kaspersky

Threat Research

The mobile malware threat landscape in 2024

Mobile malware evolution in 2024

These statistics are based on detection alerts from Kaspersky products, collected from users who consented to provide statistical data to Kaspersky Security Network. The statistics for previous years may differ from earlier publications due to a data and methodology revision implemented in 2024.

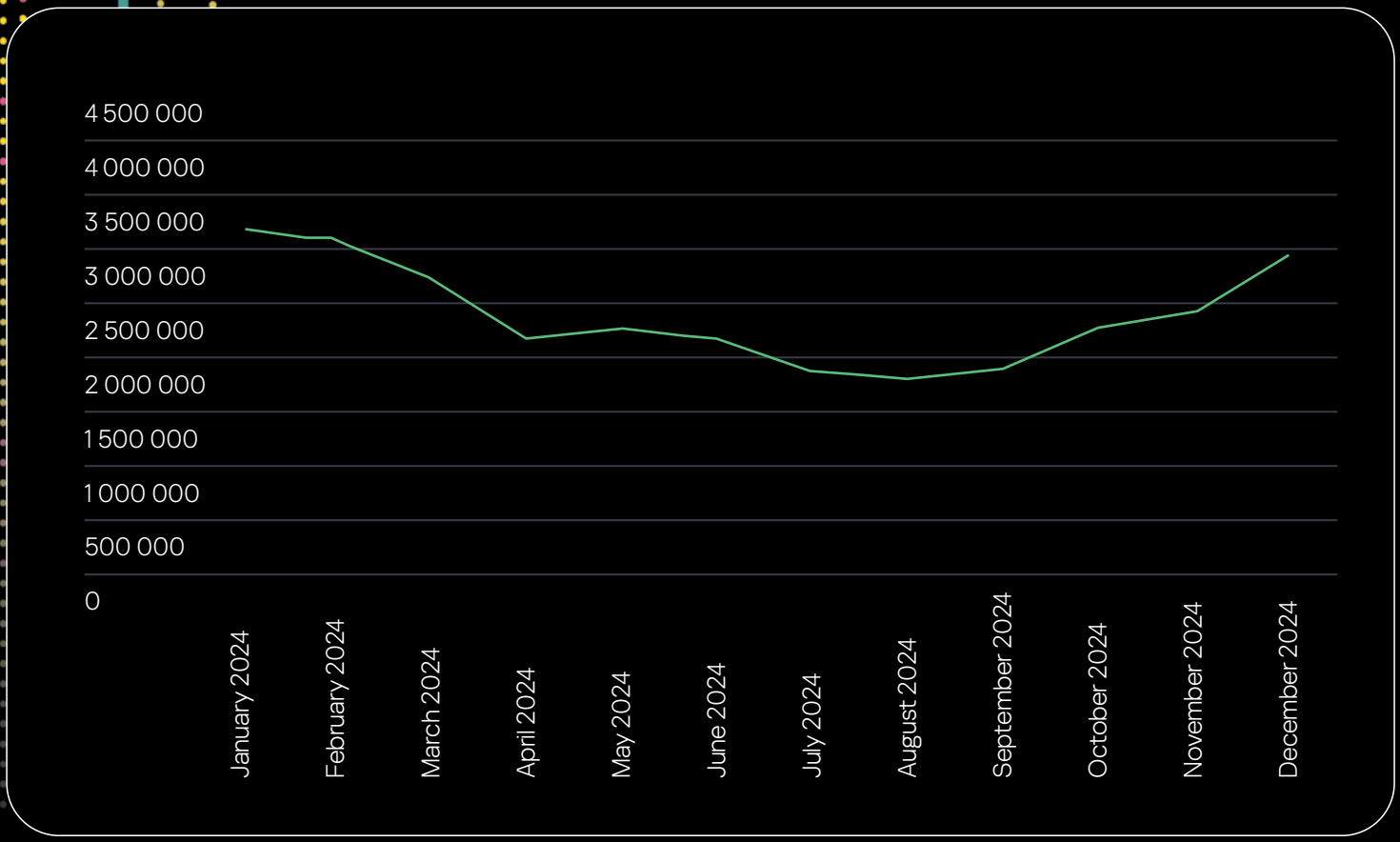
The year in figures

According to Kaspersky Security Network, in 2024:

- A total of 33.3 million attacks involving malware, adware or unwanted mobile software were prevented.
- Adware, the most common mobile threat, accounted for 35% of total detections.
- A total of 1.1 million malicious and potentially unwanted installation packages were detected, almost 69,000 of which associated with mobile banking Trojans.

