kaspersky

Statistics

2022

Kaspersky
Security Bulletin 2022

Contents

Figures of the year

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 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 2021 to October 2022, inclusive.

- During the year, 15.37% of internet user computers worldwide experienced at least one **Malware-class** attack.
- Kaspersky solutions blocked **505,879,385** attacks launched from online resources across the globe.
- **101,612,333** unique malicious URLs triggered Web Anti-Virus components.
- Our Web Anti-Virus blocked **109,183,489** unique malicious objects.
- Ransomware attacks were defeated on the computers of **271,215** unique users.
- During the reporting period, miners attacked **1,392,398** unique users.
- Attempted infections by malware designed to steal money via online access to bank accounts were logged on the devices of **376,742** users.

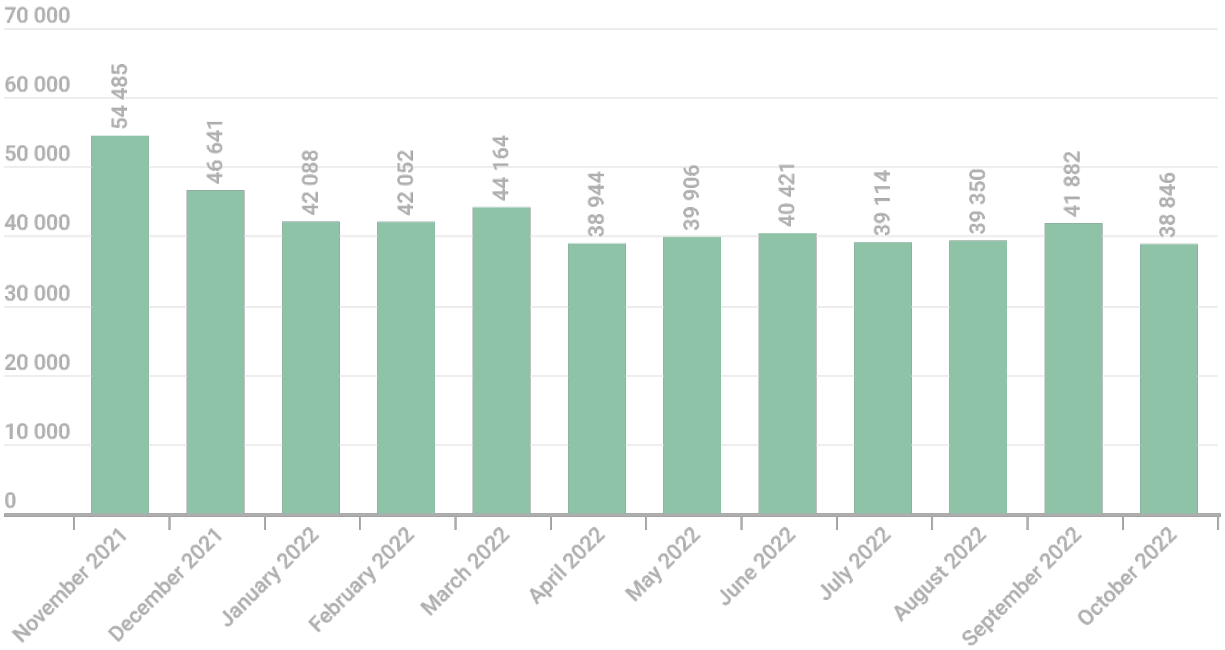
Mobile threat statistics will be given in the separate Mobile malware evolution 2022 report

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 the launch of financial malware on the computers of **376,742** users.



Number of users attacked by financial malware,
November 2021 — October 2022

Geography of attacked users

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

TOP 10 countries and territories by share of attacked users

	Countries and territories*	%**
1	Turkmenistan	6.7
2	Afghanistan	6.3
3	Tajikistan	5.2
4	Yemen	3.7
5	Uzbekistan	3.5
6	China	3.3
7	Mauritania	3.0
8	Sudan	2.7
9	Egypt	2.6
10	Azerbaijan	2.6

* Excluded are countries and territories with relatively few Kaspersky product 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.

