Kaspersky Security Bulletin 2024

Kaspersky Security Bulletin 2024. Statistics

Threat Research

kaspersky bring on the future

Contents

All statistics in this report come from Kaspersky Security Network (KSN), a global cloud service that receives information from components in our security solutions voluntarily provided by Kaspersky users. 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 2023 through October 2024. The report doesn't cover mobile statistics, which we will share in our annual mobile malware report.

The year in figures

During the reporting period, Kaspersky solutions:

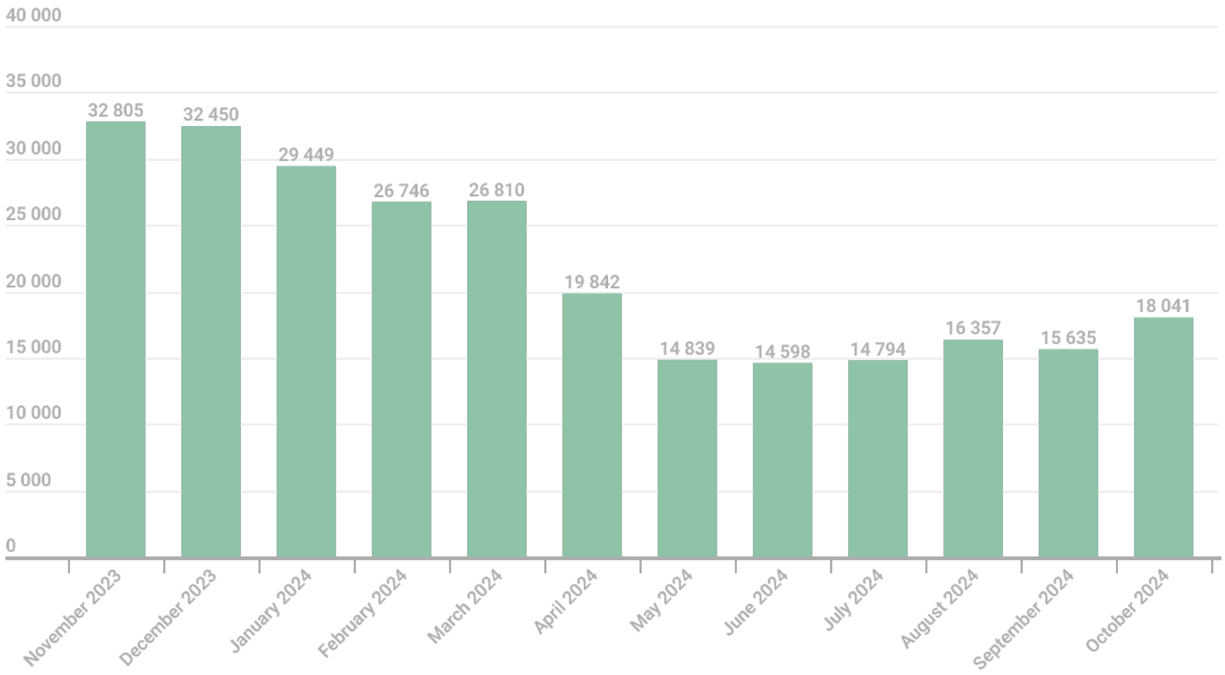
- Stopped **302,287,115** malware attacks launched from online resources across the globe.
- Detected **85,013,784** unique malicious URLs.
- Blocked **72,194,144** unique malicious objects with the help of Web Anti-Virus components.
- Prevented ransomware attacks on the computers of **303,298** unique users.
- Stopped miners from infecting **999,794** unique users.
- Prevented the launch of banking, ATM or PoS malware on the devices of **208,323** users.

Financial threats

These statistics include globally active banking malware, and malware for ATMs and point-of-sale (PoS) terminals. This year, we excluded data on Trojan banker families that no longer use banking Trojan functionality in their attacks, such as Emotet, and families that are only active in specific regions.

Number of users attacked by financial malware

During the reporting period, **208,323** users worldwide encountered financial malware at least once.



Users attacked by financial malware,
November 2023 through October 2024

The most active malware families during the reporting period were ClipBanker, CliptoShuffler, Phorpiex, Danabot and BitStealer. The majority of these monitor the system clipboard and substitute copied crypto wallet addresses with those controlled by their operators. Cryptocurrencies were always of interest to cybercriminals, and this interest is growing.

