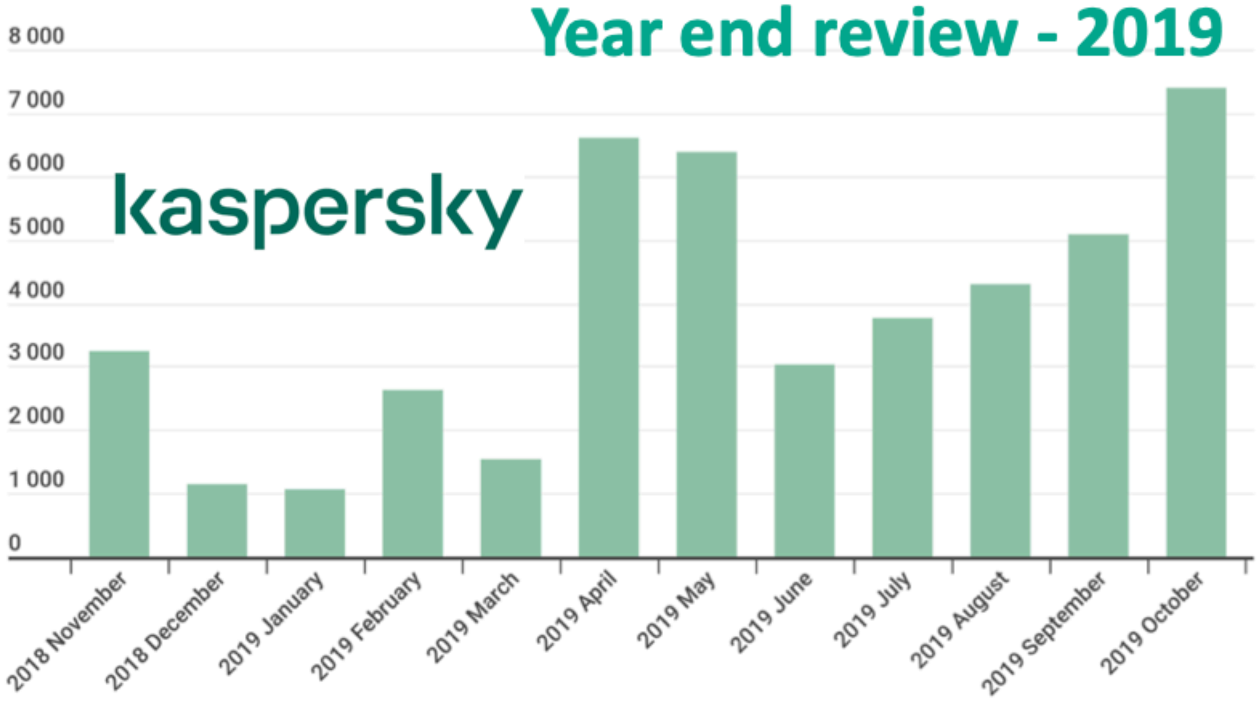
Kaspersky Security Bulletin '19

Statistics

Crypto-ransomware

Year end review - 2019

kaspersky



Number of new crypto-ransomware modifications

Kaspersky Security Bulletin ‘19

Statistics

kaspersky

Contents

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 product users from 203 countries and territories worldwide participate in this global exchange of information about malicious activity. All the statistics were collected from November 2018 to October 2019.

The year in figures

- **19.8%** of user computers were subjected to at least one Malware-class web attack over the year.
- Kaspersky solutions repelled **975 491 360** attacks launched from online resources located all over the world.
- **273 782 113** unique URLs were recognized as malicious by web antivirus components.
- Kaspersky's web antivirus detected **24 610 126** unique malicious objects.
- **755 485** computers of unique users were targeted by encryptors.
- **2 259 038** computers of unique users were targeted by miners.
- Kaspersky solutions blocked attempts to launch malware capable of stealing money via online banking on **766 728** devices.