The year's trends

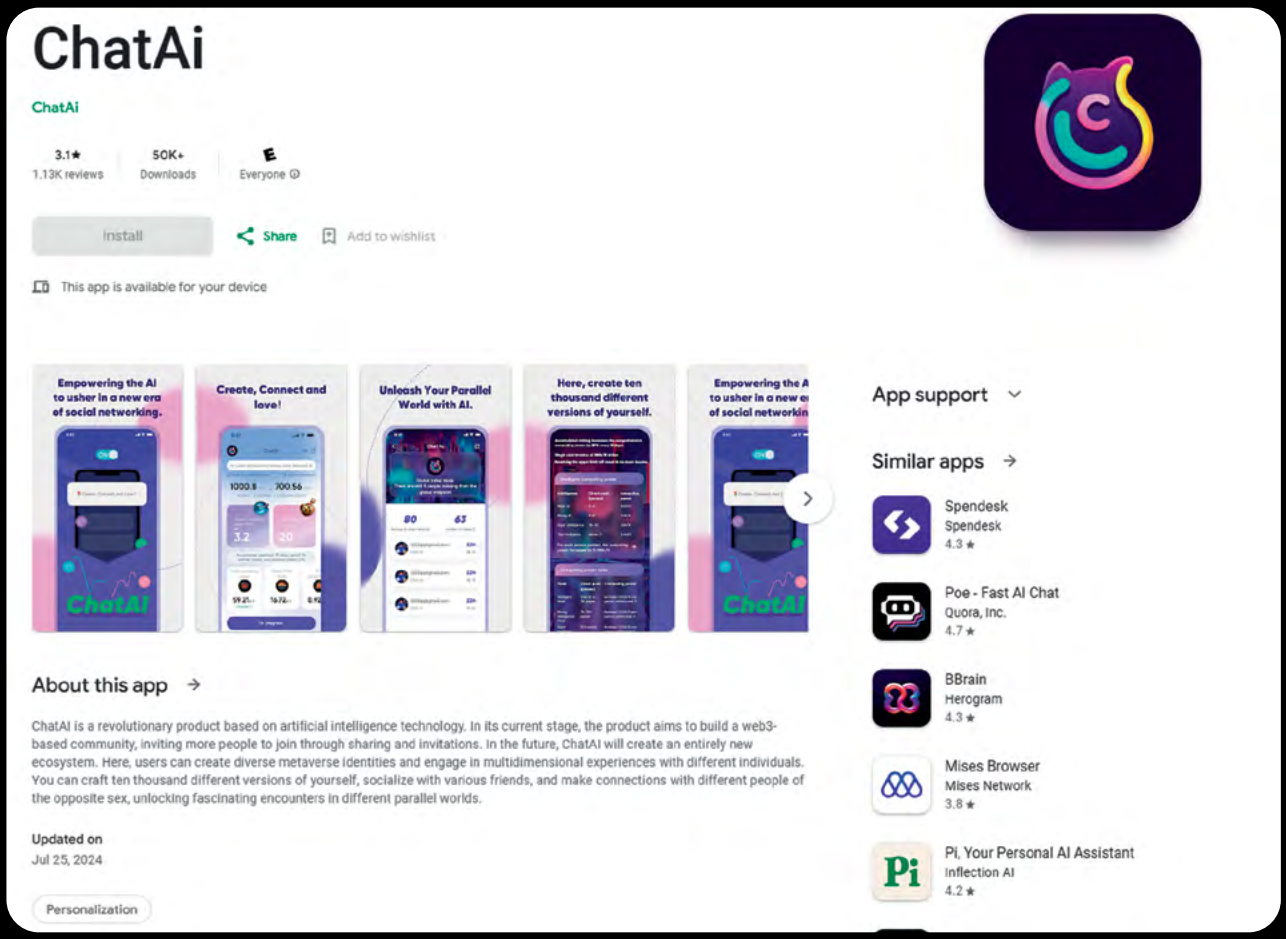
In 2024, cybercriminals launched a monthly average of 2.8 million malware, adware or unwanted software attacks targeting mobile devices. In total, Kaspersky products blocked 33,265,112 attacks in 2024.



Attacks on Kaspersky mobile users in 2024

OCR crypto stealers in Google Play and App Store

We discovered several apps on Google Play, each containing a malicious SDK implant named “SparkCat”, which began to spread at least as early as March 2024. Infected apps were deleted by the store in February 2025; nevertheless, our telemetry data shows that other apps containing SparkCat are distributed through unofficial sources.