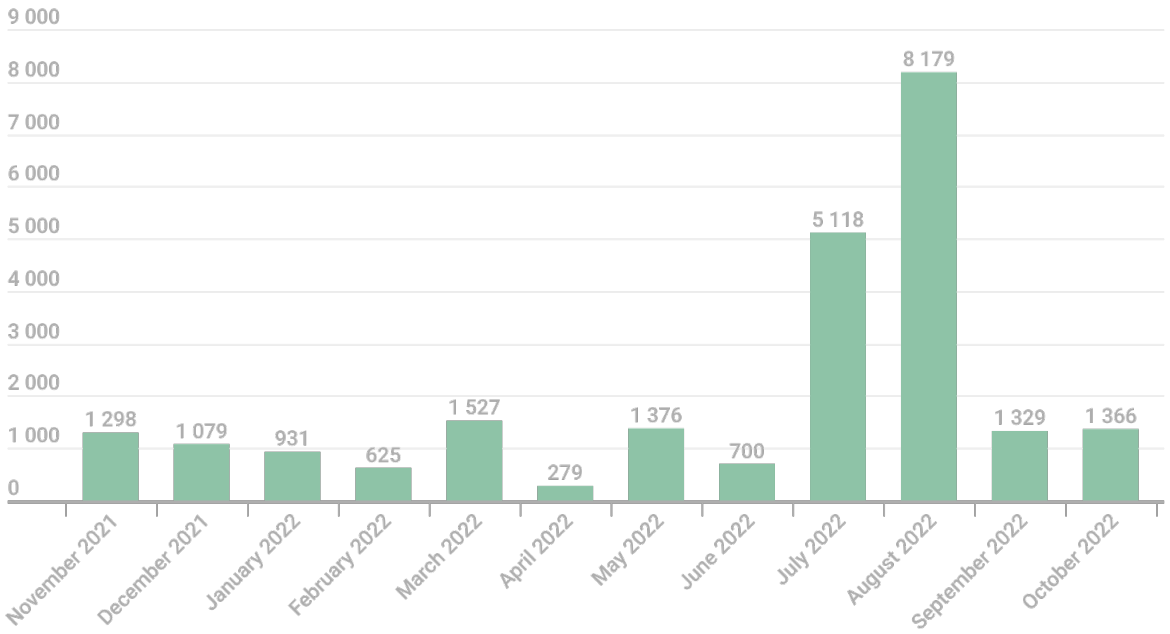
TOP 10 financial malware families

	Name	Verdict	%*
1	Ramnit/Nimnul	Trojan-Banker.Win32.Nimnul	33.8
2	Zbot/Zeus	Trojan-Spy.Win32.Zbot	15.6
3	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	6.2
4	SpyEye	Trojan-Spy.Win32.SpyEye	5.5
5	Trickster/Trickbot	Trojan.Win32.Trickster	3.9
6	IcedID	Trojan-Banker.Win32.IcedID	3.6
7	RTM	Trojan-Banker.Win32.RTM	2.5
8	Gozi	Trojan-Spy.Win32.Ursnif	2.2
9	Cridex/Dridex	Backdoor.Win32.Cridex	2.2
10	BitStealer	Trojan-Banker.MSIL.BitStealer.gen	1.5

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

Ransomware programs

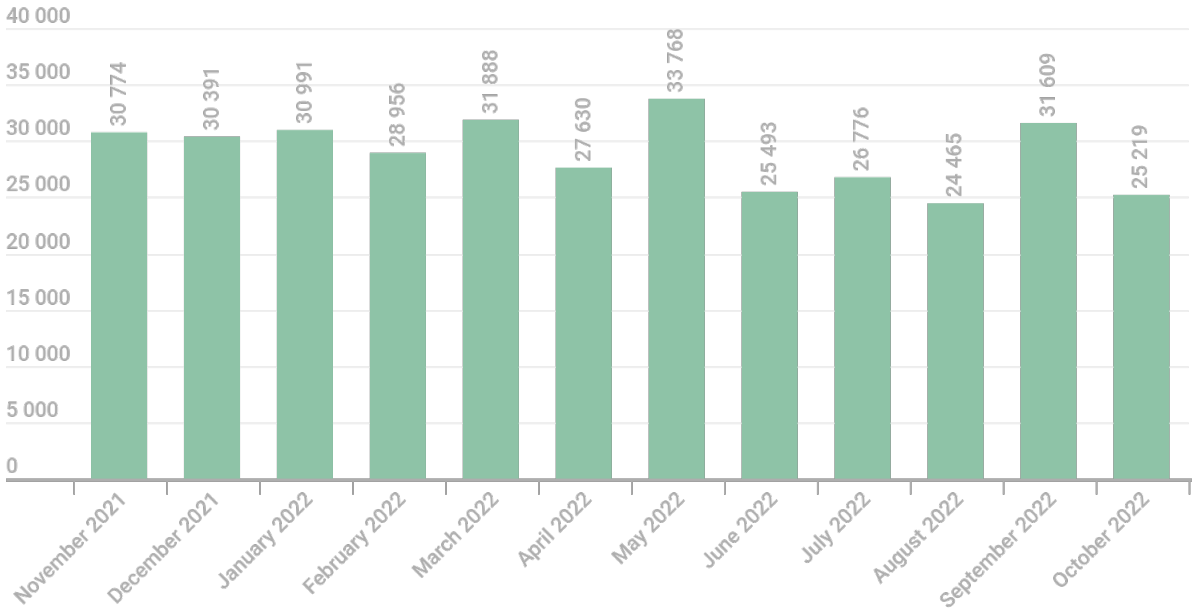
In the reporting period, we identified more than **23,807** ransomware modifications and detected **41** new families. Note that we did not create a separate family for every new piece of ransomware. Most threats of this type were assigned the generic verdict, which we give to new and unknown samples.



