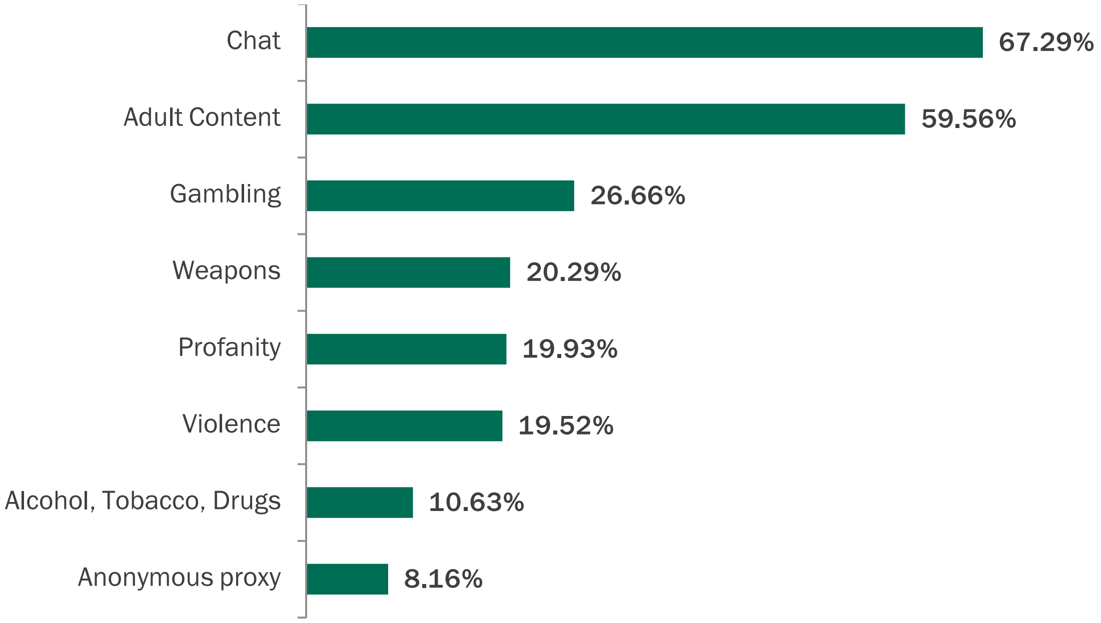

Figure 3. Percentage of unique users who encountered sites included in the dangerous categories in 2014

In 2013 the situation was a bit different:

Category	Percentage of users in 2013, %	Percentage of users in 2014, %	Year-on-year change, %
Chat	49.13	67.29	18.16
Adult content	73.74	59.56	-14.18
Gambling	37.18	26.66	-10.52
Weapons	28.17	20.29	-7.88
Obscene language	26.19	19.93	-6.26
Violence	39.40	19.52	-19.88
Alcohol, Tobacco, Drugs	14.63	10.63	-4.00
Anonymous Internet Access	24.44	8.16	-16.28

Table 1. Changes in the percentage of users who encountered different categories of dangerous sites in 2013 and 2014.

Among the changes that took place in 2014, it is worth noting an increase in the percentage of users who visited various chat sites – up 18.16 percentage points. At the same time, the proportions of users encountering other types of dangerous sites declined. The greatest decrease (19.88 pp) was in the proportion of users who encountered sites in the "violence" category; while the percentage of users who visited services offering anonymous Internet access was down 16.28 pp in 2014. The percentage of users who encountered pornography sites fell 14.18 pp.

Frequency of Parental Control Being Triggered

The percentage of users who encountered each of the unsafe content types is only part of the picture showing the scope of the danger. Looking at **all** instances of dangerous content triggering the Parental Control module (detections) provides an insight into which types of "dangerous" site were most frequently encountered by users.

