Kaspersky Security Bulletin 2023. Statistics

Contents

All statistics in this report come from the Kaspersky Security Network (KSN) global cloud service, which receives information from components in our security solutions. The data was obtained from users who had given their consent to it being sent to KSN. Millions of Kaspersky users around the globe assist us in collecting information about malicious activity. The statistics in this report cover the period from November 2022 through October 2023.

The year in figures

During the reported period, Kaspersky solutions:

- Blocked **437,414,681** malware-class attacks launched from online resources across the globe.
- Found **106,357,530** unique malicious URLs.
- Detected **112,922,612** unique malicious objects with the help of Web Anti-Virus components.
- Prevented ransomware attacks on the computers of **193,662** unique users.
- Blocked miners from infecting **1,140,573** unique users.
- Prevented the launch of malware designed to steal money via online access to bank accounts on the devices of **325 225** users.

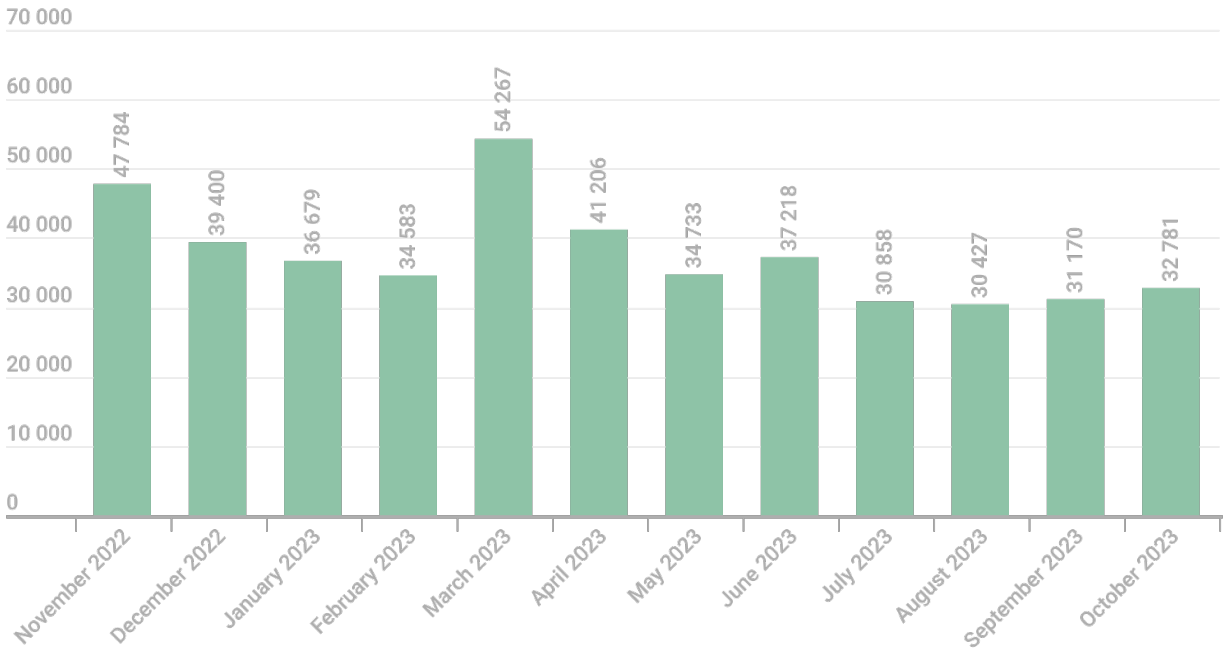
Mobile threat statistics will be given in the "Mobile malware threat landscape in 2023" report

Financial threats

The statistics include not only banking threats, but also malware for ATMs and payment terminals.

Number of users attacked by financial malware

In the reporting period, Kaspersky solutions blocked financial malware from starting on the computers of **325,225** users.



Number of users attacked by financial malware,
November 2022 through October 2023

Geography of attacked users

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

TOP 10 countries and territories by share of attacked users

	Countries and territories*	%**
1	Afghanistan	6.2
2	Turkmenistan	5.4
3	Tajikistan	4.0
4	China	3.3
5	Sudan	2.6
6	Mauritania	2.6
7	Switzerland	2.5
8	Yemen	2.4
9	Egypt	2.2
10	Paraguay	2.2

* Excluded are countries and territories with relatively few Kaspersky users (under 10,000).
** Unique users whose computers were targeted by financial malware as a percentage of all users attacked by all kinds of malware.

