IT THREAT EVOLUTION IN Q3 2015

David Emm
Maria Garnaeva
Roman Unuchek
Denis Makrushin
Anton Ivanov

CONTENTS

Q3 IN FIGURES

- According to KSN data, Kaspersky Lab solutions detected and repelled a total of **235,415,870** malicious attacks from online resources located all over the world.
- **75,408,543** unique URLs were recognized as malicious by web antivirus components.
- Kaspersky Lab's web antivirus detected **38,233,047** unique malicious objects: scripts, exploits, executable files, etc.
- There were **5,686,755** registered notifications about attempted malware infections that aim to steal money via online access to bank accounts.
- Kaspersky Lab's file antivirus detected a total of **145,137,553** unique malicious and potentially unwanted objects.
- Kaspersky Lab mobile security products detected:
    - **1,583,094** malicious installation packages;
    - **323,374** new malicious mobile programs;
    - **2516** mobile banker Trojans.

OVERVIEW

Targeted attacks

Turla's 'eye in the sky'

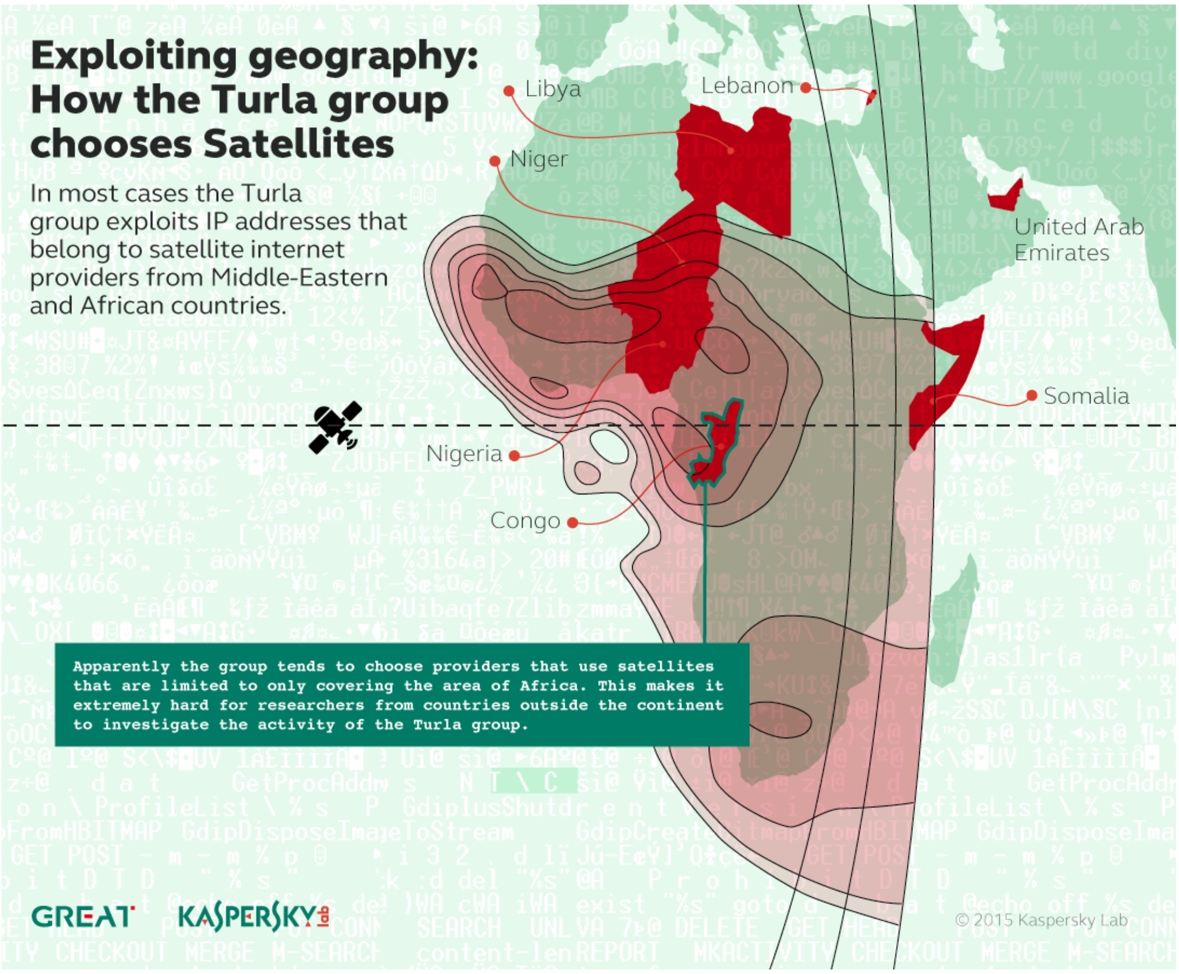
We've written about Turla several times over the last year or so (our initial report, follow-up analysis and campaign overview can be found on securelist.com). The group behind this cyber-espionage campaign has been active for more than eight years, infecting hundreds of computers in more than 45 countries. The organizations targeted include government agencies, embassies, military, education, research and pharmaceutical companies.