TOP 5 financial malware families

	Name	Verdict	%*
1	ClipBanker	Trojan-Banker.Win32.ClipBanker	73.5
2	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	10.3
3	Phorpiex	Trojan-Dropper.Win32.Phorpiex	3.8
4	Danabot	Trojan-Banker.Win32.Danabot	1.9
5	BitStealer	Trojan-Banker.MSIL.BitStealer	1.5

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

Geography of attacked users

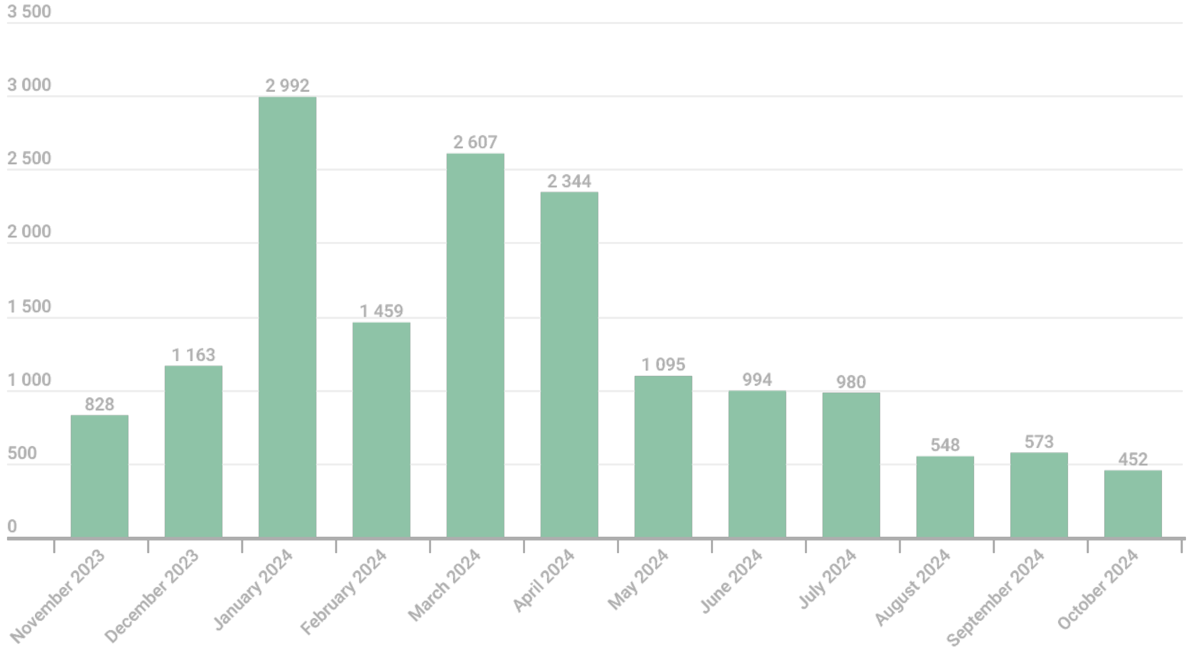
	Country/territory*	%**
1	Afghanistan	9.7
2	Turkmenistan	9.2
3	Tajikistan	6.8
4	Syria	3
5	Uzbekistan	2.8
6	Kazakhstan	2.7
7	Kyrgyzstan	2.5
8	Yemen	2.4
9	Switzerland	1.8
10	Angola	1.7

* Excluded are countries and territories with relatively few (under 10,000) Kaspersky users.

** Unique users whose computers were targeted by financial malware as a percentage of all users attacked by all types of malware.