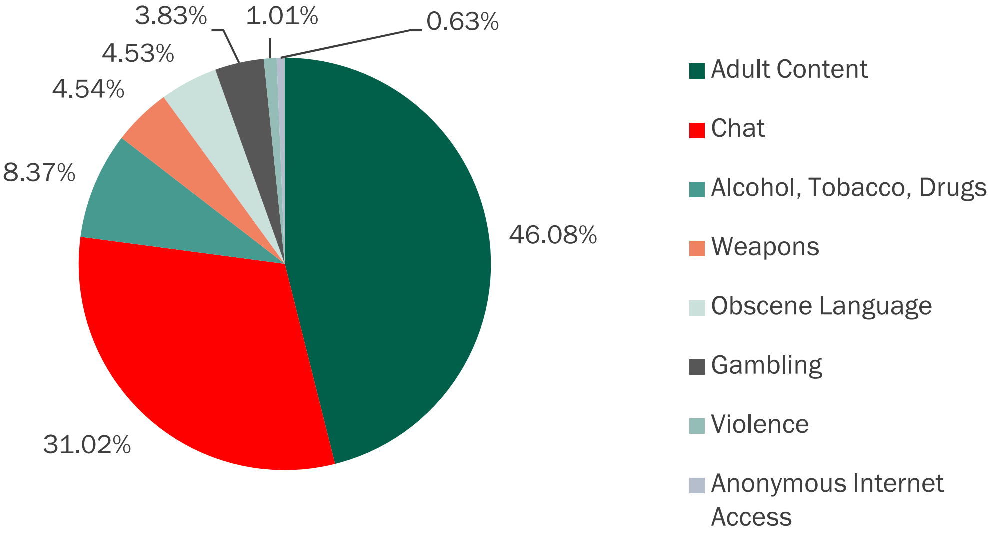

Figure 4. Distribution by site categories of instances of Parental Control being triggered by web pages containing "dangerous" content

The top position in the ranking based on the number of times the Parental Control module was triggered is occupied by adult content (46.08% of all instances). This is significantly ahead of chat, which come next with 31.02%; sites with alcohol, tobacco and narcotics-related content are in third place (8.37%).

The percentage of instances in which the module was triggered by a "dangerous" category is different from the percentage of users who have encountered that type of content. The difference is easily explained: the same user may have encountered sites of the same dangerous category several times.

A relatively accurate indicator of the prevalence of different types of unsafe content is the frequency (the number of times the module was triggered per unique user during the year) with which users encountered each content type on average during the year.

Category	2013	2014	change
Total	158.76	127.28	-31.48
Alcohol, Tobacco, Drugs	24.91	100.16	75.25
Adult Content	142.53	98.47	-44.06
Chat	61.65	58.6	-3.05
Obscene Language	12.06	28.91	16.85
Weapons	11.43	28.45	17.02
Gambling	19.65	18.26	-1.39
Anonymous Internet Access	12.91	9.77	-3.14
Violence	7.25	6.59	-0.66

Table 2. Changes in the frequency with which the Parental Control module was triggered by web pages with dangerous content.

In 2013, the situation was as follows: users most often came across adult content, chats, gambling, sites with obscene language and information about weapons. In 2014, the situation was significantly different. The “Adult” category lost its long-held lead, falling behind sites with information about alcohol, tobacco and narcotics. Visits to adult sites were down by a factor of 1.5. There was a significant increase in the frequency with which sites with obscene language (up by a factor of 2.4) and information about weapons (up by a factor of 2.5) triggered Parental Control. At the same time, the frequency with which sites from other categories were blocked decreased only slightly.

There are two reasons for the almost four-fold growth in the frequency of instances of Parental Control being triggered by web pages with information about alcohol, tobacco and narcotics. First, in the past year, Kaspersky Lab experts significantly improved its technologies that recognize content that is unsafe for children; this content is now detected in more languages than before. Second, according to Kaspersky Lab experts on web content, the number of websites used to distribute drugs is increasing. Because of the anonymity offered by some popular web technologies, drug dealers increasingly prefer to do their illegal business online, with the help of the usual SEO tricks. This means Parental Control is more regularly triggered by this type of content. So although pornography remains the most prevalent type of online content that is unsafe for children, users are almost as likely to come across sites in the “Alcohol, Tobacco, Narcotics” category, most of which are devoted to drugs.