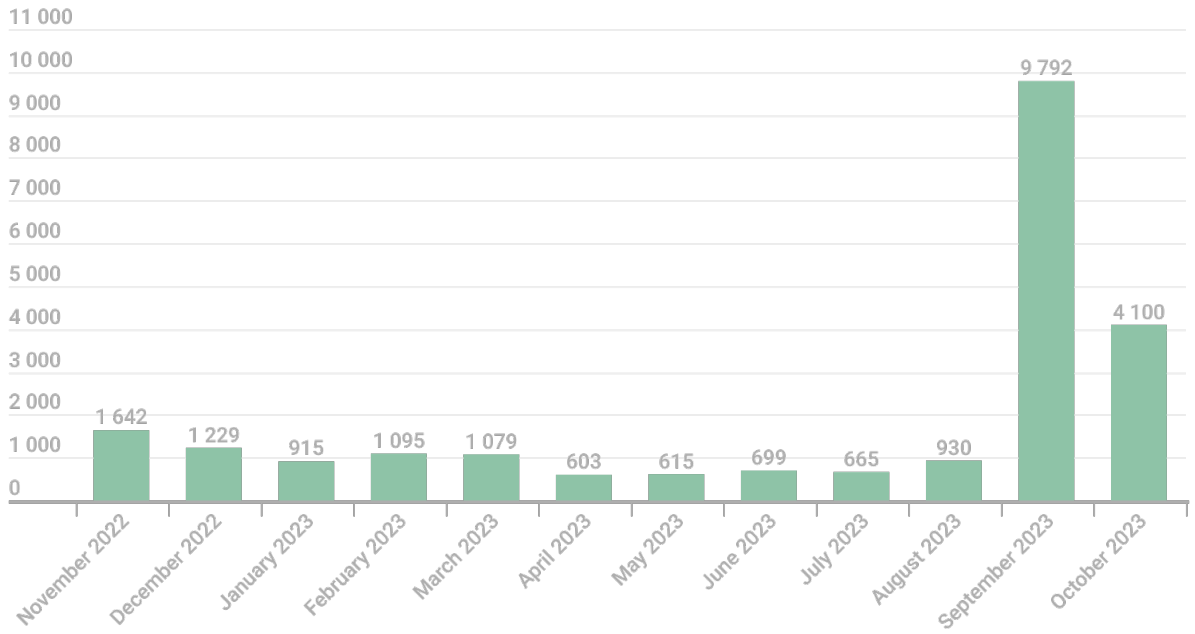
TOP 10 financial malware families

	Name	Verdict	%*
1	Ramnit/Nimnul	Trojan-Banker.Win32.Nimnul	30.4
2	Zbot/Zeus	Trojan-Spy.Win32.Zbot	18.9
3	Emotet	Trojan-Banker.Win32.Emotet	16.1
4	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	6.1
5	RTM	Trojan-Banker.Win32.RTM	2.2
6	Danabot	Trojan-Banker.Win32.Danabot	1.9
7	Qbot/Qakbot	Trojan-Banker.Win32.Qbot	1.8
8	IcedID	Trojan-Banker.Win32.IcedID	1.3
9	Tinba/TinyBanker	Trojan-Banker.Win32.Tinba	1.2
10	BitStealer	Trojan-Banker.Win32.BitStealer	1.0

* Unique users attacked by this malware as a percentage of all users attacked by financial malware.