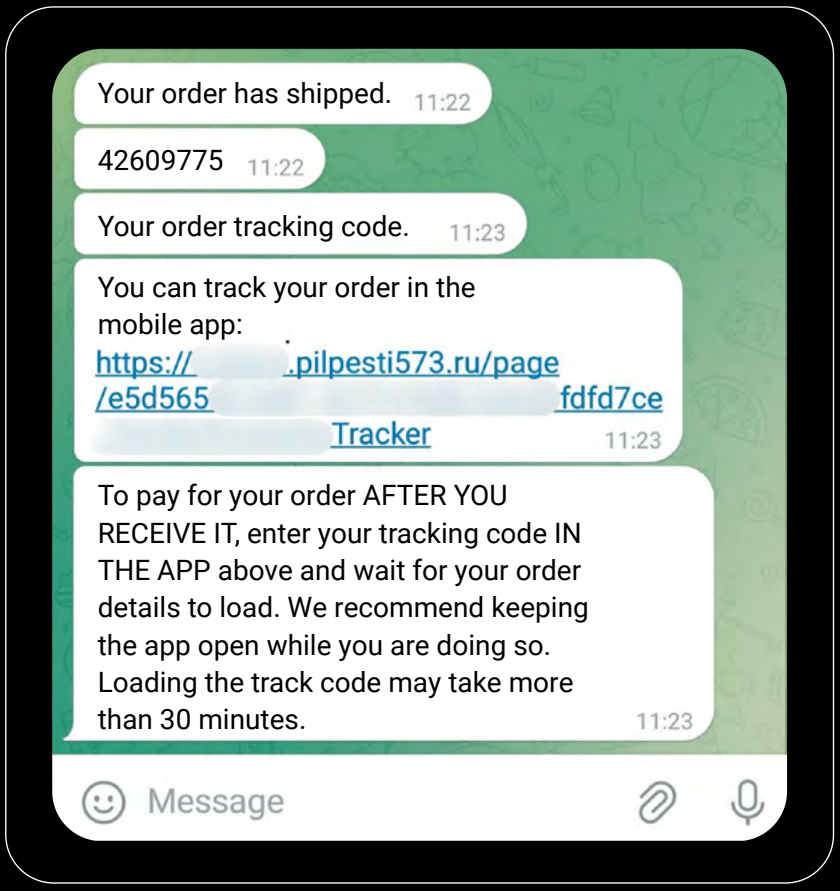
A popular app containing SparkCat

The SDK received a C2 server command with a list of keywords or dictionaries to search the gallery on the device for images to exfiltrate. Our data suggests that the Trojan was aimed at stealing recovery phrases for cryptocurrency wallets of Android users primarily in the UAE, countries in Europe and Asia.

It is worth noting that the same implant for iOS was delivered via the App Store, which makes it the first known OCR malware to sneak into Apple’s official marketplace. Apple removed the infected apps in February 2025 as well.

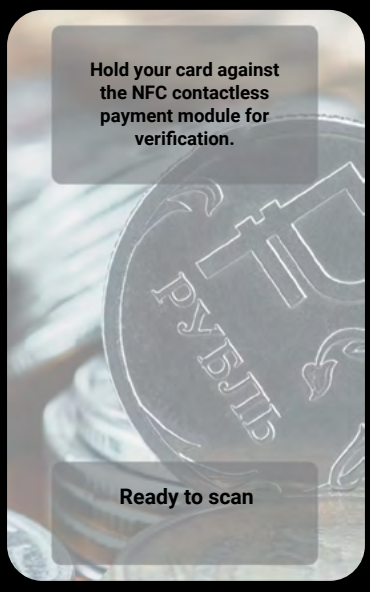
The distribution scheme for the Mamont banking Trojan

At the end of 2024, we discovered a new distribution scheme for the Mamont banking Trojan, targeting users of Android devices in Russia. The attackers lured users with a variety of discounted products. The victim had to send a message to place an order. Some time later, the user received a phishing link to download malware disguised as a shipment tracking app.



The phishing link as seen in the chat with the fraudsters

(The text in the screenshot is originally in Russian)



A screenshot of the fake mobile app

(The text in the screenshot is originally in Russian)

In August 2024, researchers at ESET described[1] a new NFC banking scam discovered in the Czech Republic. The scammers employed phishing websites to spread malicious mods of the legitimate app NFCGate. These used a variety of pretexts to persuade the victim to place a bank card next to the back of their phone for an NFC connection. The card details were leaked to the fraudsters who then made small contactless payments or withdrew money at ATMs.

A similar scheme was later spotted in Russia, where malware masqueraded as banking and e-government apps. The SpyNote RAT was occasionally used as the malware dropper and NFC activator.

