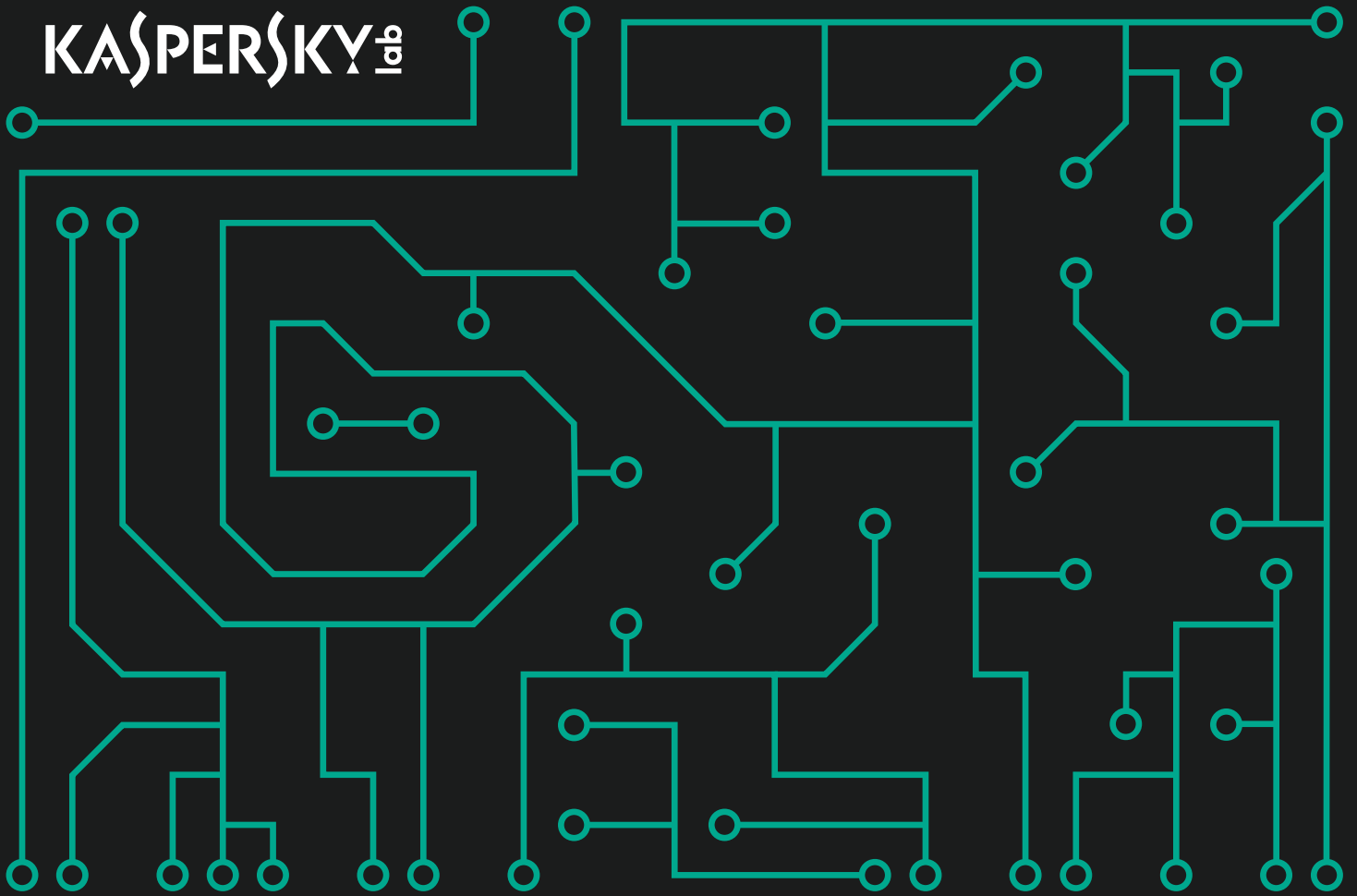


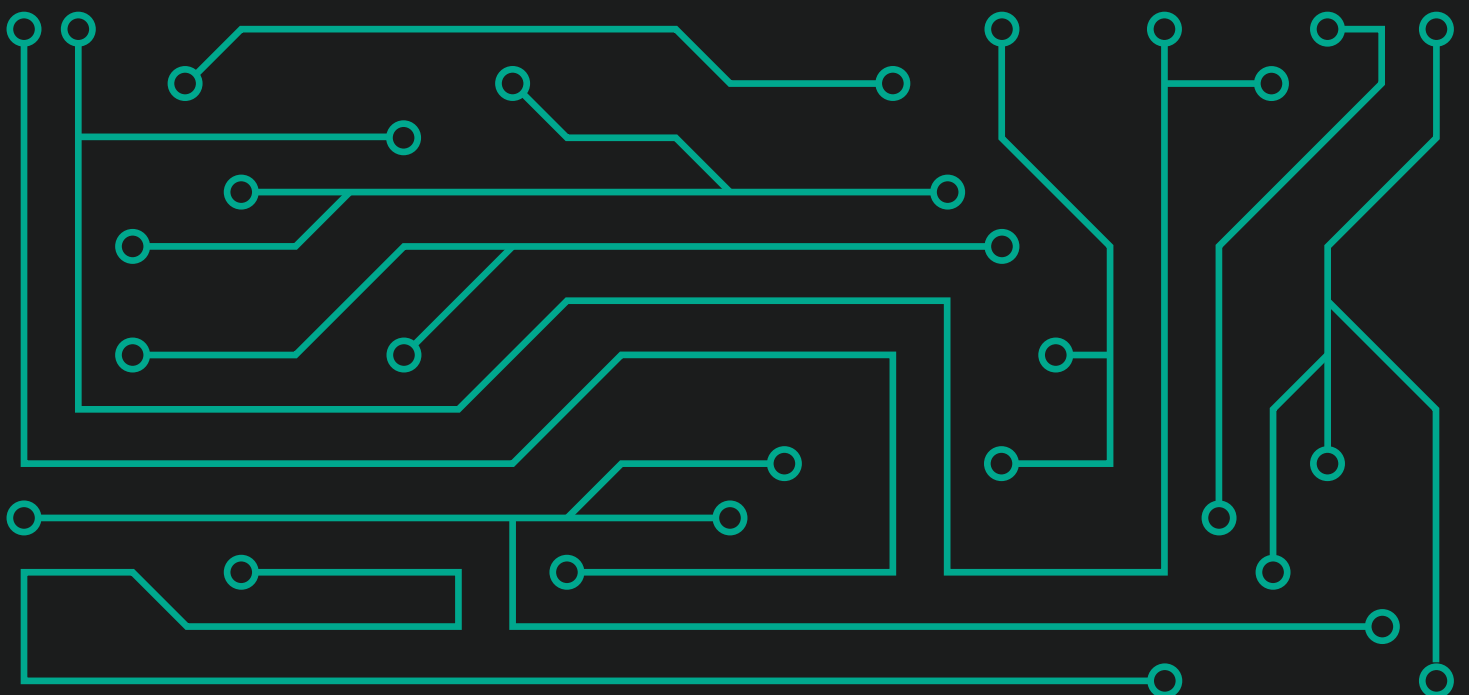


KASPERSKY^{LAB}



Kaspersky Security Bulletin 2018

STATISTICS



CONTENTS

| | |
|--|----|
| The year in figures | 3 |
| Banking malware | 4 |
| The number of users attacked by banking malware..... | 4 |
| Geography of attacks..... | 4 |
| Crypto-ransomware | 7 |
| The number of users attacked by encryptors..... | 8 |
| Geography of attacks..... | 9 |
| TOP 10 countries attacked by encryptors..... | 9 |
| TOP 10 most widespread encryptor families..... | 10 |
| Miners..... | 11 |
| The number of users attacked by miners..... | 11 |
| Geography of attacks..... | 12 |
| Vulnerable applications used in cyberattacks..... | 13 |
| Web-based attacks..... | 16 |
| Countries that are sources of web-based attacks | 16 |
| Countries where users face the greatest risk of online infection | 17 |
| TOP 20 verdicts detected online..... | 20 |
| Local threats | 22 |
| TOP 20 malicious objects detected on user computers..... | 22 |
| Countries where users face the highest risk of local infection..... | 24 |

All the statistics used in this report were obtained using Kaspersky Security Network (KSN), a distributed antivirus network that works with various anti-malware protection components. The data was collected from KSN users who agreed to provide it. Millions