Ransomware

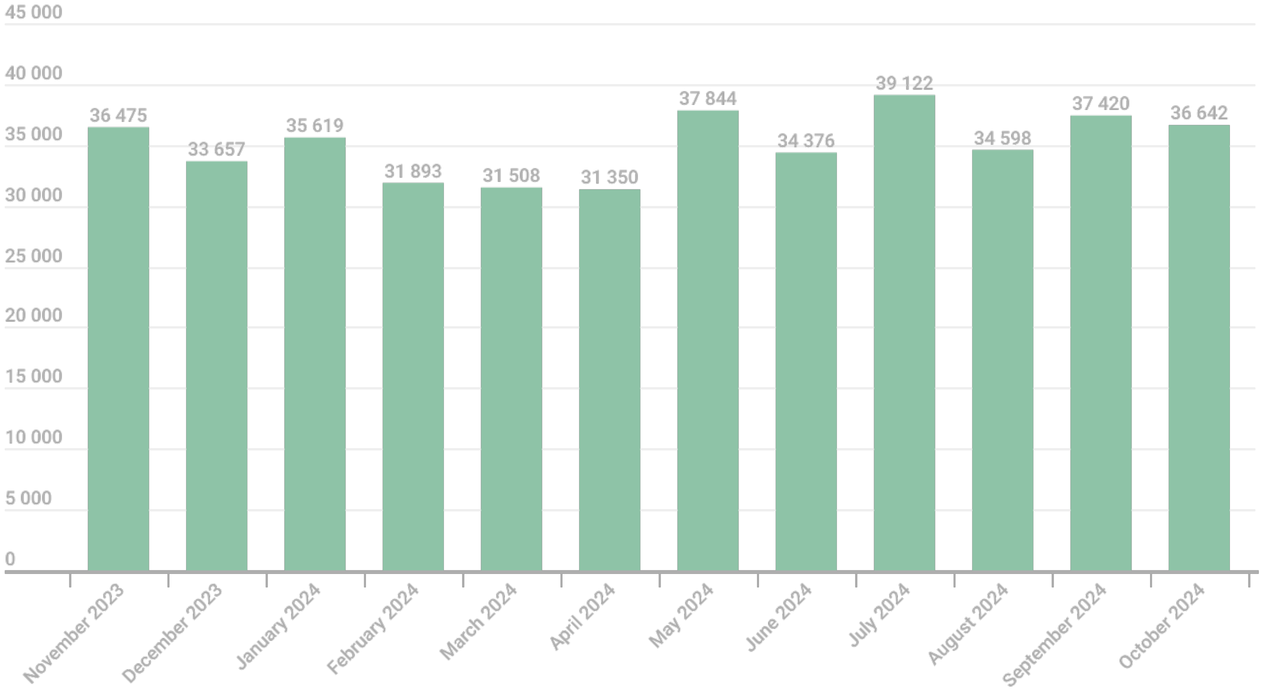
From November 2023 through October 2024, we identified **26** new ransomware families and **16,035** different variants. Note that we do not create a separate family for every new ransomware specimen. Most threats of this type were assigned a generic verdict, which we give to new and unknown samples.



New ransomware modifications detected,
November 2023 through October 2024

Number of users attacked by ransomware Trojans

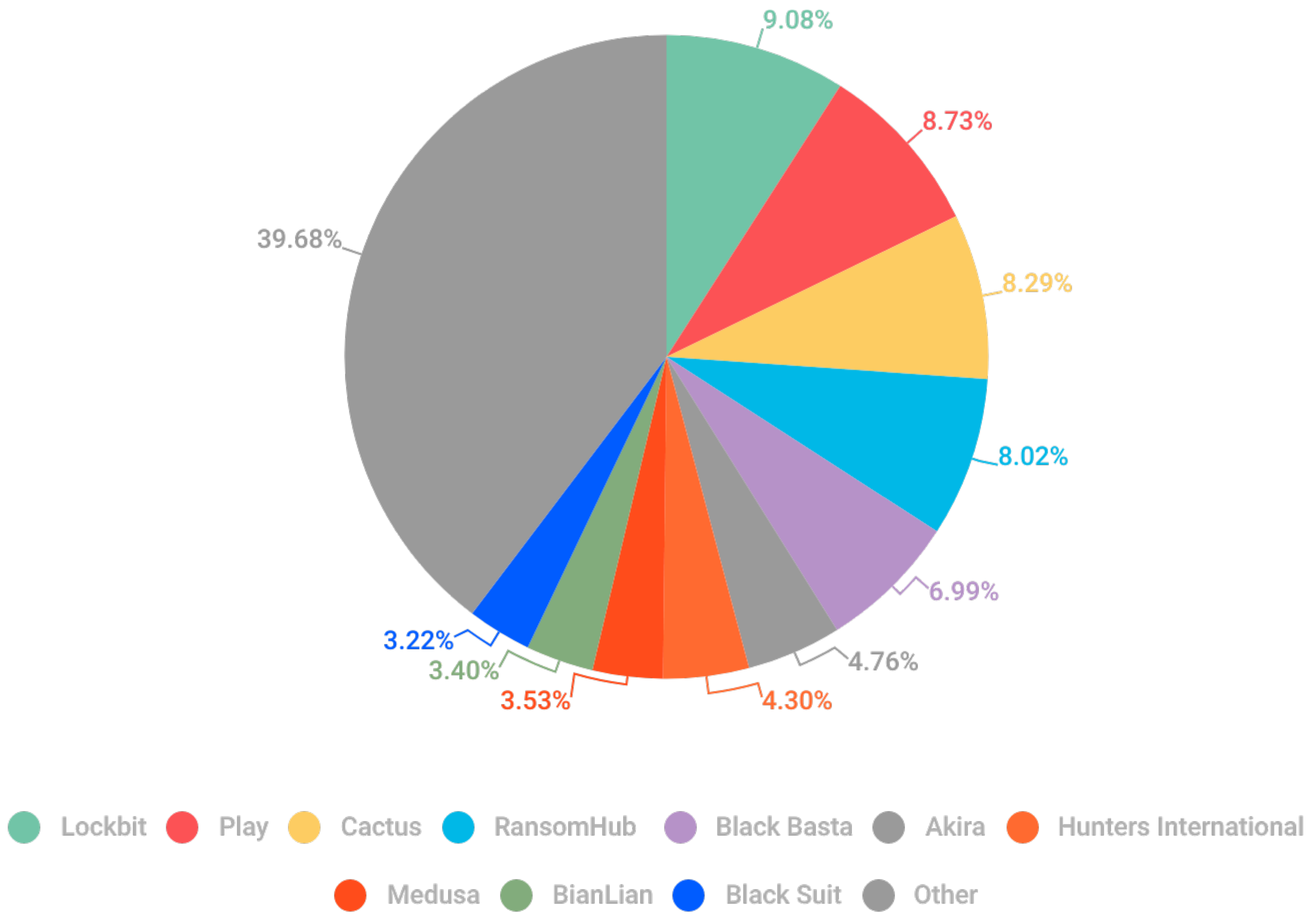
During the reporting period ransomware attacked **303,298** unique users. Of these, **98,208** were corporate (non-SMB) users, and **14,517** were associated with small and medium businesses.



