Mobile malware evolution 2019

By Victor Chebyshev

Published: 2020-02-25 · Archived: 2026-04-05 13:12:11 UTC

These statistics are based on detection verdicts of Kaspersky products received from users who consented to provide statistical data.

Figures of the year

In 2019, Kaspersky mobile products and technologies detected:

- 3,503,952 malicious installation packages.
- 69,777 new mobile banking Trojans.
- 68,362 new mobile ransomware Trojans.

Trends of the year

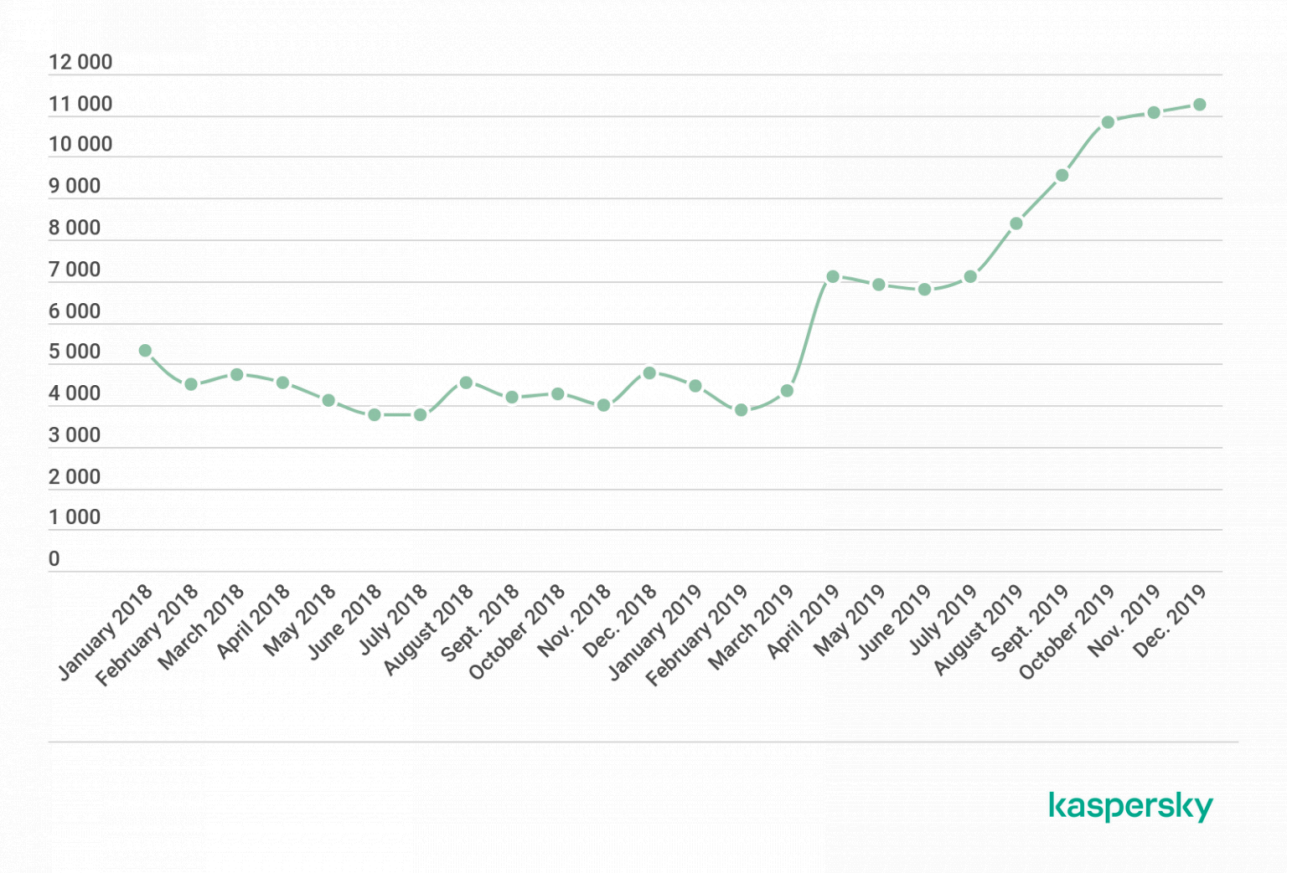
In summing up 2019, two trends in particular stick out:

- Attacks on users' personal data became more frequent.
- Detections of Trojans on the most popular application marketplaces became more frequent.

This report discusses each in more detail below, with examples and statistics.

Attacks on personal data: stalkerware

Over the past year, the number of attacks on the personal data of mobile device users increased by half: from 40,386 unique users in 2018 to 67,500 in 2019. This is not about classic spyware or Trojans, but so-called stalkerware.



Number of unique users attacked by stalkerware in 2018–2019

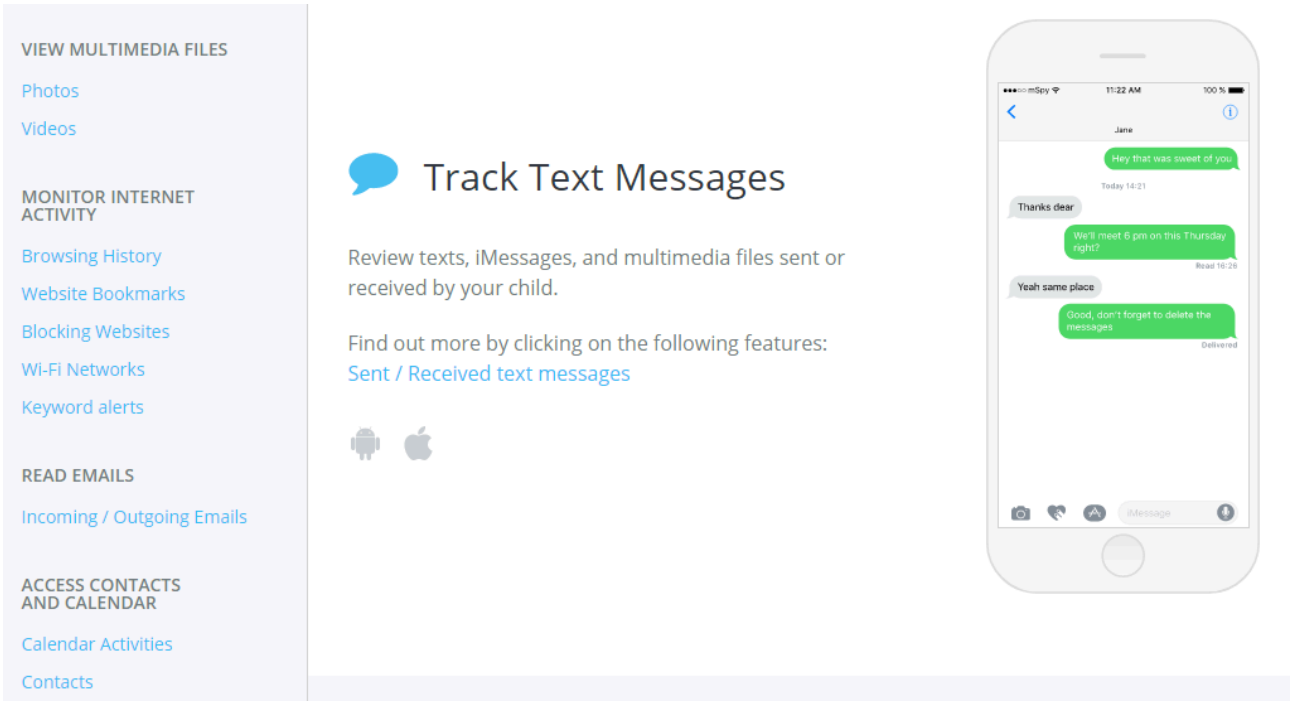
Stalkerware can be divided into two major categories:

- Trackers.
- Full-fledged tracking apps.

The creators of trackers generally focus on two main features: tracking victims' coordinates and intercepting text messages. Until recently, many such apps, mostly free, were available on the official Google Play marketplace. After Google Play changed its policy in late 2018, most of them were removed from the store, and most developers pulled support for their products. However, such trackers can still be found on their developers' and third-party sites.

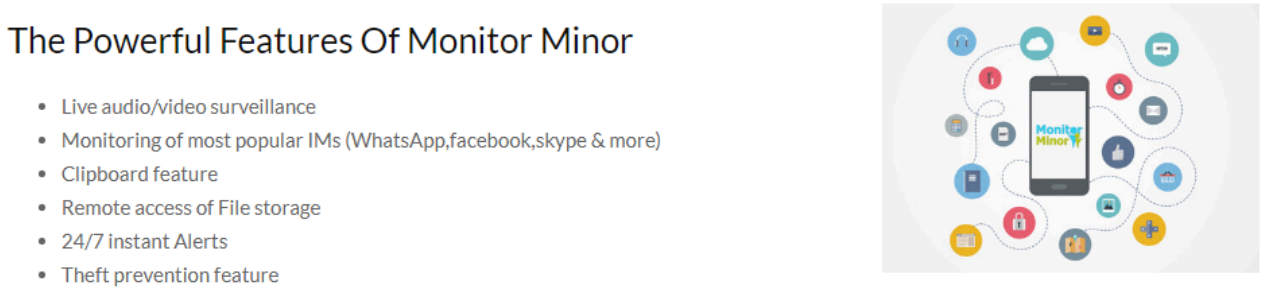
If such an app gets onto a device, messages and data about the user's location become accessible to third parties. These third parties are not necessarily only those tracking the user: the client-server interaction of some services ignores even the minimum security requirements, allowing anyone to gain access to the accumulated data.

The situation of full-fledged stalkerware is somewhat different: there are no such apps on Google Play, but they are actively supported by developers. These tend to be commercial solutions with extensive spying capabilities. They can harvest almost any data on a compromised device: photos (both entire archives and individual pictures, for example, taken at a certain location), phone calls, texts, location information, screen taps (keylogging), and so on.



Screenshot from the site of a stalkerware app developer showing the capabilities of the software

Many apps exploit root privileges to extract messaging history from protected storage in social networking and instant messaging applications. If it cannot gain the required access, the stalkerware can take screenshots, log screen taps and even extract the text of incoming and outgoing messages from the windows of popular services using the Accessibility feature. One example is the commercial spyware app Monitor Minor.



Screenshot from the site of a stalkerware app developer showing the software's ability to intercept data from social networks and messengers

The developers of the commercial spyware FinSpy went one step further by adding a feature to intercept correspondence in secure messengers, such as Signal, Threema and others. To ensure interception, the app independently obtains root privileges by exploiting the vulnerability CVE-2016-5195, aka "Dirty Cow". The expectation is that the victim is using an old device with an outdated operating system kernel in which the exploit can escalate privileges to root.