Number of new ransomware modifications detected,
November 2021 — October 2022

Number of users attacked by ransomware Trojans

During the reporting period, ransomware Trojans attacked **271,215** unique users, including **77,256** corporate users (excluding SMBs) and **8,931** users associated with small and medium-sized businesses.



Number of users attacked by ransomware Trojans,
November 2021 — October 2022

Geography of attacked users

TOP 10 countries and territories attacked by ransomware Trojans

	Countries and territories*	%**
1	Bangladesh	3.34
2	Yemen	2.07
3	South Korea	1.89
4	Mozambique	1.61
5	Sudan	1.56
6	Palestine	1.45
7	Taiwan	1.40
8	Afghanistan	1.09
9	China	0.99
10	Syria	0.97

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

TOP 10 most common families of ransomware Trojans

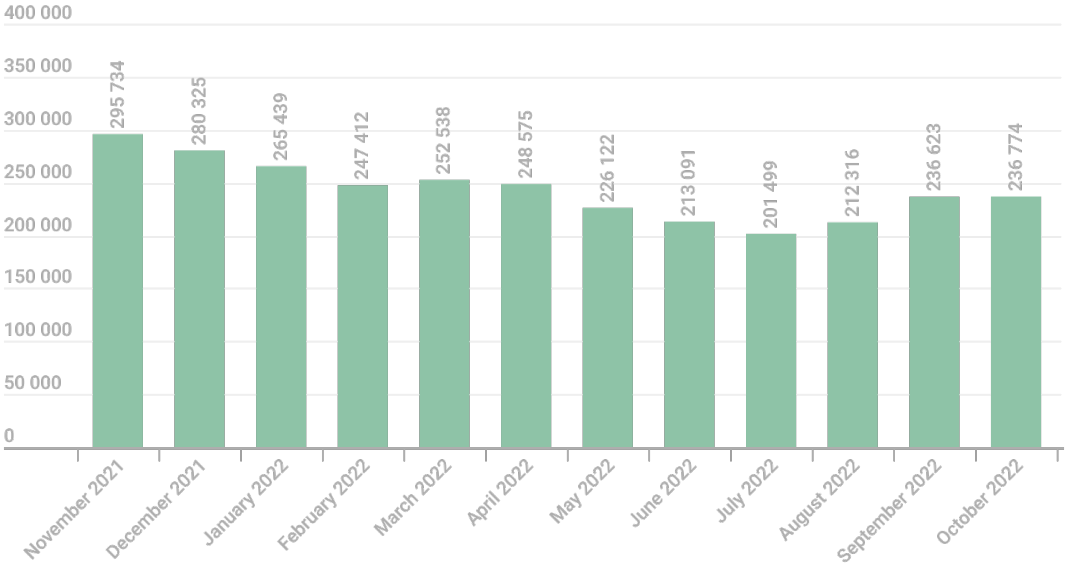
	Name	Verdict	%*
1	Stop/Djvu	Trojan-Ransom.Win32.Stop	16.49
2	WannaCry	Trojan-Ransom.Win32.Wanna	12.00
3	(generic verdict)	Trojan-Ransom.Win32.Gen	9.71
4	(generic verdict)	Trojan-Ransom.Win32.Encoder	8.42
5	(generic verdict)	Trojan-Ransom.Win32.Phny	6.26
6	PolyRansom/VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.PolyRansom	5.72
7	Magniber	Trojan-Ransom.Win64.Magni	4.81
8	(generic verdict)	Trojan-Ransom.Win32.Crypren	3.51
9	(generic verdict)	Trojan-Ransom.Win32.Crypmod	3.08
10	(generic verdict)	Trojan-Ransom.Win32.CryFile	2.35