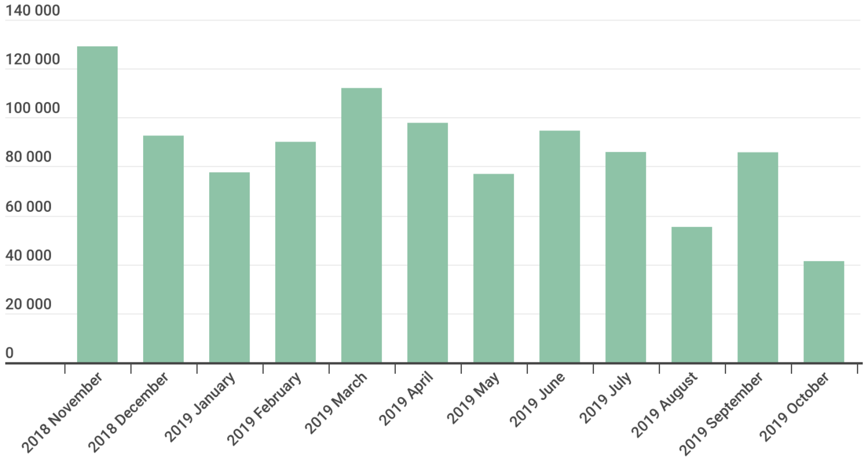
Mobile threats will be presented in the yearly report "Mobile malware evolution 2019".

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

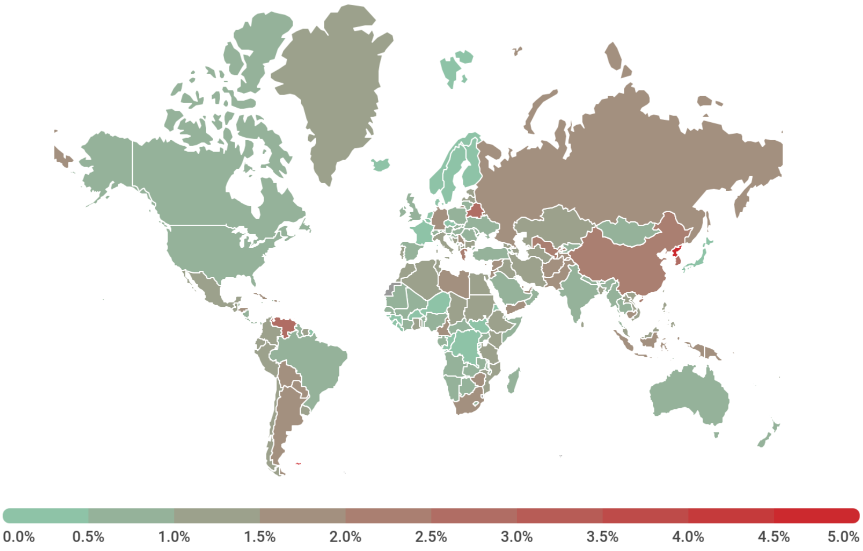
During the reporting period, Kaspersky solutions blocked attempts to launch one or more malicious programs designed to steal money from bank accounts on the computers of **766 728** users.



Number of unique users attacked by banking malware, November 2018 – October 2019

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 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 2018 – October 2019

TOP 10 countries by percentage of attacked users

	Country*	%**
1	Belarus	2.8
2	Republic of Korea	2.6
3	Venezuela	2.6
4	China	2.4
5	Greece	2.1
6	Maldives	2.0
7	Uzbekistan	2.0
8	Cameroon	1.9
9	Serbia	1.9
10	Afghanistan	1.8

* We excluded those countries where the number of Kaspersky 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's products in that country.

