Kaspersky Security Bulletin 2020. Statistics

kaspersky

Contents

kaspersky

Figures of the year

- During the year, 10.18% of Internet user computers worldwide experienced at least one **Malware-class** attack.
- Kaspersky solutions blocked **666,809,967** attacks launched from online resources in various countries across the world.
- **173,335,902** unique URLs were recognized as malicious by Web Anti-Virus.
- Our Web Anti-Virus blocked **33,412,568** unique malicious objects.
- Ransomware attacks were defeated on the computers of **549,301** unique users.
- During the reporting period, miners attacked **1,523,148** unique users.
- Attempted infections by malware designed to steal money via online access to bank accounts were logged on the devices of **668,619** users.

Mobile threat statistics will be presented in the separate Mobile Virology 2020 report

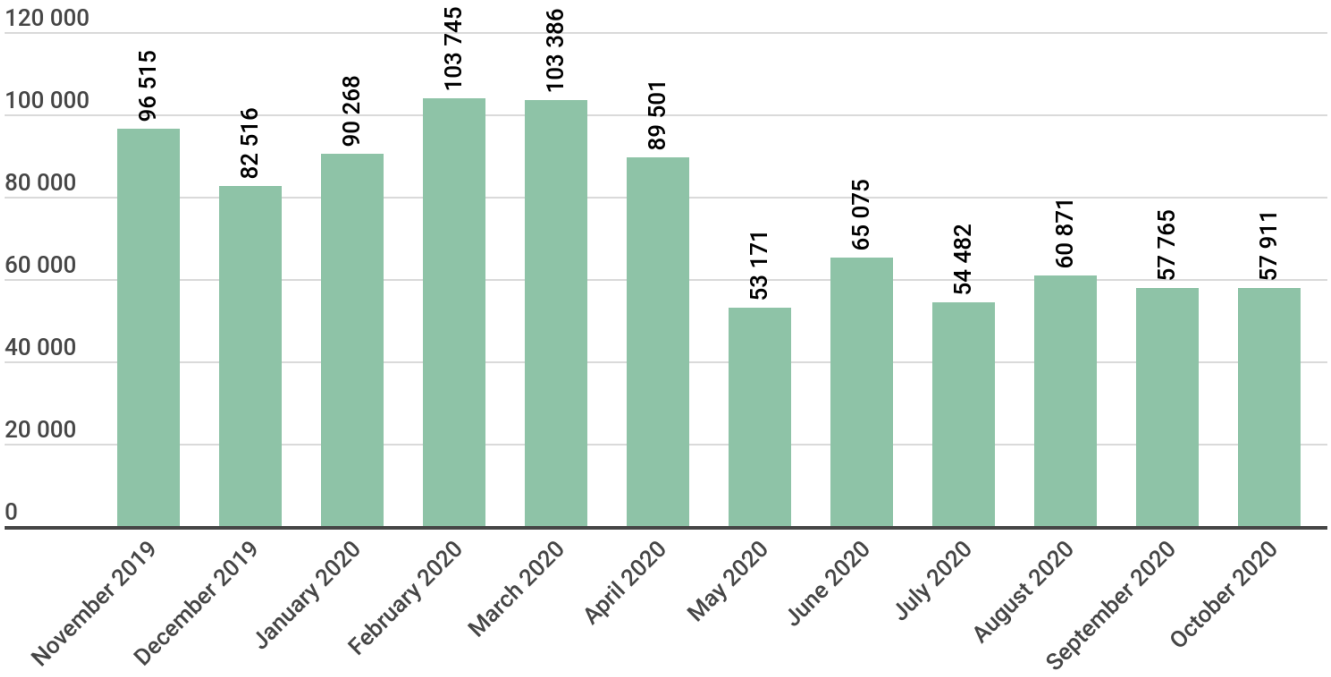
All statistics in this report are from the global cloud service Kaspersky Security Network (KSN), which receives information from components in our security solutions. The data was obtained from users who have given their consent to it being sent to KSN. Millions of Kaspersky users around the globe assist us in this endeavor to collect information about malicious activity. The statistics in this report cover the period from November 2019 to October 2020, inclusive.

Financial threats

The statistics include not only banking threats, but malware for ATMs and payment terminals. Statistics on analogous mobile threats are given in the separate report.

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 **668,619** users.