It is worth noting, however, that the percentage of users on whose computers Parental Control was triggered by the “Alcohol, Tobacco and Drugs” category is much smaller than that of many other categories. In other words, the number of users who came across this category is small, but users in this relatively small group encounter this type of information quite often.

It should also be noted that the frequency with which Parental Control was triggered and the percentages of users varied significantly from one country to the next.

▶ PART 2: GEOGRAPHY AND LOCAL VARIATIONS

In 2014, two-thirds (65%) of users whose Parental Control module blocked content, lived in just 10 countries. This is up from 62.71% of total users in 2013.

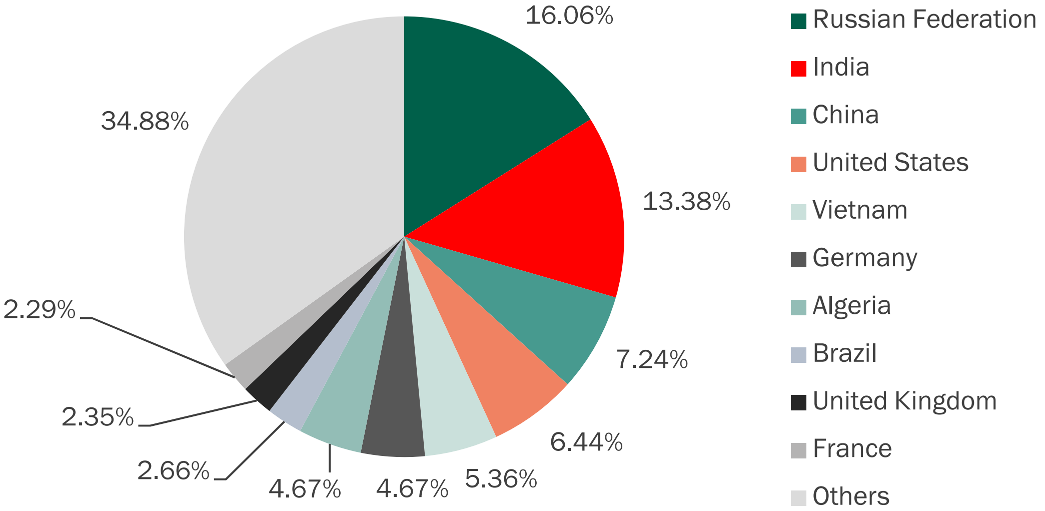

Figure 5. Top ten countries by share of Parental Control users affected by dangerous content in 2014

The list of top ten countries in terms of affected users looked almost exactly the same in 2014 as it did in 2013, with each country's share changing by no more than two per cent. This is hardly a major shift.

Country	2013, %	2014, %	Y-to-Y change (p.p.)
Russia	14.91	16.06	1.15
India	14.13	13.38	-0.75
China	6.50	7.24	0.74
US	7.06	6.44	-0.62
Vietnam	5.45	5.36	-0.09
Germany	4.92	4.67	-0.25
Algeria	3,21	4.67	1.46
Brazil	1,99	2.66	0.67
UK	2,58	2.35	-0.23
France	1,96	2.29	0.33

Table 3. The change in the share of Parental Control users who encountered dangerous content, in each of the top ten countries, in 2013 and 2014.
Key: Green – increase, Red – decrease.

The consistent distribution of users encountering dangerous content over a period of two years reveals little about the prevalence of content dangerous to children. The data is more likely to reflect the stability of Kaspersky Lab's customer base.

Comparing the share of users encountering dangerous content with an analysis of the frequency of detections paints a very different picture.