* Unique Kaspersky users attacked by the given family of ransomware Trojans as a percentage of all users who faced 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 **1,392,398** unique users. Miners accounted for 2.86% of all attacks and 16.88% of all RiskTool-type programs.



Number of users attacked by miners,
November 2021 — October 2022

During the reporting period, Kaspersky products detected Trojan.Win32.Miner.gen more often than others, accounting for 22.91% of all users attacked by miners. It was followed by Trojan.Win32.Miner.bbb (15.44%), Trojan.JS.Miner.ays (8.13%), and Trojan.Win64.Miner.all (7.73%).

Geography of attacked users

TOP 10 countries and territories attacked by miners

	Countries and territories*	%**
1	Turkmenistan	10.02
2	Afghanistan	8.03
3	Rwanda	4.47
4	Ethiopia	4.42
5	Kazakhstan	3.67
6	Myanmar	3.61
7	Sudan	3.53
8	Mongolia	3.47
9	Tanzania	3.40
10	Tajikistan	3.25

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

Vulnerable applications used by criminals during cyberattacks

Events and observations

The new reporting period was fairly interesting in terms of the variety of vulnerabilities found. Security researchers identified some of them as zero-days when analyzing this period's APT activity. Others were found during analysis of source code and patches for past vulnerabilities, as well as by numerous tools for both static and dynamic analysis, in particular, fuzzing tools.

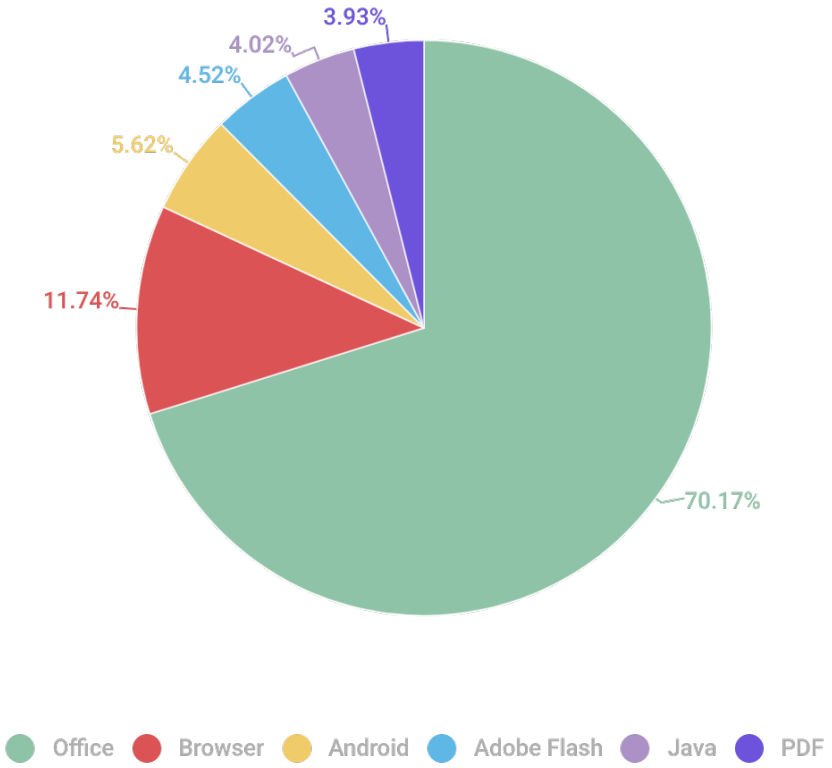
Our partners also detected attacks exploiting a range of vulnerabilities. We spotlight the most significant of them.