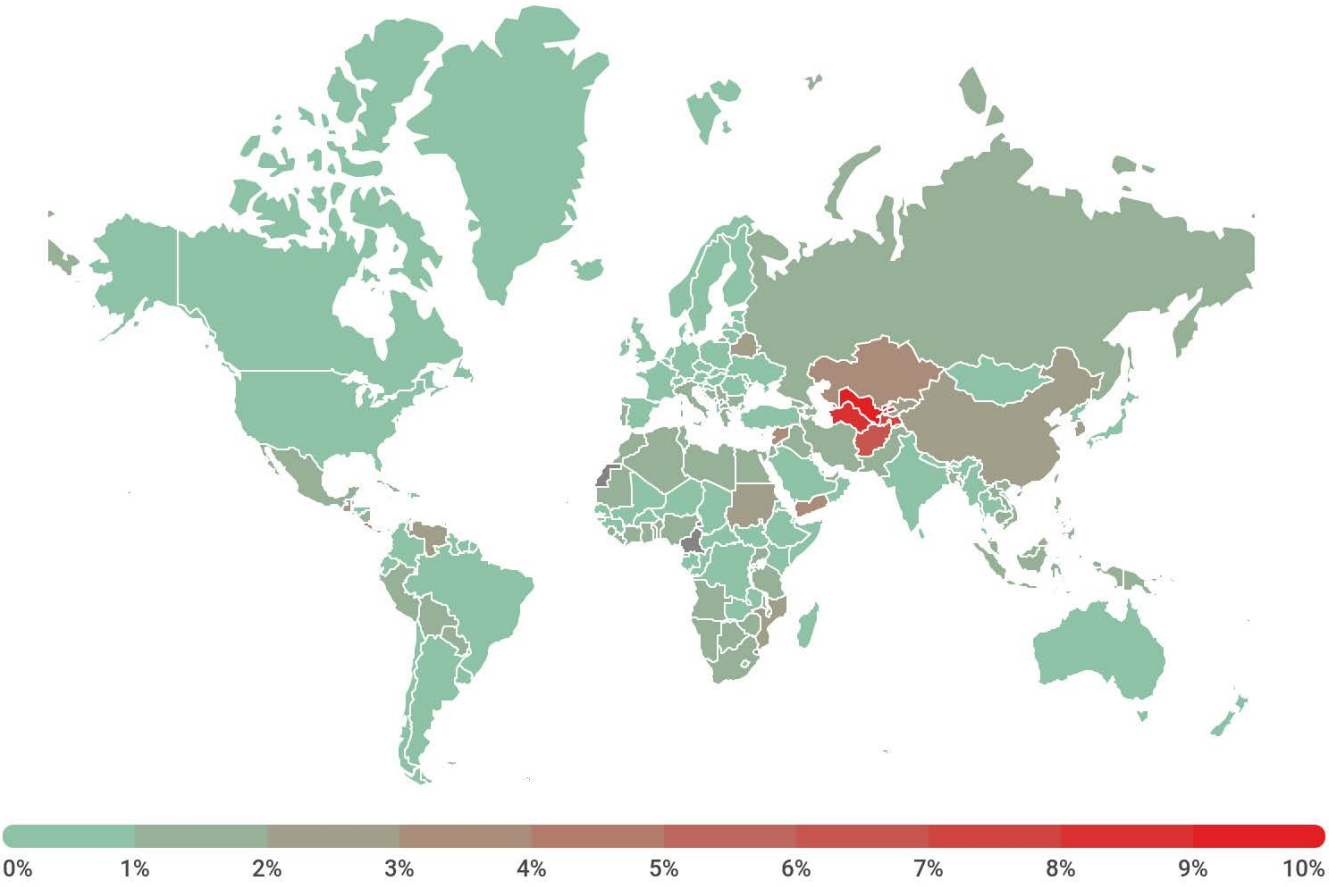


Number of users attacked by financial malware,
November 2019 — October 2020

kaspersky

Attack geography

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



Geography of banking malware attacks, November 2019 — October 2020

kaspersky

Top 10 countries by share of attacked users

	Country*	%**
1	Uzbekistan	10.4
2	Turkmenistan	8.6
3	Tajikistan	7.5
4	Afghanistan	6.6
5	Costa Rica	4.0
6	Yemen	3.9
7	Kazakhstan	3.5
8	Syria	3.3
9	Guatemala	2.8
10	South Korea	2.7

* Excluded are countries with relatively few Kaspersky product users (under 10,000).
** The share of unique users whose computers were targeted by financial malware in the total number of unique users attacked by all kinds of malware.

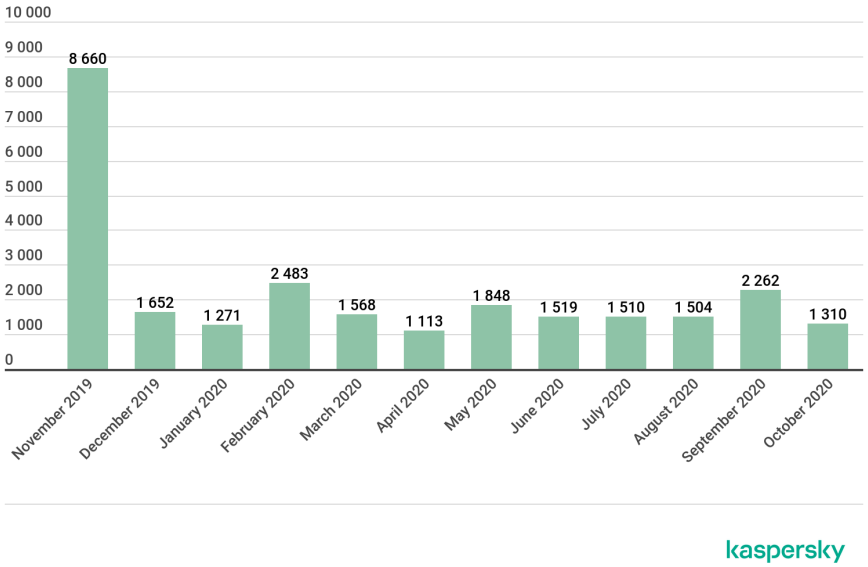
Top 10 financial malware families

	Name	%*
1	Zbot	21.6
2	Emotet	15.1
3	CliptoShuffler	15
4	RTM	11.1
5	Trickster	5.1
6	Nimnul	4.2
7	Neurevt	3.3
8	Danabot	3.2
9	SpyEye	3.2
10	Nymaim	2.1

* The share of unique users attacked by this malware in the total number of users attacked by financial malware.

Ransomware programs

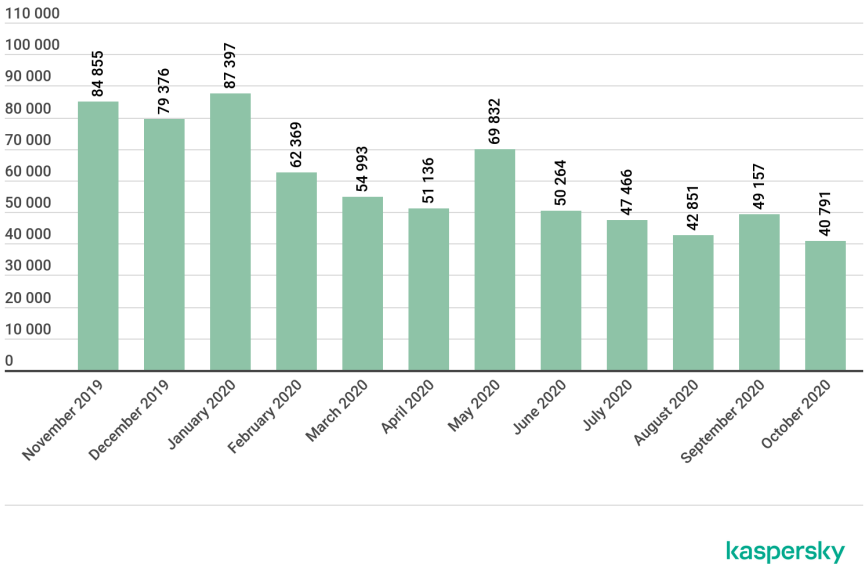
During the reporting period, we identified more than **26,700** ransomware modifications and detected **21** new families. Note that we did not create a separate family for each new piece of ransomware. Most threats of this type were assigned the generic verdict, which we give to new and unknown samples.



Number of new ransomware modifications detected,
November 2019 — October 2020

Number of users attacked by ransomware Trojans

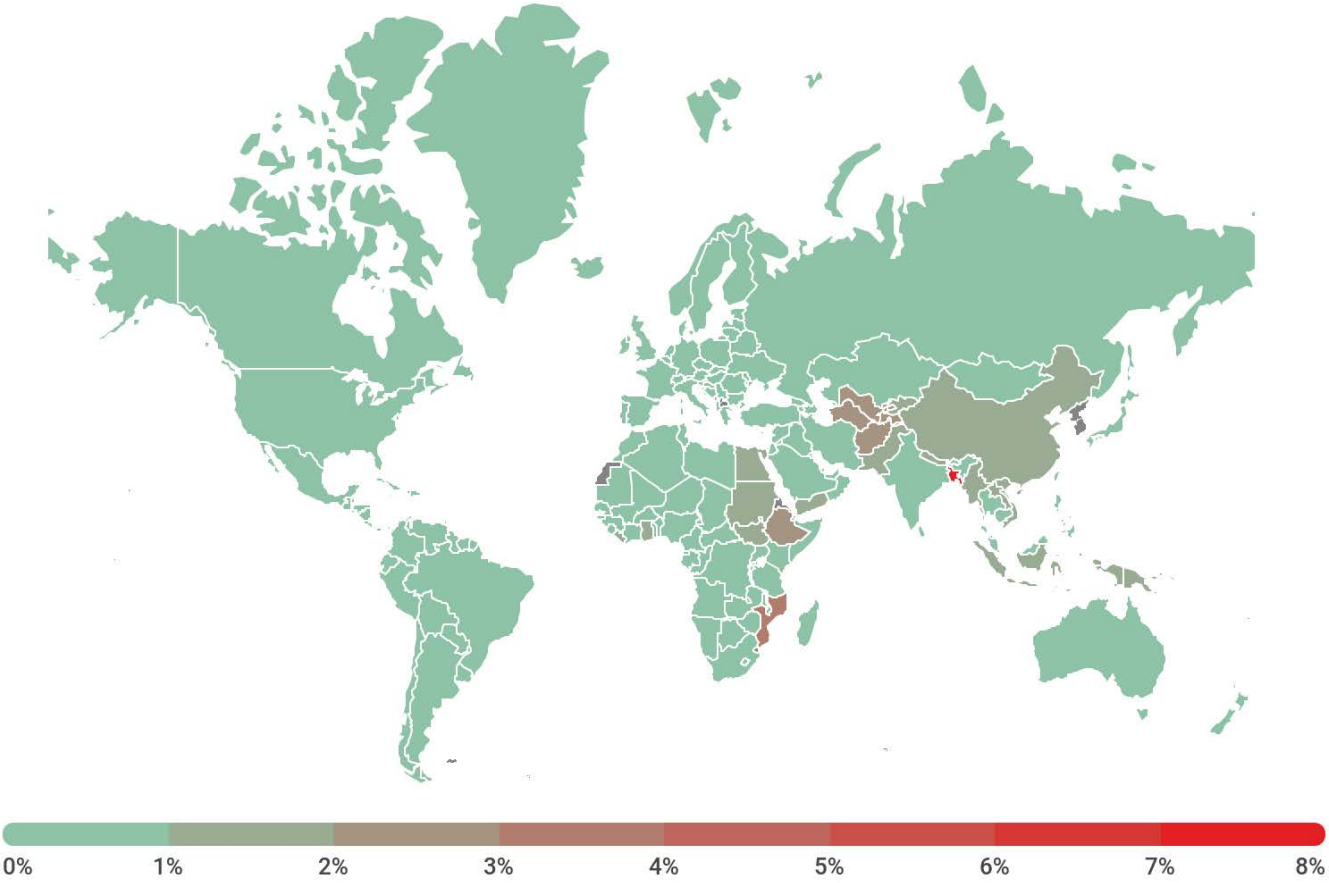
During the reporting period, ransomware Trojans attacked **549,301** unique users, including 123,630 corporate users (excluding SMBs) and 15,940 users associated with small and medium-sized businesses.