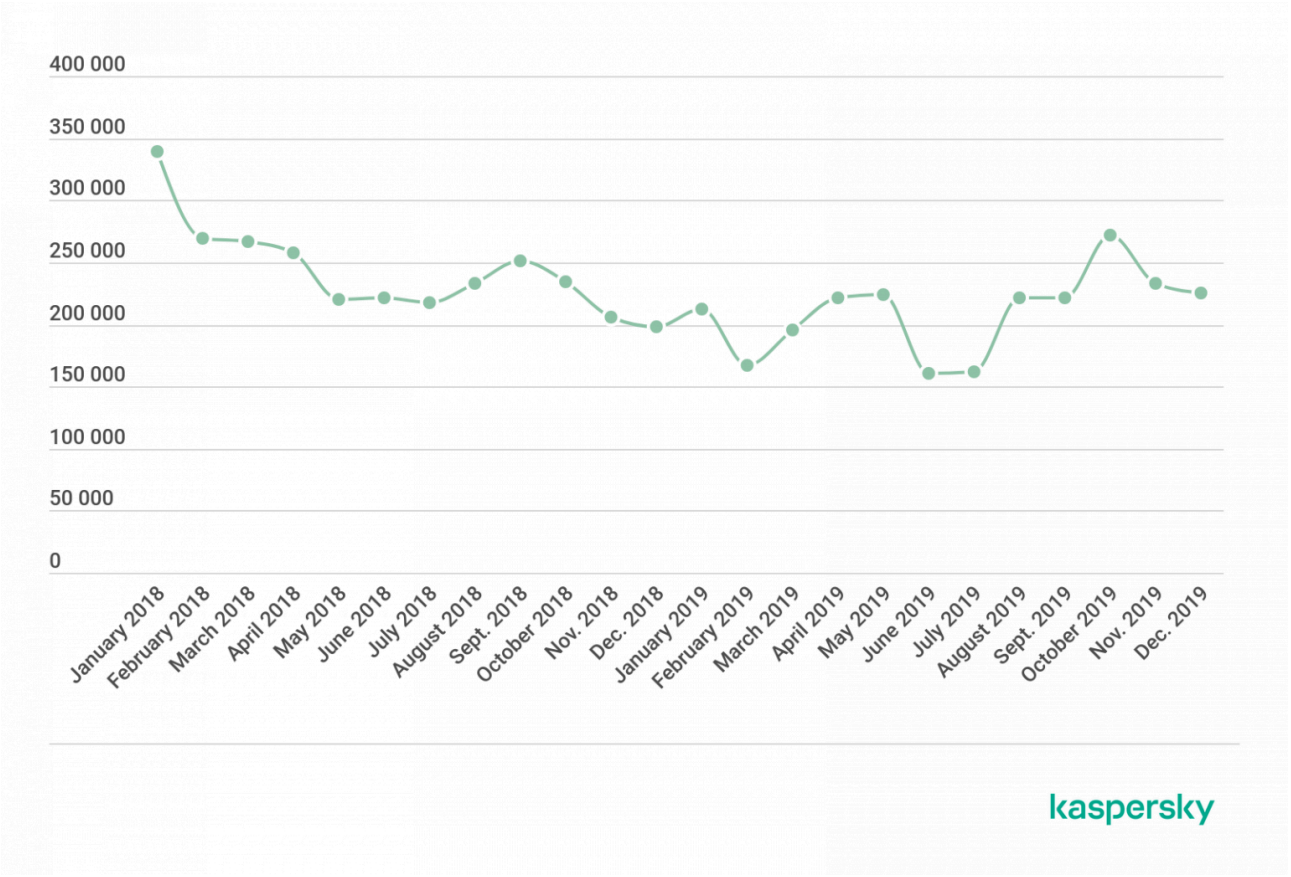
It is worth noting that the user base of messaging apps includes hundreds of millions. Classic calls and texts are being used less and less, and communication — be it text messages or voice/video calls — is gradually moving to

instant messaging applications. Hence the rising interest in data stored in such apps.

Attacks on personal data: advertising apps

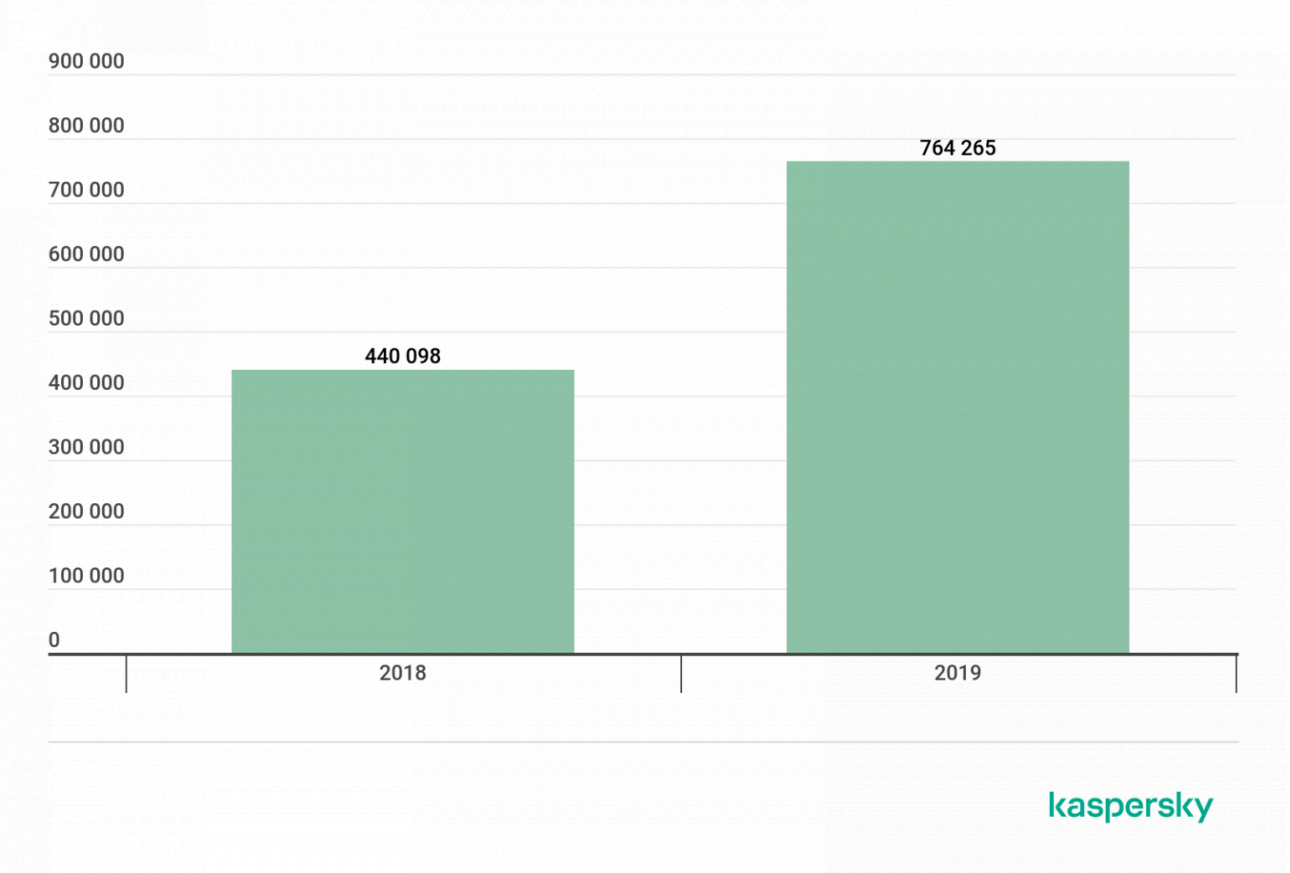
In 2019, we observed a significant increase in the number of adware threats, one purpose being to harvest personal data on mobile devices.

The statistics show that the number of users attacked by adware in 2019 is roughly unchanged from 2018.



Number of users attacked by adware in 2018 and 2019

At the same time, the number of detected adware installation packages almost doubled from 2018.



Number of detected adware installation packages in 2018 and 2019

These indicators typically correlate, but not in the case of adware. This can be explained by several factors:

- Adware installation packages are generated automatically and spread literally everywhere, but for some reason do not reach the target audience. It is possible that they get detected immediately after being generated and cannot propagate further.
- Often, such apps contain nothing useful — just an adware module; so the victim immediately deletes them, assuming that they allow removing themselves.

Nevertheless, it is the second successive year that adware has appeared in our Top 3 detected threats. KSN statistics confirm it to be one of the most common types of threats: four places in our Top 10 mobile threats by number of users attacked in 2019 are reserved for adware-class apps, with one member of the family, HiddenAd, taking the third.

	Вердикт	%*
1	DangerousObject.Multi.Generic	35,83
2	Trojan.AndroidOS.Boogr.gsh	8,30
3	AdWare.AndroidOS.HiddenAd.et	4,60
4	AdWare.AndroidOS.Agent.f	4,05

5	Trojan.AndroidOS.Hiddapp.ch	3,89
6	DangerousObject.AndroidOS.GenericML	3,85
7	AdWare.AndroidOS.HiddenAd.fc	3,73
8	Trojan.AndroidOS.Hiddapp.cr	2,49
9	AdWare.AndroidOS.MobiDash.ap	2,42
10	Trojan-Dropper.AndroidOS.Necro.n	1,84

**Share of all users attacked by this type of malware in the total number of users attacked.*

In 2019, mobile adware developers not only generated tens of thousands of packages, but also technically enhanced their products, in particular through the addition of techniques to bypass operating system restrictions.

For example, Android imposes certain restrictions on background operation of applications for battery-saving reasons. This negatively impacts the operation of various threats, including adware apps that like to lurk in the background and wait for, say, a new banner to arrive from C&C. The introduction of such restrictions made it impossible for apps to show ads outside the context of their own window, thus starving most adware of oxygen.

The creators of the KeepMusic adware family found a smart workaround. To bypass the restrictions, their software does not request permissions like, for example, malware does. Instead, the program starts looping an MP3 file that plays silence. The operating system decides that the music player is running, and does not terminate the KeepMusic background process. As a result, the adware can request a banner from the server and display it any time.

Attacks on personal data: exploiting access to Accessibility

The year 2019 saw the appearance of the first specimen of mobile financial malware (Trojan-Banker.AndroidOS.Gustuff.a), featuring enhanced autonomy. Until then, two methods had been used to steal money from bank accounts:

- **Via SMS banking on the victim end.** This is an autonomous theft technique that requires only information about the transfer recipient. This data the bot can either store in its body or receive as a command from C&C. The Trojan infects the device and sends a text with a transfer request to a special bank phone number. The bank then automatically transfers the funds to the recipient from the device owner’s account. Due to the increase in such theft, limits on mobile transfers have been tightened, so this attack vector has been relegated to backup.
- **By stealing online banking credentials.** This has been the dominant method in recent years. Cybercriminals display a phishing window on the victim’s device that mimics the bank’s login page and reels in the victim’s credentials. In this case, the cybercriminals need to carry out the transaction themselves, using the app on their own mobile device or a browser. It is possible that the bank’s anti-fraud systems can detect the abnormal activity and block it, leaving the attackers empty-handed even if the victim’s device is infected.