The Turla group profiles its victims, using watering-hole attacks in the initial stages. However, as outlined in our latest report, for subsequent operations the group makes use of satellite communications to manage its C2 (Command-and-Control) traffic.
Most people think of satellite communications as a means of broadcasting TV, but they are also used to provide Internet access. Typically, this is done in remote locations where other types of Internet access are slow, unstable or unavailable. One of the most widespread and least expensive means of obtaining satellite-based access is through a downstream-only connection.

The method used by Turla to hijack downstream satellite links does not require a valid satellite Internet subscription. The key benefit is that it's anonymous – it's very hard to identify the attackers. The satellite receivers can be located anywhere within the area covered by the satellite (typically a wide area) and the true location and hardware of the C2 server can't be easily identified or physically seized. It's also cheaper than purchasing a satellite-based link and easier than hijacking traffic between the victim and the satellite operator and injecting packets along the way.

In order to attack satellite-based Internet connections, both the legitimate users of these links, as well as the attackers' own satellite dishes, point to the specific satellite that is broadcasting the traffic. The attackers exploit the fact that packets are unencrypted. Once an IP address that is routed through the satellite's downstream link has been identified, the attackers start listening for packets coming from the Internet to this specific IP. Once a packet has been identified, they identify the source and spoof a reply packet back to the source using a conventional Internet line. At the same time, the legitimate user of the link just ignores the packet as it goes to an otherwise unused port (for instance, port 80 or 10080). You can find a graphical explanation of how Turla uses satellite links here.

The Turla group tends to focus on satellite Internet providers located in the Middle East and Africa, including Congo, Lebanon, Libya, Niger, Nigeria, Somalia and the UAE. Satellite broadcasts from these countries don't normally cover European and North American countries, making it very hard for security researchers to investigate such attacks.



Exploiting geography: How the Turla group chooses Satellites

In most cases the Turla group exploits IP addresses that belong to satellite internet providers from Middle-Eastern and African countries.

Apparently the group tends to choose providers that use satellites that are limited to only covering the area of Africa. This makes it extremely hard for researchers from countries outside the continent to investigate the activity of the Turla group.

The use of satellite-based Internet links is an interesting development. The hijacking of downstream bandwidth is cheap (around $1,000 for the initial investment and around $1,000 per year in maintenance), easy to do and offers a high degree of anonymity. On the downside, it's not always as reliable as more traditional methods such as bullet-proof hosting, multiple proxy levels and hacked web sites – all of which Turla also uses. This makes it less likely that it will be used to maintain extensive botnets. Nevertheless, if this method becomes widespread among APT groups or cybercriminals, it will pose a serious problem for the IT security industry and law enforcement agencies.