Number of users attacked by ransomware Trojans,
November 2019 — October 2020

kaspersky

Attack geography



Geography of attacks by ransomware Trojans,
November 2019 — October 2020

Top 10 countries attacked by ransomware Trojans

	Country*	%**
1	Bangladesh	8.12
2	Mozambique	3.13
3	Turkmenistan	2.65
4	Haiti	2.47
5	Uzbekistan	2.39
6	Ethiopia	2.10
7	Afghanistan	2.06
8	Nepal	1.97
9	Sudan	1.92
10	Kyrgyzstan	1.77

* Excluded are countries with relatively few Kaspersky users (under 50,000).
** The share of unique users whose computers were attacked by ransomware Trojans in the total number of unique users of Kaspersky products in the country.

Top 10 most common families of ransomware Trojans

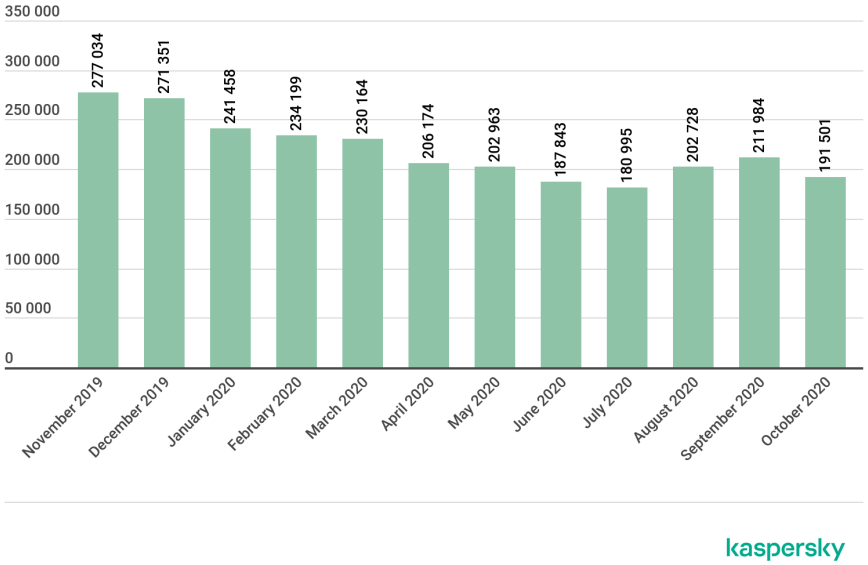
	Name	Verdict	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	16.56
2	(generic verdict)	Trojan-Ransom.Win32.Phny	11.56
3	(generic verdict)	Trojan-Ransom.Win32.Gen	11.37
4	Stop	Trojan-Ransom.Win32.Stop	7.76
5	(generic verdict)	Trojan-Ransom.Win32.Encoder	6.66
6	(generic verdict)	Trojan-Ransom.Win32.Generic	4.77
7	(generic verdict)	Trojan-Ransom.Win32.Crypren	4.07
8	PolyRansom/VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.PolyRansom	2.54
9	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	2.21
10	(generic verdict)	Trojan-Ransom.Win32.Crypmod	1.83

* The share of unique Kaspersky users attacked by the given family of ransomware Trojans in the total number of users attacked by ransomware Trojans.

Miners

Number of users attacked by miners

During the reporting period, we detected attempts to install a miner on the computers of **1,523,148** unique users. Miners accounted for 2.49% of all attacks and 13.82% of all Risktool-type programs