of Kaspersky Lab product users from 213 countries and territories worldwide participate in this global exchange of information about malicious activity. All the statistics were collected from November 2017 to October 2018.

THE YEAR IN FIGURES

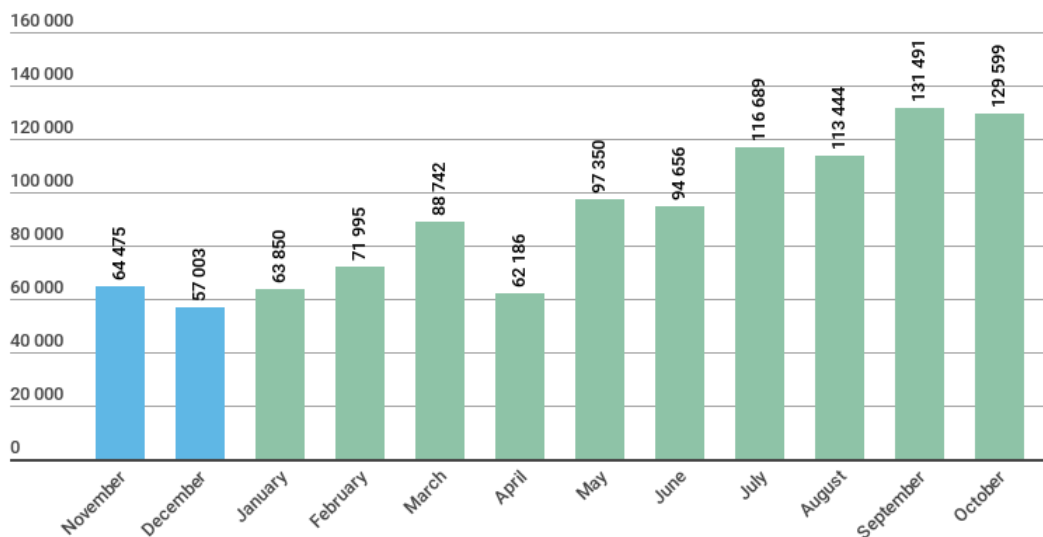
- **30.01%** of user computers were subjected to at least one Malware-class web attack over the year.
- Kaspersky Lab solutions repelled **1 876 998 691** attacks launched from online resources located all over the world.
- **554 159 621** unique URLs were recognized as malicious by web antivirus components.
- Kaspersky Lab's web antivirus detected **21 643 946** unique malicious objects.
- **765 538** computers of unique users were targeted by encryptors.
- **5 638 828** computers of unique users were targeted by miners.
- Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **830 135** devices.

BANKING MALWARE

These statistics include not only banking malware but also malicious programs for ATMs and POS terminals. Mobile financial threats can be found in the yearly mobile report.

The number of users attacked by banking malware

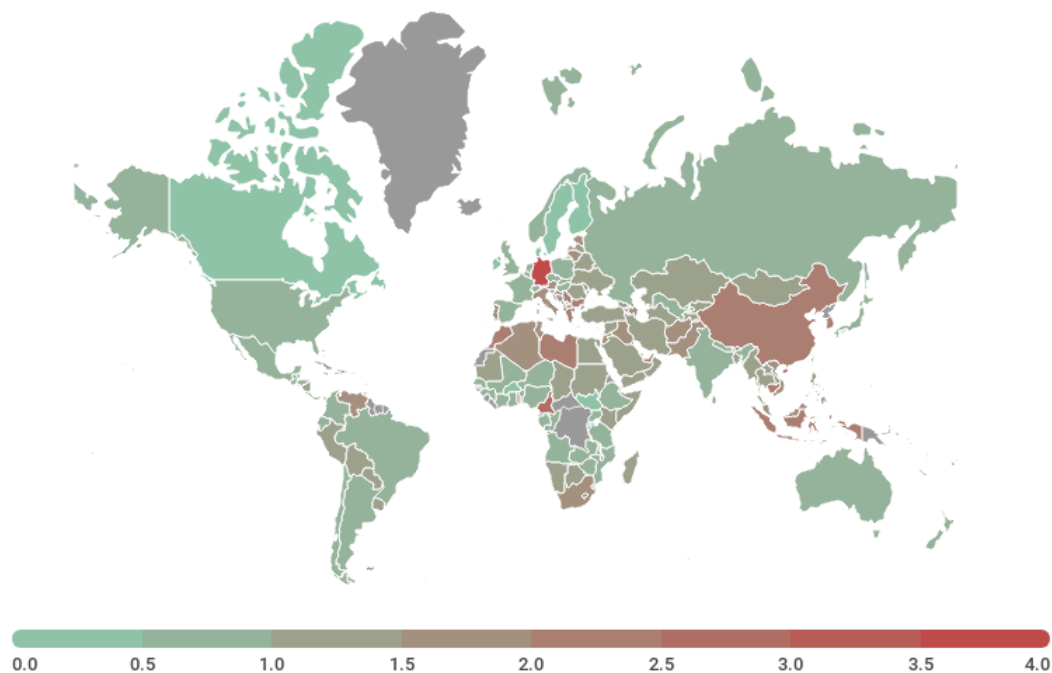
In 2018, Kaspersky Lab solutions blocked attempts to launch one or more malicious programs designed to steal money from bank accounts on the computers of **830 135** users.