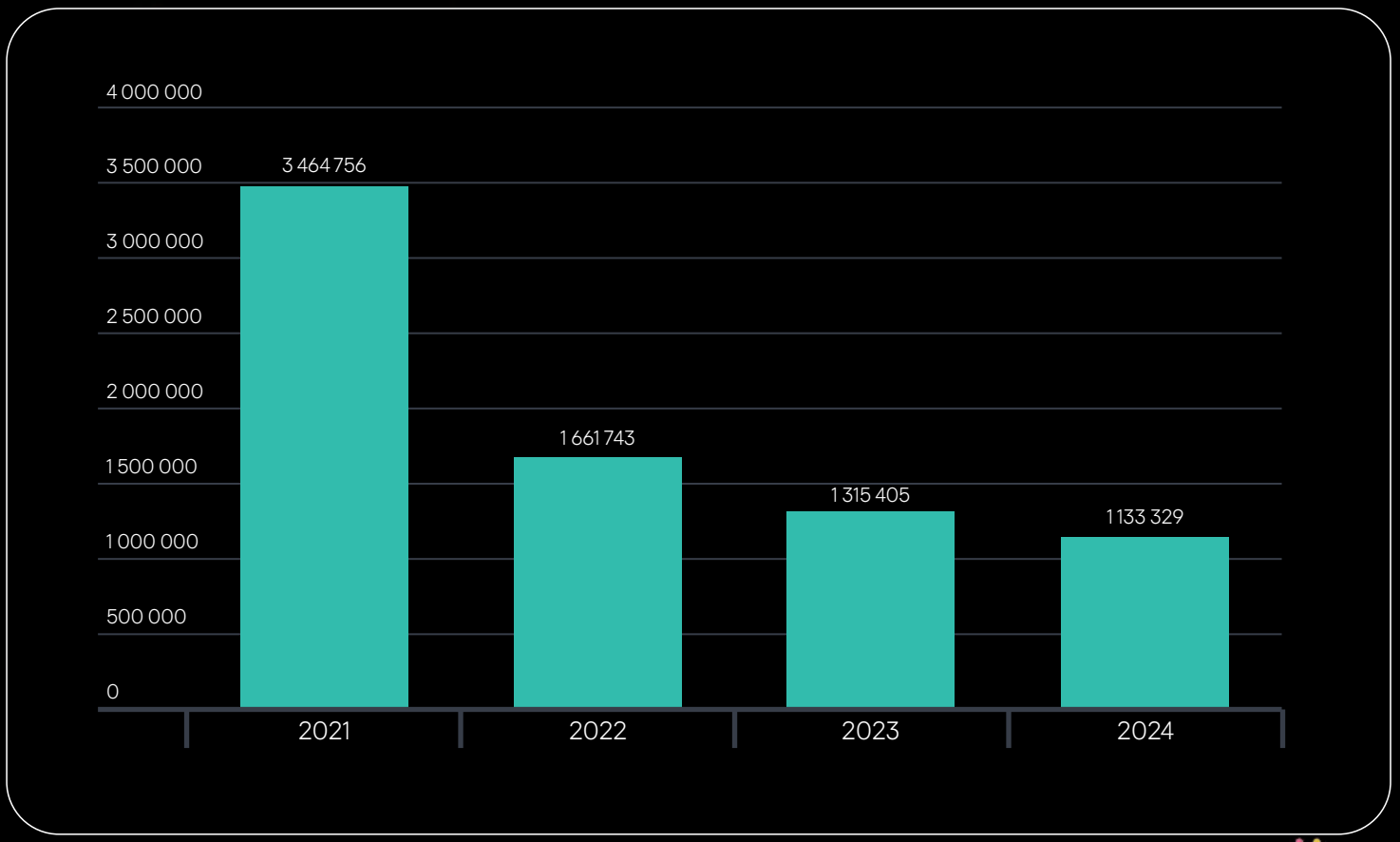
Also in 2024, we detected many new preinstalled malicious apps that we assigned the generalized verdict of Trojan.AndroidOS.Adinstall. A further discovery, made in July, was the LinkDoor backdoor, also known as Vo1d[2], installed on Android-powered TV set-top boxes. It was located inside an infected system application com.google.android.services. The malware was capable of running arbitrary executables and downloading and installing any APKs.

[1] https://www.welivesecurity.com/en/eset-research/ngate-android-malware-relays-nfc-traffic-to-steal-cash/