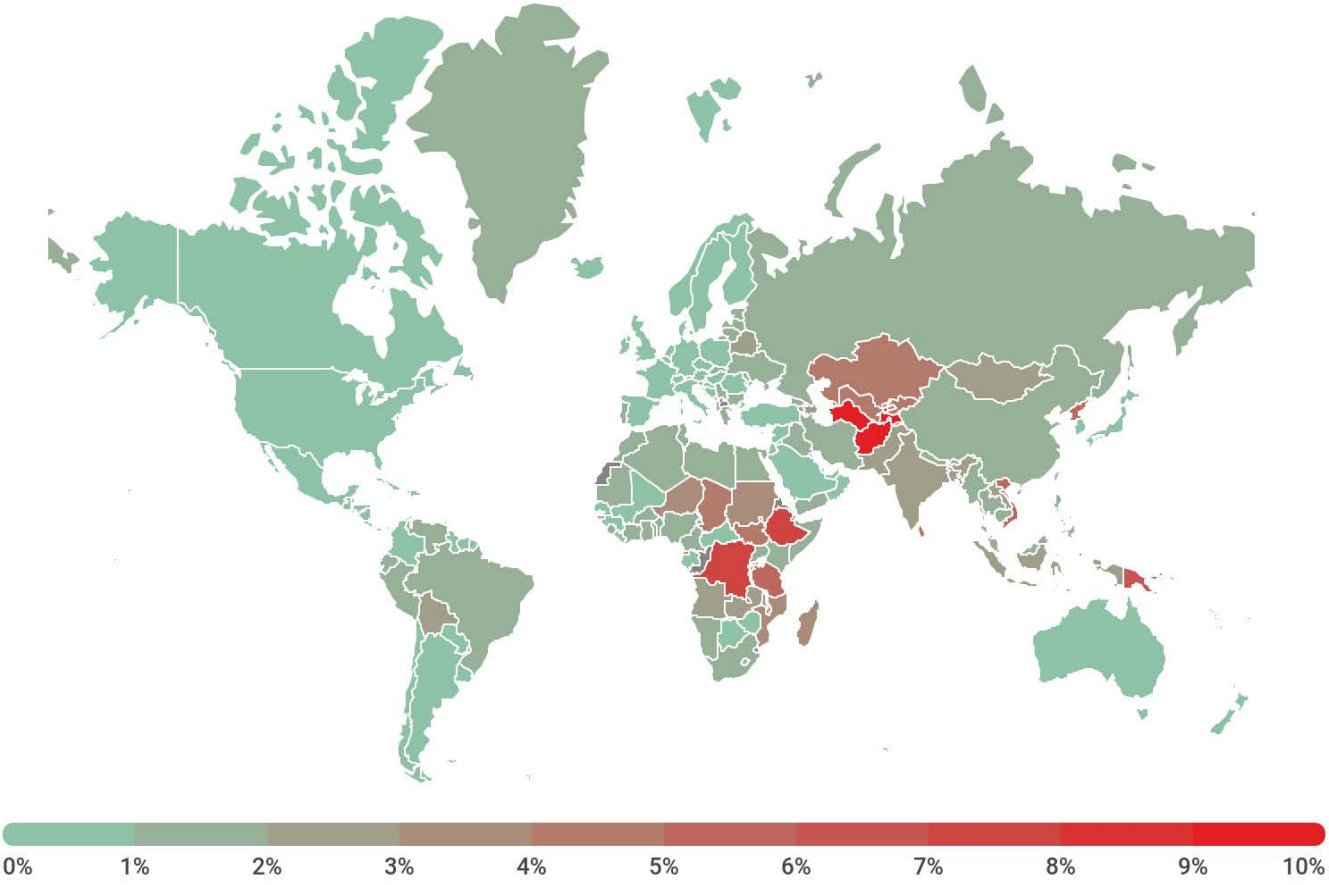


Number of users attacked by miners, November 2019 — October 2020

During the reporting period, Kaspersky products detected Trojan.Win32.Miner.bbb more often than others, which accounted for 17.53% of all users attacked by miners. It was followed by Trojan.Win32.Miner.ays (10.86%), Trojan.JS.Miner.m (10.28%) and Trojan.Win32.Miner.gen (8.00%).

kaspersky

Attack geography



Geography of miner-related attacks,
November 2019 — October 2020

kaspersky

Vulnerable applications used by cybercriminals during cyber attacks

In 2020, most vulnerabilities were discovered by researchers before attackers could exploit them. However, there was no doing without zero-day vulnerabilities, of which Kaspersky found:

- CVE-2020-1380, a use-after-free vulnerability in the Jscript9 component of Microsoft's Internet Explorer browser caused by insufficient checks during the generation of optimized JIT code. This vulnerability was most likely used by the APT group DarkHotel at the first stage of system compromise, after which the payload was delivered by an additional exploit that escalated privileges in the system;
- CVE-2020-0986 in the GDI Print/Print Spooler component of Microsoft's Windows operating system, enabling manipulation of process memory for arbitrary code execution in the context of a system service process. Exploitation of this vulnerability gives attackers the ability to bypass sandboxes, for example, in the browser.

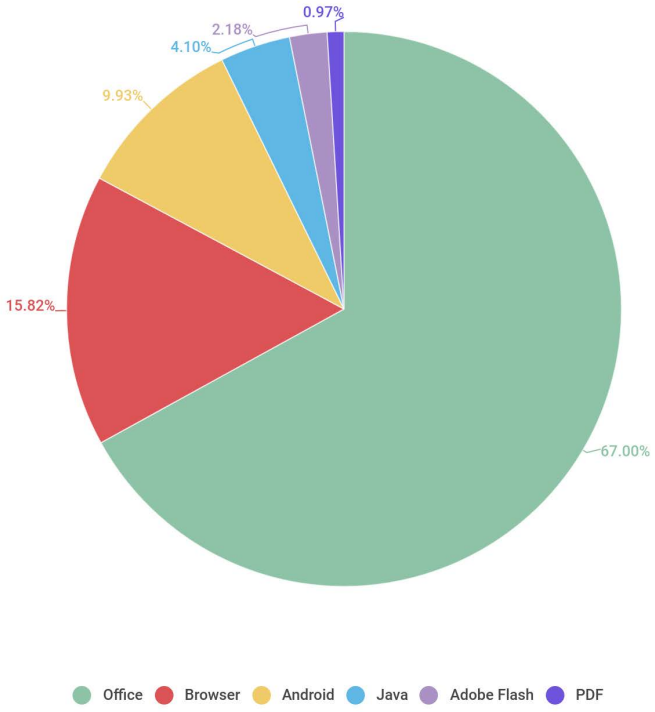
Noteworthy vulnerabilities found by our partners:

- Four zero-day vulnerabilities in Google Chrome: CVE-2020-16010, CVE-2020-16009, CVE-2020-15999 and CVE-2020-6418. All were used to compromise systems, and allowed attackers to run code on the target system. For example, CVE-2020-15999 is a bug in the popular libfreetype2 library that arises when processing PNG images embedded inside TrueType fonts. In theory, the vulnerability is also exploitable in other products that use this library;
- Three zero-day vulnerabilities in Mozilla Firefox (CVE-2020-6820, CVE-2020-6819, CVE-2019-17026), also enabling user system compromise;
- A zero-day vulnerability in Microsoft's Internet Explorer (CVE-2020-0674), apparently exploited by DarkHotel. It results in a potential use-after-free scenario, whereby the garbage collector stops tracking objects passed as arguments to the callback function when using the array sorting operation;
- Four zero-day vulnerabilities in Microsoft Windows (CVE-2020-0938, CVE-2020-1020, CVE-2020-1027, CVE-2020-17087). CVE-2020-17087, a bug in the cryptographic kernel driver caused by insufficient checks of input data when using IOCTL calls from the user level, allowing attackers to bypass the Google Chrome sandbox and infiltrate the system.

Next year, we will likely hear more about attribution and tools that used these vulnerabilities.

During the reporting period, we observed a slight drop in the number of attacks on Microsoft Office applications, but this did not prevent them from being the most popular target. Cybercriminals continued to modify and obfuscate the known vulnerabilities CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 and CVE-2017-0199, allowing them to bypass security mechanisms in some antivirus solutions for a while.

Support for Adobe Flash comes to an end this year, but our data shows that cybercriminal interest in the player continues unabated: the number of attacks exploiting Flash bugs is up by 0.7 p.p. In the reporting period, web browsers are unmoved on 11% and remain one of the main methods of infecting unprotected user systems. Attacks on Android (9.93%) using vulnerabilities fell by 2.6 p.p. The number of exploits targeting vulnerabilities in the Java platform (4.10%) and in PDF (0.97%) changed insignificantly.



Distribution of exploits used in attacks by type of application attacked, November 2019 — November 2020

The rating of vulnerable applications is based on verdicts by Kaspersky products for blocked exploits used by cybercriminals both in network attacks and in vulnerable local apps, including on users' mobile devices.

As before, network attacks were the most common method of system penetration in 2020, and a significant portion of them is made up of brute-force attacks on various network services: RDP, MSSQL, etc. In addition, this reporting period demonstrated that everything in the Windows operating system is cyclical, and that most of the detected vulnerabilities exist in the same services, for example, in the drivers of the SMB (SMBGhost, SMBBleed), DNS (SigRed) and ICMPv6 (BadNeighbor) network protocols. Two critical vulnerabilities (CVE-2020-0609, CVE-2020-0610) were found in the Remote Desktop Gateway service. An interesting vulnerability, dubbed Zerologon, was also discovered in the NetLogon service. Lastly, despite the fact that exploits for the EternalBlue and EternalRomance families are old, they are still used by attackers.