Country	Frequency	Top 10 countries: % of users affected
China	208.27	7.24
US	191.71	6.44
Germany	164.62	4.67
UK	157.11	2.35
Russia	143.49	16.06
France	115.59	2.29
Vietnam	115.28	5.36
Brazil	104.98	2.66
Algeria	88.51	4.67
India	77.51	13.38

Table 4. Frequency of Parental Control module detections in the top ten most-affected countries in 2014.
Key: Red – higher than average; Green – lower than average

China, the USA, Germany, the UK and Russia lead the list of countries with the greatest frequency of Parental Control detections in 2014. In the previous year the situation was more or less the same, with the exception of China, which jumped from fourth place in 2013 to first place in 2014.

The global frequency rate in 2014 was 127.2 detections per user. The ten countries listed in the table above can be divided in two groups: those that showed higher than average levels of intensity (China, the USA, Germany, the UK and Russia) and those that showed lower than average levels. Users of Kaspersky Lab's products in France, Vietnam, Brazil, Algeria and India had a significantly lower risk of encountering content that was potentially dangerous for children.

The situation in different countries

When looking at the different content types encountered by users in the top ten countries, it became obvious that for almost every country listed some types of content were encountered by a higher percentage of users than the global average.

Country	Adult Content, %	Alcohol, Tobacco, Drugs, %	Violence, %	Obscene language, %	Weapons, %	Gambling, %	Chat, %	Anonymous Internet Access, %
Global average	59.56	10.63	19.52	19.93	20.29	26.66	67.29	8.16
Germany	50.14	13.94	22.08	22.47	23.88	31.12	66.82	7.99
US	49.82	17.04	28.72	20.58	27.56	31.91	71.93	11.36
Russia	64.73	14.09	19.73	29.50	37.97	30.11	59.03	11.30
China	80.20	5.93	6.66	12.71	15.76	21.44	69.58	2.90
UK	51.35	12.04	26.06	18.39	23.96	39.24	63.84	9.30
France	51.66	12.53	23.40	19.89	19.87	36.63	72.44	6.58
Vietnam	55.87	8.39	9.29	24.60	9.72	24	79.80	12.14
India	61.46	9.08	20.14	16.45	12.55	16.65	67.18	5.47
Brazil	59.04	9.38	21.11	21.14	15.48	14.78	75.93	3.48
Algeria	64.81	6.89	16.32	14.58	11.67	27.66	68.65	8.46

Table 5. Percentage of Kaspersky Lab Parental Control users encountering content dangerous to children in the top ten most-affected countries in 2014.
Key: Red – significantly higher than global share of users; Green – significantly lower than global share of users; Blue – more or less the same as global share of users.

For example, in Germany the most "popular" categories were Alcohol, Tobacco, Drugs, Violence, Weapons and Gambling; while in the US it was Alcohol, Tobacco, Drugs, Violence, Weapons, Gambling, Chats and Anonymizing services.

It is also worth noting that the share of users encountering Adult content in Russia, China, India, Brazil and Algeria was noticeably higher than that in other countries in the top ten.

Country	Adult Content	Alcohol, Tobacco, Drugs	Violence	Obscene language	Weapons	Gambling	Chat	Anonymous Internet Access
Global average	98.47	100.16	6.59	28.91	28.45	18.26	58.6	9.77
Germany	172.09	181.76	5.11	59.69	7.001	12.7	48.34	6.26
US	126.16	151.65	15.32	33.05	14.77	30.74	106.62	10.81
Russia	81.84	196.65	4.62	34.74	67.17	17.44	34.19	6.15
China	144.18	50.69	2.02	40.41	14.6	9.49	114.75	5.1
UK	96.06	99.52	8.4	39.87	6.93	36.13	107.14	21.63
France	73.56	100.87	7.42	37.7	5.52	16.82	66.53	3.55
Vietnam	89.61	5.82	7.53	14.42	19.28	10.93	69.39	5.01
India	78.25	8.82	3.16	19.78	4.41	7.61	33.57	6.23
Brazil	87.05	100.2	4.47	17.81	3.85	8.28	49.14	9.17
Algeria	67.54	23.85	6.17	13.27	7.34	8.27	52.62	10.26

Table 6. The frequency rate of Parental Control detections in 2014 in the top ten most-affected countries.
Key: Red – significantly higher than global Frequency rate; Green – significantly lower than global frequency rate; Blue – more or less the same as the global frequency rate.