*Number of unique users attacked by banking malware,
November 2017 – October 2018*

Geography of attacks

To evaluate and compare the risk of being infected by banking Trojans and ATM/POS malware worldwide, we calculated the share of users of Kaspersky Lab products in each country that faced this threat during the reporting period out of all users of our products in that country.



Geography of banking malware attacks, November 2017 – October 2018

TOP 10 countries by percentage of attacked users

| | Country* | %** |
|----|----------------------|-----|
| 1 | Germany | 4.0 |
| 2 | Cameroon | 2.6 |
| 3 | South Korea | 2.4 |
| 4 | Republic of Maldives | 2.4 |
| 5 | Togo | 2.3 |
| 6 | Indonesia | 2.2 |
| 7 | Lebanon | 2.2 |
| 8 | UAE | 2.1 |
| 9 | Greece | 2.1 |
| 10 | China | 2.0 |

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (under 10,000).

** Unique users attacked by banking malware in the country as a percentage of all users of Kaspersky Lab's products in that country.

TOP 10 banking malware families

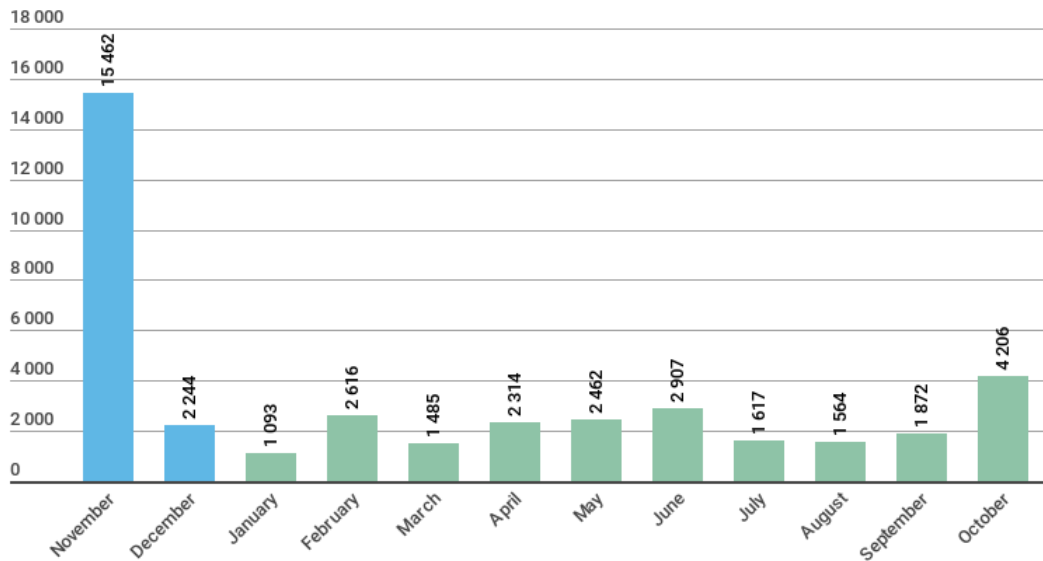
The table below shows the 10 malware families most commonly used in 2018 to attack banking users.

| | Name | %* |
|----|-------------------------------|------|
| 1 | Trojan.Win32.Zbot | 26.3 |
| 2 | Trojan.Win32.Nymaim | 19.8 |
| 3 | Backdoor.Win32.SpyEye | 14.7 |
| 4 | Backdoor.Win32.Caphaw | 5.2 |
| 5 | Trojan-Banker.Win32.RTM | 5.2 |
| 6 | Backdoor.Win32.Emotet | 4.9 |
| 7 | Trojan.Win32.Neurevt | 3.9 |
| 8 | Trojan-Banker.Win32.Tinba | 1.9 |
| 9 | Trojan.Win32.Gozi | 1.8 |
| 10 | Trojan-Banker.Win32.Trickster | 1.5 |

* Unique users attacked by the given malware as a percentage of all users that were attacked by banking threats.

CRYPTO-RANSOMWARE

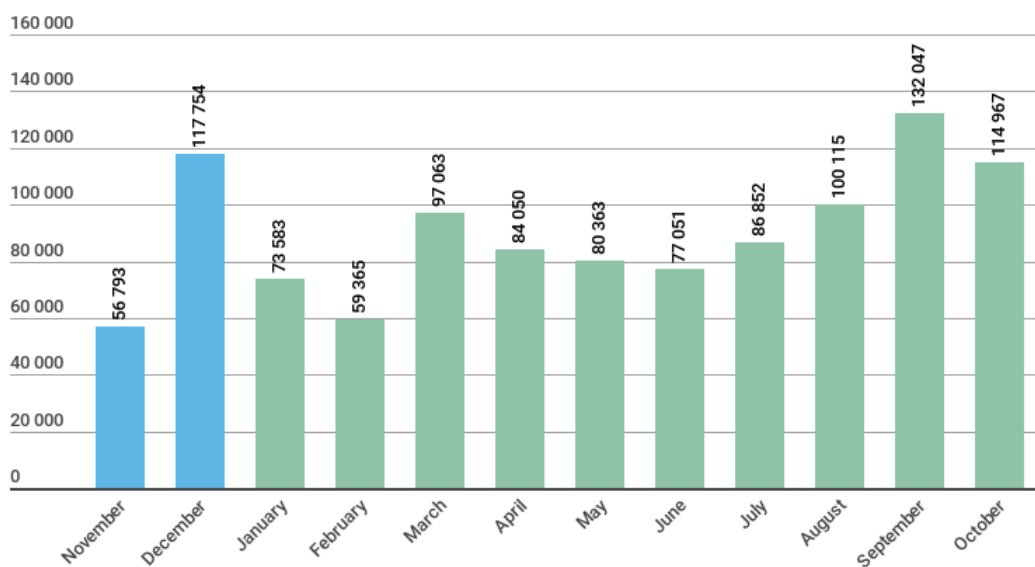
During the year, we detected **39 842** modifications of encryptors and discovered **11** new families. Note that we didn't create a new family for every new malware we found. Most threats of this type are assigned with generic verdicts that we use when detecting new and unknown samples.