Users attacked by ransomware Trojans,
November 2023 through October 2024

Most prolific groups

This section includes statistics on ransomware groups operating according to a "double extortion" scheme that have posted the highest number of victims on their DLS (data leak site). The diagram shows each group's share in the total number of victims published on all the groups' DLSs.



The most prolific ransomware gangs,
November 2023 through October 2024

Geography of attacked users

TOP 10 countries and territories attacked by ransomware

	Country/territory*	%**
1	Yemen	4.23
2	Afghanistan	1.47
3	South Korea	1.41
4	China	1.40
5	Pakistan	1.31
6	Uruguay	1.28
7	Libya	1.22
8	Bangladesh	1.22
9	Syria	1.10
10	Iran	1.02

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

** Unique users whose computers were targeted by ransomware as a percentage of all unique users of Kaspersky products in the country or territory.

TOP 10 most widespread ransomware families

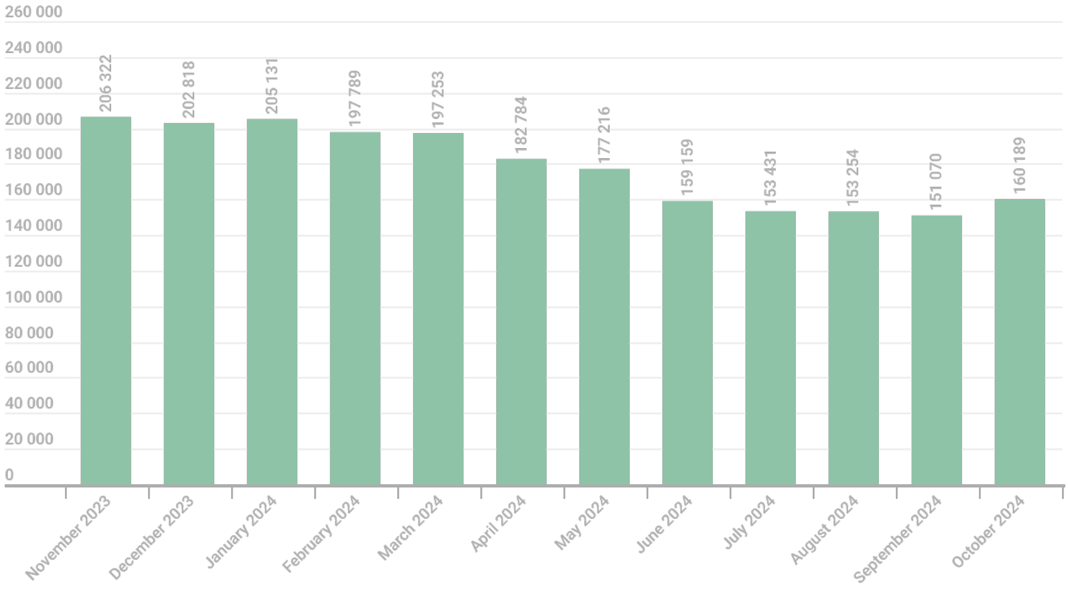
	Name	Verdict	%*
1	(generic verdict)	Trojan-Ransom.Win32.Gen	23.95
2	WannaCry	Trojan-Ransom.Win32.Wanna	9.11
3	(generic verdict)	Trojan-Ransom.Win32.Encoder	7.91
4	(generic verdict)	Trojan-Ransom.Win32.Crypren	6.11
5	(generic verdict)	Trojan-Ransom.MSIL.Agent	4.94
6	Stop/Djvu	Trojan-Ransom.Win32.Stop	4.39
7	Lockbit	Trojan-Ransom.Win32.Lockbit	4.20
8	PolyRansom/VirLock	Virus.Win32.PolyRansom / Trojan-Ransom.Win32.PolyRansom	3.21
9	(generic verdict)	Trojan-Ransom.Win32.Agent	2.92
10	(generic verdict)	Trojan-Ransom.Win32.Phny	2.81

* Unique users whose computers were targeted by a specific ransomware family as a percentage of all Kaspersky 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 **999,794** unique users. Miners accounted for 3.24% of all attacks and 17.95% of all RiskTool-type threats.