- 8 Google Chrome vulnerabilities (**CVE-2022-0604**, **CVE-2022-0605**, **CVE-2022-0609**, **CVE-2022-1096**, **CVE-2022-1364**, **CVE-2022-2294**, **CVE-2022-2856**, **CVE-2022-3075**) were found in different subsystems of the browser. In particular, they are exploited through bugs in the V8 script engine and multimedia parsers, and through other flaws. The most common type of vulnerability is Use-After-Free, caused by an application continuing to use a previously freed area of memory, potentially leading to arbitrary code execution. These vulnerabilities allow cybercriminals to escape the browser's sandbox and attack actual components of the operating system.
- 4 similar Mozilla Firefox vulnerabilities (**CVE-2022-1097**, **CVE-2022-1802**, **CVE-2022-1529**, **CVE-2022-28281**) were found in the JavaScript engine and other components of the browser.
- 22 Microsoft Windows vulnerabilities (**CVE-2022-21836**, **CVE-2022-21882**, **CVE-2022-21919**, **CVE-2022-22022**, **CVE-2022-22026**, **CVE-2022-22034**, **CVE-2022-22038**, **CVE-2022-22047**, **CVE-2022-22049**, **CVE-2022-24521**, **CVE-2022-30206**, **CVE-2022-30220**, **CVE-2022-30226**, **CVE-2022-34713**, **CVE-2022-35743**, **CVE-2022-35750**, **CVE-2022-35803**, **CVE-2022-37969**, **CVE-2022-41040**, **CVE-2022-41082**, **CVE-2022-26925**, **CVE-2022-30190**) were discovered in various OS subsystems, including graphics (win32k), Common Log File System (CLFS), User Profile Services, Print Spooler, the important Client/Server Runtime Subsystem (CSRSS), Remote Procedure Call (RPC) mechanism, and others. Attackers exploiting these vulnerabilities can escalate the privileges of infected processes, inject malicious code into user files, steal confidential data, and cause other damage. The best-known of them, **CVE-2022-30190**, even got its own name in the media: Follina. Although spread through Office documents, this vulnerability exploits a logical error in link handling, which allows an attacker to run programs remotely in the system.
- A notorious Linux vulnerability (**CVE-2022-0847**) dubbed DirtyPipe is associated with OS kernel memory corruption and allows system file data in memory to be spoofed, which, in turn, can be used to escalate user privileges.

Among network attacks, brute-forcing of passwords for various network services, such as RDP, Microsoft SQL Server, and SMB, remains popular. Also still in demand are Equation Group exploits, in particular EternalBlue and EternalRomance for outdated and unpatched Microsoft Windows systems. Several serious vulnerabilities were found in the Network File System (NFS) driver, most notably **CVE-2022-24491** and **CVE-2022-24497**. In theory, these can be used to carry out RCE attacks by sending a specially crafted network message via the NFS protocol. Prominent among vulnerabilities for Windows Server versions is **LSA Spoofing** (**CVE-2022-26925**) — an unauthenticated attacker can call a LSARPC interface method that will force the Windows domain controller to authenticate them. A media stir was caused by two vulnerabilities in Microsoft Exchange Server (**CVE-2022-41040**, **CVE-2022-41082**), dubbed **ProxyNotShell** for their similarity in terms of exploitation to the previously closed ProxyShell vulnerabilities. Lastly, in the reporting period, two vulnerabilities (**CVE-2022-22965**, **CVE-2022-22947**) were found in such web frameworks as Spring Framework and Spring Cloud Gateway.

Exploit statistics

In the reporting period, we again saw an upward trend in the popularity of attacks using the Microsoft Office suite (70.17%). This was due to two easy-to-exploit vulnerabilities (**CVE-2021-40444** and **CVE-2022-30190**) found in quick succession. Cybercriminals also continued to use the old, but still current vulnerabilities: **CVE-2017-11882**, **CVE-2018-0802**, **CVE-2017-8570**, and **CVE-2017-0199**. As a result, the number of unique triggerings in response to attempts to exploit Microsoft Office vulnerabilities increased by more than 20 p.p. against the previous reporting period.



Distribution of exploits used in attacks by type of application attacked, November 2021 — October 2022

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.