In 2019, cybercriminals mastered a third method: stealing by manipulating banking apps. First, the victim is persuaded to run the app and sign in, for example, using a fake push notification supposedly from the bank. Tapping the notification does indeed open the banking app, which the attackers, using Accessibility, gain full control over, enabling them to fill out forms, tap buttons, etc. Moreover, the bot operator does not need to do anything, because the malware performs all actions required. Such transactions are trusted by banks, and the maximum transfer amount can exceed the limits of SMS banking by an order of magnitude. As a result, the cybercriminals can clean out the account in one go.

Stealing funds from bank accounts is just one malicious use of Accessibility. In effect, any malware with these permissions can control all on-screen processes, while any Android app is basically a visual representation of buttons, data entry forms, information display, and so on. Even if developers implement their own control elements, such as a slider that needs to be moved at a certain speed, this too can be done using Accessibility commands. Thus, cybercriminals have tremendous leeway to create what are perhaps the most dangerous classes of mobile malware: spyware, banking Trojans and ransomware Trojans.

The misuse of the Accessibility features poses a serious threat to users' personal data. Where previously cybercriminals had to overlay phishing windows and request a bunch of permissions in order to steal personal information, now victims themselves output all necessary data to the screen or enter it in forms, where it can be easily gleaned. And if the malware needs more, it can open the Settings section by itself, tap a few buttons, and obtain the necessary permissions.

Mobile Trojans on popular marketplaces: Google Play

Slipping malware into the main Android app store delivers much better results than social engineering victims into installing apps from third-party sources. In addition, this approach enables attackers to:

- Bypass SafetyNet, Android's built-in antivirus protection. If a user downloads an app from Google Play, the likelihood that it will be installed without additional requests — for example, to disable the built-in protection under an imaginary pretext — is very high. The only thing that can protect the user from infection in that situation is a third-party security solution.
- Overcome psychological barriers. Official app stores enjoy far greater trust than third-party "markets," and act as store windows of sorts that can be used for distributing software much more efficiently.
- Target victims without unnecessary spending. Google Play can be used to host fakes that visually mimic, say, popular banking apps. This was the distribution vector used in a spate of attacks on mobile users in Brazil: we detected numerous malicious programs on Google Play under the guise of mobile apps for Brazilian banks.

In addition to malicious doppelgangers, cybercriminals deployed several other tricks to maximize device infection rates:

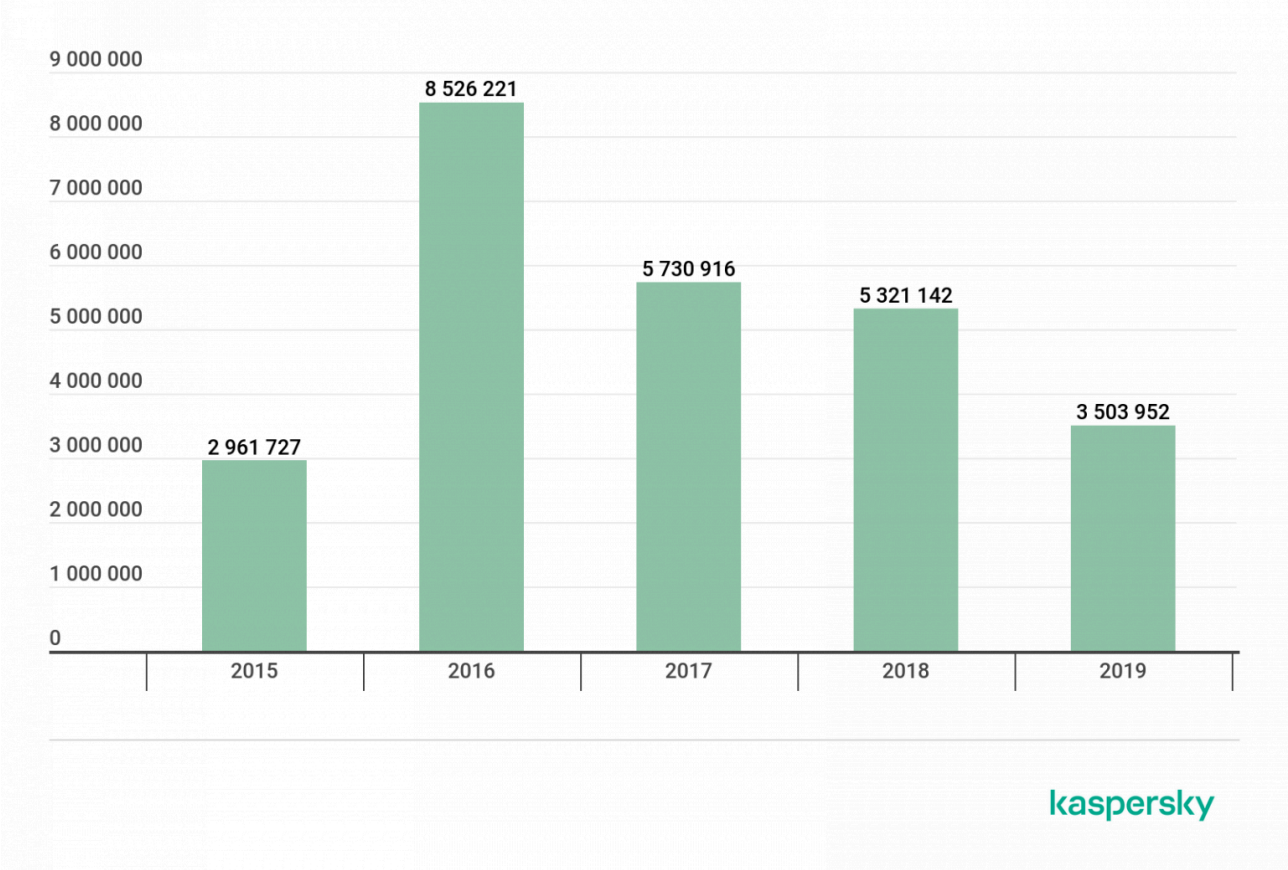
- The case of CamScanner showed that an app's legitimate behavior can be supplemented with malicious functions by updating its code for handling advertising. This could be described as the most sophisticated attack vector, since its success depends on a large number of factors, including the user base of the host app, the developer's trust in third-party advertising code and the type of malicious activity.

- Another example demonstrates that attackers sometimes upload to Google Play fairly well-behaved apps from popular user categories. In this case, it was photo editors.
- The most depressing case involves a Trojan from the Joker family, of which we have found many samples on Google Play, and still are. Deploying the tactic of mass posting, cybercriminals uploaded apps under all kinds of guises: from wallpaper-changing tools and security solutions to popular games. In some cases, the Trojan scored hundreds of thousands of downloads. No other attack vector can reach this kind of audience within such a short space of time.

The good news is that Google and the antivirus industry have teamed up to fight threats on the site. This approach should prevent most malware from penetrating the official Google app store.

Statistics

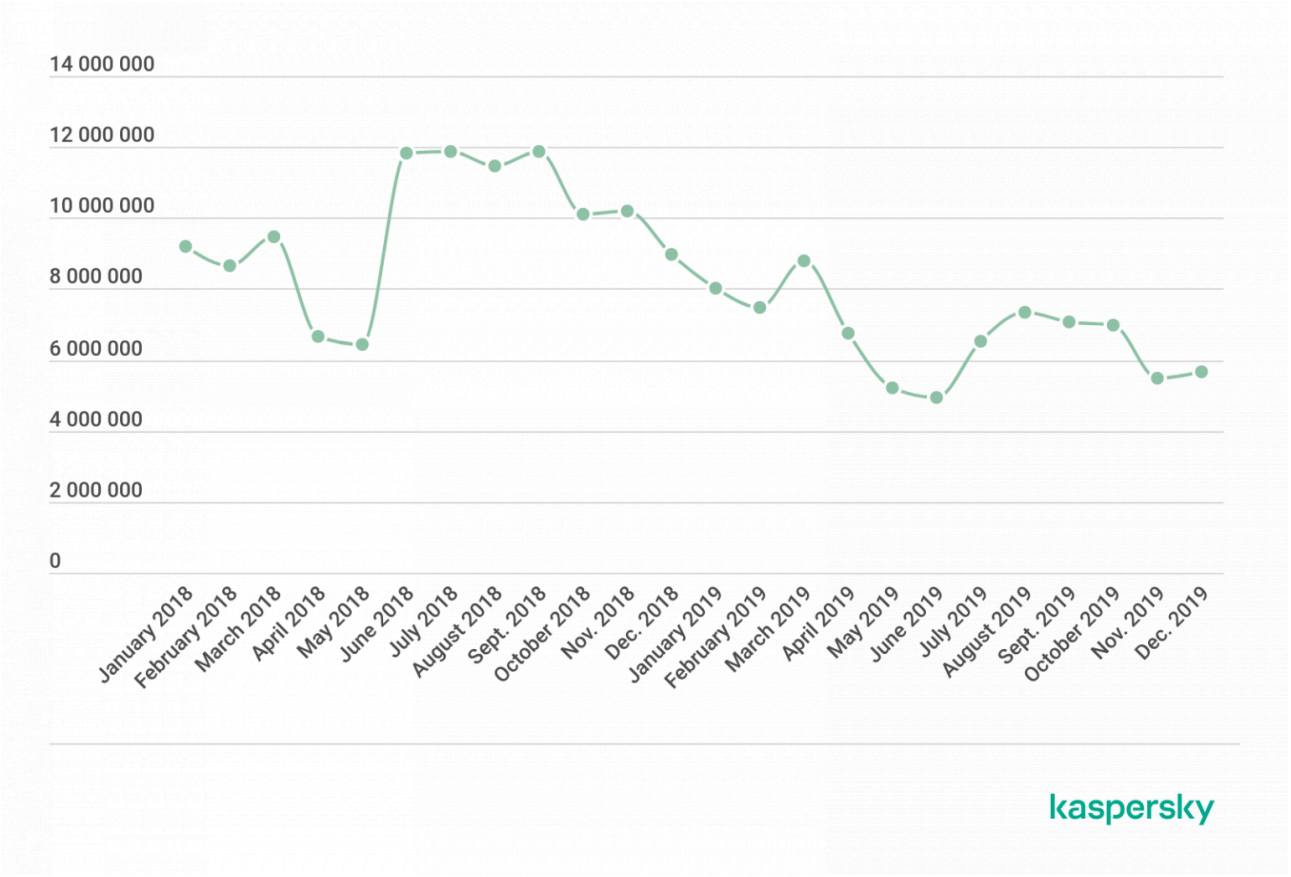
In 2019, we discovered 3,503,952 mobile malicious installation packages, which is 1,817,190 less than in the previous year. We have not detected so few mobile threats since 2015.