Darkhotel extends its 'guest' list

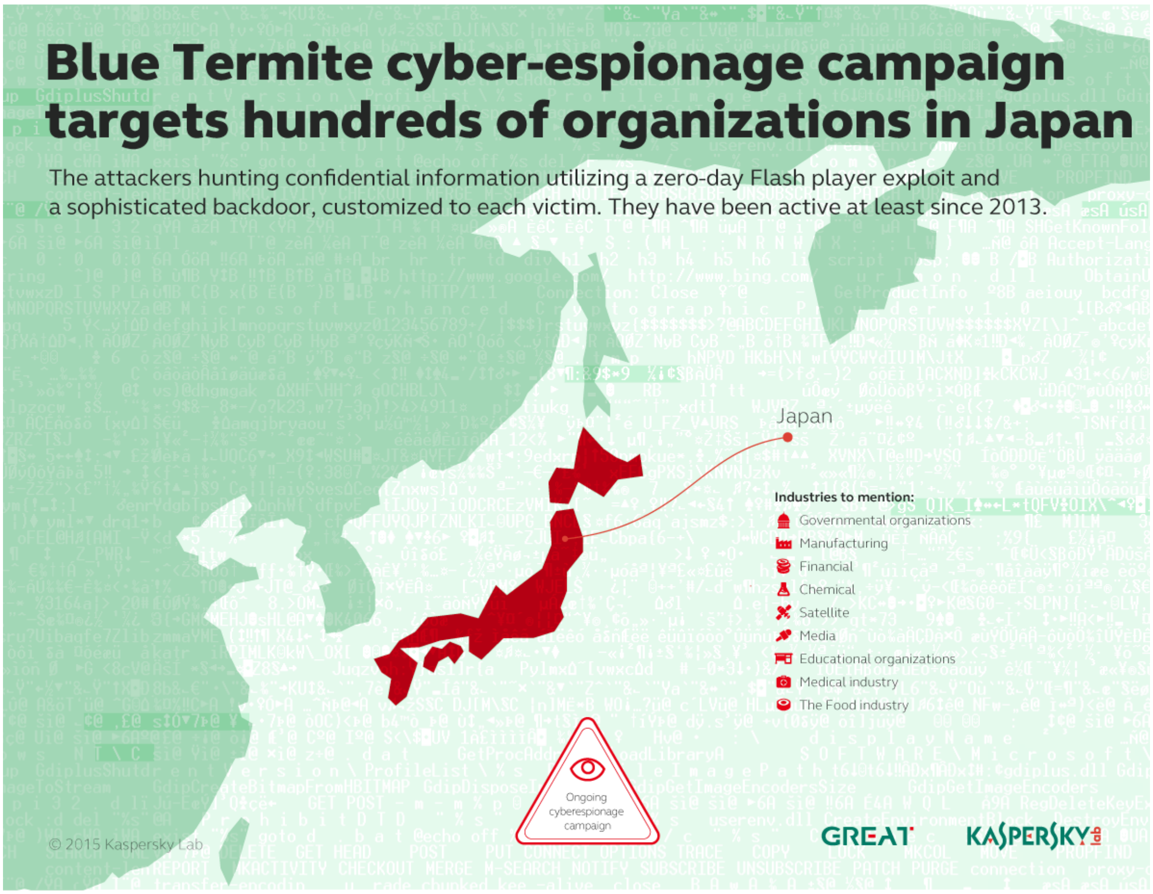
In November 2014, we reported on the Darkhotel APT. These attacks were characterized by the misuse of stolen certificates, the deployment of HTA files using multiple methods and the infiltration of hotel Wi-Fi networks to place backdoors on targets' computers.

Recently we published an update on Darkhotel. While the attackers behind this APT continue to use the above methods, they have also supplemented their armoury. They have shifted their attention more towards spear-phishing of their chosen victims. As well as using HTA files, they are also deploying infected RAR files, using the RTLO (right to left override) mechanism to mask the real extension of the file. The attackers also use Flash exploits, including a zero-day exploit leaked as a result of the Hacking Team security breach.

In 2015, Darkhotel extended its geographic reach, to include victims in North Korea, Russia, South Korea, Japan, Bangladesh, Thailand, India, Mozambique and Germany.

Blue Termite

In August, we reported on the Blue Termite APT, a targeted attack campaign focused on stealing information from organizations in Japan. These include government agencies, local government bodies, public interest groups, universities, banks, financial services, as well as companies working in sectors such as energy, communication, heavy industry, chemical, automotive, electrical, news media, information services, health care, real estate, food, semiconductor, robotics, construction, insurance, transportation, and more. One of the most high profile targets was the Japan Pension Service.


Blue Termite cyber-espionage campaign targets hundreds of organizations in Japan
The attackers hunting confidential information utilizing a zero-day Flash player exploit and a sophisticated backdoor, customized to each victim. They have been active at least since 2013.
Japan
Industries to mention:
Governmental organizations
Manufacturing
Financial
Chemical
Satellite
Media
Educational organizations
Medical industry
The Food industry
Ongoing cyberespionage campaign
© 2015 Kaspersky Lab
GREAT
KASPERSKY lab

The malware is customized according to the specific victim. The Blue Termite backdoor stores data about itself – including C2, API name, strings for anti-analysis, values of mutexes, as well as the MD5 checksum of backdoor commands and the internal proxy information. The data are stored in encrypted form, making analysis of the malware more difficult – a unique decryption key is required for each sample.

The main method of infection, as with so many targeted attack campaigns, is via spear-phishing e-mails. However, we have detected other methods of infection. These include drive-by downloads using a Flash exploit (CVE-2015-5119) – one of the exploits leaked following the

Hacking Team security breach. Several Japanese web sites were compromised this way. We also found some watering-hole attacks, including one on a web site belonging to a prominent member of the Japanese government.

Malware stories

End of the line for CoinVault?