Second place in the distribution of attacks belongs to exploits for browsers; however, their share actually decreased by that same 20 p.p. margin. In the reporting period, any security issues identified were usually fixed promptly by developers. Continuous fuzzing tests also helped, as did a high-quality review of the codebase. The elimination of possible risks is further aided by automatic user-transparent browser updating, which has a major effect in reducing the number of attacks that involve malicious sites, since the browser prevents these attacks from being carried out.

As before, the remaining positions in the statistics were taken by Google Android (5.62%), Adobe Flash (4.52%), Java (4.02%), and Adobe PDF (3.93%). Their shares remained almost unchanged, and no high-profile vulnerabilities for these platforms were discovered during the reporting period.

Attacks on macOS

The reporting period was notable for the large number of multi-platform finds aimed at users of various operating systems, including macOS (Gimmick, SysJoker, Earth Berberoka, TraderTraitor, LuckyMouse, Alchimist). Also worth noting is the use of open source tools in attacks (the Sliver framework disguised as a fake VPN application and a Salesforce update), as well as the new version of XCSSET for macOS Monterey and Python 3 — this Trojan infects Xcode development environment projects and steals data from browsers and other applications.

TOP 20 threats for macOS

	Verdict	%*
1	AdWare.OSX.Amc.e	13.64
2	AdWare.OSX.Pirrit.ac	12.26
3	AdWare.OSX.Pirrit.j	10.11
4	AdWare.OSX.Agent.ai	7.42
5	AdWare.OSX.Bnodlero.at	6.92
6	Trojan-Downloader.OSX.Shlayer.a	6.63
7	AdWare.OSX.Pirrit.ae	6.42
8	AdWare.OSX.Pirrit.o	6.28
9	Monitor.OSX.HistGrabber.b	6.00
10	AdWare.OSX.Pirrit.aa	5.94

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

As usual, most of our TOP 10 in this reporting period consisted of adware. At the top of the list is the newcomer AdWare.OSX.Amc.e (known as Advanced Mac Cleaner): it shows fake messages about system issues and prompts the user to buy the full version of the program to fix them. The Shlayer Trojan, which we wrote about back in early 2020, slipped from fourth place in the last reporting period down to sixth.

Threat geography

TOP 10 countries and territories by share of attacked users

	Countries and territories*	%**
1	Ecuador	5.29
2	France	4.63
3	Canada	4.23
4	Spain	4.01
5	Russian Federation	3.83
6	United States	3.83
7	Italy	3.79
8	India	3.79
9	Vietnam	3.34
10	South Africa	3.33

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

IoT attacks

IoT threat statistics

During the reporting period, almost three-quarters of devices that attacked Kaspersky traps used the Telnet protocol.

Telnet	73.89%
SSH	26.11%

Distribution of attacked services by number of unique IP addresses of devices that carried out attacks, November 2021 — October 2022

As for the distribution of sessions, Telnet again prevailed, accounting for almost 94% of all working sessions.

Telnet	93.92%
SSH	6.08%

Distribution of cybercriminal working sessions with Kaspersky traps, November 2021 — October 2022

TOP 10 countries and territories hosting devices from which attacks were carried out on Kaspersky Telnet traps

	Countries and territories*	%**
1	China	44.48
2	India	9.32
3	Russian Federation	5.12
4	Brazil	4.28
5	United States	3.46
6	Egypt	3.39
7	South Korea	2.92
8	Taiwan	2.67
9	Iran	1.46
10	Mexico	1.39

* Devices from which attacks were carried out in the country or territory as a percentage of the total number of attacking devices.

TOP 10 countries and territories hosting devices from which attacks were made on Kaspersky SSH traps

	Countries and territories*	%**
1	China	23.13
2	United States	17.32
3	Germany	5.90
4	Brazil	4.89
5	Hong Kong	4.41
6	India	3.26
7	Vietnam	3.19
8	South Korea	3.17
9	Russian Federation	2.85
10	France	2.60

* Devices from which attacks were carried out in the country or territory as a percentage of the total number of attacking devices.