*Number of new crypto-ransomware modifications,
November 2017 – October 2018*

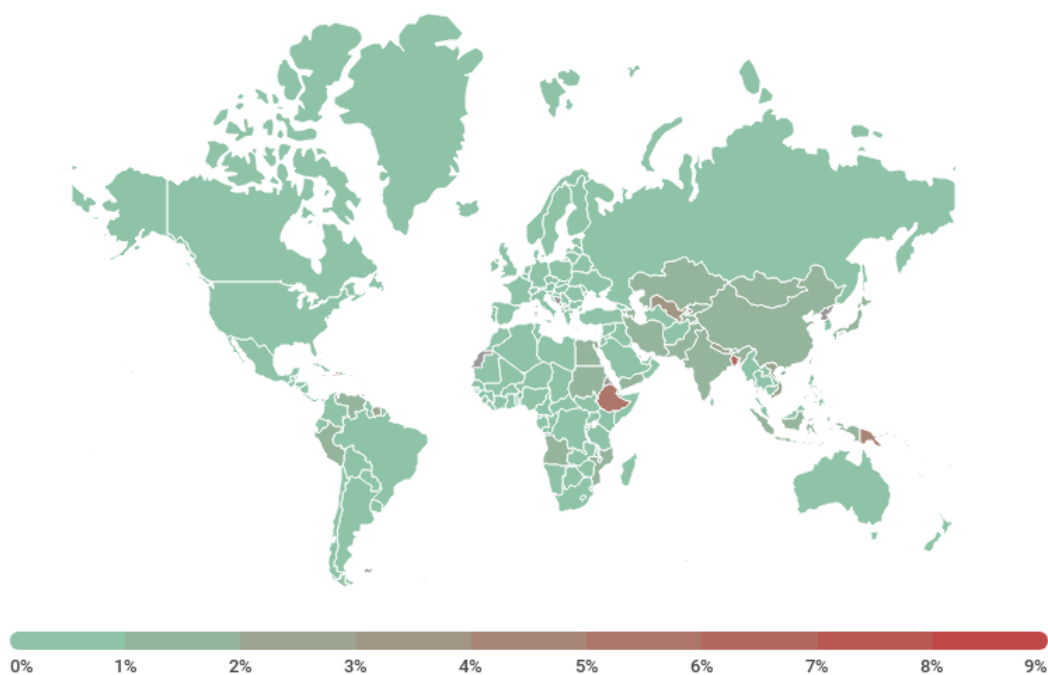
The number of users attacked by encryptors

During the reporting period, **765 538** unique KSN users were attacked by encryptors, including more than 220 thousand corporate users and more than 27 thousand SMB users.



Number of users attacked by crypto-ransomware,
November 2017 – October 2018

Geography of attacks



Geography of crypto-ransomware attacks, November 2017 – October 2018

TOP 10 countries attacked by encryptors

| | Country* | %** |
|---|------------|------|
| 1 | Bangladesh | 6.65 |
| 2 | Ethiopia | 5.25 |
| 3 | Uzbekistan | 3.50 |
| 4 | Nepal | 2.79 |
| 5 | Vietnam | 2.12 |
| 6 | Indonesia | 1.95 |
| 7 | India | 1.87 |

| | Country* | %** |
|----|----------|------|
| 8 | Angola | 1.84 |
| 9 | Pakistan | 1.78 |
| 10 | China | 1.72 |

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (under 50,000).

** Unique users whose computers have been targeted by crypto-ransomware as a percentage of all unique users of Kaspersky Lab products in the country.

TOP 10 most widespread encryptor families

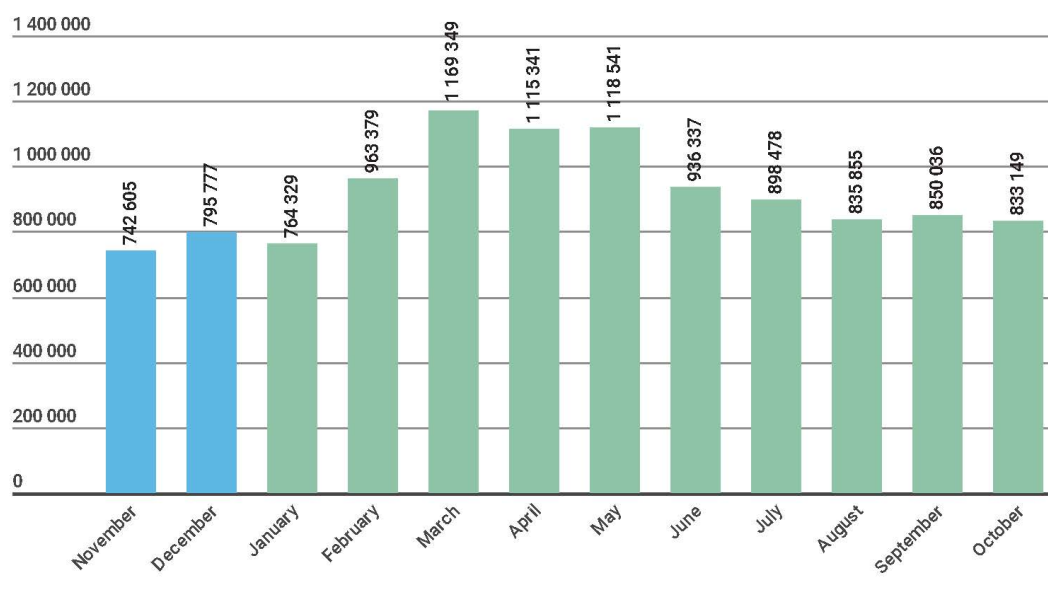
| | Name | Verdict | %* |
|----|-----------------------|-------------------------------|-------|
| 1 | WannaCry | Trojan-Ransom.Win32.Wanna | 29.32 |
| 2 | (generic verdict) | Trojan-Ransom.Win32.Phny | 11.43 |
| 3 | GandCrab | Trojan-Ransom.Win32.GandCrypt | 6.67 |
| 4 | Cryakl | Trojan-Ransom.Win32.Cryakl | 4.59 |
| 5 | PolyRansom/VirLock | Virus.Win32.PolyRansom | 2.86 |
| 6 | (generic verdict) | Trojan-Ransom.Win32.Gen | 2.40 |
| 7 | Shade | Trojan-Ransom.Win32.Shade | 2.29 |
| 8 | Cerber | Trojan-Ransom.Win32.Zerber | 2.20 |
| 9 | Purgen/GlobelImposter | Trojan-Ransom.Win32.Purgen | 1.82 |
| 10 | Crysis/Dharma | Trojan-Ransom.Win32.Crusis | 1.72 |