TOP 10 banking malware families

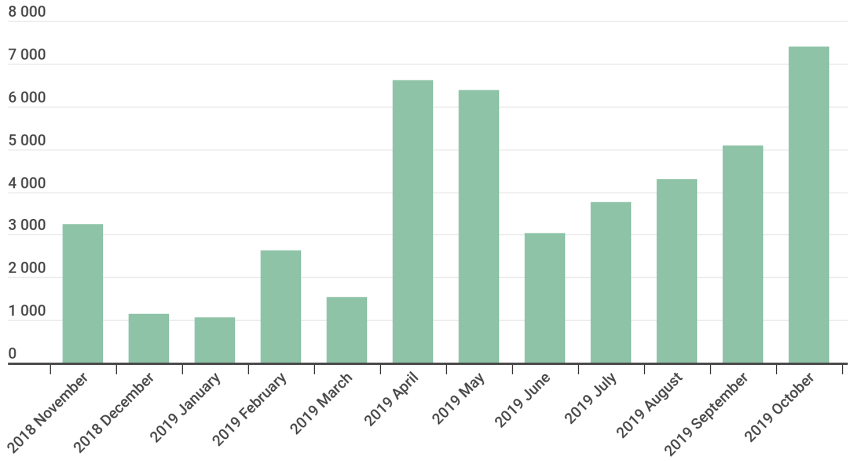
The table below shows the 10 malware families most commonly used to attack banking users during the reporting period.

	Name	%*
1	Trojan.Win32.Zbot	23.10
2	Trojan-Banker.Win32.RTM	21.60
3	Backdoor.Win32.Emotet	12.30
4	Backdoor.Win32.SpyEye	7.10
5	Trojan.Win32.Nymaim	5.80
6	Trojan-Banker.Win32.Trickster	4.80
7	Trojan-Banker.Win32.Ramnit	4.40
8	Trojan.Win32. Neurevt	3.10
9	Trojan-Banker.Win32.CliptoShuffler	1.90
10	Trojan-Banker.Win32.Danabot	1.30

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

Crypto-ransomware

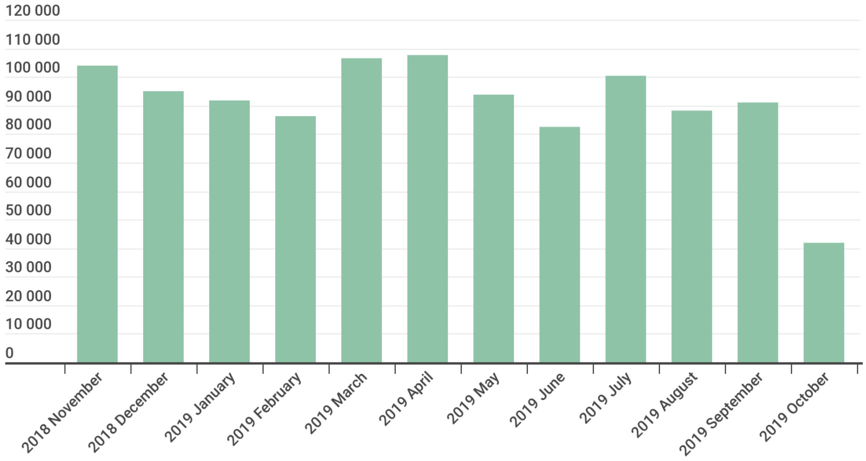
During the year, we detected **46 156** modifications of encryptors and discovered **22** new families. Note that we didn't create a new family for every new malware we found. Most threats of this type are assigned with generic verdicts that we use when detecting new and unknown samples.



Number of new crypto-ransomware modifications, November 2018 – October 2019

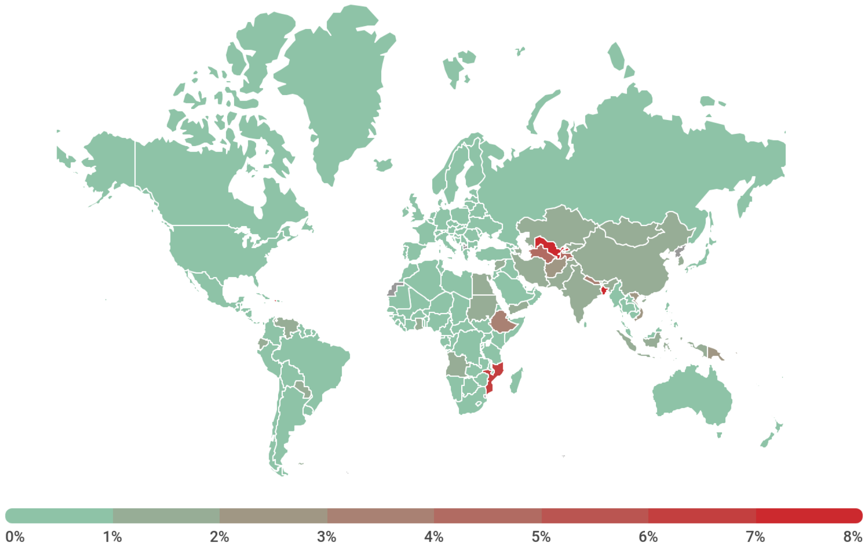
The number of users attacked by encryptors

During the reporting period, **755 485** unique KSN users were attacked by encryptors, including 209 679 corporate users (excluding SMB) and 22 440 SMB users.