Threats loaded into traps

	Verdict	%*
1	Backdoor.Linux.Mirai.b	33.16
2	Trojan-Downloader.Linux.NyaDrop.b	14.73
3	Backdoor.Linux.Mirai.ba	9.60
4	Backdoor.Linux.Mirai.cw	4.99
5	Backdoor.Linux.Mirai.ek	3.73
6	Backdoor.Linux.Gafgyt.a	3.71
7	Trojan-Downloader.Shell.Agent.p	2.88
8	Backdoor.Linux.Agent.bc	2.35
9	Backdoor.Linux.Mirai.ad	1.84
10	Backdoor.Linux.Mirai.ew	1.75

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

Attacks via web resources

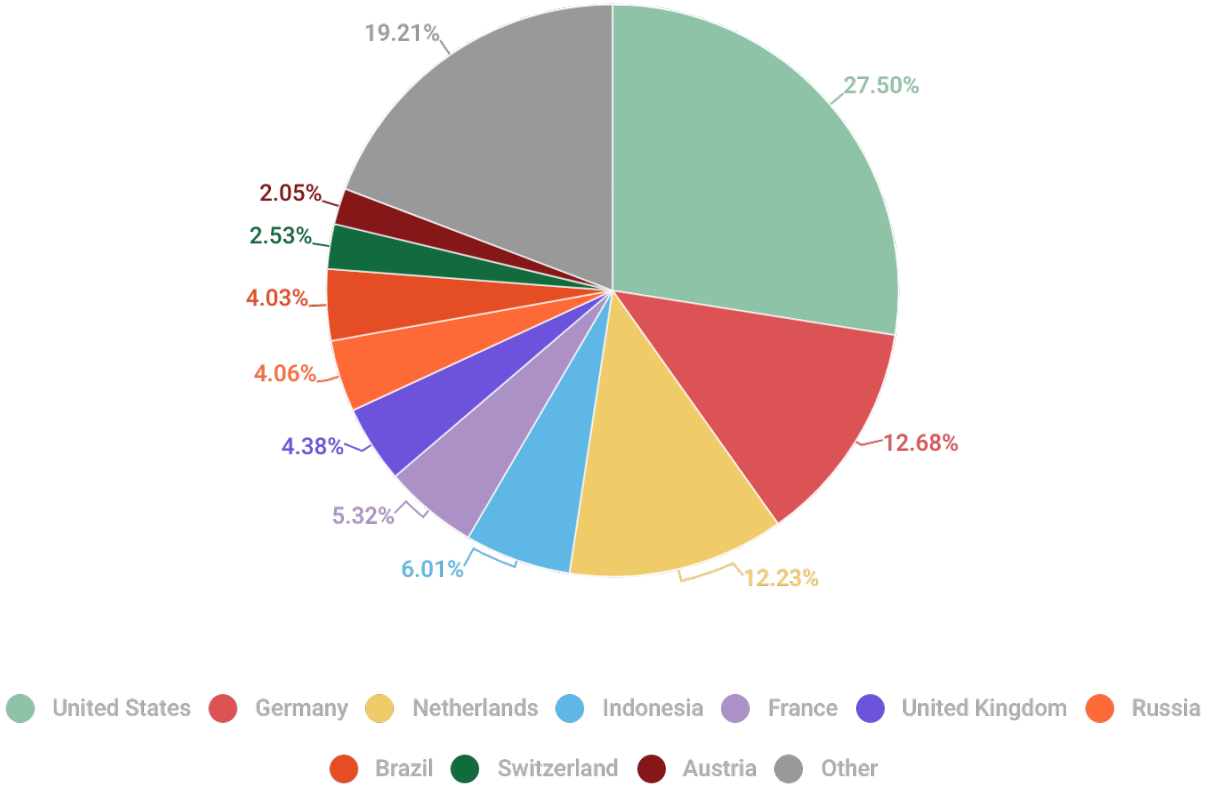
The statistics in this section are based on Web Anti-Virus, which protects users when malicious objects are downloaded from malicious/infected web pages. Cybercriminals create malicious websites on purpose; web resources with user-created content (for example, forums), as well as hacked legitimate resources,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

In the reporting period, Kaspersky solutions blocked **505,879,385** attacks launched from online resources across the globe. Moreover, 89.9% of these resources were located in just 10 countries.



Distribution of web attack sources by country or territory,
November 2021 — October 2022

In the reporting period, the US returned to first place (27.50%), its share having increased by under 3 p.p. Germany (12.68%), which showed similar growth, lies in second position. The Netherlands (12.23%) took third place. The Czech Republic, which led our ranking in 2021, this time failed to make the TOP 10.

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

To assess the risk of online infection faced by users, for 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 only Malware-class attacks are included in this ranking. 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 its components were registered on **89%** of users' computers on which the Web Anti-Virus was triggered.