* Unique users whose computers have been targeted by a specific crypto-ransomware family as a percentage of all users of Kaspersky Lab products attacked by crypto-ransomware

MINERS

The number of users attacked by miners

During the reporting period, **5 638 828** unique KSN users were attacked by miners. In the total volume of detections, the share of miners was 8.50%; for Risktool it was 16.88%.

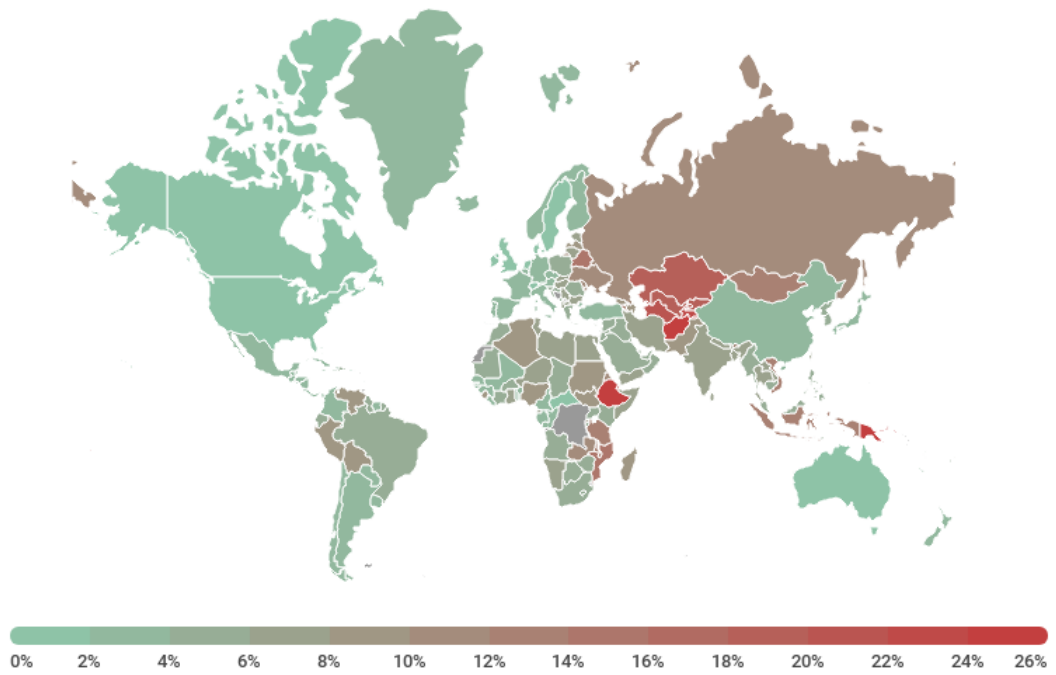


KASPERSKY lab

*Number of users attacked by miners,
November 2017 – October 2018*

The most active miner this year was Trojan.JS.Miner.m; its accounted for almost 22% of the total number of users attacked by miners. It was followed by members of the Trojan.Win32.Miner family: Miner.gen (9.44%), Miner.ays (5.30%) and Miner.bbb (2.71%).

Geography of attacks



Geography of miners attacks, November 2017 – October 2018

VULNERABLE APPLICATIONS USED IN CYBERATTACKS

2018 will be remembered for the large number of targeted attacks using exploits for zero-day vulnerabilities. Notable incidents included:

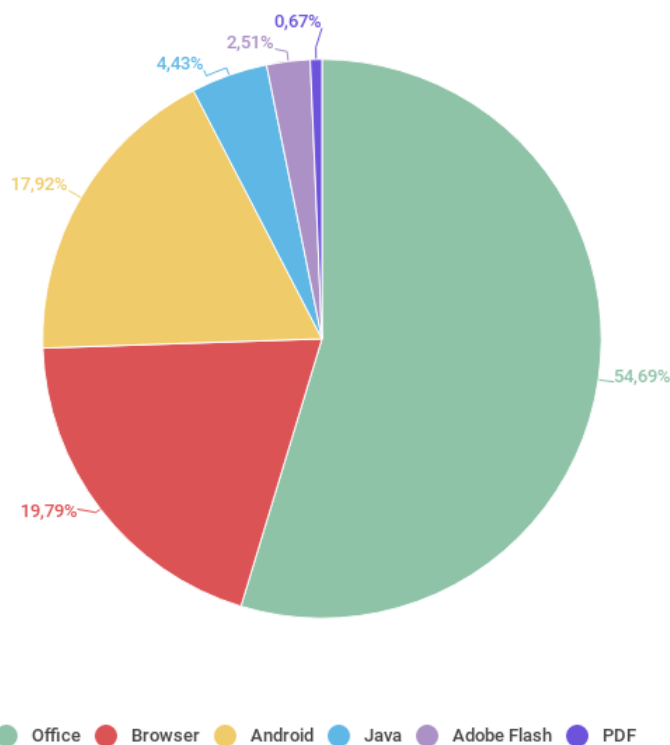
- The exploiting of vulnerabilities in Adobe Flash at the end of its lifecycle (CVE-2018-4878, CVE-2018-5002);
- The first case in a long time of Acrobat Reader vulnerability CVE-2018-4990 being exploited;
- Vulnerabilities in VBScript – one of the Windows script engines used, among others, in Internet Explorer (CVE-2018-8174, CVE-2018-8373);
- Several vulnerabilities in the win32k.sys driver that were used by cybercriminals both to escalate privileges in the Windows system and (together with other vulnerabilities) to bypass a sandbox (CVE-2018-8120, CVE-2018-8453, CVE-2018-8589).

As in the previous year, the share of users attacked by exploits for vulnerabilities in Adobe Flash Player and Internet Explorer has decreased, even though some new zero-day publicly exploited vulnerabilities have been found in both products. For example, the CVE-2018-4878 vulnerability in Adobe Flash Player, the proof-of-concept for which was released publicly by a researcher, was included in many popular exploit kits less than two months after the patch was released. Despite this, the share of these platforms in our statistics has more than halved.