Users attacked by miners,
November 2023 — October 2024

During the reporting period, Kaspersky products detected Trojan.Win32.Miner.gen more often than others. This type of miner accounted for 22.27% of all users attacked by the malware category in question. It was followed by Worm.NSIS.BitMin.d (5.48%), Trojan.BAT.Miner (5.1%) and Trojan.Win64.Miner.pef (4.62%).

Geography of attacked users

TOP 10 countries and territories attacked by miners

	Country/territory*	%**
1	Turkmenistan	8.05
2	Afghanistan	5.61
3	Kazakhstan	2.75
4	Tajikistan	2.50
5	Belarus	2.42
6	Venezuela	2.40
7	Ethiopia	2.19
8	Mongolia	2.15
9	Moldova	1.91
10	Uzbekistan	1.87

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

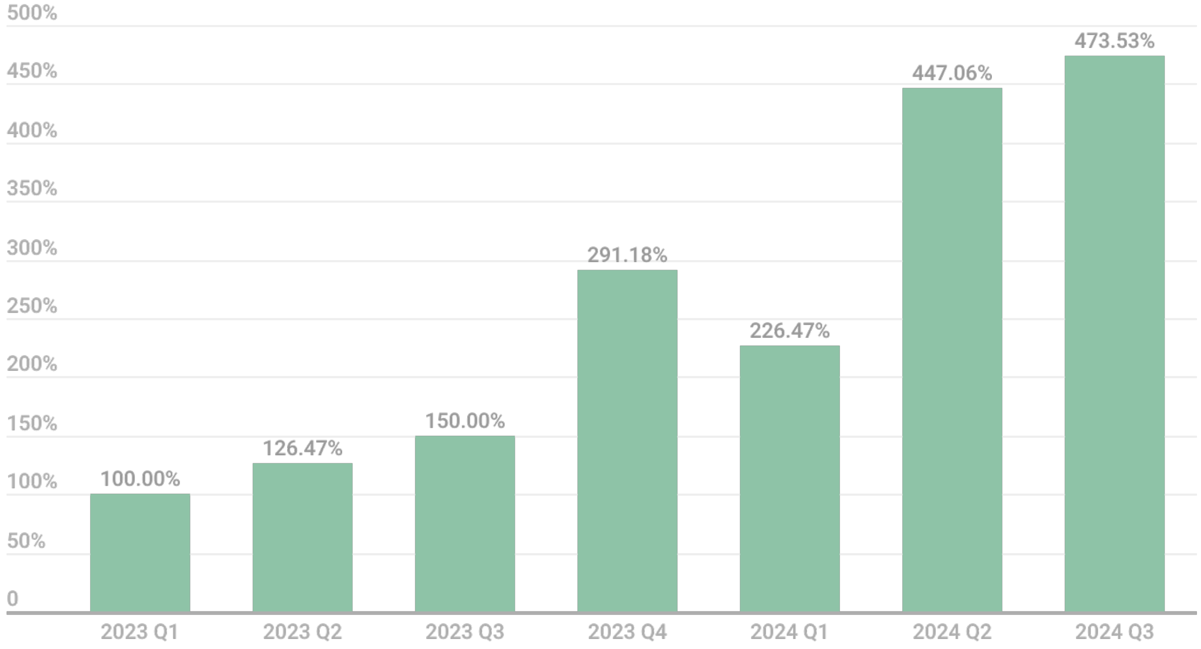
Vulnerable applications used by criminals in cyberattacks

The year 2024 saw a number of dangerous vulnerabilities, such as **CVE-2024-3094**, also known as the XZ backdoor, which was deliberately introduced into the XZ data compression utility for Linux following a long-term social engineering campaign. Another notorious vulnerability was **CVE-2024-6387**, or **regreSSHion**, affecting OpenSSH software. Although we have not seen the exploitation of the latter vulnerability in the wild, attackers created fake exploits for it to lure cybersecurity researchers into downloading and running malware.