Ransomware

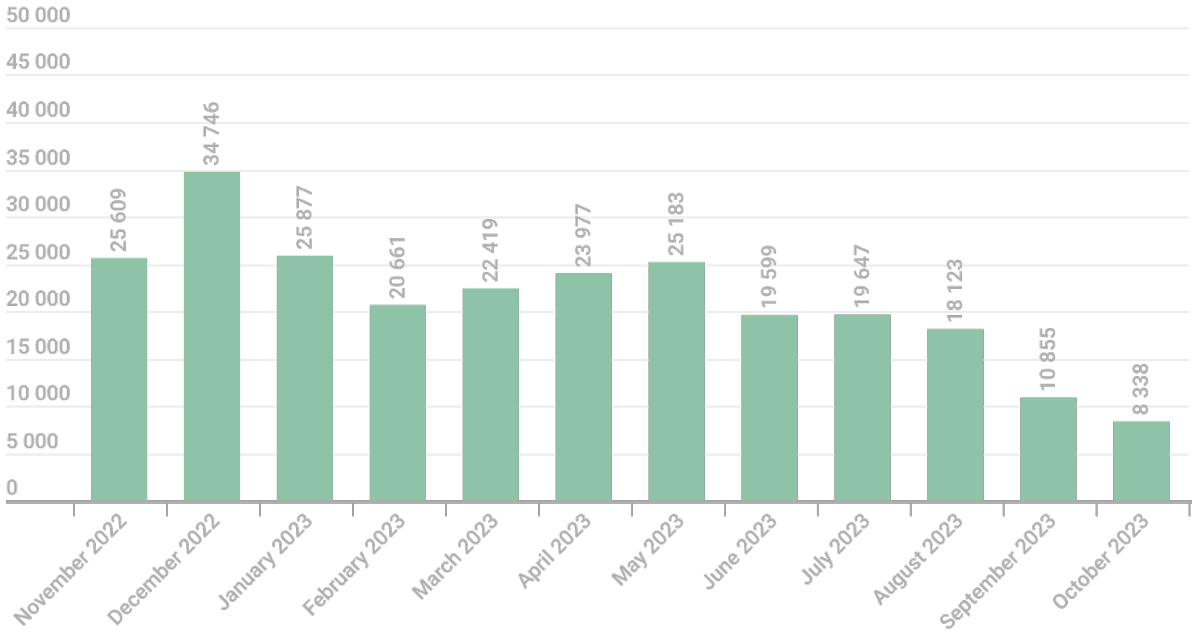
In the reporting period, we identified more than **23,364** ransomware modifications and detected **43** new families. Note that we did not create a separate family for every new ransomware specimen. Most threats of this type were assigned the generic verdict, which we give to new and unknown samples.



Number of new ransomware modifications detected,
November 2022 through October 2023

Number of users attacked by ransomware Trojans

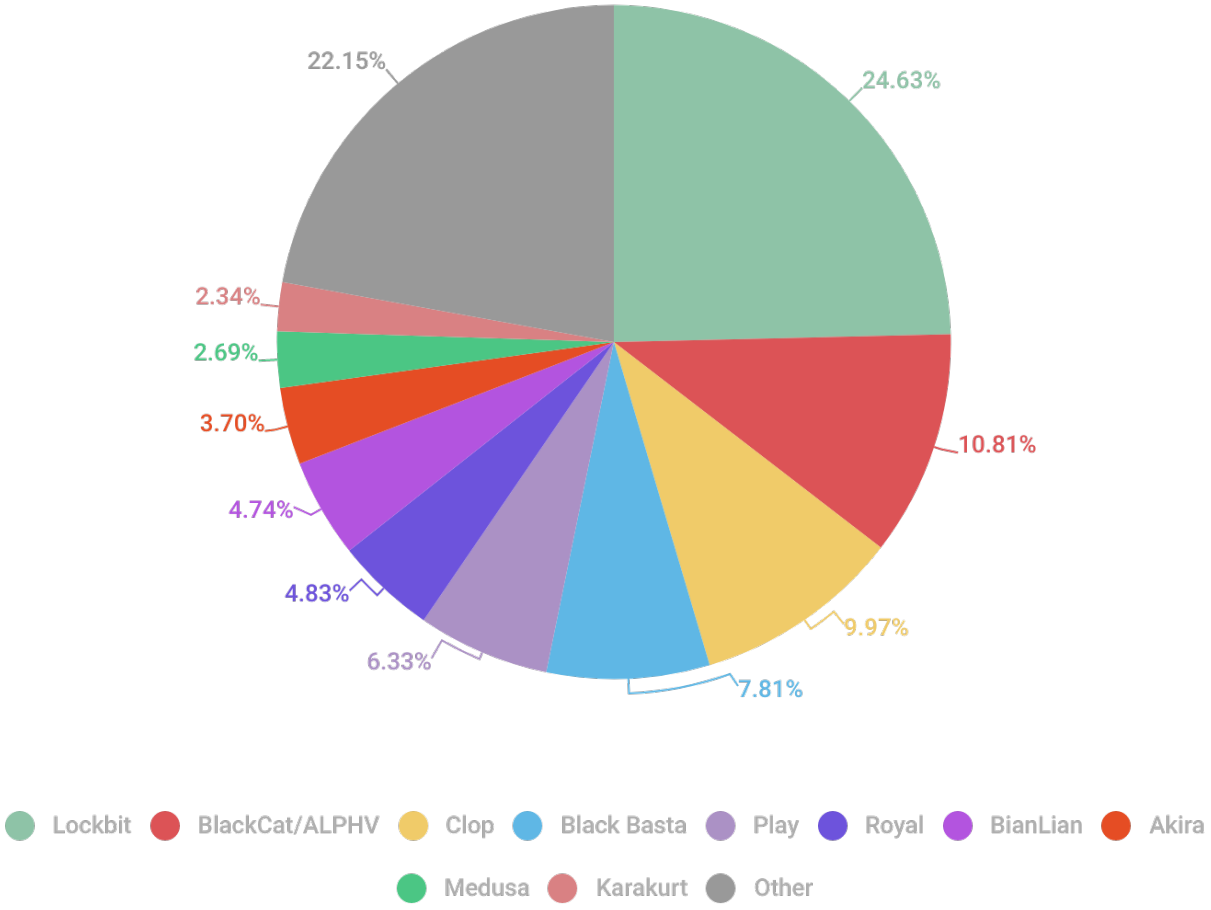
During the reporting period, ransomware Trojans attacked **193,662** unique users, including **52,999** corporate users (SMBs excluded) and **6,351** users associated with small and medium-sized businesses.