The share of the exploits for Android fell to 18% (-9 p.p. compared to the previous year), which leads to the conclusion that the safety of this OS is increasing. This may be partly down to a more aggressive policy of updating devices to the latest version of the system. For example, according to our data up to October 2018, Android 8.0+ Oreo was installed on 22% of Android devices. By way of comparison, in October 2017, Android 7.0+ Nougat, the latest version of Android at that time, was used by just 16% of Android users.

At the same time, there was a significant increase in the number of users attacked by Microsoft Office exploits – four times more compared to the average for 2017. This led to an increase in the share of Microsoft Office exploits in our statistics, from 17.63% to an incredible 55%. The reason for this growth was the mass spam mailings that spread documents with exploits for vulnerabilities CVE-2017-11882 and CVE-2018-0802. Exploits for these vulnerabilities have gained popularity among cybercriminals due to their stability and ease of use – all that's required to create an exploit is to modify the exploit builder script published on a public resource. A significant role was played by the ability to implement obfuscation to avoid detection as well as wide coverage of various versions of Microsoft Office – without the patch, all versions of the office suite released over the past 18 years are vulnerable.

Exploits for the other popular vulnerabilities (CVE-2017-8570, CVE-2018-4878, CVE-2018-8174) that were distributed with MS Office documents, also played a role in increasing the share of this application in our statistics.



Distribution of exploits used in cyberattacks, by type of application attacked, November 2017 – October 2018

Vulnerable applications are ranked based on Kaspersky Lab product reports of blocked exploits used by cybercriminals both in web-borne attacks and in compromised local applications, including those on users' mobile devices.

In 2018, there were no such incidents like Shadow Brokers group's release of the Lost In Translation archive, which contains a large number of network exploits. However, the number of malicious files using exploits from this archive, as well as the number of attempts to attack using them, continued to grow: during the year, our intrusion detection component blocked 10 times more attempted attacks using the network exploit EternalBlue.

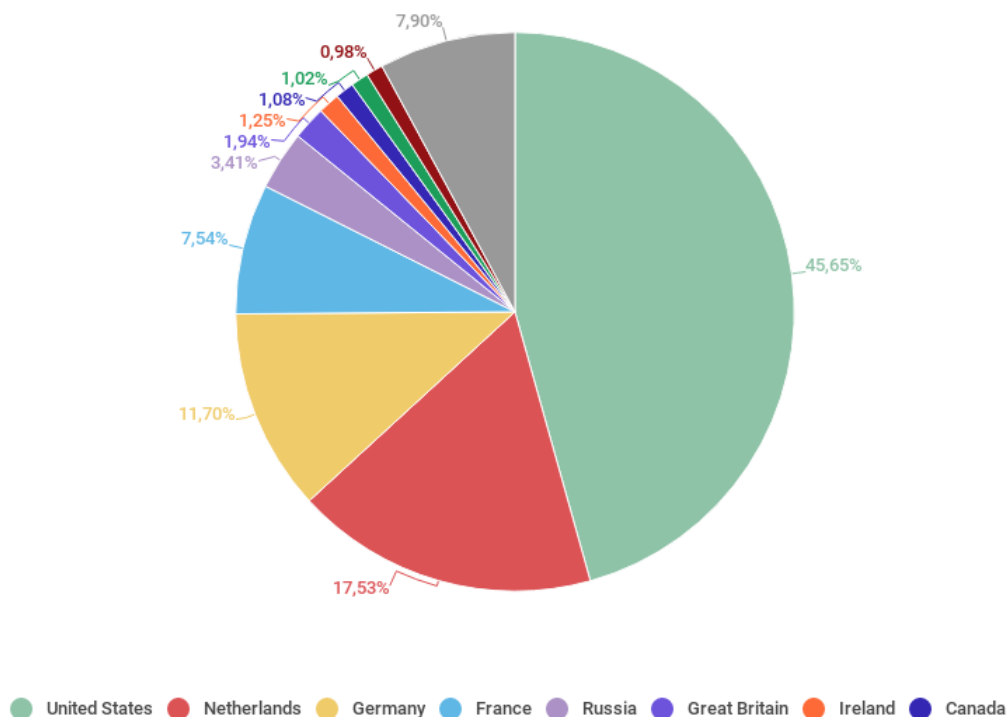
WEB-BASED ATTACKS

The statistics in this section were derived from web antivirus components that protect users from attempts to download malicious objects from a malicious/infected website. Malicious websites are deliberately created by malicious users; infected sites include those with user-contributed content (such as forums), as well as compromised legitimate resources.

Countries that are sources of web-based attacks

The following statistics are based on the physical location of the online resources used in attacks and blocked by our antivirus components (web pages containing redirects to exploits, sites containing exploits and other malware, botnet command centers, etc.). Any unique host could be the source of one or more web attacks. In order to determine the geographical source of web-based attacks, domain names are matched against their actual domain IP addresses, and then the geographical location of a specific IP address (GEOIP) is established.

In 2018, Kaspersky Lab solutions blocked **1 876 998 691** attacks launched from web resources located in various countries around the world. **92.1%** of notifications about attacks blocked by antivirus components were received from online resources located in 10 countries.



Distribution of web attack sources by country, November 2017 – October 2018

Compared to last year’s results, the distribution of web attack sources has not changed much. The United States (45.65%) is still in first place, followed by the Netherlands (17.53%) and Germany (11.70%). Finland, Ukraine and China left the TOP 10; their places were taken by Ireland (1.25%), Luxembourg (1.02%) and Singapore (0.98%).

Countries where users face the greatest risk of online infection

In order to assess the countries in which users most often face cyberthreats, we calculated how often Kaspersky Lab users encountered detection verdicts on their machines in each country. The resulting data characterizes the risk of infection that computers are exposed to in different countries across the globe, providing an indicator of the aggressiveness of the environment facing computers in different parts of the world.

This rating only includes attacks by malicious programs that fall under the Malware class. The rating does not include web antivirus module detections of potentially dangerous or unwanted programs such as RiskTool or Adware.

Note that during the year, adware programs and their components were detected on 53% of user computers on which the web antivirus was triggered.