On 14 September 2015, Dutch police arrested two men for suspected involvement in CoinVault ransomware attacks, following a joint effort by Kaspersky Lab, Panda Security and the Dutch National High Tech Crime Unit (NHTCU) – highlighting the benefit of collaboration between police and security researchers. This malware campaign started in May 2014 and continued into this year, targeting victims in more than 20 countries, with the majority of victims in the Netherlands, Germany, the United States, France and Great Britain. They successfully encrypted files on more than 1,500 Windows-based computers, demanding payment in bitcoin to decrypt data on victims' machines.

The cybercriminals responsible for this ransomware campaign modified their creations several times to keep on targeting new victims. We published our first analysis of CoinVault in November 2014, soon after the first sample of the malicious program appeared. The campaign then stopped until April 2015, when we found a new sample. In the same month, Kaspersky Lab and the Dutch NHTCU launched a web site to act as a repository of decryption keys. In addition, we also made available online a decryption tool to help victims recover their data without having to pay the ransom.

After publishing the site, Kaspersky Lab was contacted by Panda Security, which had found information about additional malware samples. We were able to confirm that the samples were related to CoinVault. We passed this information to the Dutch NHTCU.

You can find our analysis of the twists and turns employed by the CoinVault authors here.

Ransomware has become a notable fixture of the threat landscape. While this case shows that collaboration between researchers and law enforcement agencies can lead to positive results, it's essential for consumers and businesses alike to take steps to mitigate the risks of this type of malware. Ransomware operations rely on their victims paying up. On top of anti-malware protection, it's important to make regular backups of data, to avoid data loss and the need to make such ransom payments.

A serpent in Apple's walled garden

The recent appearance of malicious apps in the App Store has made it clear that, contrary to what many people believe, iOS is not immune to malware.

The malware, called 'Xcodeghost', infected dozens of apps, including WeChat, NetEase's music download app, business card scanner CamCard and Didi Kuadi's car-hailing app. The Chinese versions of Angry Birds 2 were also infected.

The attackers didn't hack the App Store, but hosted a malicious version of Apple's Xcode. Xcode is a free suite of tools used by software developers to create iOS apps. It is officially distributed by Apple, but also unofficially by third parties: someone in China hosted a version of Xcode that contained XcodeGhost. Some Chinese developers choose to download development tools such as this from local servers because it is much quicker.

Any apps created using the modified version of Xcode would be infected. The infected apps steal data from their victims and send it to the attackers. It was initially believed that 39 infected apps had bypassed Apple's scanning process and had been successfully uploaded to the App Store. Infected apps have been removed by Apple. However, the compromised version of Xcode has been available for around six months, so the total number of infected apps could be much higher, not least because the source code for XcodeGhost has been published on Github.

You can find an analysis of XcodeGhost by researchers at Palo Alto Networks here.

The incident highlights the danger of programs being infected at source if tools used by developers are compromised.

The Gaza cyber-gang

At the end of September we reported on the activities of another regional APT, the Gaza cyber-gang. This is a politically motivated Arabic group operating in the MENA region (Middle East and North Africa) – mainly focused on Egypt, the UAE and Yemen. The group is interested in government agencies – especially embassies, where security and IT operations might not be well-established or reliable. The Gaza cyber-gang has been active since 2012, but became particularly active in the second quarter of 2015.

The gang actively sends malware to IT and Incident Response (IR) staff in target organizations: the file names they use reflect IT functions and IR tools used to investigate cyber-attacks. It's not hard to work out why. IT staff typically have greater access rights than other employees, because it's their job to manage the corporate infrastructure. IR employees are likely to have access to sensitive data related to ongoing cyber-investigations, as well as extended access rights to help them look for suspicious activities across the network. This means the attackers not only gain access to the target organization but also extend their reach across the network.

The main infection modules used by the group are widely used remote access Trojans (RATs): XtremeRAT and PoisonIvy. Their activities are heavily reliant on social engineering. They use filenames related to IT and IR functions and content and domain names that are likely to be of interest to their victims (e.g. '.gov.uae.kim').

STATISTICS

All the statistics used in this report were obtained using Kaspersky Security Network (KSN), a distributed antivirus network that works with various anti-malware protection components. The data was collected from KSN users who agreed to provide it. Millions of Kaspersky Lab product users from 213 countries and territories worldwide participate in this global exchange of information about malicious activity.

Mobile threats

Displaying adverts to users is still the main method of making money from mobile threats. The number of programs displaying intrusive advertising on mobile devices (adware) continued to grow in the third quarter and accounted for more than half of all detected mobile objects.

We have also observed a growing number of programs that use advertising as the main monetization method while also using other methods from the virus writers' arsenal. They often root the device of a victim and use superuser privileges, making it very difficult, if not impossible, to combat them. In Q3 2015, these Trojans accounted for more than half of the Top 20 most popular mobile malware.