[2] https://news.drweb.com/show/?i=14900

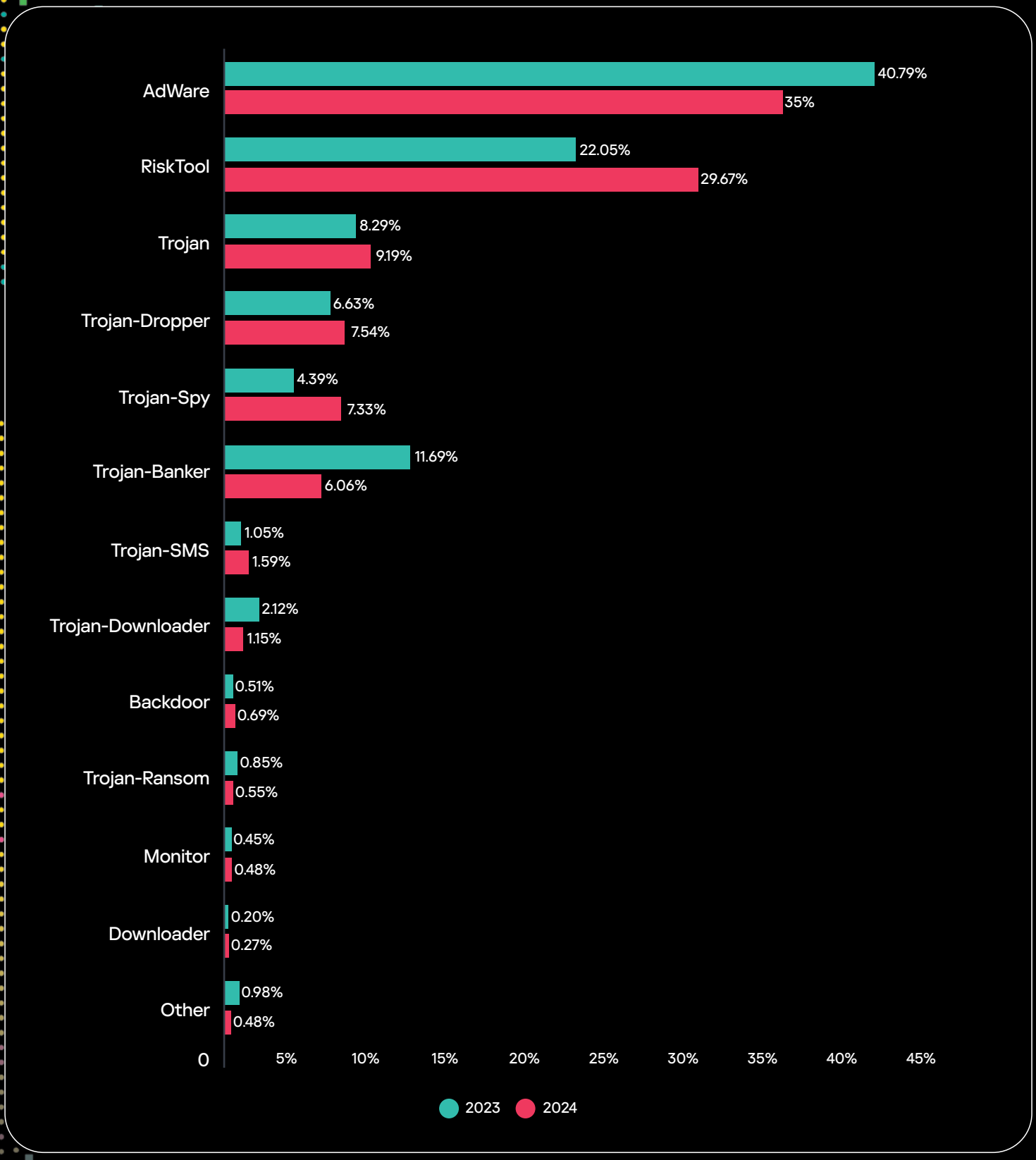
Mobile threat statistics

We discovered 1,133,329 malicious and potentially unwanted installation packages in 2024. This was below the 2023 figure, but the difference was smaller than the year before. The trend in the number of new unique malware installation packages appears to be plateauing.