Number of mobile malicious installation packages for Android in 2015–2019

For three consecutive years, we have seen an overall decline in the number of mobile threats distributed as installation packages. The picture largely depends on specific cybercriminal campaigns: some have become less active, others have completely ceased, and new players have yet to gain momentum.

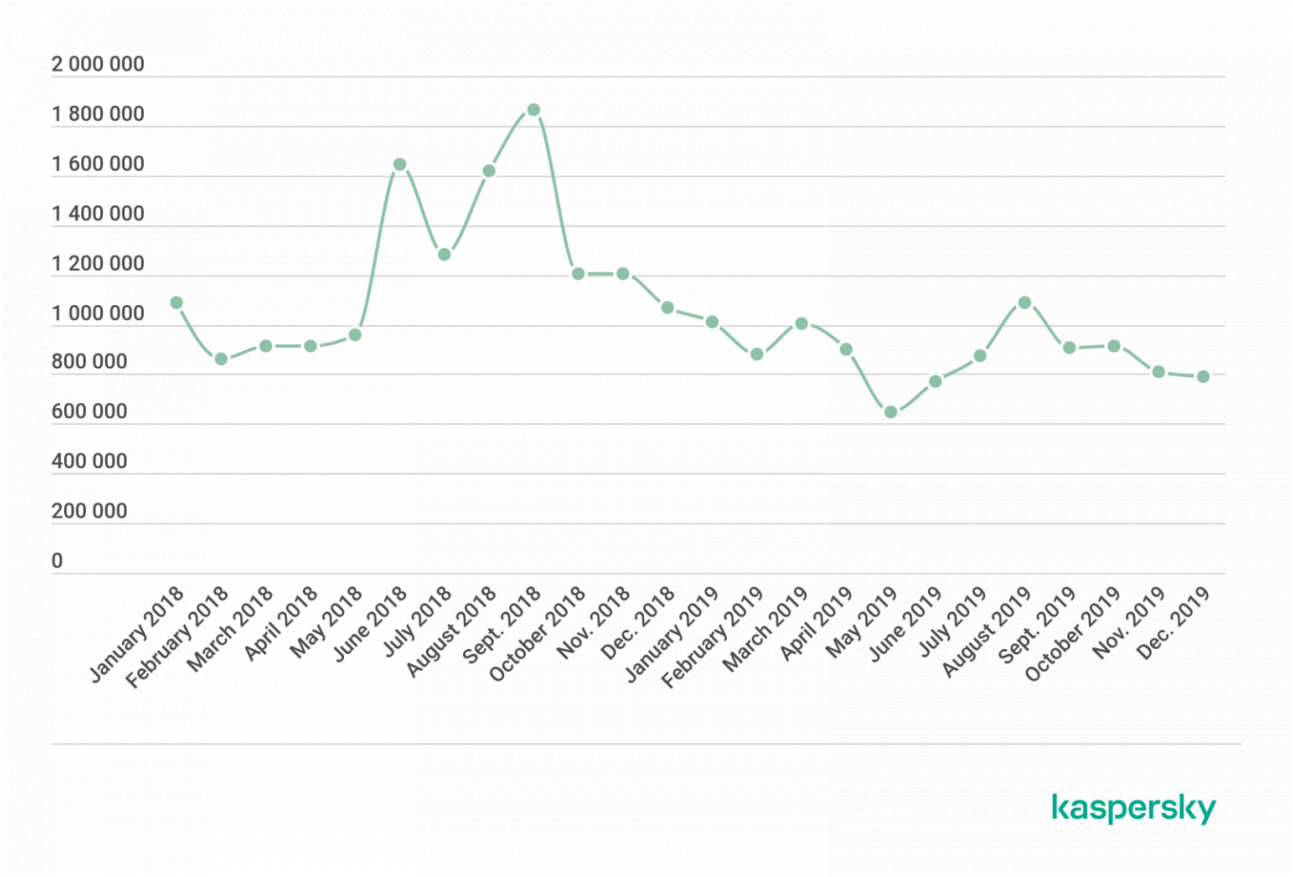
The situation is similar with the number of attacks using mobile threats: whereas in 2018 we observed a total of **116.5 million** attacks, in 2019 the figure was down to **80 million**.



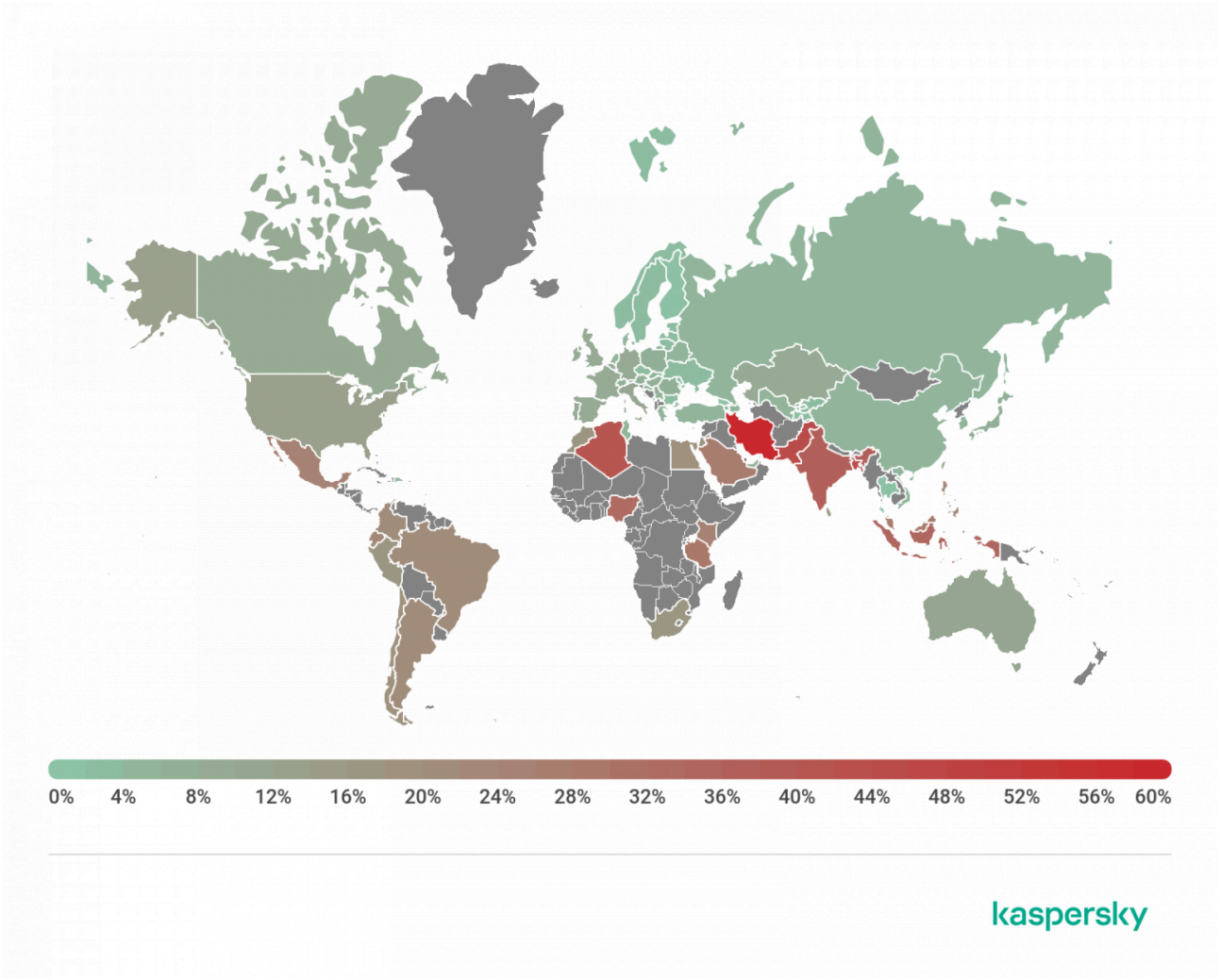
Number of attacks defeated by Kaspersky mobile solutions in 2018–2019

The figures were back to the year before, before the start of the Asacub banking Trojan epidemic.

Since the number of attacks correlates with the number of users attacked, we observed a similar picture for this indicator.



Number of users attacked by mobile malware in 2018–2019



Geography of attacked users in 2019

Top 10 countries by share of users attacked by mobile malware:

Country*	%**
Iran	60.64
Pakistan	44.43
Bangladesh	43.17
Algeria	40.20
India	37.98
Indonesia	35.12
Nigeria	33.16
Tanzania	28.51

Saudi Arabia	27.94
Malaysia	27.36

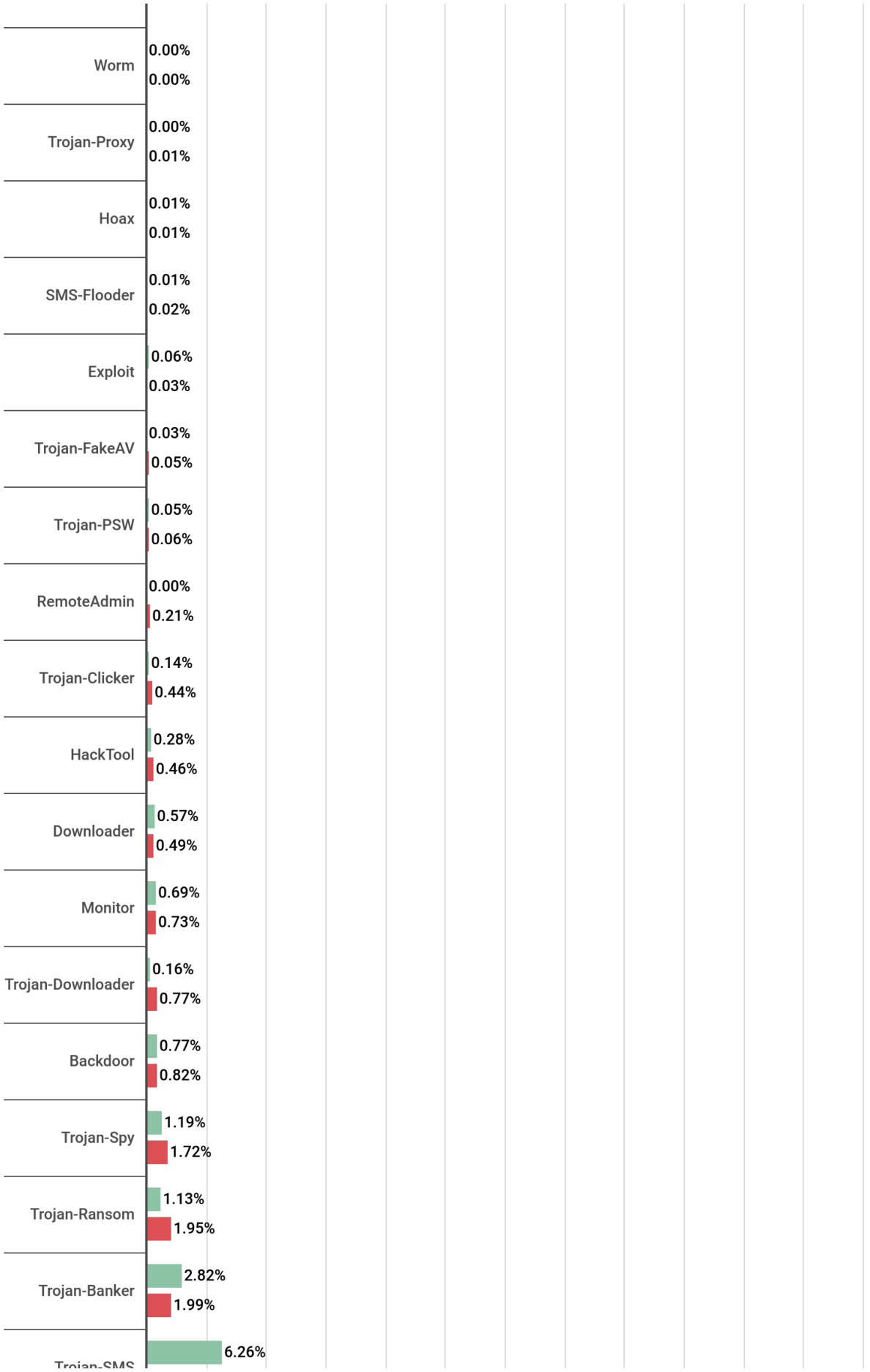
**Excluded from the rankings are countries with fewer than 25,000 active users of Kaspersky mobile security solutions in the reporting period.*