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

	Countries and territories*	%**
1	Tunisia	32.77
2	Taiwan	32.59
3	Algeria	24.70
4	Serbia	24.13
5	Greece	22.27
6	Libya	21.55
7	Mongolia	21.24
8	Nepal	21.09
9	Belarus	21.04
10	Sri Lanka	20.80
11	Bangladesh	20.79
12	Morocco	20.60
13	Qatar	20.27
14	Hong Kong	19.97
15	Philippines	19.31
16	Turkey	19.04
17	Moldova	18.53
18	Bosnia and Herzegovina	18.40
19	Kenya	18.15
20	Ecuador	17.97

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

On average, **15.37%** of internet user computers worldwide experienced at least one Malware-class attack during the reporting period.

TOP 10 malicious programs most actively used in online attacks

During the reporting period, Kaspersky's Web Anti-Virus detected **109,183,489** unique malicious objects (scripts, exploits, executable files, etc.), as well as **101,612,333** unique malicious URLs. Based on the collected data, we identified the 20 malicious programs most actively used in online attacks on user computers.

	Verdict*	%**
1	Malicious URL	43.68
2	Trojan.Script.Generic	19.49
3	Trojan.Script.Miner.gen	11.72
4	Trojan.BAT.Miner.gen	11.21
5	Trojan.Multi.Preqw.gen	1.65
6	Hoax.HTML.Phish.gen	1.46
7	Trojan.PDF.Badur.gen	1.34
8	Trojan-Downloader.Script.Generic	0.53
9	Trojan.Script.Agent.gen	0.50
10	Trojan.JS.Miner.gen	0.41
11	Hoax.HTML.FraudLoad.m	0.31
12	Exploit.Script.CVE-2021-26855.e	0.31
13	DangerousObject.Multi.Generic	0.30
14	Exploit.Win32.CVE-2011-3402.a	0.29
15	Trojan-PSW.Script.Generic	0.24
16	Exploit.MSOffice.CVE-2017-11882.gen	0.21
17	Trojan.MSOffice.Generic	0.18
18	Trojan-PSW.MSIL.Agensla.gen	0.15
19	Trojan.Script.Malcrack.gen	0.14
20	Trojan-Clicker.HTML.IFrame.dg	0.13

* 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 users of Kaspersky products.

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 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 threats and adware.

	Verdict*	%**
1	Malicious URL	43.68
2	Trojan.Script.Generic	19.49
3	Trojan.Script.Miner.gen	11.72
4	Trojan.BAT.Miner.gen	11.21
5	Trojan.Multi.Preqw.gen	1.65
6	Hoax.HTML.Phish.gen	1.46
7	Trojan.PDF.Badur.gen	1.34
8	Trojan-Downloader.Script.Generic	0.53
9	Trojan.Script.Agent.gen	0.50
10	Trojan.JS.Miner.gen	0.41
11	Hoax.HTML.FraudLoad.m	0.31
12	Exploit.Script.CVE-2021-26855.e	0.31
13	DangerousObject.Multi.Generic	0.30
14	Exploit.Win32.CVE-2011-3402.a	0.29
15	Trojan-PSW.Script.Generic	0.24
16	Exploit.MSOffice.CVE-2017-11882.gen	0.21
17	Trojan.MSOffice.Generic	0.18
18	Trojan-PSW.MSIL.Agensla.gen	0.15
19	Trojan.Script.Malcrack.gen	0.14
20	Trojan-Clicker.HTML.IFrame.dg	0.13

* 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.

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 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 and territories by level of risk of local infection

	Countries and territories*	%**
1	Turkmenistan	58.51
2	Afghanistan	57.37
3	Myanmar	56.86
4	Bangladesh	56.79
5	Uzbekistan	56.49
6	Ethiopia	53.61
7	Algeria	51.89
8	Venezuela	49.01
9	Benin	48.95
10	Iraq	48.80
11	Rwanda	48.31
12	Sudan	48.17
13	China	47.89
14	Mongolia	47.87
15	Tanzania	47.80
16	Belarus	47.24
17	Vietnam	47.04
18	Bolivia	46.30
19	Burkina Faso	46.01
20	Cameroon	45.39

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

In the reporting period, on average, at least one piece of malware was detected on **29.15%** of computers, hard drives, or removable media belonging to users of Kaspersky solutions.