Number of users attacked by ransomware Trojans,
November 2022 through October 2023

Most prolific groups

This section looks at ransomware groups that engage in so-called "double extortion", that is stealing and encrypting confidential data. Most of these groups target large companies and often maintain a DLS (data leak site) to publish a list of organizations they have attacked.



The most prolific ransomware gangs,
November 2022 through October 2023

The diagram shows each group's share in the total number of victims published on all the groups' DLSs.

Geography of attacked users

TOP 10 countries and territories attacked by ransomware Trojans

	Countries and territories*	%**
1	Bangladesh	2.41
2	Yemen	1.85
3	Taiwan	1.62
4	South Korea	1.47
5	Sudan	1.15
6	Mozambique	1.09
7	Palestine	0.97
8	Afghanistan	0.97
9	Pakistan	0.88
10	Turkmenistan	0.63

* Excluded are countries and territories with relatively few Kaspersky users (under 50,000).
** Unique users whose computers were attacked by ransomware Trojans as a percentage of all unique Kaspersky users in the country or territory.

TOP 10 most common families of ransomware Trojans

	Name	Verdict	%*
1	Magniber	Trojan-Ransom.Win64.Magni	17.14
2	(generic verdict)	Trojan-Ransom.Win32.Gen	12.39
3	WannaCry	Trojan-Ransom.Win32.Wanna	11.46
4	(generic verdict)	Trojan-Ransom.Win32.Encoder	9.43
5	Stop/Djvu	Trojan-Ransom.Win32.Stop	6.39
6	(generic verdict)	Trojan-Ransom.Win32.Phny	5.69
7	(generic verdict)	Trojan-Ransom.Win32.Crypren	4.54
8	PolyRansom/VirLock	Virus.Win32.PolyRansom / Trojan-Ransom.Win32.PolyRansom	3.13
9	(generic verdict)	Trojan-Ransom.Win32.Agent	2.91
10	(generic verdict)	Trojan-Ransom.MSIL.Crypmodng	1.75

* Unique Kaspersky users attacked by the given family of ransomware Trojans as a percentage of all users who experienced attacks 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 **1,140,573** unique users. Miners accounted for 3.12% of all attacks and 17.09% of all RiskTool-type programs.

Number of users attacked by miners,
November 2022 through October 2023

During the reporting period, Kaspersky products detected Trojan.Win32.Miner.gen more often than others, accounting for 25.12% of all users attacked by miners. It was followed by Worm.NSIS.BitMin.d (12.39%), Trojan.Win32.Miner.ays (10.41%), and Trojan.Win64.Miner.all (8.51%).