Attacks on macOS

During the reporting period, we detected not only modifications of known malware for macOS, but a handful of new threats as well. Among them are two backdoors, Capip and Lador. The latter is of particular note for being written in the Go language and weighing 5.5 MB (several times larger than similar malware written in Objective C). Another curiosity is the self-replicating ransomware Virus.OSX.ThifQseut.a, aka EvilQuest.

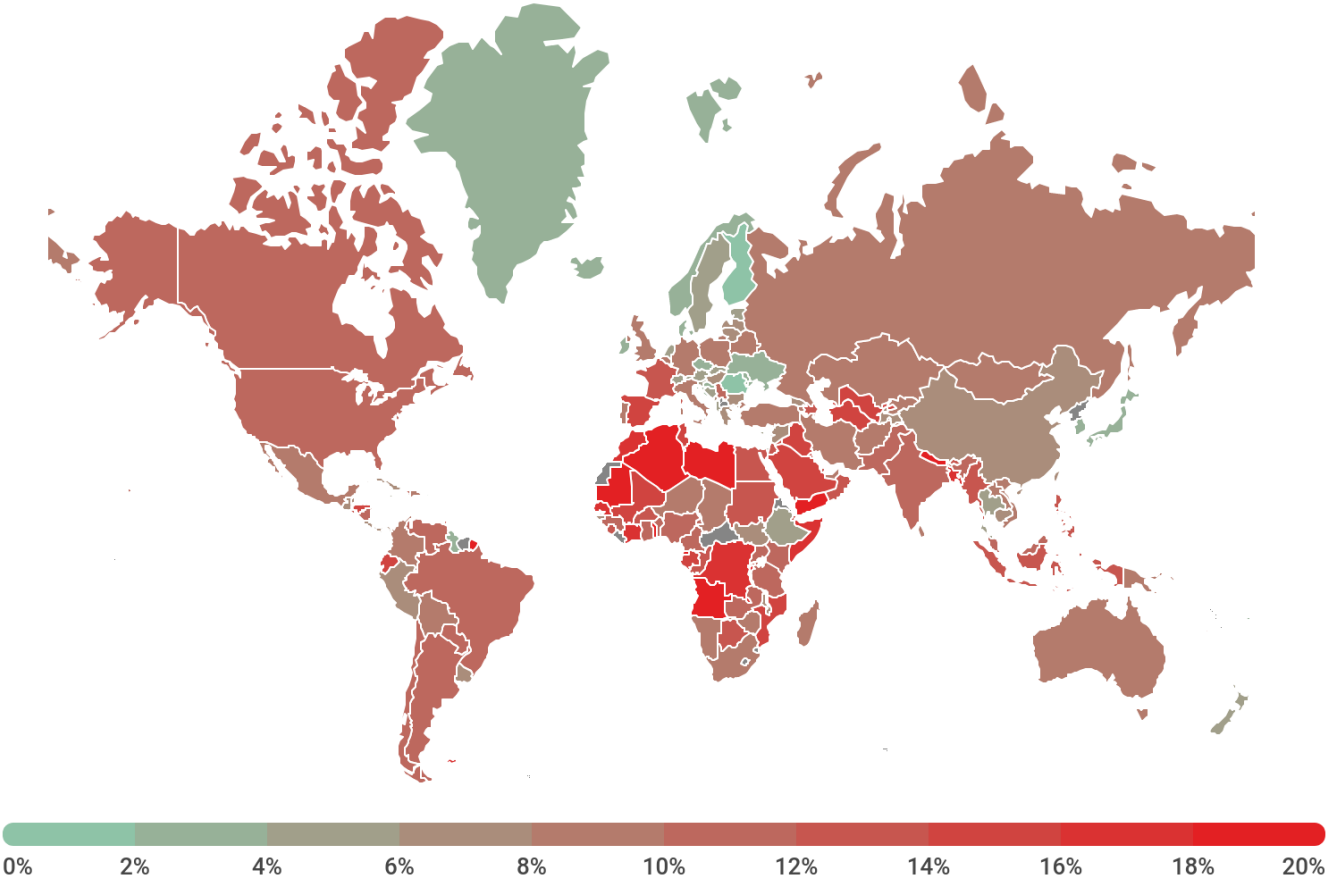
Top 20 threats for macOS

	Verdict	%*
1	Trojan-Downloader.OSX.Shlayer.a	17.27
2	Monitor.OSX.HistGrabber.b	9.10
3	AdWare.OSX.Pirrit.j	8.08
4	AdWare.OSX.Cimpli.k	6.99
5	AdWare.OSX.Pirrit.x	6.93
6	AdWare.OSX.Bnodlero.at	6.33
7	AdWare.OSX.Pirrit.o	5.41
8	AdWare.OSX.Ketin.h	5.33
9	AdWare.OSX.Bnodlero.t	5.14
10	AdWare.OSX.Spc.a	4.95%

* The share of unique users who encountered this malware in the total number of users of Kaspersky security solutions for macOS who were attacked.

Most of this reporting period's Top 10 was made up of adware. That said, first place was taken by the Shlayer Trojan, which we wrote about in early 2020.

Threat geography



Attack geography for macOS,
November 2019 — October 2020

kaspersky

Top 10 countries by share of attacked users

	Country*	%**
1	Spain	14.03
2	France	13.54
3	Canada	11.35
4	USA	10.76
5	India	10.53
6	Brazil	10.22
7	Mexico	9.86
8	Italy	9.80
9	Australia	9.09
10	Great Britain	8.99

* Excluded from the rating are countries with relatively few users of Kaspersky security solutions for macOS (under 5,000).
** The share of unique users attacked in the total number of users of Kaspersky security solutions for macOS in the country.

IoT attacks

IoT threat statistics

During the reporting period, more than 80% of attacks on Kaspersky traps were carried out using the Telnet protocol.