The TOP 20 countries where users face the greatest risk of online infection

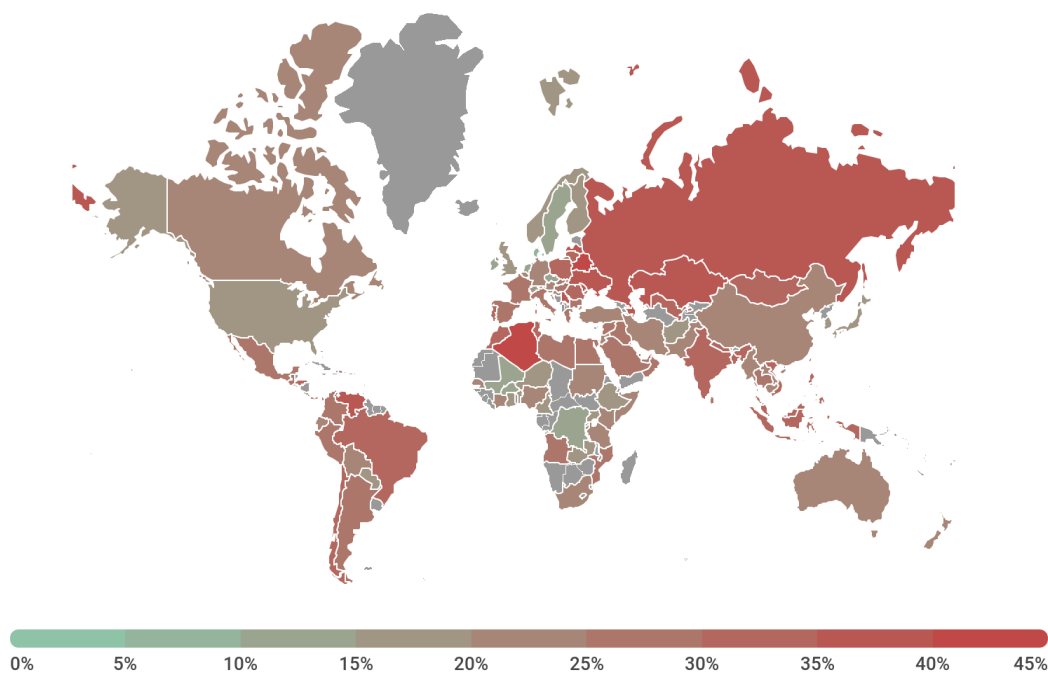
| | Country* | %** |
|----|-------------|-------|
| 1 | Algeria | 43.31 |
| 2 | Belarus | 43.0 |
| 3 | Venezuela | 39.48 |
| 4 | Kazakhstan | 37.76 |
| 5 | Moldova | 37.39 |
| 6 | Azerbaijan | 36.82 |
| 7 | Russia | 36.22 |
| 8 | Ukraine | 35.52 |
| 9 | Latvia | 34.63 |
| 10 | Serbia | 34.62 |
| 11 | Vietnam | 34.45 |
| 12 | Qatar | 34.37 |
| 13 | Tunisia | 34.35 |
| 14 | Indonesia | 33.69 |
| 15 | Romania | 33.09 |
| 16 | Mongolia | 32.88 |
| 17 | Philippines | 32.81 |

| | Country* | %** |
|----|----------|-------|
| 18 | Morocco | 32.7 |
| 19 | Brazil | 31.0 |
| 20 | Nepal | 31.90 |

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (less than 50,000).

** Unique users whose computers have been targeted by Malware-class web attacks as a percentage of all unique users of certain Kaspersky Lab products in the country

On average, during the year a Malware-class attack was detected at least once on 30.01% of computers around the world.



Geography of malicious web attacks, November 2017 – October 2018

TOP 20 verdicts detected online

Throughout 2018, Kaspersky Lab's web antivirus detected 21 643 946 unique malicious objects (scripts, exploits, executable files, etc.) and **554 159 621** unique URLs that were blocked by web antivirus components. We identified the 20 malicious programs most actively involved in online attacks launched against computers in 2018.

| | Verdict | %* |
|----|----------------------------------|-------|
| 1 | Malicious URL | 89.50 |
| 2 | Trojan.Script.Generic | 6.19 |
| 3 | Trojan.Script.Miner.gen | 1.95 |
| 4 | Trojan.Script.Agent.gen | 0.38 |
| 5 | Trojan.JS.Miner.m | 0.27 |
| 6 | Trojan-Clicker.HTML.Iframe.dg | 0.26 |
| 7 | Trojan.JS.Agent.eak | 0.13 |
| 8 | Trojan.JS.Miner.d | 0.12 |
| 9 | Hoax.HTML.FraudLoad.m | 0.08 |
| 10 | Trojan.Win32.Miner.ays | 0.06 |
| 11 | Trojan-Dropper.VBS.Agent.bp | 0.05 |
| 12 | Trojan-Downloader.Script.Generic | 0.05 |
| 13 | Trojan.Win64.Shelma.a | 0.04 |
| 14 | Packed.Multi.MultiPacked.gen | 0.04 |
| 15 | Trojan.JS.Miner.x | 0.04 |
| 16 | Trojan.JS.Miner.y | 0.04 |
| 17 | Hoax.Script.Generic | 0.03 |

| | Verdict | %* |
|----|-------------------------------|------|
| 18 | DangerousObject.Multi.Generic | 0.03 |
| 19 | Trojan.Script.Iframer | 0.03 |
| 20 | Trojan.JS.Agent.ecp | 0.02 |

* The share of all malware web attacks detected on the computers of unique users.

This year's TOP 20 includes many web miners; the Trojan.JS.Miner family boasted the biggest representation – four places out of 20. At the same time, web exploits, which were collected under the Exploit.Script.Generic verdict and which occupied 10th place last year, left the TOP 20 this time round.

LOCAL THREATS

Local infection statistics for user computers are a very important indicator: they reflect threats that have penetrated computer systems by infecting files or removable media, or initially got on the computer in an encrypted format (for example, programs integrated in complex installers, encrypted files, etc.). In addition, these statistics include objects detected on user computers after the first scan of the system by Kaspersky Lab's file antivirus.

This section contains an analysis of the statistical data obtained based on antivirus scans of files on the hard drive at the moment they are created or accessed, and the results of scanning various removable data storages.