Geography of attacked users

TOP 10 countries and territories attacked by miners

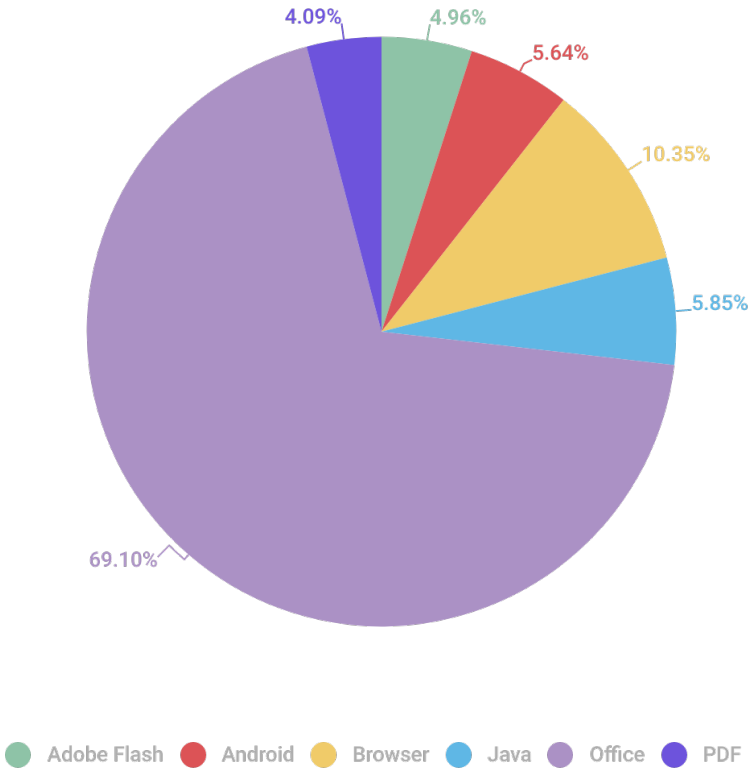
	Countries and territories*	%**
1	Turkmenistan	10.38
2	Afghanistan	7.67
3	Kazakhstan	3.77
4	Tajikistan	3.33
5	Uzbekistan	2.92
6	Mongolia	2.83
7	Mozambique	2.82
8	Belarus	2.80
9	Sudan	2.65
10	Kyrgyzstan	2.61

* Excluded are countries and territories with relatively few Kaspersky users (under 50,000)..
** Unique users whose computers were attacked by miners as a percentage of all unique Kaspersky users in the country or territory.

Vulnerable applications used by criminals in cyberattacks

The reporting period was remembered for a number of dangerous vulnerabilities in business applications, like **CVE-2023-34362**, **CVE-2023-35036** and **CVE-2023-35708** in MoveIT Transfer or **CVE-2023-23397** in Microsoft Outlook.

Speaking of attacks on consumers, it is worth noting the "zero-day" vulnerabilities CVE-2023-4863, CVE-2023-5217 and CVE-2023-4762 in Google Chrome, and CVE-2023-28252 in OS Windows. As usual, we saw attempts to exploit well-known vulnerabilities in the Equation Editor, such as CVE-2017-11882 and CVE-2018-0802, and other Microsoft Office components.



Distribution of exploits used in attacks by type of application attacked, November 2022 through October 2023

The rankings of vulnerable applications are based on Kaspersky verdicts for blocked exploits used by cybercriminals both in network attacks and in vulnerable local apps, both on desktop and mobile devices.

Attacks on macOS

During the reporting period, a few interesting samples of macOS malware were observed:

- Trojan-Spy that steals Keychain data
- Infostealer pretending to be a macOS game to collect data from browsers, instant messengers, and crypto wallets
- Infected Xcode project trying to download a backdoor
- Selling MacStealer and AMOS Trojans via Telegram
- Trojanized 3CXDesktopApp in the supply-chain attack downloading a macOS backdoor
- The BlueNoroff group's backdoors written in Rust and disguised as PDF viewers

Kaspersky's solutions detect these and other threats targeted at macOS.

TOP 20 threats for macOS

	Verdict	%*
1	AdWare.OSX.Pirrit.ac	11.21
2	AdWare.OSX.Agent.ai	10.47
3	AdWare.OSX.Amc.e	8.83
4	AdWare.OSX.Pirrit.j	7.92
5	AdWare.OSX.Agent.gen	7.34
6	AdWare.OSX.Bnodlero.ax	6.77
7	AdWare.OSX.Pirrit.ae	5.83
8	Trojan-Downloader.OSX.Agent.h	4.85
9	Monitor.OSX.HistGrabber.b	4.70
10	Hoax.OSX.MacBooster.a	4.32

* Unique users who encountered this malware as a percentage of all Kaspersky macOS users who were attacked.