Telnet	81.02%
SSH	18.98%

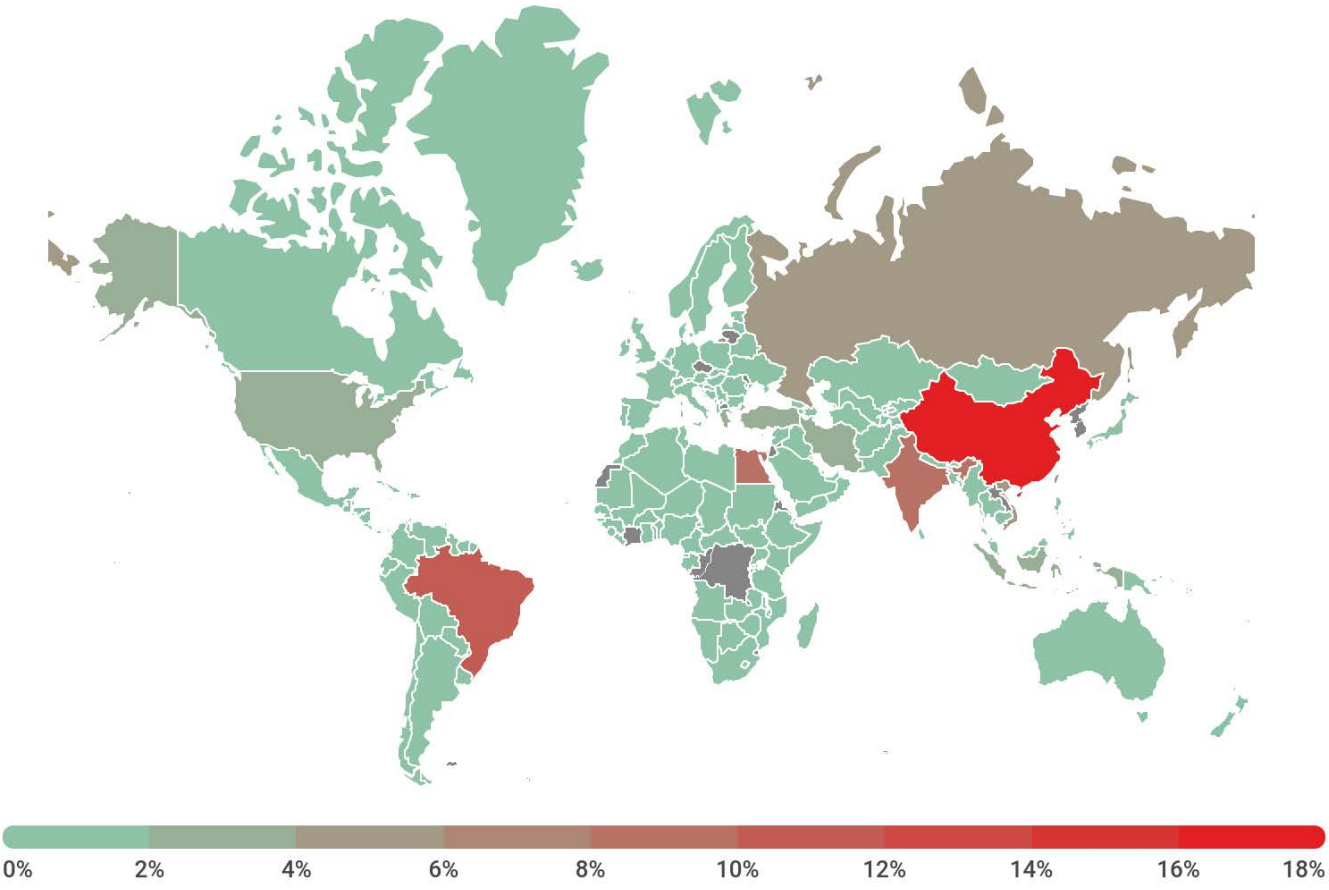
Distribution of attacked services by number of unique IP addresses of devices that carried out attacks, November 2019 — October 2020

As for distribution of sessions, Telnet also prevails, accounting for two-thirds of all working sessions.

Telnet	67.60%
SSH	32.40%

Distribution of cybercriminal working sessions with Kaspersky traps, November 2019 — October 2020

As a result, devices that carried out attacks using the Telnet protocol were selected to build the map of attackers' IP addresses.



Geography of IP addresses of devices from which attempts were made to attack Kaspersky Telnet traps, November 2019 — October 2020

Top 10 countries by location of devices from which attacks were carried out on Kaspersky Telnet traps

	Country*	%**
1	China	17.95
2	Brazil	10.35
3	Egypt	9.26
4	India	8.51
5	Taiwan, Province of China	5.11
6	Vietnam	4.94
7	Russia	4.00
8	Iran	3.96
9	Turkey	2.46
10	USA	2.42

* The share of devices from which attacks were carried out in the given country in the total number of devices.

Threats loaded into traps

	Verdict	%*
1	Trojan-Downloader.Linux.NyaDrop.b	42.43
2	Backdoor.Linux.Mirai.b	27.01
3	Backdoor.Linux.Mirai.ba	10.09
4	Backdoor.Linux.Gafgyt.a	7.46
5	Backdoor.Linux.Gafgyt.bj	1.54
6	Trojan-Downloader.Shell.Agent.p	0.83
7	Backdoor.Linux.Mirai.cn	0.73
8	Backdoor.Linux.Mirai.cw	0.64
9	Backdoor.Linux.Mirai.h	0.53
10	Backdoor.Linux.Mirai.c	0.51

* The share of malware type in the total number of malicious programs downloaded to IoT devices following a successful attack.

Attacks via web resources

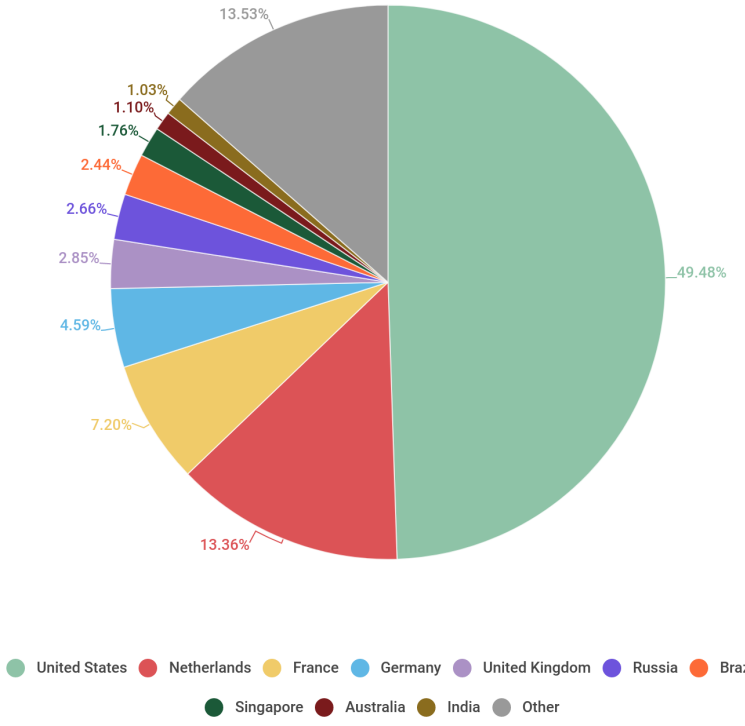
The statistics in this section are based on Web Anti-Virus, which protects users when malicious objects are downloaded from malicious/infected web pages. Cybercriminals create such sites on purpose and web resources with user-created content (for example, forums), as well as hacked legitimate resources, can be infected.

Countries that are sources of web-based attacks:

The following statistics show the distribution by country of the sources of Internet attacks blocked by Kaspersky products on user computers (web pages with redirects to exploits, sites containing exploits and other malicious programs, botnet C&C centers, etc.). Any unique host could be the source of one or more web-based attacks.

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.

Kaspersky solutions blocked **666,809,967** attacks launched from online resources in various countries across the globe. Moreover, 86.47% of these resources were located in just 10 countries.



Distribution of web attack sources by country,
November 2019 — October 2020

kaspersky

As in 2019, the top source of web attacks is the US (49.48%), up by 6 p.p. Germany (4.59%) dropped from third to fourth position, replaced by France (7.20%).

Countries where users faced the greatest risk of online infection

To assess the risk of online infection faced by users, for each country we calculated the percentage of Kaspersky users on whose computers Web Anti-Virus was triggered during the reporting period. The resulting data provides an indication of the aggressiveness of the environment in which computers operate in different countries.