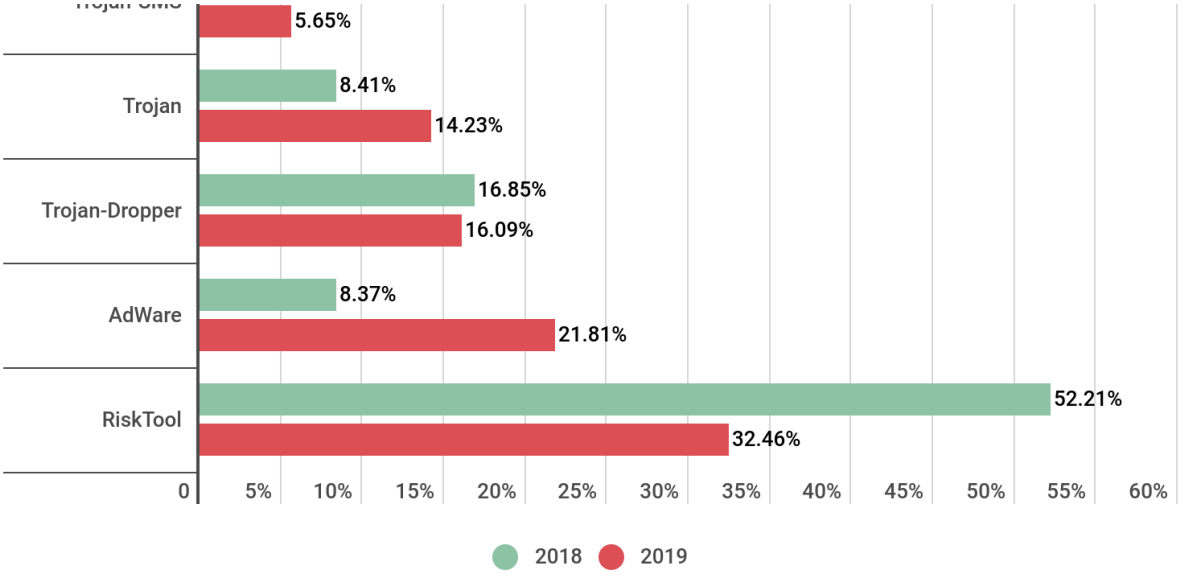
***Unique users attacked in the country as a percentage of all users of Kaspersky mobile security solutions in the country.*

In 2019, Iran (60.64%) again topped the list for the third year in a row. The most common threats in that country come from adware and potentially unwanted software: Trojan.AndroidOS.Hiddapp.bn, AdWare.AndroidOS.Agent.fa, and RiskTool.AndroidOS.Dnotua.yfe.

Pakistan (44.43%) climbed from seventh to second place, mainly on the back of a rise in the number of users attacked by adware. The largest contribution was made by members of the AdWare.AndroidOS.HiddenAd family. A similar picture can be seen in Bangladesh (43.17%), whose share has grown due to the same adware families.

Types of mobile threats


Worm
0.00%
0.00%
Trojan-Proxy
0.00%
0.01%
Hoax
0.01%
0.01%
SMS-Flooder
0.01%
0.02%
Exploit
0.06%
0.03%
Trojan-FakeAV
0.03%
0.05%
Trojan-PSW
0.05%
0.06%
RemoteAdmin
0.00%
0.21%
Trojan-Clicker
0.14%
0.44%
HackTool
0.28%
0.46%
Downloader
0.57%
0.49%
Monitor
0.69%
0.73%
Trojan-Downloader
0.16%
0.77%
Backdoor
0.77%
0.82%
Trojan-Spy
1.19%
1.72%
Trojan-Ransom
1.13%
1.95%
Trojan-Banker
2.82%
1.99%
6.26%



kaspersky

Distribution of new mobile threats by type in 2018 and 2019

In 2019, the share of RiskTool-class threats decreased by 20 p.p. (32.46%). We believe the main reason to be the sharp drop in the generation of threats from the SMSreg family. A characteristic feature of this family is payments via SMS: for example, money transfers or subscriptions to mobile services. Moreover, the user is not explicitly informed of the payment or money being charged to their mobile account. Whereas in 2018, we picked up 1,970,742 SMSreg installation packages, the number decreased by an order of magnitude to 193,043 in 2019. At the same time, far from declining, the number of packages of other members of this class of threats increased noticeably.

	Name of family	%*
1	Agent	27.48
2	SMSreg	16.89
3	Dnotua	13.83
4	Wapron	13.73
5	SmsSend	9.15
6	Resharer	4.62
7	SmsPay	3.55
8	PornVideo	2.51
9	Robtes	1.23

10	Yoga	1.03

**Share of packages of this family in the total number of riskware-class packages detected in 2019.*

Skymobi and Paccy dropped out of the Top 10 families of potentially unwanted software; the number of installation packages of these families detected in 2019 decreased tenfold. Their creators likely minimized or even ceased their development and distribution. However, a new player appeared: the Resharer family (4.62%), which ranked sixth. This family is noted for its self-propagation through posting information about itself on various sites and mailing it to the victim's contacts.

Adware demonstrated the most impressive growth, up by 14 p.p. The main source of this growth was HiddenAd (26.81%); the number of installation packages of this family increased by two orders of magnitude against 2018.

	Name of family	%*
1	HiddenAd	26.81
2	MobiDash	20.45
3	Ewind	16.34
4	Agent	15.27
5	Dnotua	5.51
6	Kuguo	1.36
7	Dowgin	1.28
8	Triada	1.20
9	Feiad	1.01
10	Frupi	0.94

**Share of packages of this family in the total number of adware-class packages detected in 2019.*

Significant growth also came from the MobiDash (20.45%) and Ewind (16.34%) families. Meanwhile, the Agent family (15.27%), which held a leading position in 2018, dropped to fourth place.

Compared to 2018, the number of mobile Trojans detected decreased sharply. A downward trend has been observed for two consecutive years now, yet droppers remain one of the most numerous malware classes. The Hqwar family showed the most notable decrease: down from 141,000 packages in 2018 to 22,000 in 2019. At the same time, 2019 saw the debut of the Ingopack family: we detected 115,654 samples of this dropper.

Meanwhile, the share of Trojan-class threats rose by 6 p.p., with the two most numerous malware families of this class being Boogr and Hiddapp. The Boogr family contains various Trojans that have been detected using

machine-learning (ML) technology. A feature of the Hiddapp family is that it hides its icon in the list of installed apps while continuing to run in the background.

The share of mobile ransomware Trojans slightly increased. The Top 3 families of this class of threats remained the same as in 2018: Svpeng, Congur, and Fusob — in that order.

Top 20 mobile malware programs

The following malware rankings omit potentially unwanted software, such as RiskTool and AdWare.

	Verdict	%*
1	DangerousObject.Multi.Generic	49.15
2	Trojan.AndroidOS.Boogr.gsh	10.95
3	Trojan.AndroidOS.Hiddapp.ch	5.19
4	DangerousObject.AndroidOS.GenericML	5.08
5	Trojan-Dropper.AndroidOS.Necro.n	3.45
6	Trojan.AndroidOS.Hiddapp.cr	3.28
7	Trojan-Banker.AndroidOS.Asacub.snt	2.35
8	Trojan-Dropper.AndroidOS.Hqwar.bb	2.10
9	Trojan-Dropper.AndroidOS.Lezok.p	1.76
10	Trojan-Banker.AndroidOS.Asacub.a	1.66
11	Trojan-Downloader.AndroidOS.Helper.a	1.65
12	Trojan-Banker.AndroidOS.Svpeng.ak	1.60
13	Trojan-Downloader.AndroidOS.Necro.b	1.59
14	Trojan-Dropper.AndroidOS.Hqwar.gen	1.50
15	Exploit.AndroidOS.Lotoor.be	1.46
16	Trojan.AndroidOS.Hiddapp.cf	1.35
17	Trojan.AndroidOS.Dvmap.a	1.33
18	Trojan-Banker.AndroidOS.Agent.ep	1.31
19	Trojan.AndroidOS.Agent.rt	1.28
20	Trojan-Dropper.AndroidOS.Tiny.d	1.14