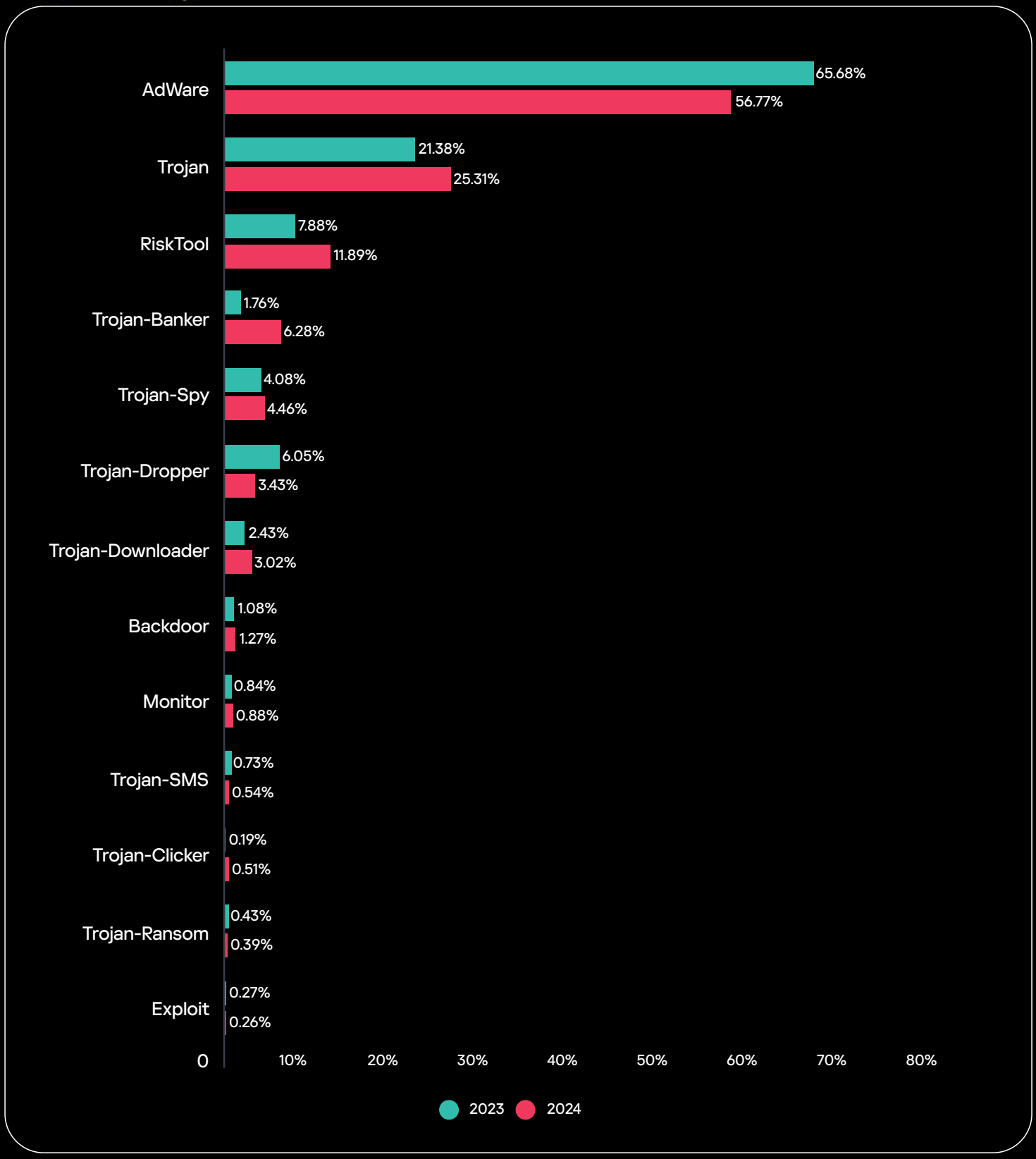
Detected Android-specific malware and unwanted software installation packages in 2021–2024

Detected packages by type



Detected mobile apps by type in 2023 and 2024

Adware and RiskTool apps continued to dominate the rankings of detected threats by type. The BrowserAd (22.8%), HiddenAd (20.3%) and Adlo (16%) families accounted for the largest number of new installation packages in the former category. RiskTool's share grew largely due to an increase in the number of Fakapp pornographic apps.



Share* of users attacked by the given type of malware or unwanted software out of all targeted Kaspersky mobile users in 2023–2024

*The total may exceed 100% if the same users experienced multiple attack types.

Banking Trojans gained three positions as compared with 2023 to occupy fourth place, following the usual leaders: adware, Trojans, and RiskTool.

TOP 20 most frequently detected types of mobile malware

Note that the malware rankings below exclude riskware and potentially unwanted apps, such as adware and RiskTool.

Verdict	%* 2023	%* 2024	Difference in p.p.	Change in ranking
Trojan.AndroidOS.Fakemoney.v	11.76	16.64	+4.88	+2
DangerousObject.Multi.Generic.	14.82	11.13	–3.70	–1
Trojan.AndroidOS.Triada.ga	0.00	6.64	+6.64	
Trojan-Banker.AndroidOS.Mamont.bc	0.00	5.36	+5.36	
Trojan.AndroidOS.Boogr.gsh	6.81	4.71	–2.10	–3
Trojan.AndroidOS.Triada.fd	1.16	4.45	+3.29	+19
DangerousObject.AndroidOS.GenericML	2.39	4.35	+1.96	+3
Trojan-Downloader.AndroidOS.Dwphon.a	0.77	3.59	+2.82	+26
Trojan-Spy.AndroidOS.SpyNote.bz	0.43	3.40	+2.97	+48
Trojan-Spy.AndroidOS.SpyNote.bv	0.37	2.69	+2.32	+57
Trojan.AndroidOS.Fakeapp.hk	0.00	2.51	+2.51	
Trojan.AndroidOS.Triada.gs	0.00	2.50	+2.50	
Trojan.AndroidOS.Triada.gn	0.00	2.02	+2.02	
Trojan-Downloader.AndroidOS.Agent.mm	1.46	1.91	+0.45	+6
Trojan.AndroidOS.Triada.gm	0.00	1.84	+1.84	
Trojan.AndroidOS.Generic.	3.63	1.83	–1.80	–8
Trojan.AndroidOS.Fakemoney.bw	0.00	1.82	+1.82	
Trojan-Banker.AndroidOS.Agent.rj	0.00	1.63	+1.63	
Trojan.AndroidOS.Fakemoney.bj	0.00	1.61	+1.61	
Trojan-Spy.AndroidOS.SpyNote.cc	0.06	1.54	+1.47	