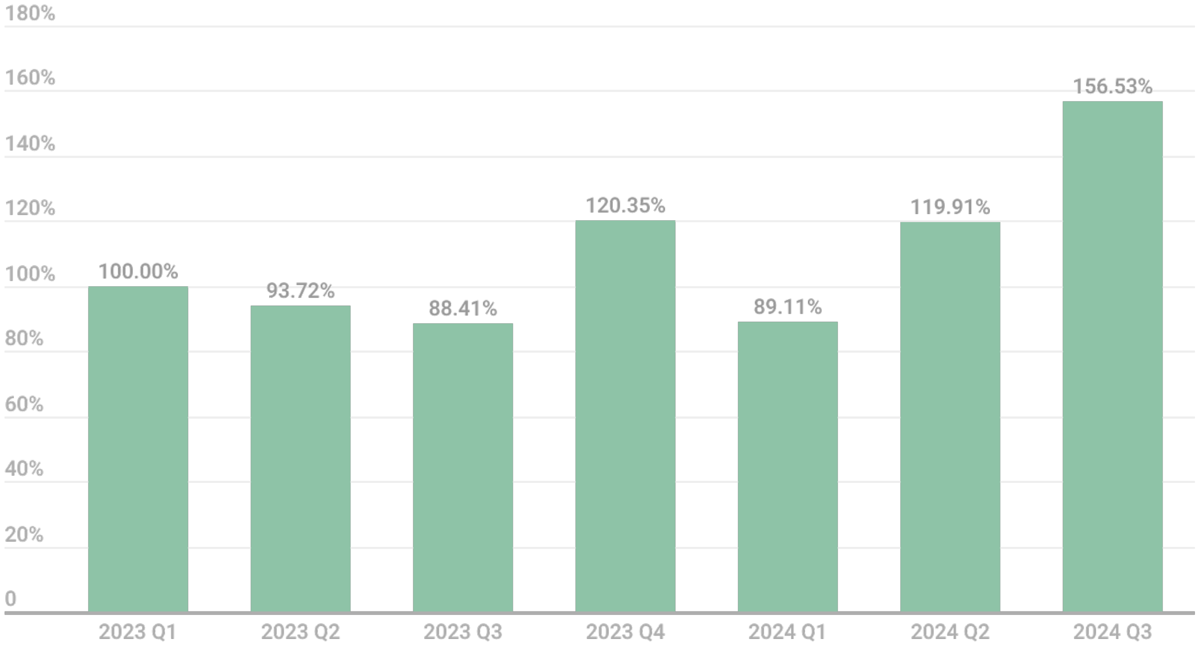
Among Windows vulnerabilities, it is worth mentioning the zero-day CVE-2024-30051, exploited in QakBot attacks, along with the Windows Defender vulnerability **CVE-2024-21412**, which allows the attacker to bypass the SmartScreen feature.

There were a number of zero-day vulnerabilities actively exploited in APT attacks, such as CVE-2024-21887, CVE-2024-21888 and CVE-2024-21893 in Ivanti Connect Secure; CVE-2024-1708 and CVE-2024-1709 in ConnectWise ScreenConnect; CVE-2024-3400 in PAN-OS; CVE-2024-20353 and CVE-2024-20359 in Cisco Adaptive Security Appliance; CVE-2024-4577 in PHP; and CVE-2024-38112 in the Windows MSHTML platform. An older vulnerability in WinRAR, CVE-2023-38831, remained popular among attackers throughout the year.

The statistics below cover the year 2023 and the first three quarters of 2024. As can be seen from the bar charts, the number of users encountering exploits in 2024 grew for both Windows and Linux.



Dynamics of the number of Linux users who encountered exploits, Q1 2023–Q3 2024.
The number of users who encountered exploits in Q1 2023 is taken as 100%



Dynamics of the number of Windows users who encountered exploits, Q1 2023–Q3 2024.
The number of users who encountered exploits in Q1 2023 is taken as 100%

Attacks on macOS

The following new threats to macOS were discovered during the reporting period:

- Several new backdoors including SpectralBlur, which may be linked to the BlueNoroff group; a crypto-stealing backdoor bundled with cracked software; a backdoor written in Rust; and the HZ Rat backdoor, which targets users of WeChat and DingTalk
- New stealers Banshee Stealer and Cthulhu Stealer closely resembling AMOS, first discovered in 2023
- New versions of AMOS and BeaverTail stealers, and a new version of the LightRiver spyware
- VNote and Notepad-- versions infected with the Cobalt Strike agent

Kaspersky solutions successfully detect these and other threats targeting macOS users.