The frequency of Parental Control detections for different content categories does not depend on the number of unique users encountering such content. The difference between the frequency of detection and the proportion of users encountering that particular threat is likely to reflect one of three basic threat situations.

The first type of situation: When the frequency of detection is noticeably lower than the global level for that content category, this indicates that the risk of users regularly encountering that type of dangerous content is fairly low. For instance, in 2014 9.08% of users from India encountered at least once content dedicated to the sale or distribution of narcotics, alcohol or tobacco. However the frequency level for the category Alcohol, Tobacco, Drugs in India in 2014 was only 8.82 detections per user, while the global frequency for the category was as high as 100.16 detections per user. This means that drugs, tobacco and alcohol are not significant online content threats for children surfing the web in this country.

The second type of situation: When the proportion of users encountering a certain type of dangerous content is more or less the same as the global share, but the frequency level is much higher, this could indicate a relatively high risk of encountering such content in that particular country. For example, in the UK the percentage of PC users on whose computers Parental Control detected at least one attempt to download a website offering anonymous web access is almost the same as the global share: 9.3% for the UK compared with 8.18% globally. However, the frequency rate is much higher: 21.63 detections per user in the UK compared with 9.77 globally.

The third type of situation: When both frequency and the share of users are significantly higher than the global level, it indicates that the risk of encountering this type of dangerous content is fairly high and parents should pay extra attention to what their children are doing online.

Local Variations

According to Kaspersky Lab's research findings, the level of risk for dangerous content categories differs significantly from country to country.

Adult Content

In 2014, adult content was the biggest threat for users in China (144.18 detections per user affecting 80.2% of Kaspersky Lab Parental Control users), Germany (172 detections per user affecting 50.14% of Parental Control users) and in the US (126.16 detections per user affecting 49.82% of Parental Control users).

Country	% of users that encountered the threa	Frequency
Global average	59.56	98.47
Germany	50.14	172.09
China	80.20	144.18
US	49,82	126.16
UK	51.35	96.06
Vietnam	55.87	89.61
Brazil	59.04	87.05
Russia	64.73	81.84
India	61.46	78.25
France	51.66	73.56
Algeria	64.81	67.54

Table 7. Adult content: Frequency of detections and the share of Kaspersky Lab's Parental Control users hit in the top ten most-affected countries in 2014.

Vietnam, France, Brazil, Russia, India and Algeria were lower on the list in terms of frequency, but the overall percentage of users encountering adult content in these countries was noticeably high.

Alcohol, Tobacco, Drugs

Country	% of users that encountered the threat	Frequency
Global average	10.63	100.16
Russia	14.09	196.65
Germany	13.94	181.76
US	17.04	151.65
France	12.53	100.87
Brazil	9.38	100.2
UK	12.04	99.52
China	5.93	50.69
Algeria	6.89	23.85
India	9.08	8.82
Vietnam	8.39	5.82

Table 8. Alcohol, Tobacco, Drugs: Frequency of detections and the share of Kaspersky Lab's Parental Control users hit in the top ten most-affected countries in 2014.

Content relating to alcohol, tobacco and drugs was a real threat for users in Russia, Germany, the US and France. Both the level of frequency and the share of users in these countries were especially high. This kind of content was also prevalent in Brazil and the UK, with users in Vietnam and India in less danger.

Violence

Country	% of users that encountered the threat	Frequency
Global average	19.52	6.59
US	28.72	15.32
UK	26.06	8.4
Vietnam	9.29	7.53
France	23.40	7.42
Algeria	16.32	6.17
Germany	22.08	5.11
Russia	19.73	4.62
Brazil	21.11	4.47
India	20.14	3.16
China	6.66	2.02

Table 8. Violence: Frequency of detections and the share of Kaspersky Lab's Parental Control users hit in the top ten most-affected countries in 2014.