Threat geography

TOP 10 countries and territories by share of attacked users

	Countries and territories*	%**
1	France	2.41
2	China	2.38
3	Italy	2.38
4	Spain	2.23
5	United States	2.16
6	India	2.16
7	Mexico	2.12
8	Canada	1.99
9	Australia	1.85
10	Great Britain	1.84

* Excluded from the rankings are countries and territories with relatively few Kaspersky macOS users (under 5,000).
** Unique users attacked in the country or territory as a percentage of all Kaspersky macOS users there..

IoT attacks

IoT threat statistics

During the reporting period, most devices that attacked Kaspersky honeypots used the Telnet protocol.

Telnet	83.85%
SSH	16.15%

Distribution of attacked services by number of unique IP addresses of attacking devices, November 2022 through October 2023

As for the distribution of sessions, Telnet again prevailed, with more than 98% of all working sessions.

Telnet	98.60%
SSH	1.40%

Distribution of malware sessions with Kaspersky honeypots, November 2022 through October 2023

TOP 10 countries and territories hosting devices that attacked Kaspersky Telnet honeypots

	Countries and territories*	%**
1	China	35.99
2	India	18.01
3	Brazil	4.57
4	Russian Federation	4.18
5	United States	3.45
6	South Korea	2.35
7	Venezuela	2.31
8	Taiwan	2.11
9	Argentina	1.85
10	Iran	1.84

* Devices that launched attacks in the country or territory as a percentage of the total number of attacking devices.

TOP 10 countries and territories hosting devices that attacked Kaspersky SSH honeypots

	Countries and territories*	%**
1	China	18.44
2	United States	11.64
3	South Korea	6.36
4	India	5.25
5	Singapore	4.65
6	Germany	4.50
7	Brazil	4.34
8	Russian Federation	3.62
9	Taiwan	3.01
10	Vietnam	2.83

* Devices that launched attacks in the country or territory as a percentage of the total number of attacking devices.

Threats uploaded to honeypots

	Verdict	%*
1	Trojan-Downloader.Linux.NyaDrop.b	36.46
2	Backdoor.Linux.Mirai.b	18.67
3	Backdoor.Linux.Mirai.cw	8.23
4	Backdoor.Linux.Mirai.ba	7.12
5	Backdoor.Linux.Mirai.fg	3.64
6	Trojan.Linux.Agent.nx	3.12
7	Backdoor.Linux.Mirai.es	2.90
8	Backdoor.Linux.Gafgyt.a	2.36
9	Trojan-Downloader.Shell.Agent.p	2.04
10	Backdoor.Linux.Mirai.ew	1.83

* Share of malware type in the total number of malicious programs uploaded to IoT devices in a successful attack.