TOP 20 threats for macOS

	Verdict	%*
1	Trojan-Downloader.OSX.Agent.gen	8.98
2	Trojan.OSX.Agent.gen	8.22
3	AdWare.OSX.Agent.gen	6.91
4	AdWare.OSX.Agent.ai	6.51
5	AdWare.OSX.Agent.ap	6.23
6	AdWare.OSX.Amc.e	4.31
7	AdWare.OSX.Pirrit.ac	4.03
8	Hoax.OSX.Agent.g	3.93
9	Monitor.OSX.HistGrabber.b	3.29
10	Trojan.OSX.MalChat.gen	3.12
11	AdWare.OSX.Bnodlero.ax	2.73
12	AdWare.OSX.Pirrit.j	2.60
13	HackTool.OSX.DirtyCow.a	2.37
14	AdWare.OSX.Mhp.a	2.07
15	AdWare.OSX.Pirrit.ae	1.92
16	Hoax.OSX.MacBooster.a	1.88
17	AdWare.OSX.Pirrit.gen	1.86
18	Backdoor.OSX.Agent.l	1.75
19	Trojan-Downloader.OSX.Agent.h	1.66
20	AdWare.OSX.Pirrit.o	1.58

* 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

	Country/territory*	%**
1	Philippines	2.01
2	Hong Kong	1.93
3	Mainland China	1.93
4	Spain	1.91
5	Canada	1.85
6	France	1.71
7	Mexico	1.67
8	Italy	1.62
9	Colombia	1.58
10	Australia	1.43

* Excluded from the rankings are countries and territories with relatively few (under 5,000) Kaspersky macOS users.

** Unique users attacked in the country or territory as a percentage of all Kaspersky macOS users there.

IoT attacks

IoT threat statistics

From November 2023 through October 2024, most devices that attacked Kaspersky honeypots used the Telnet protocol. Its share increased compared to the previous reporting period.

Telnet	87.79%
SSH	12.21%

Distribution of attacked services by number of unique attacking device IP addresses, November 2023 through October 2024

Telnet sessions accounted for the absolute majority of the attacks on Kaspersky honeypots.

Telnet	98.15%
SSH	1.85%

Distribution of malware sessions with Kaspersky honeypots, November 2023 through October 2024

TOP 10 countries and territories hosting devices that attacked Kaspersky honeypots

	Country/Territory	%**
1	Mainland China	32.37
2	India	25.67
3	Brazil	3.50
4	Russia	3.30
5	Japan	3.26
6	Taiwan	2.80
7	Thailand	2.44
8	South Korea	2.28
9	United States	2.13
10	Tanzania	1.79

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

Online threats (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 cybercriminals; infected sites include those with user-contributed content (such as forums), and compromised legitimate resources.

The TOP 20 malicious objects detected online

During the reporting period, Kaspersky solutions blocked **302,287,115** malware attacks launched from web resources located all across the world. Kaspersky's Web Anti-Virus detected **72,194,144** unique malicious objects, including scripts, exploits, executable files, etc. Web Anti-Virus components recognized **85,013,784** unique URLs as being malicious.

We identified 20 malicious programs most actively involved in online attacks launched against computers.

	Name*	%**
1	Malicious URL	50.32
2	Trojan.Script.Generic	20.10
3	Trojan.BAT.Miner.gen	5.33
4	Trojan.PDF.Badur.gen	4.69
5	Hoax.HTML.Phish.gen	3.58
6	Trojan.Multi.Preqw.gen	2.10
7	Trojan.Script.Agent.gen	1.35
8	Exploit.Win32.CVE-2011-3402.a	0.80
9	Trojan-Clicker.Script.Generic	0.78
10	Trojan-Downloader.Script.Generic	0.60
11	Trojan.BAT.Setter.gen	0.56
12	Trojan.Script.Miner.gen	0.55
13	Trojan.JS.Agent.eqq	0.47
14	Trojan-PSW.Script.Generic	0.39
15	DangerousObject.Multi.Generic	0.38
16	Hoax.Script.Phish.gen	0.22
17	Trojan.MSOffice.Generic	0.21
18	Exploit.Win32.MS05-036	0.21
19	Trojan.PDF.Meme.gen	0.20
20	Trojan.VBS.SAgent.gen	0.19

* Threats identified as HackTool are excluded from this list.
** Attacks by the malware as the percentage of all web-based malware attacks recorded on the computers of Kaspersky users.

During the year, adware and its components were registered on **85%** of user computers where Web Anti-Virus was triggered.

The TOP 10 countries and territories where malicious online resources were located

The following statistics are based on the physical location of the online resources that were 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 can be the source of one or more web attacks. The statistics do not include sources used for spreading adware or hosts linked to adware activity.

In order to determine the geographical source of web-based attacks, domain names are mapped to their actual domain IP addresses, and then the geographical location of the specific IP address (GEOIP) is established.

As many as 72.36% of online resources detected as malicious by the Web Anti-Virus component were located in 10 countries.