TOP 20 malicious objects detected on user computers

For this rating, we identified the 20 most frequently detected threats on user computers in 2018. This rating does not include the Adware and Riskware classes of program.

| | Verdict | %* |
|----|----------------------------------|-------|
| 1 | DangerousObject.Multi.Generic | 32.15 |
| 2 | Trojan.Script.Generic | 14.46 |
| 3 | Trojan.Multi.GenAutorunReg.a | 5.76 |
| 4 | Trojan.WinLNK.Agent.gen | 4.56 |
| 5 | Trojan.WinLNK.Starter.gen | 3.47 |
| 6 | HackTool.Win32.KMSAuto.c | 3.14 |
| 7 | HackTool.Win64.HackKMS.b | 2.69 |
| 8 | Trojan.Win32.Generic | 2.56 |
| 9 | Trojan.Script.Miner.gen | 2.44 |
| 10 | Trojan.Win32.AutoRun.gen | 2.43 |
| 11 | Trojan-Downloader.Script.Generic | 2.33 |
| 12 | Virus.Win32.Sality.gen | 2.30 |
| 13 | HackTool.Win32.KMSAuto.m | 2.05 |

| | Verdict | %* |
|----|-------------------------------|------|
| 14 | Trojan.AndroidOS.Boogr.gsh | 1.96 |
| 15 | Trojan.Win32.Agentb.bqyr | 1.48 |
| 16 | Trojan.Win32.Miner.gen | 1.41 |
| 17 | Trojan.Multi.GenAutorunBITS.a | 1.28 |
| 18 | Trojan.Multi.Babits.genw | 1.19 |
| 19 | Virus.Win32.Nimnul.a | 1.18 |
| 20 | HackTool.MSIL.KMSAuto.ba | 1.13 |

* The share of individual users on whose computers the file antivirus detected these programs as a percentage of all individual users of Kaspersky Lab products on whose computers any malicious program was detected.

Traditionally, first place in our TOP 20 went to DangerousObject.Multi.Generic (32.15%), the verdict we use for malware detected [using cloud-based technologies](#). Cloud technologies work when the antivirus databases lack the data to detect a piece of malware, but the cloud of the antivirus company already contains information about the object. This is basically how the latest malicious programs are detected.

Various variations of WinLNK malware are still being spread: Trojan.WinLNK.Agent.gen (4.56%) is in fourth place, followed immediately by Trojan.WinLNK.Starter.gen (3.47%). This malware can change the settings of the victim's browser or be used to download other malware.

Trojan.AndroidOS.Boogr.gsh (1.96%) takes 14th place; this threat is detected using machine learning technologies for Android OS malware detection.

Trojan.Multi.GenAutorunBITS.a (1.28%) and Trojan.Multi.Babits.genw (1.19%) occupy 17th and 18th places respectively. These malicious programs, like many others, use the [Background Intelligent Transfer Service](#) component to gain a foothold in the system.

Countries where users face the highest risk of local infection

For each country, we calculated the number of file antivirus detections users faced during the year. The data includes malicious programs located on user computers or on removable media connected to computers, such as flash drives, camera and phone memory cards, or external hard drives. This statistic reflects the level of infected personal computers in different countries around the world.

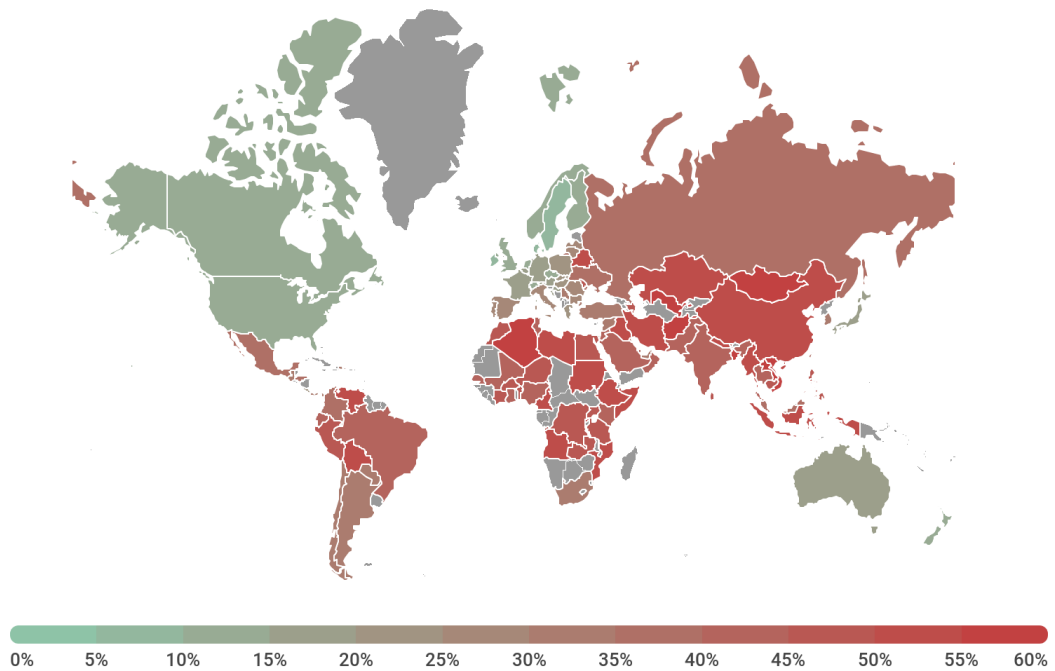
TOP 20 countries with the highest risk of local infection

| | Country* | %** |
|----|-------------|-------|
| 1 | Vietnam | 62.29 |
| 2 | Afghanistan | 61.93 |
| 3 | Uzbekistan | 60.22 |
| 4 | Laos | 58.94 |
| 5 | Mongolia | 58.35 |
| 6 | Algeria | 58.13 |
| 7 | Bangladesh | 56.58 |
| 8 | Rwanda | 54.88 |
| 9 | Syria | 54.76 |
| 10 | Myanmar | 54.03 |
| 11 | Sudan | 53.77 |
| 12 | Ethiopia | 53.69 |
| 13 | Iraq | 53.5 |
| 14 | Mozambique | 53.31 |
| 15 | Kazakhstan | 53.15 |
| 16 | Nepal | 53.14 |
| 17 | Belarus | 52.38 |

| | Country* | %** |
|----|-----------|-------|
| 18 | Lebanon | 51.92 |
| 19 | Venezuela | 51.18 |
| 20 | China | 51.17 |

* When calculating, we excluded countries where there are fewer than 50,000 Kaspersky Lab users.

** The percentage of unique users in the country with computers that blocked Malware-class local threats as a percentage of certain unique users of Kaspersky Lab products.



Geography of local malware attacks, November 2017 – October 2018

In 2018, at least one malicious program was found on an average of 35.06% of computers, hard drives or removable media belonging to KSN users.