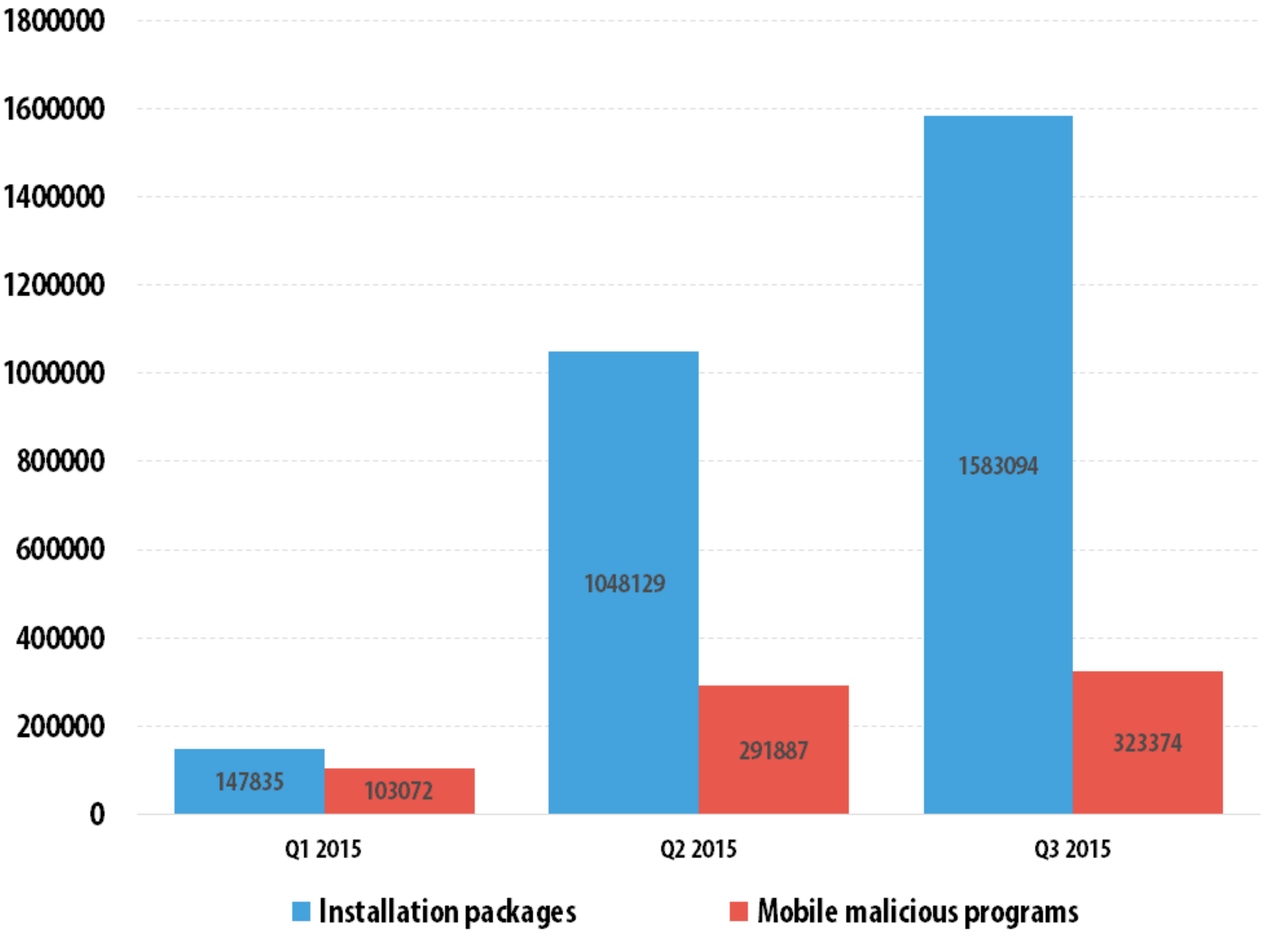
SMS Trojans are still relevant as a monetization method, especially in Russia. These programs send paid messages from an infected device without the user's knowledge. Although their overall traffic share among mobile threats continues to fall, the malicious mobile Trojan-SMS still leads in terms of the number of new samples detected in the third quarter.

The pursuit of profit is not limited to displaying adverts or sending paid text messages – cybercriminals are also very interested in users' bank accounts. In Q3 2015, the total share of mobile bankers and spyware designed to steal personal information exceeded that of SMS Trojans in new mobile malware traffic by 0.7 p.p.