**Share of users attacked by this type of malware out of all attacked users*

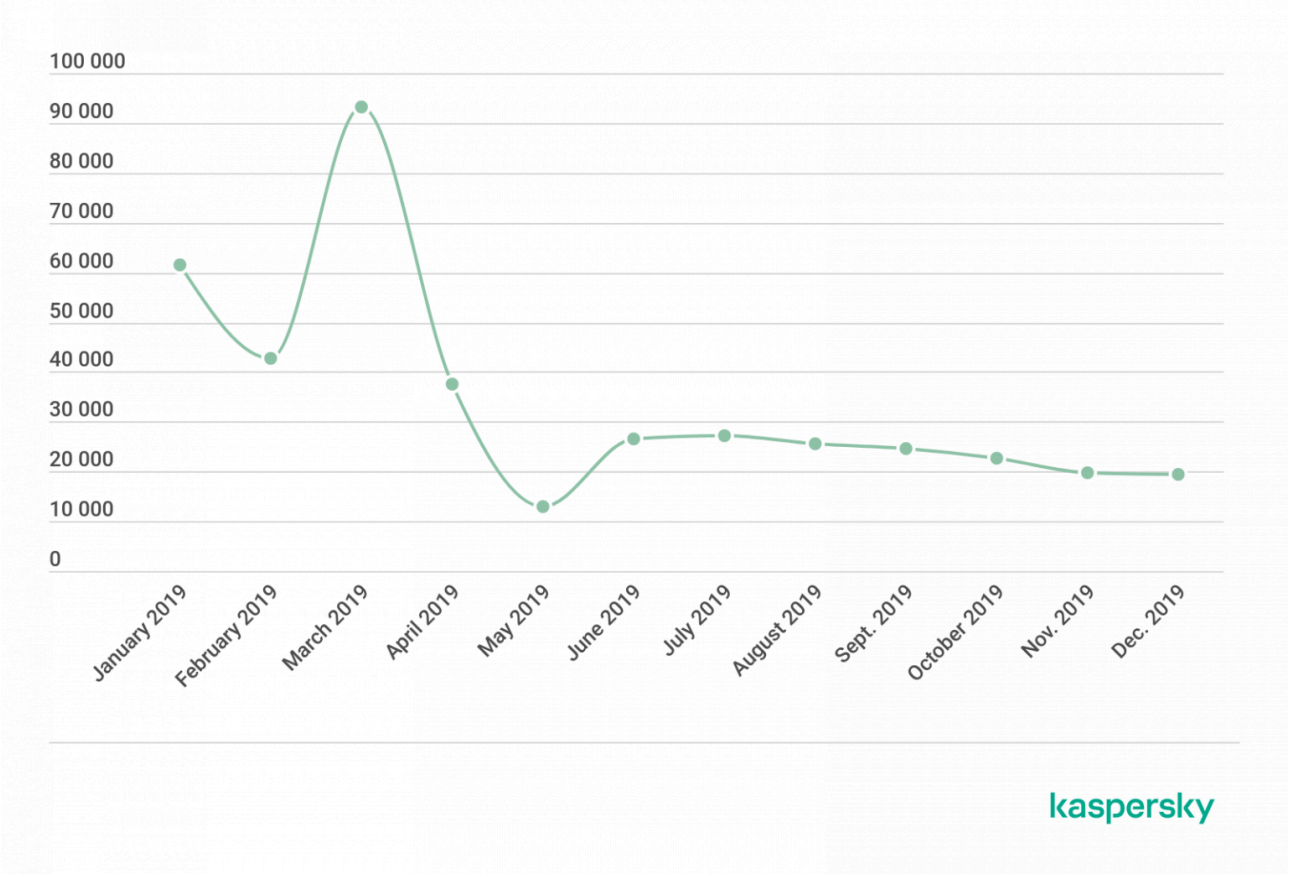
As we wrap up the year 2019, first place in our Top 20 mobile malware, as in previous years, goes to the verdict DangerousObject.Multi.Generic (49.15%), which we use for malware detected with cloud technology. The verdict is applied where the antivirus databases still have no signatures or heuristics for malware detection. This way, the most recent malware is uncovered.

In second place came the verdict Trojan.AndroidOS.Boogr.gsh (10.95%). This verdict is assigned to files recognized as malicious by our ML-based system. Another result of this system's work is objects with the verdict DangerousObject.AndroidOS.GenericML (5.08%, fourth place in the rating). This verdict is assigned to files whose structure is identical to that of malicious files.

Third, sixth, and sixteenth places were taken by members of the Hiddapp family. We assign this verdict to any app that hides its icon in the list of apps immediately after starting. Subsequent actions of such apps may be anything from downloading or dropping other apps to displaying ads.

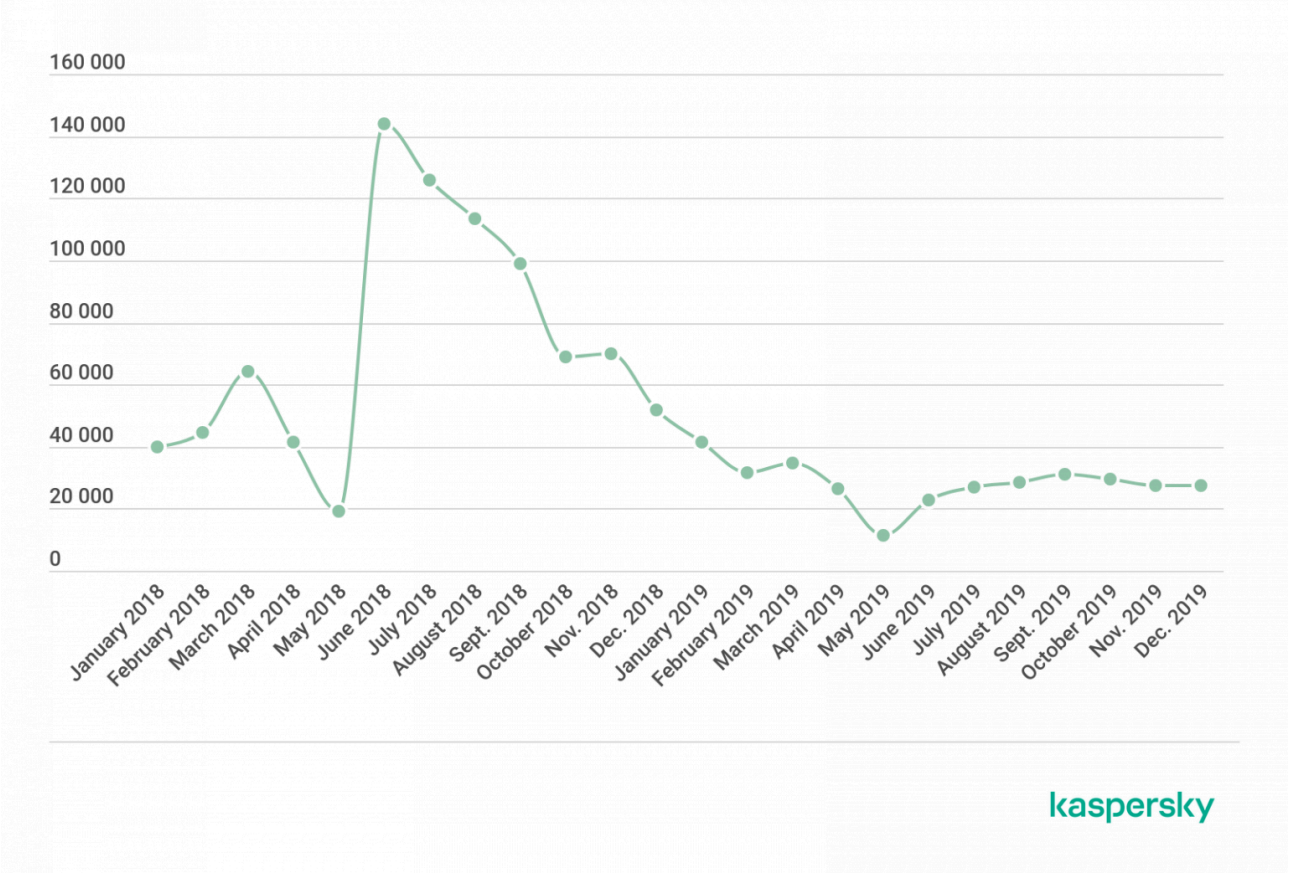
Fifth and thirteenth places went to members of the Necro family of droppers and loaders. In both threat classes, Necro members did not make it into the Top 10 by number of detected files. Even the weakened Hwar family of droppers strongly outperformed Necro by number of generated objects. That said, users often encountered Necro members due to the family's penetration of Google Play.

Seventh and tenth places went to the Asacub family of banking Trojans. Whereas at the start of the year, the Trojan's operators were still actively spreading the malware, starting in March 2019, we noticed a drop in this family's activity.



Number of unique users attacked by the Asacub mobile banking Trojan in 2019

Eighth and fourteenth places were reserved for droppers in the Hqwar family. Their activity dropped significantly from 80,000 attacked users in 2018 to 28,000 in 2019. However, we continue to register infection attempts by this family, and do not rule out its return to the top.



Number of unique users attacked by the Hqwar mobile dropper in 2019

In ninth position is another dropper, this time from the Lezok family: Trojan-Dropper.AndroidOS.Lezok.p (1.76%). A notable difference between this Trojan and Hqwar is that the malware penetrates the device before it arrives at the store. This is evidenced by KSN statistics showing that the Trojan was most often detected in the system directory under the names PhoneServer, GeocodeService, and similar.

	Path to the detected threat	Number of unique users attacked
1	/system/priv-app/PhoneServer/	49,688
2	/system/priv-app/GeocodeService/	9747
3	/system/priv-app/Helper/	6784
4	/system/priv-app/com.android.telephone/	5030
5	/system/priv-app/	1396