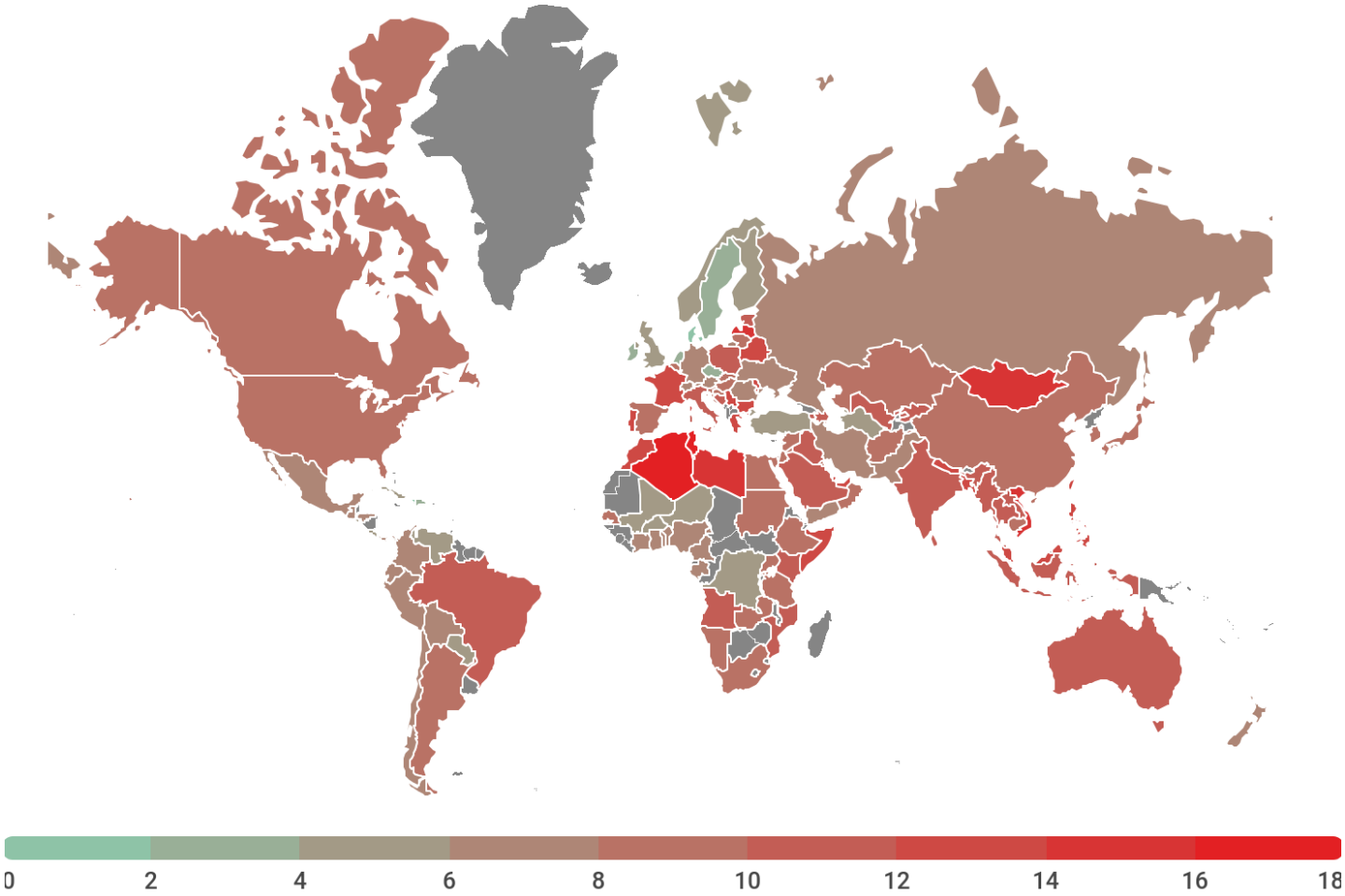
This rating only includes attacks by malicious programs that fall under the Malware class; it does not include Web Anti-Virus detections of potentially dangerous or unwanted programs such as RiskTool or adware. Overall, during the reporting period, adware and its components were registered on 78% of users' computers on which the Web Anti-Virus was triggered.

Top 20 countries where users faced the greatest risk of online infection

	Country*	%**
1	Tunisia	18.27
2	Algeria	16.42
3	Mongolia	15.94
4	Vietnam	15.61
5	Latvia	14.73
6	Libya	14.25
7	Greece	13.96
8	Bangladesh	13.75
9	Taiwan, Province of China	13.62
10	France	13.58
11	Bulgaria	13.37
12	Nepal	13.15
13	Philippines	12.99
14	Portugal	12.79
15	Qatar	12.75
16	Morocco	12.71
17	Malaysia	12.55
18	Moldova	12.55
19	Belarus	12.54
20	Somalia	12.45

* Excluded are countries with relatively few Kaspersky users (under 50,000).
** The share of unique users targeted by Malware-class attacks in the total number of unique users of Kaspersky products in the country.

On average, **10.18%** of Internet user computers worldwide experienced at least one Malware-class attack during the reporting period.



**Geography of malicious web-based attacks,
November 2019 — October 2020**

Top 20 malicious programs most actively used in online attacks

During the reporting period, Kaspersky's Web Anti-Virus detected **33,412,568** unique malicious objects (scripts, exploits, executable files, etc.), as well as **173,335,902** unique malicious URLs on which Web Anti-Virus was triggered. Based on the collected data, we identified the 20 most actively used malicious programs in online attacks on users' computers.

	Verdict*	%**
1	Malicious URL	66.07
2	Trojan.Script.Generic	9.25
3	Trojan.Multi.Preqw.gen	6.10
4	Trojan.BAT.Miner.gen	3.57
5	Trojan.Script.Miner.gen	3.43
6	Hoax.HTML.FraudLoad.m	1.38
7	Trojan.PDF.Badur.gen	1.12
8	Backdoor.HTTP.TeviRat.gen	0.51
9	Trojan-Downloader.Script.Generic	0.50
10	Trojan-PSW.Script.Generic	0.47
11	Exploit.MSOffice.CVE-2017-11882.gen	0.38
12	DangerousObject.Multi.Generic	0.36
13	Trojan-Clicker.HTML.IFrame.dg	0.23
14	Trojan.Script.Redirector.gen	0.22
15	Hoax.Script.Loss.gen	0.19
16	Exploit.Script.Generic	0.17
17	Trojan.MSOffice.SAgent.gen	0.13
18	Trojan.Script.Agent.bg	0.13
19	Trojan-Downloader.JS.SLoad.gen	0.12
20	Trojan-Downloader.MSOffice.SLoad.gen	0.12

* Excluded from the list are HackTool-type threats.
** The share of attacks by the given malicious program in the total number of Malware-class web attacks registered on the computers of unique users of Kaspersky products.

In the reporting period, first place as ever went to the Malicious URL verdict (66.07%). Users see it when our solutions block redirection attempts via known dangerous links to resources with exploits/other malware, C&C botnets, ransomware sites, etc.

A few web miners, such as Trojan.Script.Miner.gen, still rank in our Top 20, but hidden mining is nowhere near as prevalent as a couple of years ago.

The detections in our Top 20 that contain MS Office or PDF in their names represent a range of malicious documents used in spam mailings. The task is usually to deliver a payload, for example, the Emotet banker, and it is this download that our Web Anti-Virus blocks.