In 2014, the leader of this category was the US. The frequency of detections per user (15.32) and the share of users (28.72%) encountering violence-related content was remarkably higher than the global average (6.59 detections and 19.52% of users) and higher than the levels seen in other top ten countries. The UK is in second place with 8.4 detections and 26.06% of users, with France in third place with 7.42 detections and 23.4% of users. For Parental Control users in China, this category represented the smallest threat (2.02 detections and 6.66% users).

Obscene language

Country	% of users that encountered the threat	Frequency
Global average	19.93	28.91
Germany	22.47	59.69
China	12.71	40.41
UK	18.39	39.87
France	19.89	37.7
Russia	29.50	34.74
US	20.58	33.05
India	16.45	19.78
Brazil	21.14	17.81
Vietnam	24.60	14.42
Algeria	14.58	13.27

Table 9. Obscene language: Frequency of detections and the share of Kaspersky Lab's Parental Control users hit in the top ten most-affected countries in 2014.

Websites containing strong language were detected most often on the PCs of users in Russia, Germany, the US, the UK and France. The highest level of frequency was registered in Germany where results were almost double the global average. Incidents of strong language were less noticeable, but still prevalent in China and India.

Weapons

Country	% of users that encountered the threat	Frequency
Global average	20.29	28.45
Russia	37.97	67.17
Vietnam	9.72	19.28
US	27.56	14.77
China	15.76	14.6
Algeria	11.67	7.34
Germany	23.88	7.001
UK	23.96	6.93
France	19.87	5.52
India	12.55	4.41
Brazil	15.48	3.85

Table 10. Weapons: Frequency of detections and the share of Kaspersky Lab's Parental Control users hit in the top ten most-affected countries in 2014.

Content relating to weapons posed a big threat for users in Russia. While the average global frequency rate was 28.45 detections per user and the share of users encountering this kind of content was 20.29%, in Russia these indicators were as high as 67.17 detections per user in terms of frequency and 37.97% in terms of share of users.

Online content relating to weapons was also encountered by many users in the US, Germany and the UK, but overall frequency remained low.

Gambling

Country	% of users that encountered the threat	Frequency
Global average	26.66	18.26
UK	39.24	36.13
US	31.91	30.74
Russia	30.11	17.44
France	36.63	16.82
Germany	31.12	12.7
Vietnam	24	10.93
China	21.44	9.49
Brazil	14.78	8.28
Algeria	27.66	8.27
India	16.65	7.61

Table 11. Gambling: Frequency of detections and the share of Kaspersky Lab's Parental Control users hit in the top ten most-affected countries in 2014.

In 2014, gambling websites represented the most common type of dangerous content for users in the UK. The frequency level was 36.13 detections per user and the share of users that encountered such content was 39.24%; while the global average was 18.26 for detections and 26.66% for share of users. The USA was in second place with 30.74 detections per user and a 31.91% user share.

Anonymous Internet Access

Country	% of users that encountered the threat	Frequency
Global average	8.16	9.77
UK	9.30	21.63
US	11.36	10.81
Algeria	8.46	10.26
Brazil	3.48	9.17
Germany	7.99	6.26
India	5.47	6.23
Russia	11.30	6.15
China	2.90	5.1
Vietnam	12.14	5.01
France	6.58	3.55

Table 12. Frequency of detections and the share of Kaspersky Lab's Parental Control users hit in the top ten most-affected countries in 2014.

The UK also topped the list in terms of frequency and share of users for the category of Anonymous Internet Access services. These services allow users to visit websites anonymously even if those websites are blocked by a network administrator or another Parental Control module. A slightly higher than average level of frequency and user share was seen in the US (10.81 detections and 11.36% of users) and Algeria (10.26 detections per user and 8.46%of users).

Chat

An extremely popular category, in 2014 frequency levels for chat services were high across all countries, as was the share of users affected. However, both indicators were significantly higher than average in China (114.75 detections and 69.58% of users). The UK was in second place with 107.14 detections and 63.84% of users, while the US ranked third with 106.62 detections and 71.93% of users. Frequency levels slightly higher than average were detected in Vietnam (69.39 detections and 79.8% of users) and France (66.53 detections and 72.44% of users). Parental Control users in other top ten countries encountered chat services far less often.