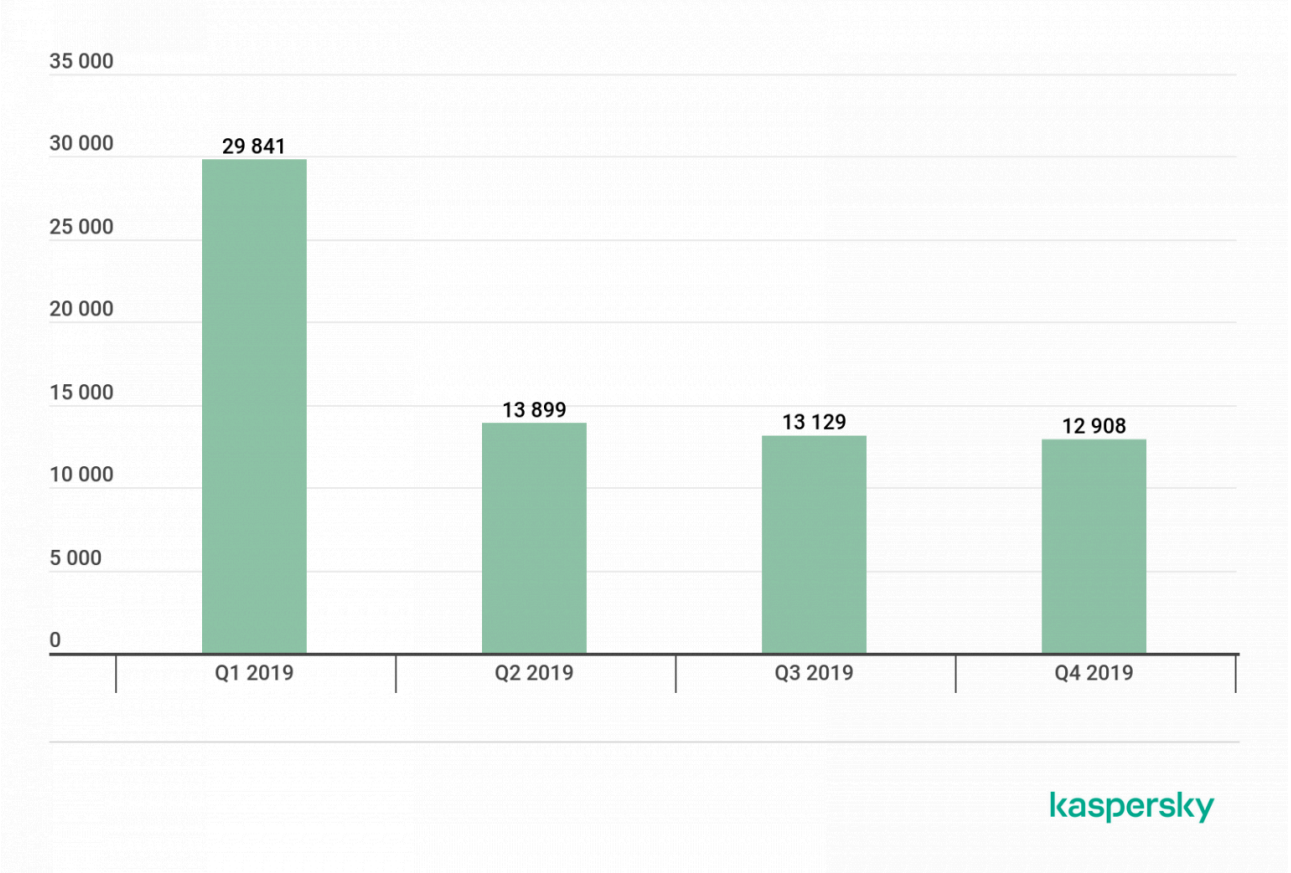
6	/system/priv-app/CallerIdSearch/	1343

When the device is turned on, Lezok dumps its payload into the system; it does so even if the victim deletes the dumped files using regular OS tools or resets the device to the factory settings. The trick is that the Trojan forms part of the factory firmware and can reload (restore) the deleted files.

The final Trojan worthy of attention is Trojan-Downloader.AndroidOS.Helper.a (1.56%), which finished eleventh in the rankings. Despite claims to the contrary, it can be removed. However, the infected system contains another Trojan that installs a helper app, which cannot be removed that easily. According to KSN statistics, members of the Trojan-Downloader.AndroidOS.Triada and Trojan.AndroidOS.Dvmap families can act as delivery vehicles for the helper. After the victim removes the helper, a member of one of these two families loads and reinstalls it.

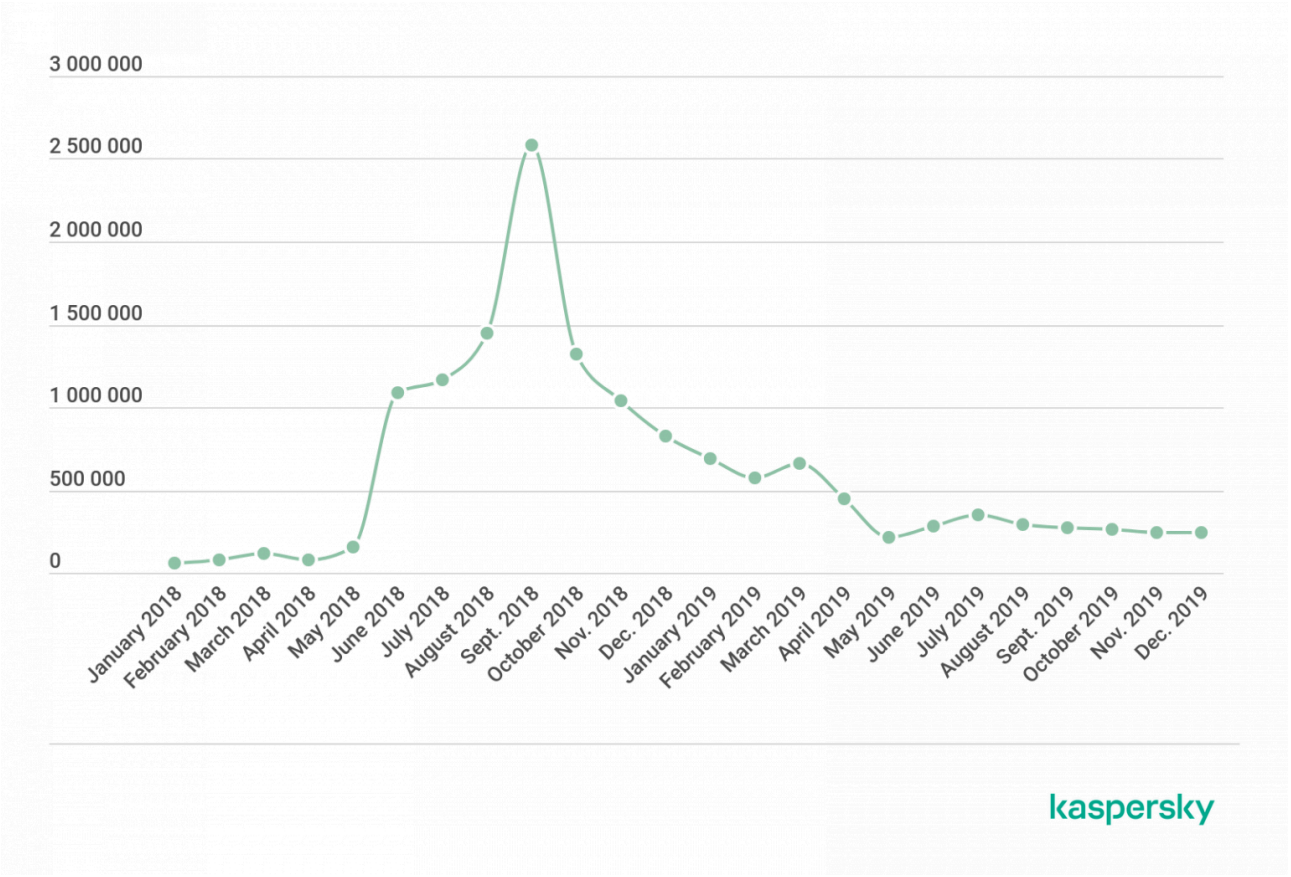
Mobile banking Trojans

In 2019, we detected 69,777 installation packages for mobile banking Trojans, which is half last year's figure. However, the share of banking Trojans out of all detected threats grew slightly as a consequence of the declining activity of other classes and families of mobile malware.



Number of installation packages of mobile banking Trojans detected by Kaspersky in 2019

The number of detected installation packages for banking Trojans as well as the number of attacks were influenced by the campaign to distribute the Asacub Trojan, whose activity has plummeted starting in April 2019.



Number of attacks by mobile banking Trojans in 2018–2019

It is worth noting that the average number of attacks over the year was approximately 270,000 per month.

Top 10 countries by share of users attacked by banking Trojans

	Country	%*
1	Russia	0.72
2	South Africa	0.66
3	Australia	0.59
4	Spain	0.29
5	Tajikistan	0.21
6	Turkey	0.20
7	USA	0.18
8	Italy	0.17
9	Ukraine	0.17

10	Armenia	0.16

**Share of users attacked by mobile bankers out of all attacked users*

Russia (0.72%) has headed our Top 10 for three consecutive years: many different Trojan families are focused on stealing credentials from Russian banking apps. These Trojans operate in other countries as well. Thus, Asacub is the number one threat in Tajikistan, Ukraine, and Armenia, while the Svpeng family of Trojans is active in Russia and the US.

In South Africa (0.66%), the most common Trojan was Trojan-Banker.AndroidOS.Agent.dx, accounting for 95% of all users attacked by banking threats.

The most widespread Trojan in Australia (0.59%) was Trojan-Banker.AndroidOS.Agent.eq (77% of all users attacked by banking threats).

In Spain (0.29%), banking malware from the Cebruser and Trojan-Banker.AndroidOS.Agent.ep families are popular with cybercriminals (49% and 22% of all users attacked by banking threats, respectively).

Top 10 families of mobile bankers in 2019

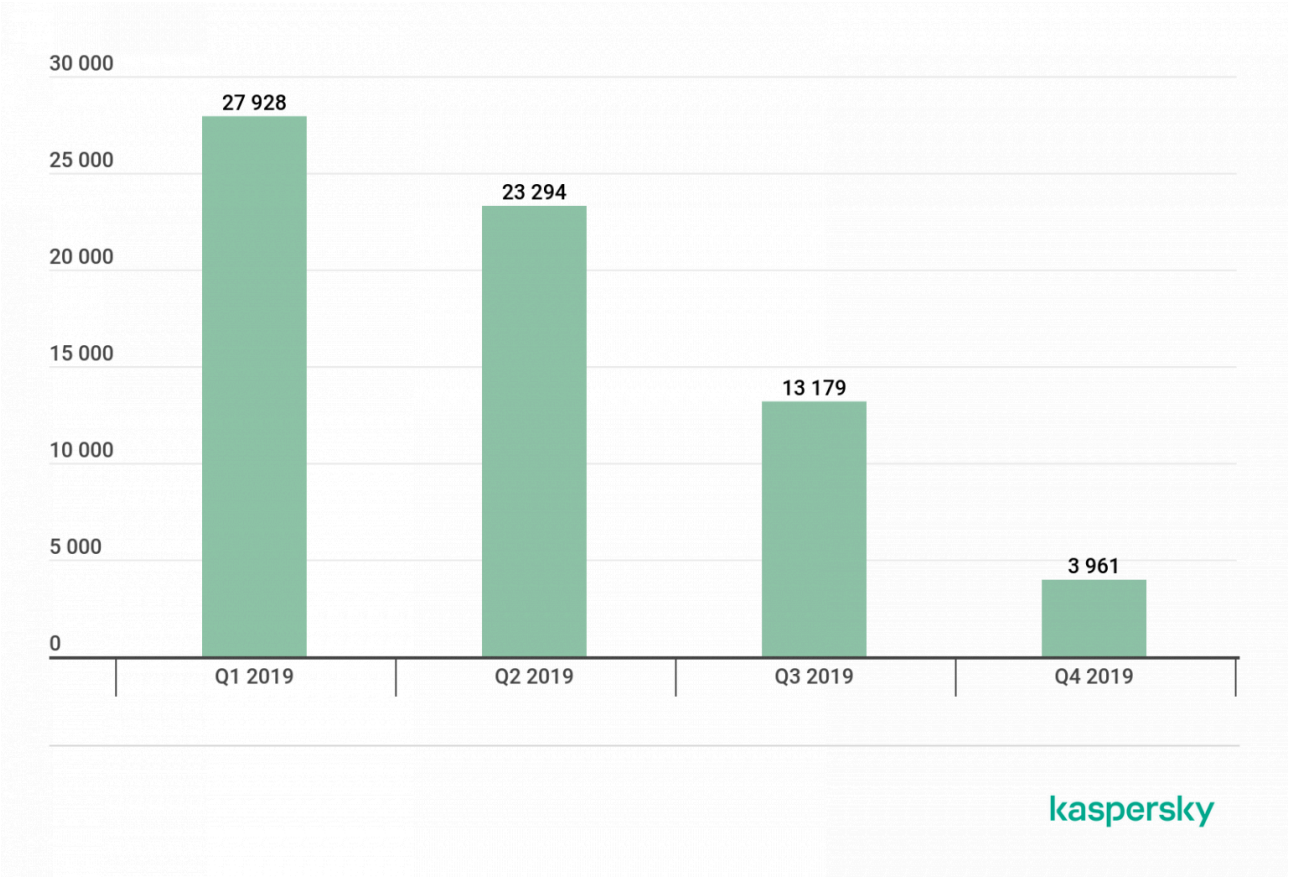
	Family	%*
1	Asacub	44.40
2	Svpeng	22.40
3	Agent	19.06
4	Faketoken	12.02
5	Hqwar	3.75
6	Anubis	2.72
7	Marcher	2.07
8	Rotexy	1.46
9	Gugi	1.34
10	Regon	1.01