The number of new mobile threats

In Q3 2015, Kaspersky Lab mobile security products detected **323,374** new malicious mobile programs – a 1.1-fold increase on Q2 2015 and a 3.1-fold increase on Q1.

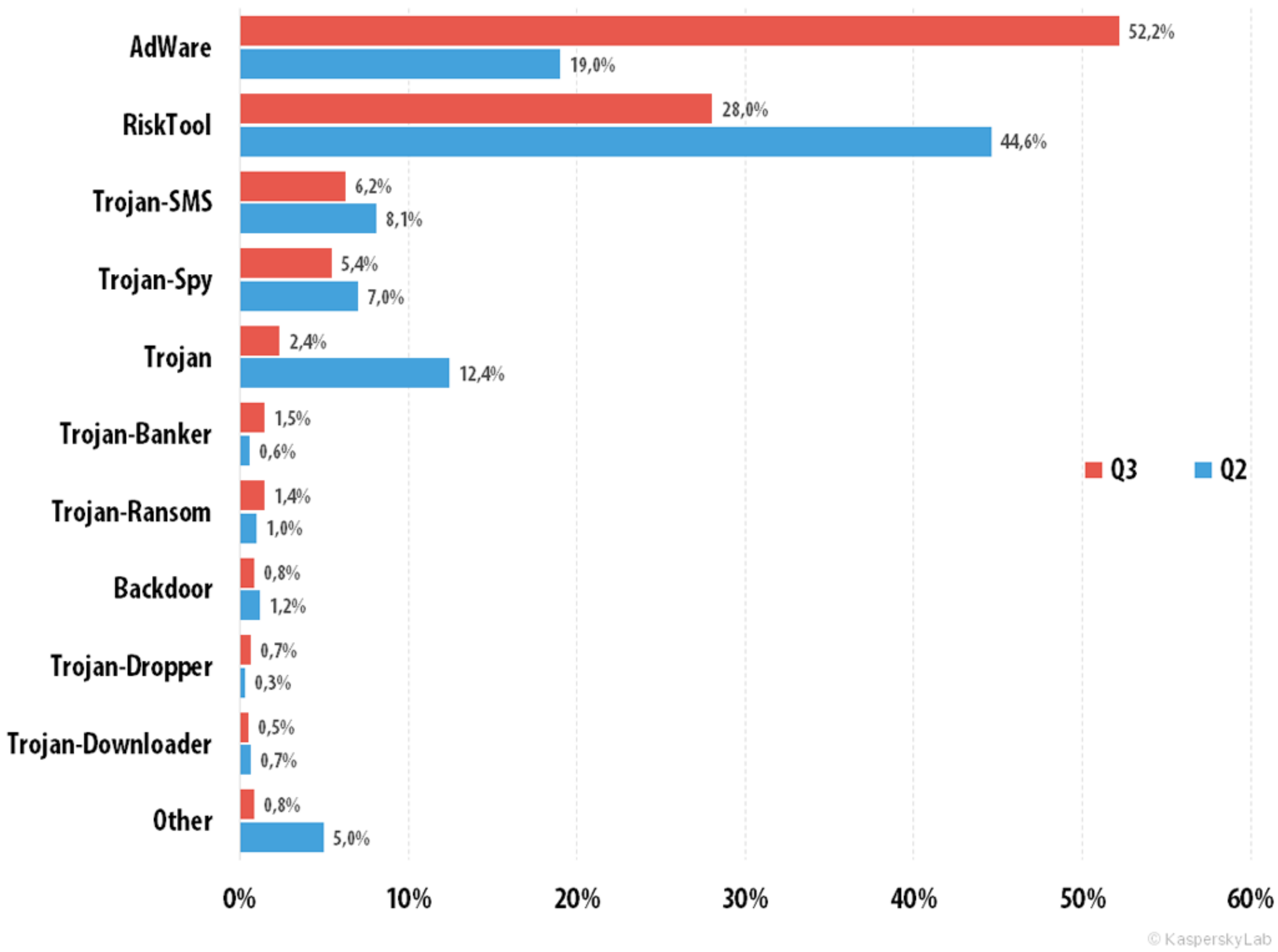
The number of malicious installation packages detected was **1,583,094** – this is 1.5 times more than in the previous quarter.



© KasperskyLab

Number of malicious installation packages and new malicious mobile programs detected (Q1 2015 – Q3 2015)

Distribution of mobile malware by type



Distribution of new mobile malware by type, Q2 and Q3 2015

Potentially unwanted advertising programs (adware) headed the ranking of malicious objects detected for mobile devices in Q3 2015. In the previous quarter this category of programs occupied second place with 19%; in Q3 their share grew considerably and reached 52.2%.