Attacks via web resources

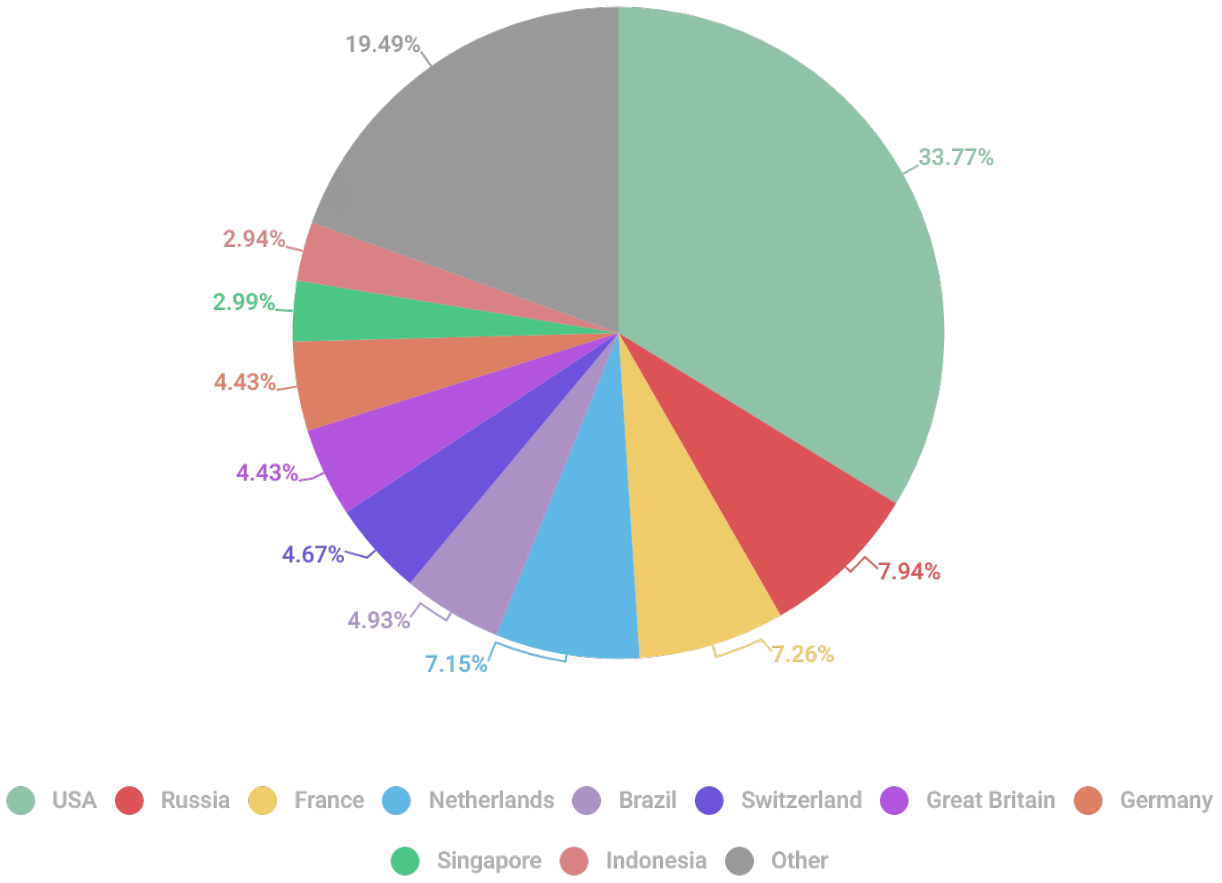
The statistics in this section draw on data from Web Anti-Virus, which protects users against malicious objects downloaded from malicious/infected web pages. Cybercriminals create malicious websites on purpose; web resources with user-generated content, such as message boards, and hacked legitimate resources can be infected.

Countries and territories that are sources of web-based attacks

The following statistics show the distribution by country or territory 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, and so on. Any unique host can be the source of one or more web-based attacks.

To locate a source of web-based attacks, we match domain names against the actual domain IP addresses to establish the geographical location of a specific IP address (GEOIP).

In the reporting period, Kaspersky solutions blocked **437,414,681** malware-class attacks launched from online resources across the globe; **80.49%** of these resources were located in just 10 countries.



Distribution of web attack sources by country or territory,
November 2022 through October 2023

Countries and territories where users faced the greatest risk of online infection

To assess the risk of online infection faced by users in each country or territory, 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 and territories.

Note that these rankings only include Malware-class attacks. We did not take into account Web Anti-Virus triggerings in response to potentially dangerous and unwanted programs, such as RiskTool and adware. Overall, during the reporting period, adware and adware components were registered on **88%** of users' computers where the Web Anti-Virus was triggered.

TOP 10 countries and territories where users faced the greatest risk of online infection

	Countries and territories*	%**
1	Taiwan	24.41
2	Greece	24.12
3	Belarus	22.65
4	Algeria	22.64
5	Turkey	22.54
6	Serbia	22.09
7	Tunisia	21.17
8	Moldova	21.10
9	Nepal	20.99
10	Bangladesh	20.81
11	Sri Lanka	20.47
12	Bosnia and Herzegovina	20.20
13	Portugal	19.87
14	Qatar	19.62
15	Morocco	19.50
16	Ecuador	19.02
17	Philippines	18.55
18	Mongolia	18.51
19	Peru	18.36
20	Russian Federation	18.22

* Excluded are countries and territories with relatively few Kaspersky users (under 50,000).
** Unique users targeted by Malware-class attacks as a percentage of all unique Kaspersky users in the country or territory.

On average, **16.31%** of internet user computers worldwide experienced at least one Malware-class attack during the reporting period.

TOP 20 malicious programs most commonly used in online attacks

During the reporting period, Kaspersky's Web Anti-Virus detected **112,922,612** unique malicious objects (scripts, exploits, executable files, and so on), and **106,357,530** unique malicious URLs. We used the data to identify 20 malicious programs most commonly used in online attacks on user computers.