Number of users attacked by crypto-ransomware, November 2018 – October 2019

Geography of attacks



Geography of crypto-ransomware attacks, November 2018 – October 2019

TOP 10 countries attacked by encryptors

	Country*	%**
1	Bangladesh	13.78
2	Uzbekistan	7.20
3	Mozambique	6.08
4	Turkmenistan	4.23
5	Ethiopia	3.97
6	Nepal	3.86
7	Afghanistan	2.45
8	Vietnam	2.34
9	China	1.94
10	India	1.91

* We excluded those countries where the number of Kaspersky 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 products in the country.

TOP 10 most widespread encryptor families

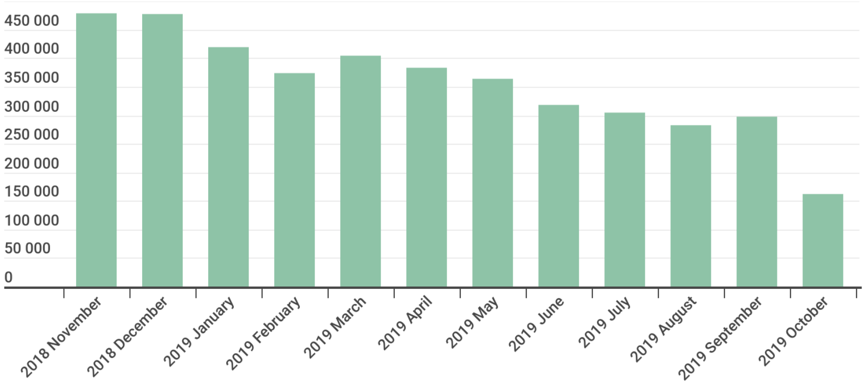
	Name	Verdict	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	23.56
2	(generic verdict)	Trojan-Ransom.Win32.Phny	16.81
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	12.17
4	(generic verdict)	Trojan-Ransom.Win32.Gen	6.26
5	(generic verdict)	Trojan-Ransom.Win32.Crypmod	5.08
6	(generic verdict)	Trojan-Ransom.Win32.Encoder	4.65
7	Shade	Trojan-Ransom.Win32.Shade	2.66
8	PolyRansom/ VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.Win32.PolyRansom	2.43
9	(generic verdict)	Trojan-Ransom.Win32.Crypren	2.28
10	Stop	Trojan-Ransom.Win32.Stop	1.94

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

Miners

The number of users attacked by miners

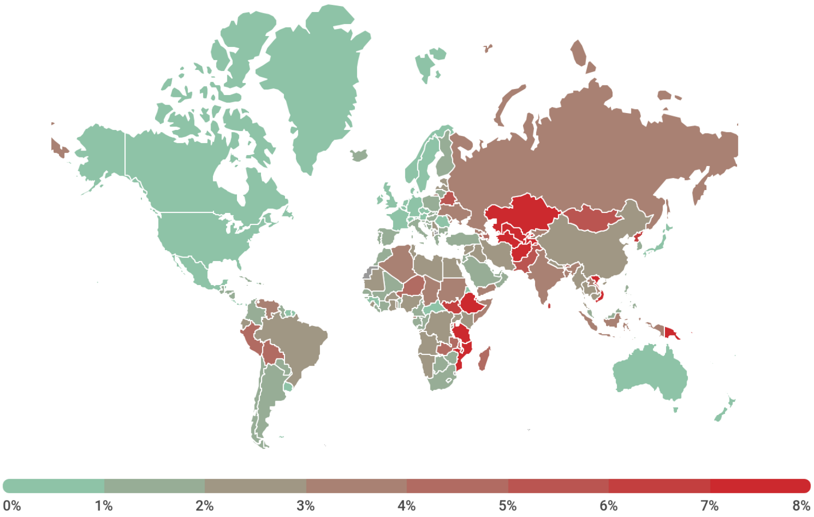
During the reporting period, **2 259 038** unique KSN users were attacked by miners. In the total volume of detections, the share of miners was 3.64%; for Risktool it was 6.94%.