Second came RiskTool. The programs in this category are legitimate applications that are potentially dangerous for users – if used carelessly or manipulated by a cybercriminal, they could lead to financial losses. RiskTool was knocked off top spot after its share decreased by 16.6 p.p. from the previous quarter.

The percentage of SMS Trojans in the overall flow of mobile threats decreased by another 1.9 p.p. and amounted to 6.2%. Despite this, they are still among the leading mobile malicious programs.

SMS Trojans were followed by Spy Trojans (5.4%). These programs steal personal data from users, including incoming text messages (mTANs) from banks.

In the third quarter of 2015, the biggest growth rates were demonstrated by Trojan-Banker whose share more than doubled and accounted for 1.5% compared to 0.6% in the previous quarter. In Q2, 630 of these programs were detected, while Q3 saw their number increase four-fold and exceed 2500.

Top 20 malicious mobile programs

Please note that the ranking of malicious programs does not include potentially dangerous or unwanted programs such as RiskTool or adware.

	Name	% of attacked users*
1	DangerousObject.Multi.Generic	46.6
2	Trojan.AndroidOS.Rootnik.d	9.9
3	Trojan-SMS.AndroidOS.Podec.a	7.4
4	Trojan-Downloader.AndroidOS.Leech.a	6.0
5	Trojan.AndroidOS.Ztorg.a	5.5
6	Exploit.AndroidOS.Lotoor.be	4.9
7	Trojan-Dropper.AndroidOS.Gorpo.a	3.3
8	Trojan-SMS.AndroidOS.Opfake.a	3.0
9	Trojan.AndroidOS.Guerrilla.a	2.9
10	Trojan-SMS.AndroidOS.FakeInst.fz	2.6
11	Trojan-Ransom.AndroidOS.Small.o	2.3
12	Trojan-Spy.AndroidOS.Agent.el	2.1
13	Trojan.AndroidOS.Ventica.a	1.9
14	Trojan.AndroidOS.Ztorg.b	1.9
15	Trojan.AndroidOS.Ztorg.pac	1.8
16	Trojan.AndroidOS.Fadeb.a	1.6
17	Trojan-SMS.AndroidOS.Smaps.a	1.5
18	Trojan.AndroidOS.Iop.a	1.5
19	Trojan.AndroidOS.Guerrilla.b	1.5
20	Trojan-SMS.AndroidOS.FakeInst.fi	1.4

* Percentage of users attacked by the malware in question, relative to all users attacked.

The top position in the rankings was occupied by DangerousObject.Multi.Generic (46.6%). This is how new malicious applications are detected by the KSN cloud technologies, which help our products to significantly shorten the response time to new and unknown threats. The proportion of DangerousObject.Multi.Generic increased almost three-fold: from 17.5% in Q2 to 46.6% in Q3.

The number of Trojans that use advertising as the main means of monetization significantly increased from the previous quarter. In the second quarter of 2015 this Top 20 included six of these programs, while in Q3 their number increased to 11: three programs belong to the Trojan.AndroidOS.Ztorg family, and two each belong to the Trojan.AndroidOS.Guerrilla, Trojan.AndroidOS.Rootnik.d, Trojan-Downloader.AndroidOS.Leech.a, Trojan-Dropper.AndroidOS.Gorpo.a, Trojan-Spy.AndroidOS.Agent.el, Trojan.AndroidOS.Ventica.a and Trojan.AndroidOS.Fadeb.a families.