	Verdict*	%**
1	Malicious URL	47.62
2	Trojan.Script.Generic	26.21
3	Trojan.BAT.Miner.gen	4.57
4	Trojan.Script.Miner.gen	2.93
5	Hoax.HTML.Phish.gen	2.26
6	Trojan.PDF.Badur.gen	1.72
7	Trojan.Multi.Preqw.gen	1.53
8	Hoax.HTML.FraudLoad.m	1.16
9	Trojan.Script.Agent.gen	1.04
10	Trojan-Downloader.Script.Generic	1.01
11	Trojan.JS.Miner.gen	0.70
12	Trojan.JS.Agent.eqq	0.53
13	Trojan-PSW.Script.Generic	0.50
14	Exploit.Win32.CVE-2011-3402.a	0.44
15	DangerousObject.Multi.Generic	0.44
16	Exploit.Multi.Desert.gen	0.26
17	Trojan-Banker.PowerShell.CoinStealer.gen	0.23
18	Trojan.MSOffice.Generic	0.17
19	Exploit.MSOffice.CVE-2017-11882.gen	0.16
20	Trojan.MSOffice.Agent.gen	0.15

* Excluded from the list are HackTool-type threats.
** Attacks by the given malicious program as a percentage of all Malware-class web attacks registered on the computers of unique Kaspersky users.

Local threats

Statistics on local infections of user computers are an important indicator. They include objects that penetrated the target computer by infecting files or removable media, or initially made their way onto the computer in non-open form, as programs inside complex installers, encrypted files, and so on. These statistics further include objects detected on user computers after an initial system scan by Kaspersky Anti-Virus.

This section analyzes statistics produced by Anti-Virus scans of files on the hard drive at the moment they were created or accessed, and 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 threats and adware.

	Verdict*	%**
1	DangerousObject.Multi.Generic	17.87
2	Trojan.Multi.BroSubsc.gen	12.70
3	Trojan.Multi.Misslink.a	6.40
4	Trojan.Multi.GenAutorunReg.a	5.98
5	Trojan.Script.Generic	5.63
6	Trojan.Win32.Agent.gen	5.10
7	Trojan.Win32.SEPEH.gen	3.06
8	Trojan.WinLNK.Agent.gen	2.87
9	Trojan.Win32.Hosts2.gen	2.15
10	Trojan.Multi.GenBadur.gen	2.08
11	Trojan.Multi.Agent.gen	1.91
12	Virus.Win32.Pioneer.cz	1.78
13	Worm.Python.Agent.gen	1.65
14	Trojan.Win32.Agentb.bqyr	1.51
15	Trojan.Win32.Generic	1.48
16	Worm.Python.Agent.c	1.45
17	Trojan.Script.Agent.gen	1.41
18	VHO:Trojan.Win32.Sdum.gen	1.38
19	Trojan.Multi.Powesta.d	1.37
20	Trojan.MSIL.Agent.gen	1.34

* 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 Kaspersky users whose Anti-Virus was triggered by malware.

Countries and territories where users faced the highest risk of local infection

For each country or territory, 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 these (flash drives, camera/phone memory cards, external hard drives). These statistics reflect the level of personal computer infection in different countries.

TOP 20 countries and territories by level of local infection risk

	Countries and territories*	%**
1	Yemen	59.74
2	Turkmenistan	59.71
3	Afghanistan	58.74
4	Bangladesh	51.82
5	Myanmar	51.22
6	Algeria	49.40
7	Benin	48.32
8	Rwanda	48.19
9	Uzbekistan	47.97
10	Guinea	47.97
11	Cameroon	47.08
12	Burkina Faso	47.05
13	Tanzania	46.99
14	Iraq	46.13
15	Democratic republic of Kongo	45.94
16	Niger	45.05
17	Venezuela	44.70
18	Mali	44.64
19	Belarus	44.57
20	Vietnam	44.18

* Excluded are countries and territories with relatively few Kaspersky users (under 50,000).
** Unique users on whose computers Malware-class local threats were blocked, as a percentage of all unique Kaspersky users in the country or territory.

In the reporting period, on the average, at least one piece of malware was detected on **26.33%** of computers, hard drives, or removable media belonging to users of Kaspersky products.

kaspersky bring on the future