Number of users attacked by crypto-ransomware, November 2018 – October 2098

During the reporting period, the most active miner was Trojan.Win32.Miner.bbb; its accounted for 13.45% of the total number of users attacked by miners. It was followed by Trojan.Win32.Miner.ays (11.35%), Trojan.JS.Miner.m (11.12%) and Trojan.Win32.Miner.gen (9.32%).

Geography of attacks



Geography of miners attacks, November 2018 – October 2019

Vulnerable applications used in cyberattacks

This reporting period will stick in our memory for a great number of targeted attacks based on zero-day exploits. During 2019, Kaspersky experts made the following discoveries:

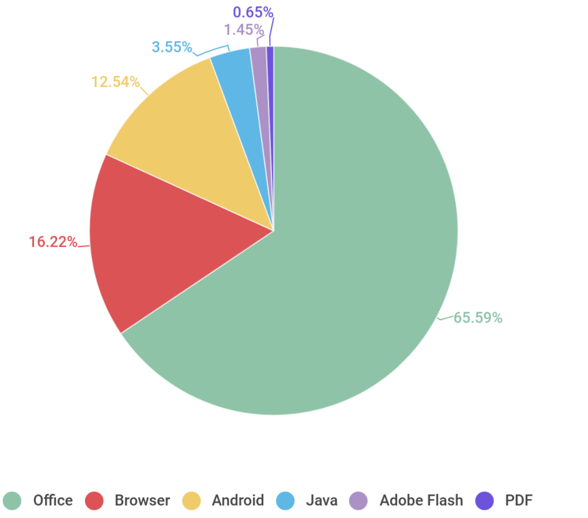
- The vulnerability CVE-2018-8611 patched in the December collection of fixes was used by FruityArmor and SandCat hacker groups, and possibly others. By the time an exploit was detected for this vulnerability, FruityArmor was already quite a famous hacker group with a history of using zero-day exploits, while SandCat, on the contrary, was relatively new on the scene. The detected vulnerability proved a very serious one, as it allowed to obtain system privileges and execute kernel-level code in all Windows versions, including the then most current Windows 10 RS4. In addition, it resided in the Kernel Transaction Manager driver, enabling the exploit to bypass web browser sandboxes.
- The vulnerability CVE-2019-0797 was detected in February and patched in the March collection of fixes. Same as the previous one — CVE-2018-8611 — the new vulnerability could potentially be used by different hacker groups, including FruityArmor and SandCat. It became the fourth actively exploited zero-day vulnerability detected by Kaspersky during the first six months of the year. Same as the ones detected earlier, it was used to obtain elevated privileges in Windows, but unlike CVE-2018-8611, the vulnerable component was the win32k.sys diver in charge of graphics and interface.
- In March, the actively exploited vulnerability CVE-2019-0859 was discovered, which allowed to elevate Windows user rights through yet another win32k.sys driver error. Its rather peculiar payload, provided together with shellcode, may indicate that the exploit was used by one of the cybercriminal groups targeting the financial sector.
- The vulnerability CVE-2019-13720 was discovered in late August in the aftermath of a series of attacks on fresh versions of Google Chrome. After we alerted Google about this actively exploited vulnerability, the company updated its Chrome browser to version 78.0.3904.87. We tagged these attacks Operation WizardOpium, for even though the code was somewhat similar, we were unable to get clear connections with other groups.

Compared to last year, the total number of actively used zero-day exploits we detected together with other industry peers in 2019 increased.

During the reporting period, we registered a drop in the number of exploits for Adobe Flash Player, which will cease to be supported by the end of next year. The share of web browser exploits has slightly shrunk, too, despite the arrival of some new publicly exploited zero-day vulnerabilities. The same is true for Android, the share of exploits for which has dropped to 12%. The share of PDF exploits, on the contrary, has somewhat grown.