**Share of users attacked by this family of mobile bankers out of all users attacked by mobile banking Trojans*

Mobile ransomware Trojans

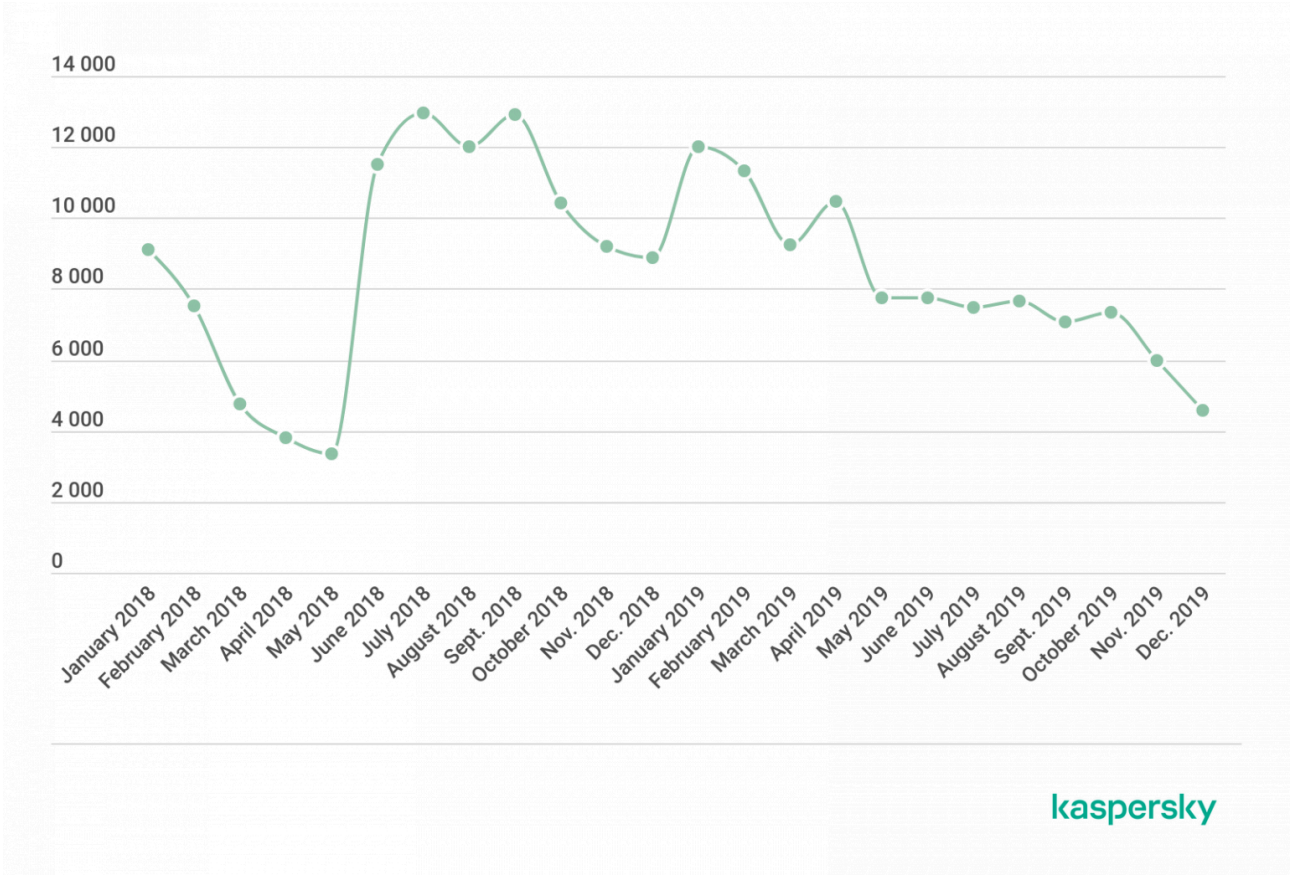
In 2019, we detected 68,362 installation packages for ransomware Trojans, which is 8,186 more than in the previous year. However, we observed a decline in the generation of new ransomware packages throughout 2019.

The minimum was recorded in December.

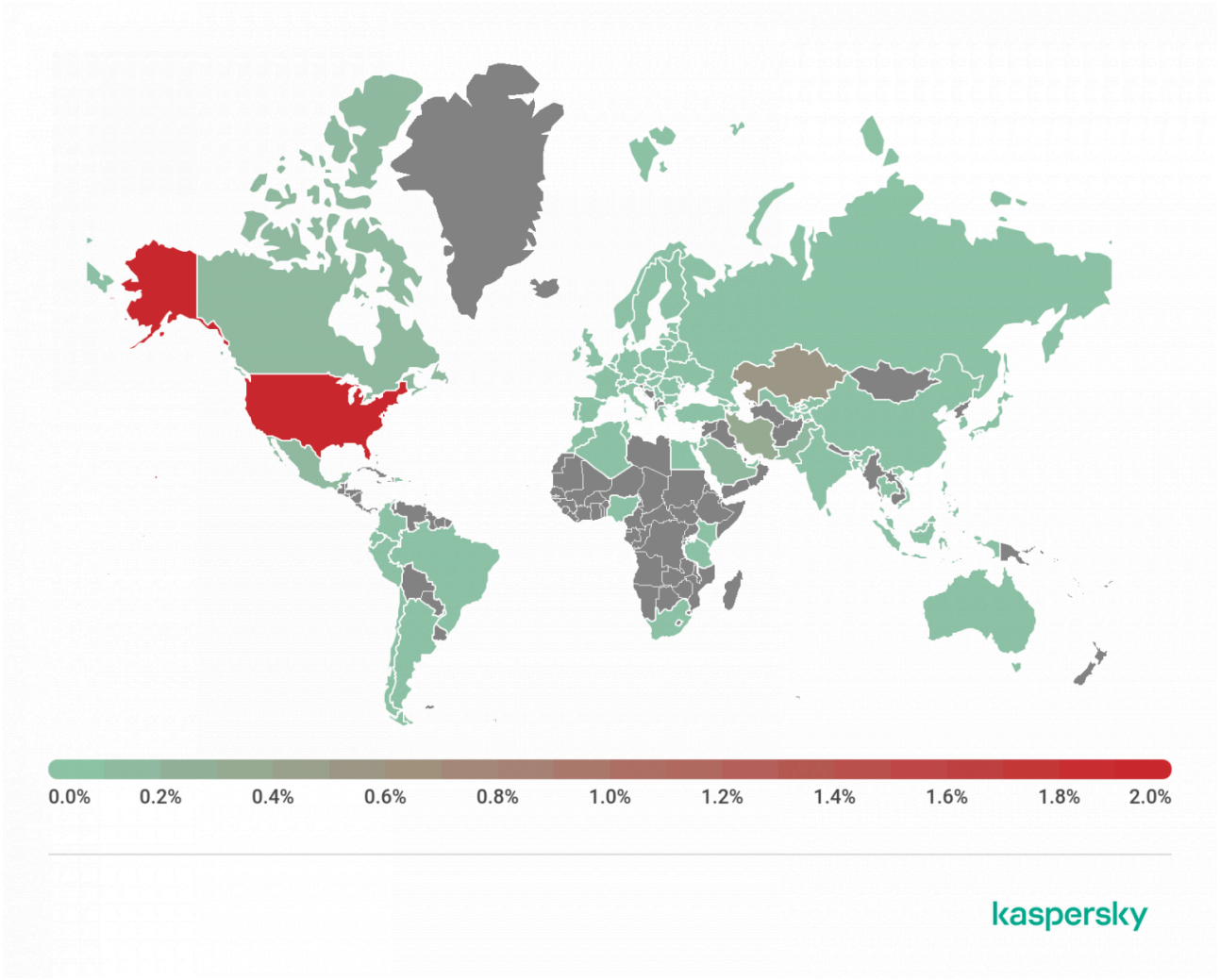


Number of new installation packages for mobile banking Trojans in Q1–Q4 2019

A similar picture is seen for attacked users. Whereas in early 2019, the number of attacked users peaked at 12,004, by the end of the year, the figure had decreased 2.6 times.



Number of users attacked by mobile ransomware Trojans in 2018–2019



Countries by share of users attacked by mobile ransomware in 2019

Top 10 countries by share of users attacked by ransomware Trojans

	Country*	%**
1	USA	2.03
2	Kazakhstan	0.56
3	Iran	0.37
4	Mexico	0.11
5	Saudi Arabia	0.10
6	Pakistan	0.10
7	Canada	0.10
8	Italy	0.09

9	Indonesia	0.08
10	Australia	0.06

**Excluded from the rating are countries with fewer than 25,000 active users of Kaspersky mobile solutions in the reporting period.*

***Unique users attacked by mobile ransomware in the country as a percentage of all users of Kaspersky mobile solutions in the country.*

For the third year in a row, first place by share of users attacked by mobile ransomware went to the US (2.03%). Same as last year, the Svpeng ransomware family was the most commonly encountered in the country. It was also the most widespread in Iran (0.37%).

The situation in Kazakhstan (0.56%) was unchanged: the country still ranks second, and the most prevalent threat there remains the Rkor family.

Conclusion

The year 2019 saw the appearance of several highly sophisticated mobile banking threats, in particular, malware that can interfere with the normal operation of banking apps. The danger they pose cannot be overstated, because they cause direct losses to the victim. It is highly likely that this trend will continue into 2020, and we will see more such high-tech banking Trojans.

Also in 2019, attacks involving the use of mobile stalkerware became more frequent, the purpose being to monitor and collect information about the victim. In terms of sophistication, stalkerware is keeping pace with its malware cousins. It is quite likely that 2020 will see an increase in the number of such threats, with a corresponding rise in the number of attacked users.

Judging by our statistics, adware is gaining ever more popularity among cybercriminals. In all likelihood, going forward we will encounter new members of this class of threats, with the worst-case scenario involving adware modules pre-installed on victims' devices.

Source: https://securelist.com/mobile-malware-evolution-2019/96280/