* Share of unique users who encountered this malware as a percentage of all attacked Kaspersky mobile users

Fakemoney, a family of investment and payout scam apps, showed the highest level of activity in 2024. Third-party WhatsApp mods with the Triada.ga embedded Trojan were third, following the generalized cloud-specific verdict of DangerousObject.Multi.Generic. Many other messaging app mods in the same family, namely Triada.fd, Triada.gs, Triada.gn and Triada.gm, hit the TOP 20 too.

Mamont banking Trojans, ranking fourth by number of attacked users, gained high popularity with cybercriminals. These malicious apps come in a multitude of variants. They typically target users' funds via SMS or USSD requests. One of them spreads under the guise of a parcel tracking app for fake online stores.

A crimeware report on Android malware

Various malware files detected by machine learning technology ranked fifth (Trojan.AndroidOS.Boogr.gsh) and seventh (DangerousObject.AndroidOS.GenericML). They were followed by the Dwphon Trojan that came preinstalled on certain devices. The SpyNote RAT Trojans, which remained active throughout the year, occupied ninth, tenth and twentieth places.

Region-specific malware

This section describes malware types that mostly affected specific countries.

Verdict	Country*	%**
Trojan-Banker.AndroidOS.Agent.nw	Turkey	99.58
Trojan.AndroidOS.Piom.axdh	Turkey	99.58
Trojan-Banker.AndroidOS.BrowBot.q	Turkey	99.18
Trojan-Banker.AndroidOS.BrowBot.w	Turkey	99.15
Trojan.AndroidOS.Piom.bayl	Turkey	98.72
Trojan-Banker.AndroidOS.BrowBot.a	Turkey	98.67
Trojan-Spy.AndroidOS.SmsThief.wp	India	98.63
Trojan-Banker.AndroidOS.Rewardsteal.fa	India	98.33
Trojan.AndroidOS.Piom.bbfv	Turkey	98.31
Trojan-Banker.AndroidOS.BrowBot.n	Turkey	98.14
HackTool.AndroidOS.FakePay.c	Brazil	97.99
Backdoor.AndroidOS.Tambir.d	Turkey	97.87
Trojan.AndroidOS.Piom.bcqp	Turkey	97.79
HackTool.AndroidOS.FakePay.i	Brazil	97.65
Backdoor.AndroidOS.Tambir.a	Turkey	97.62
Trojan-Banker.AndroidOS.Coper.b	Turkey	97.45
HackTool.AndroidOS.FakePay.h	Brazil	97.39
Trojan-Spy.AndroidOS.SmsThief.ya	India	97.09
Trojan-Spy.AndroidOS.SmsThief.wm	India	97.09
Trojan-Banker.AndroidOS.Rewardsteal.hi	India	96.68