During the previous reporting period, we observed a rapid growth in the number of users attacked by Microsoft Office exploits, and by Q4 2018 exploits for this application package were leading by the number of attacks. In the current period of report, Microsoft Office remains in the lead among the most attacked applications, but unlike previous years, this year the cybercriminals' arsenal has not suffered any major changes: CVE-2017-11882, CVE-2018-0802, CVE-2017-8570, and CVE-2017-0199 are still the most used exploits. Even though the exploit lineup is basically the same, the attackers keep finding new methods to obfuscate documents and avoid static detection techniques, but this topic deserves a separate Securelist review.

The rating list of vulnerable applications is based on verdicts returned by Kaspersky products for the blocked exploits used by cybercriminals, both in network attacks and vulnerable local applications, including those run on mobile devices.



Malicious exploits broken down by type of target applications, November 2018 — November 2019

During this reporting period, network attacks continued to be one of the most common types of attacks. It is safe to say that the year 2019 will be remembered for discovery of multiple vulnerabilities in the remote desktop subsystem in different versions of Windows OS. These received the general designations of BlueKeep and DejaBlue. At present we observe no widespread exploiting of these vulnerabilities, which may be down to the complexity of the process. Same as in previous years, the network attacks list is topped by various exploits for the SMB protocol, known as EternalBlue, EternalRomance, etc. It also should not go unmentioned that a large share of malicious network traffic comes from password mining queries targeting popular network services and servers like Remote Desktop Protocol and Microsoft SQL Server, respectively.

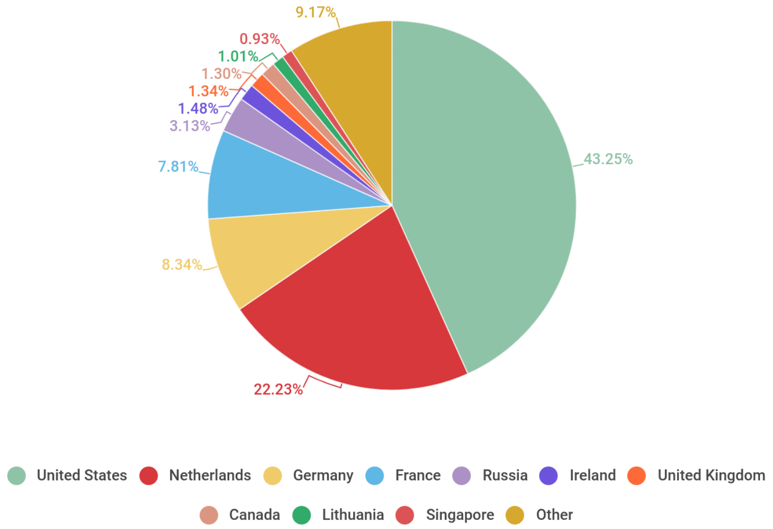
Web-based attacks

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.

During the reporting period, Kaspersky solutions blocked **975 491 360** attacks launched from web resources located in various countries and territories around the world. **90.83%** 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 2018 – October 2019

Compared to last year's results, the distribution of web attack sources has not changed much. The United States (43.25%) is in first place, followed by the Netherlands (22.23%) and Germany (8.34%).

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 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 reporting period, adware programs and their components were detected on 78% of user computers on which the web antivirus was triggered.