Country	% of users that encountered the threat	Frequency
Global average	67.29	58.6
China	69.58	114.75
UK	63.84	107.14
US	71.93	106.62
Vietnam	79.80	69.39
France	72.44	66.53
Algeria	68.65	52.62
Brazil	75.93	49.14
Germany	66.82	48.34
Russia	59.03	34.19
India	67.18	33.57

Table 13. Chat: Frequency of detections and the share of Kaspersky Lab's Parental Control users hit in the top ten most-affected countries in 2014.

As mentioned earlier in the report, it is important to bear in mind that only some of the chat detections represented times when users tried to join services that were potentially dangerous for children (such as those with a lot of adult users and anonymity functions). As a result it would be inaccurate to use the above numbers as an indicator of the level of threat posed to young Internet users. However, the data does reveal the popularity of chat services: and the higher the popularity of chat in a given country, the higher the probability that children will occasionally or intentionally enter into an unsafe chat environment. So a high level of frequency could be a sign for parents to pay more attention to exactly which chat services their children choose to join.

▶ CONCLUSIONS AND RECOMMENDATIONS

At the start of this report we presented the results of a survey conducted by Kaspersky Lab and B2B International. Among other things, the results revealed the kind of activities that, according to respondents, were undertaken online by their children. Based on the results of this research it is safe to say that children's web-activity is not limited to playing online games and visiting educational websites. Unfortunately there are many websites that pose a real threat to users; and many people, including the very young, encounter such sites regularly. The Internet is no longer the preserve of grownups but – as the results of this report show – it has yet to become a 100% safe territory for children.

In order to protect children from Internet threats and provide a safe online experience for them, Kaspersky Lab recommends the following measures:

- When choosing a protection solution for a home computer that will be used by your children, make sure that the solution is equipped with Parental Control technologies.
- Use special "children" modes in online search systems and applications that allow access to multimedia content.
- Educate your children about the kind of cyber threats they could encounter while online.
- Remember that Parental Control technologies can block web sites carrying content that is potentially dangerous to children, but they can't protect reliably against situations where safe-by-default web-services like social networks or chat are misused by predators and users waging cyberbullying campaigns.
- Play an active part in your children's real and digital lives, just to be sure that you don't miss the moment when they need your support.

▶ NOTE ON RESPONSIBLE DISTRIBUTION OF INFORMATION

This document presents an analysis of the landscape of cyber-threat to children. It is based on information about instances of Kaspersky Lab security products equipped with Parental Control module detecting content considered as dangerous. To avoid possible misinterpretation of the facts presented in this document. Kaspersky Lab would like to highlight a number of issues related to the way this report was prepared.

1. Terminology

The report uses several terms describing how a security product interacts with webpages. The term “Detection” is among those used most frequently. In Kaspersky Lab’s terminology, detection is an instance of a security product detecting any content considered dangerous on the protected device. The term “User” denotes exclusively the owner of the device protected by Kaspersky Lab’s product.

2. Dataset and its geographical distribution

All calculations and conclusions made as part of this study rely exclusively on data from Kaspersky Lab’s customer community which exceeds 80 million users in over 200 countries and territories. It should be emphasized that the number of Kaspersky Lab’s product users varies from country to country, so the results of this study may not fully reflect the situation existing in some countries. However .many years’ experience of monitoring the statistics processed by Kaspersky Security Network (KSN) shows that in most cases KSN data is about 95% accurate concerning the prevalence of specific cyber-threats or cyber-threat classes and concerning the percentage distribution of consumers using devices running different operating systems.

Responsible distribution of information

This study can be freely shared or distributed. Kaspersky Lab requests that those who find the information presented in this document interesting and useful make allowances for the abovementioned issues related to the ways in which KSN statistics are collected when preparing public materials in which this information is to be used.

Securelist, the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation
more contact details
Tel: +7-495-797-8700
Fax: +7-495-797-8709