	Country/territory	%
1	US	34.40
2	Brazil	5.52
3	Germany	5.25
4	France	4.97
5	Singapore	4.96
6	UK	4.22
7	Switzerland	3.95
8	Netherlands	3.29
9	Australia	3.23
10	Russia	2.57
11	Other	27.64

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

In order to identify the countries and territories in which users most often face cyberthreats, we calculated how often Web Anti-Virus was triggered on the machines of Kaspersky users in each country or territory. The resulting data describes the risk of infection that computers are exposed to in different countries and territories across the globe, providing an indicator of the aggressiveness of the environment facing computers in different parts of the world.

This rankings only include attacks by objects that fall under the **Malware** category. They do not include Web Anti-Virus detections of potentially dangerous or unwanted applications like RiskTool or adware. During the reporting period, **14.81%** of computers experienced at least one web-based malware attack while their owners were online.

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

	Country/territory*	%**
1	Greece	21.77
2	Peru	20.65
3	Ecuador	20.43
4	Qatar	19.51
5	Tunisia	19.09
6	Belarus	18.59
7	Algeria	18.35
8	Bosnia and Herzegovina	18.31
9	Serbia	18.27
10	Sri Lanka	18.24
11	Moldova	18.07
12	South Africa	17.88
13	Bangladesh	17.76
14	Morocco	17.55
15	Nepal	17.39
16	Bolivia	17.33
17	Kenya	17.17
18	Philippines	17.15
19	Argentina	17.11
20	Slovakia	17.08

* We excluded countries and territories with relatively few (under 50,000) users of Kaspersky products.
** Unique users whose computers were targeted by web-based malware attacks as a percentage of all unique users of Kaspersky products in the country/territory.

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 entered the computer in an encrypted format: applications bundled with complex installers, encrypted files and so on. These statistics further include objects detected on user computers after the system is scanned by Kaspersky File Anti-Virus for the first time.

This section contains an analysis of the data 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 media.

The TOP 20 malicious objects detected on user computers

For these rankings, we identified the 20 most frequently detected threats on user computers during the reporting period. The rankings do not include adware or riskware.

	Name*	%**
1	DangerousObject.Multi.Generic	19.35
2	Trojan.Multi.BroSubsc.gen	7.92
3	Trojan.AndroidOS.Fakemoney.v	4.83
4	Trojan.Multi.Misslink.a	4.61
5	Trojan.Script.Generic	3.49
6	Trojan.Win32.Agent.gen	2.82
7	Trojan.Win32.SEPEH.gen	2.33
8	Trojan.Multi.GenAutorunReg.a	2.23
9	Trojan.WinLNK.Agent.gen	2.23
10	Trojan.Multi.Agent.gen	1.98
11	Trojan.Multi.GenBadur.gen	1.67
12	Trojan.Win32.Hosts2.gen	1.54
13	Trojan.AndroidOS.Boogr.gsh	1.49
14	Virus.Win32.Pioneer.cz	1.41
15	Trojan.Script.Agent.gen	1.41
16	Trojan.Win32.Generic	1.30
17	Trojan.AndroidOS.Triada.gm	1.30
18	Trojan.Win32.Agentb.bqyr	1.23
19	VHO:Trojan.Win32.Sdum.gen	1.22
20	Worm.Python.Agent.gen	1.18

* Threats identified as HackTool are excluded from this list.
** Users on whose computers the antivirus module detected a particular object as a percentage of all users of Kaspersky products on whose computers malware was detected.

The DangerousObject.Multi.Generic verdict, which is used for malware detected with the help of cloud technology, is in first place (19.35%). Cloud technology is used when the antivirus databases contain neither signatures nor heuristics to detect the malicious application but Kaspersky's cloud antivirus database already has information about the object. In fact, this is how the latest malware is detected.

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

For each country or territory, we calculated the number of File Anti-Virus detections users faced during the year. The data includes detected objects located on user computers or on removable media connected to the computers, such as flash drives, camera and phone memory cards, or external hard drives. The statistics reflect the scale of personal computer infection in different countries and territories around the world.

The TOP 20 countries and territories by level of infection

	Country/territory*	%**
1	Turkmenistan	61.06
2	Afghanistan	57.43
3	Yemen	56.18
4	Uzbekistan	48.36
5	Bangladesh	47.05
6	Niger	43.62
7	Tanzania	43.58
8	Algeria	43.30
9	Burkina Faso	43.01
10	Iran	42.99
11	Benin	42.97
12	Myanmar	42.95
13	Vietnam	42.75
14	Iraq	42.70
15	Belarus	42.63
16	Cameroon	42.43
17	Mali	40.16
18	Venezuela	39.97
19	Bolivia	39.67
20	Guinea	39.51

* When calculating, we excluded countries and territories with fewer than 50,000 Kaspersky users.
** Users in the country or territory who encountered local malware threats as a percentage of all Kaspersky users in the country or territory.

On average, at least one malware object was found on **25.31%** of computers, hard drives or removable media belonging to Kaspersky users.

bring on
the future