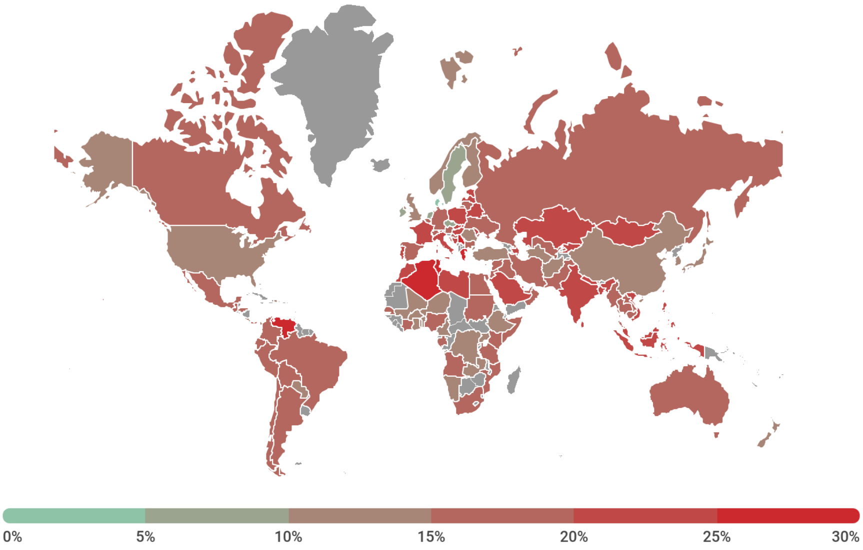
The TOP 20 countries where users face the greatest risk of online infection

	Country*	%**
1	Algeria	33.02
2	Venezuela	30.25
3	Tunisia	29.50
4	Greece	26.07
5	Serbia	25.80
6	Bangladesh	24.95
7	Moldova	24.78
8	Azerbaijan	24.74
9	Belarus	24.52
10	Poland	24.13
11	Mongolia	24.05
12	Philippines	23.89
13	Morocco	23.87
14	Latvia	23.22
15	Qatar	22.94
16	Vietnam	22.57
17	Taiwan, province of China	22.13
18	France	21.99
19	Portugal	21.97
20	Italy	21.96

On average, during the reporting period a Malware-class attack was detected at least once on 19.8% of computers around the world.

* We excluded those countries where the number of Kaspersky 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 products in the country



Geography of malicious web attacks, November 2018 – October 2019

TOP 20 verdicts detected online

During the reporting period, Kaspersky's web antivirus detected **24 610 126** unique malicious objects (scripts, exploits, executable files, etc.) and **273 782 113** unique URLs that were blocked by web antivirus components. We identified the 20 malicious programs most actively involved in online attacks launched against computers.

	Verdict	%*
1	Malicious URL	85.40
2	Trojan.Script.Generic	5.89
3	Trojan.Script.Miner.gen	3.89
4	Trojan-Clicker.HTML.Iframe.dg	0.65
5	Trojan.BAT.Miner.gen	0.26
6	Trojan-Downloader.JS.Inor.a	0.22
7	Trojan.PDF.Badur.gen	0.21
8	DangerousObject.Multi.Generic	0.21
9	Trojan-Downloader.Script.Generic	0.17
10	Trojan-PSW.Script.Generic	0.15
11	Trojan.Script.Agent.gen	0.15
12	Hoax.HTML.FraudLoad.m	0.13
13	Exploit.Script.Generic	0.08
14	Trojan.Script.Agent.bg	0.07
15	Trojan.Multi.Preqw.gen	0.06
16	Exploit.MSOffice.CVE-2017-11882.gen	0.06
17	Trojan-Downloader.JS.SLoad.gen	0.05
18	Hoax.Script.Loss.gen	0.05
19	Trojan.JS.Miner.m	0.05
20	Trojan-Downloader.VBS.SLoad.gen	0.04

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

Though several detections related to web-miners still can be seen in this top, number of mining Javascripts downloads and attempts to connect web-mining related esources dropped down significantly in comparison to 2018. This affects overall number of web-detections and Malicious URLs blocks particularly.

Malicious URL (85.40%) in the first place is the verdict identifying links from our black list (links to web pages containing redirects to exploits, sites with exploits and other malicious programs, botnet control centers, extortion websites, etc.).

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'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 during the reporting period. This rating does not include the Adware and Riskware classes of program.