* Country where the malware was most active

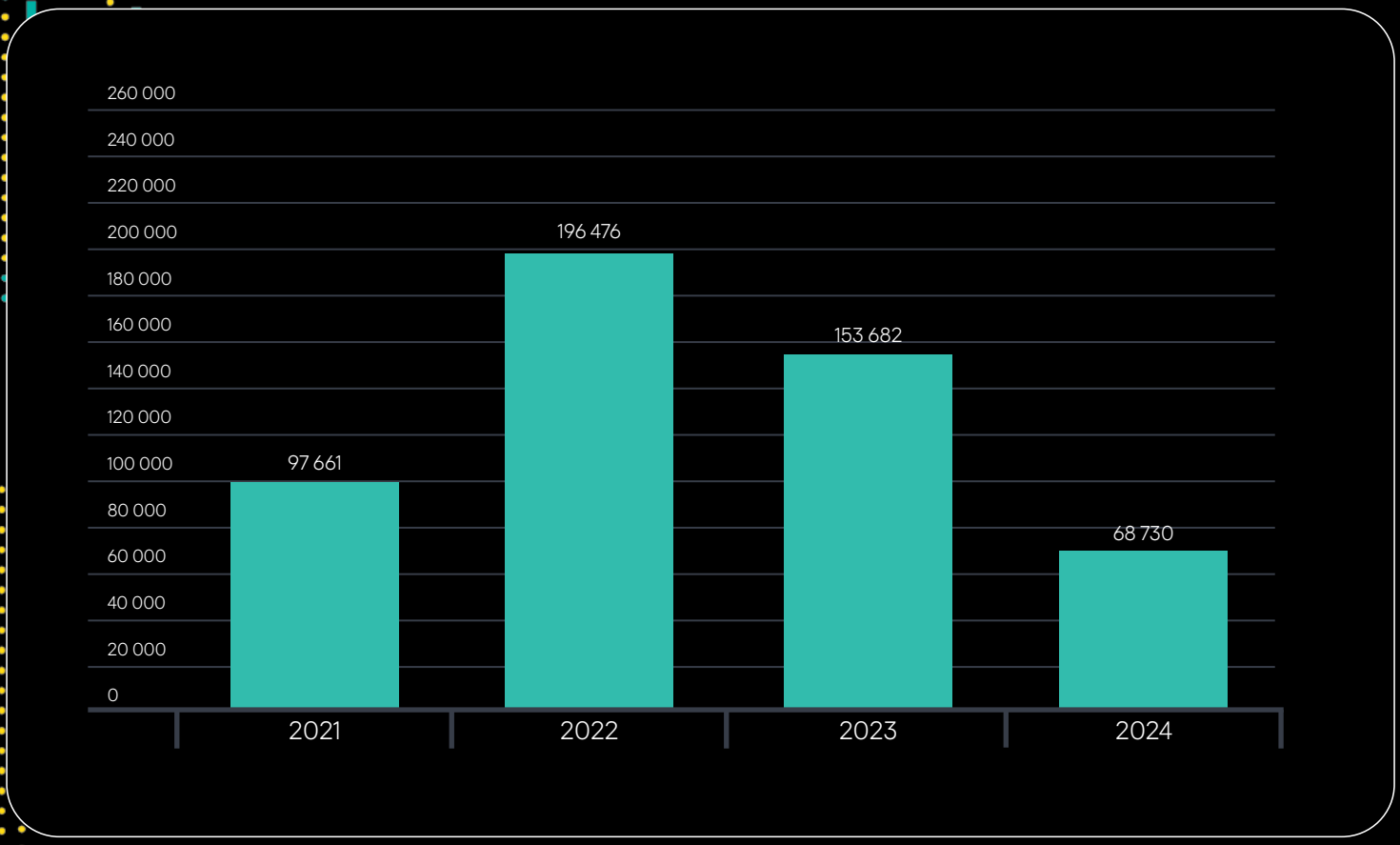
* Share of unique users who encountered the malware in the indicated country as a percentage of all Kaspersky mobile security users attacked by the malware

Turkey and India accounted for the majority of region-specific threats in 2024. A variety of banking Trojans continued to be active in Turkey. Piom Trojans were associated with GodFather and BrowBot banker campaigns.

Users in India were attacked by Rewardsteal bankers and a variety of SmsThief SMS spies. Our quarterly reports have covered FakePay utilities widespread in Brazil and designed to defraud sellers by imitating payment transactions.

Mobile banking Trojans

The number of new banking Trojan installation packages dropped again to 68,730 as compared to the previous year.



The number of mobile banking Trojan installation packages detected by Kaspersky in 2021–2024

The total number of banker attacks increased dramatically over 2023's level despite the drop in the number of unique installation packages. The trend has persisted for years. This may suggest that scammers began to scale down their efforts to generate unique applications, focusing instead on distributing the same files to a maximum number of victims.

TOP 10 mobile bankers

Verdict	%* 2023	%* 2024	Difference in p.p.	Change in ranking
Trojan-Banker.AndroidOS.Mamont.bc	0.00	36.70	+36.70	
Trojan-Banker.AndroidOS.Agent.rj	0.00	11.14	+11.14	
Trojan-Banker.AndroidOS.Mamont.da	0.00	4.36	+4.36	
Trojan-Banker.AndroidOS.Coper.a	0.51	3.58	+3.07	+30
Trojan-Banker.AndroidOS.UdangaSteal.b	0.00	3.17	+3.17	
Trojan-Banker.AndroidOS.Agent.eq	21.79	3.10	–18.69	–4
Trojan-Banker.AndroidOS.Mamont.cb	0.00	3.05	+3.05	
Trojan-Banker.AndroidOS.Bian.h	23.13	3.02	–20.11	–7
Trojan-Banker.AndroidOS.Faketoken.z	0.68	2.96	+2.29	+18
Trojan-Banker.AndroidOS.Coper.c	0.00	2.84	+2.84	

* Share of unique users who encountered this malware as a percentage of all users of Kaspersky mobile security solutions who encountered banking threats

Conclusion

The number of unique malware and unwanted software installation packages continued to decline year to year in 2024. However, the rate of that decline slowed down. The upward trend in mobile banking Trojan activity persisted despite the years-long decrease in unique installation packages.

Cybercriminals kept trying to sneak malware into official app stores like Google Play, but we also discovered a fair number of diverse preinstalled malicious apps in 2024. Speaking of interesting techniques first spotted last year, the use of NFC for stealing bank card data stands out.

Check Kaspersky's security software

kaspersky

www.kaspersky.com