Local threats

Statistics on local infections of user computers is an important indicator. They include objects that penetrated the target computer through infecting files or removable storage media, or initially made their way onto the computer in non-open form (for example, programs in complex installers, encrypted files, etc.). These statistics additionally include objects detected on user computers after the first system scan by Kaspersky's Anti-Virus application.

This section analyzes statistics produced by Anti-Virus scans of files on the hard drive at the moment they were created or accessed, as well as the results of scanning removable storage media.

Top 20 malicious objects detected on user computers

We identified the 20 most commonly detected threats on user computers during the reporting period. Not included are Riskware-type programs and adware.

	Verdict*	%**
1	DangerousObject.Multi.Generic	26.59
2	Trojan.Multi.BroSubsc.gen	20.44
3	Trojan.Multi.GenAutorunReg.a	7.99
4	Trojan.Multi.Misslink.a	7.47
5	Trojan.Script.Generic	6.45
6	Trojan.WinLNK.Agent.gen	3.00
7	Trojan.Win32.SEPEH.gen	2.88
8	Trojan.Win32.Generic	2.53
9	Trojan.WinLNK.Starter.gen	2.45
10	Trojan.Multi.Agent.gen	2.12
11	Trojan.WinLNK.Runner.jo	2.02
12	Trojan.Win32.AutoRun.gen	1.91
13	Trojan.Multi.GenAutorunTask.c	1.91
14	Virus.Win32.Sality.gen	1.84
15	Trojan.Multi.GenAutorunTask.a	1.76
16	Trojan.Multi.GenAutorunTaskFile.a	1.73
17	Trojan-Downloader.Script.Generic	1.64
18	Trojan.AndroidOS.Boogr.gsh	1.59

	Verdict*	%**
19	Trojan.Multi.GenBadur.gen	1.52
20	Virus.Win32.Pioneer.cz	1.51

* Excluded from the list are HackTool-type threats.
** The share of unique users on whose computers File Anti-Virus detected the given object in the total number of unique users of Kaspersky products whose Anti-Virus was triggered by malware.

First place in our Top 20 was taken by the verdict DangerousObject.Multi.Generic (26.59%), which we assign to malware detected using cloud technologies. These technologies are deployed when the antivirus databases lack data for detecting a piece of malware, but the antivirus company's cloud already contains information about the object. This is basically how the latest malicious programs are detected.

Countries where users faced the highest risk of local infection

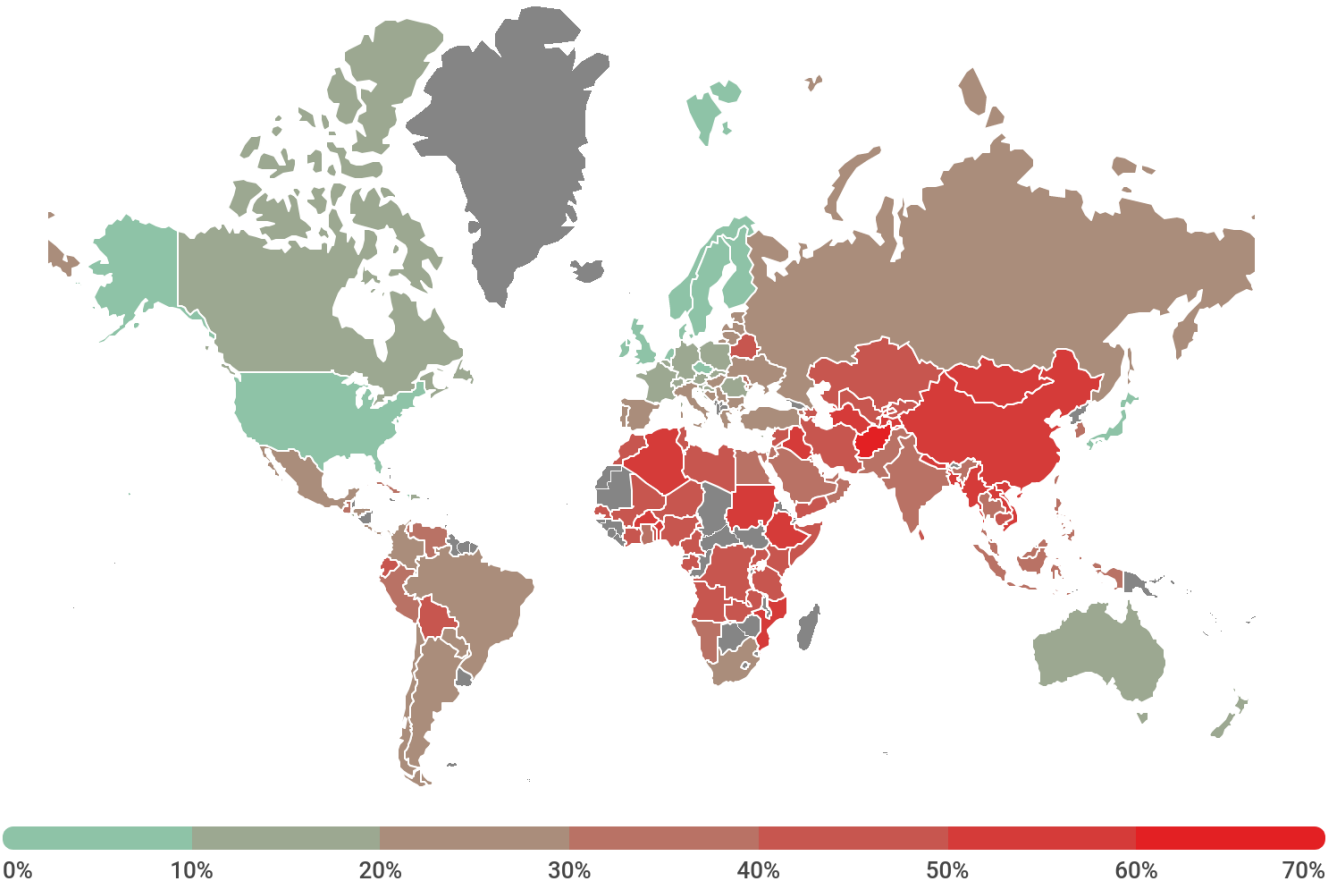
For each country, we calculated how often users there encountered a File Anti-Virus triggering during the year. Included are detections of objects found on user computers or removable media connected to them (flash drives, camera/phone memory cards, external hard drives). These statistics reflect the level of personal computer infection in different countries.

Top 20 countries by level of risk of local infection

	Country*	%**
1	Afghanistan	63.52
2	Myanmar	59.89
3	Laos	57.40
4	Vietnam	56.84
5	Mongolia	55.11
6	China	54.81
7	Bangladesh	54.74
8	Ethiopia	54.67
9	Rwanda	53.22
10	Burkina Faso	52.57
11	Turkmenistan	52.47
12	Benin	52.43
13	Tajikistan	52.29
14	Algeria	51.85
15	Iraq	51.73
16	Mozambique	50.98
17	Sudan	50.88

	Country*	%**
18	Nepal	50.07
19	Tanzania	49.34
20	Ivory Coast	49.31

* Excluded are countries with relatively few Kaspersky users (under 50,000).
** The share of unique users on whose computers Malware-class local threats were blocked in the total number of unique users of Kaspersky products in the country.



Geography of local infections by malware, November 2019 — October 2020

During the reporting period, on average, at least one piece of malware was detected on **28.65%** of computers, hard drives or removable media belonging to KSN users.