	Verdict	%*
1	DangerousObject.Multi.Generic	26.43
2	Trojan.Multi.BroSubsc.gen	9.48
3	Trojan.Script.Generic	6.19
4	Trojan.Multi.GenAutorunReg.a	5.94
5	HackTool.Win64.HackKMS.b	4.40
6	HackTool.MSIL.KMSAuto.by	3.69
7	HackTool.Win32.KMSAuto.bu	3.54
8	Trojan.WinLNK.Agent.gen	3.45
9	HackTool.MSIL.KMSAuto.a	3.43
10	Trojan.WinLNK.Starter.gen	3.42
11	HackTool.MSIL.KMSAuto.dh	2.83
12	HackTool.Win32.KMSAuto.c	2.75
13	HackTool.MSIL.KMSAuto.di	2.65
14	Trojan.Win32.Generic	2.53
15	HackTool.Win32.KMSAuto.cb	2.50
16	HackTool.Win64.HackKMS.c	2.47
17	HackTool.MSIL.KMSAuto.bx	2.18
18	Trojan.Win32.AutoRun.gen	1.93
19	Virus.Win32.Sality.gen	1.90
20	HackTool.Win32.KMSAuto.m	1.90

The entities in our TOP 20 are quite the same as in the previous year, though their order slightly differs.

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

On the 1st place is DangerousObject.Multi.Generic (26.43%) verdict, which is used for malware detected with the help of cloud technologies. Cloud technologies work when the antivirus databases do not yet contain either signatures or heuristics to detect a malicious program but the company's cloud antivirus database already has information about the object. In fact, this is how the very latest malware is detected.

The second place in the top is taken by relatively new threat, that appears to be widely spread – Trojan.Multi.BroSubsc.gen (9.48%). Malware of this family is installed on browsers deceptively after the user visits fraudulent or advertising resources. This malware displays advertising messages even if a browser is inactive.

It is also noticeable, that rather old family Virus.Win32.Sality.gen still persists and it is the only Virus threat that keeps appearing in the TOP 20.

Overall, we have noticed that local Miners became less popular, and has left the top of local threats.

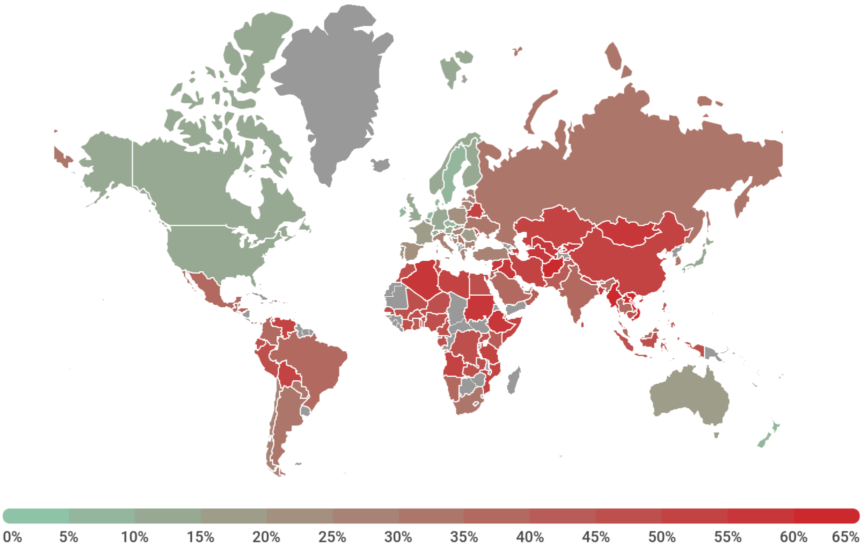
Countries where users face the highest risk of local infection

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	Afghanistan	65.55
2	Vietnam	61.84
3	Lao people's democratic republic	61.95
4	Myanmar	60.80
5	Bangladesh	59.51
6	Mongolia	59.41
7	Uzbekistan	58.06
8	Turkmenistan	57.57
9	Algeria	57.50
10	Iraq	57.33
11	Syriac	57.04
12	Sudan	55.41
13	Kyrgyzstan	55.15
14	Ethiopia	55.08

	Country*	%**
15	Bolivia	54.85
16	China	54.64
17	Nepal	54.57
18	Mozambique	54.52
19	Libya	54.36
20	Rwanda	54.14



Geography of local malware attacks, November 2018 – October 2019

In 2018, at least one malicious program was found on an average of 34.05% of computers, hard drives or removable media belonging to KSN users.

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