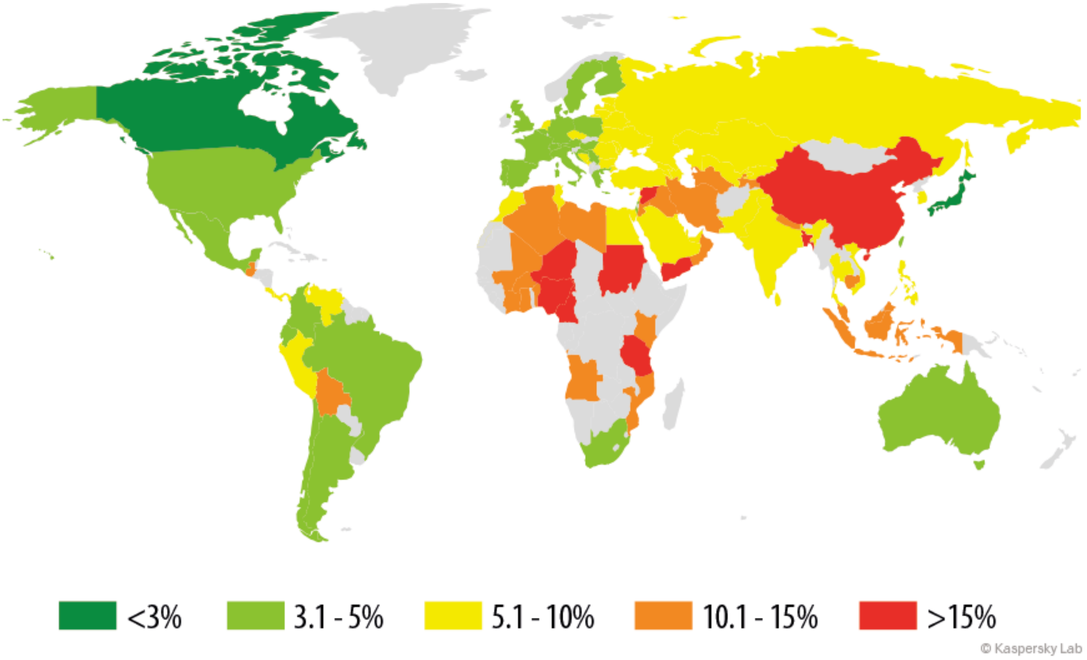
Unlike the usual advertising modules, these programs do not contain any useful functionality. Their goal is to deliver as many adverts as possible to the recipient using a variety of methods, including the installation of new advertising programs. These Trojans can use superuser privileges to conceal their presence in the system folder, from where it will be very difficult to remove them.

Of special note is Trojan-Spy.AndroidOS.Agent.el, which is even encountered in the official firmware of some developers.

Trojan-SMS.AndroidOS.Podec.a (7.4%) has been among the Top 3 malicious mobile programs for four quarters in a row due to how actively it is spread. It is worth mentioning that the functionality of the latest versions of this Trojan has changed and no longer includes the sending of text messages. The Trojan is now fully focused on paid subscriptions, making use of CAPTCHA recognition.

Seventeenth place is occupied by Trojan-SMS.AndroidOS.Smaps.a. Some of its versions are able to send spam upon receiving a command from the server via the Viber app if it is installed on the victim's device. No special permission or actions on the part of the user are required by the Trojan to do this.

The geography of mobile threats



The geography of mobile malware infection attempts in Q3 2015 (percentage of all users attacked)

Top 10 counties attacked by mobile malware (ranked by percentage of users attacked)

	Country*	% of users attacked **
1	Bangladesh	22.57
2	China	21.45
3	Nigeria	16.01
4	Tanzania	15.77

5	Iran	13.88
6	Malaysia	13.65
7	Algeria	12.73
8	Nepal	12.09
9	Kenya	11.17
10	Indonesia	10.82

* We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.

** Percentage of unique users attacked in each country relative to all users of Kaspersky Lab's mobile security product in the country.

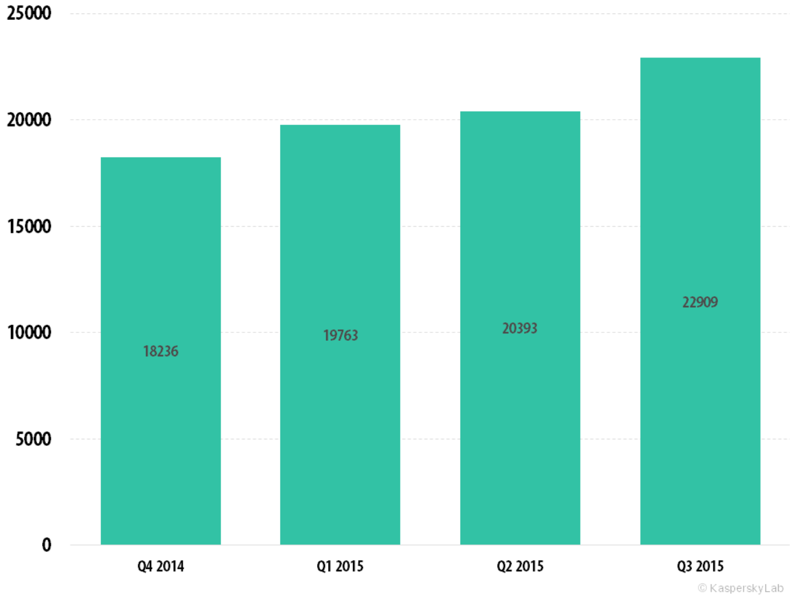
The most secure countries in this respect are:

	Country	% of users attacked **
1	Japan	1.13
2	Canada	2.87
3	Denmark	3.20
4	Sweden	3.45
5	Australia	3.48

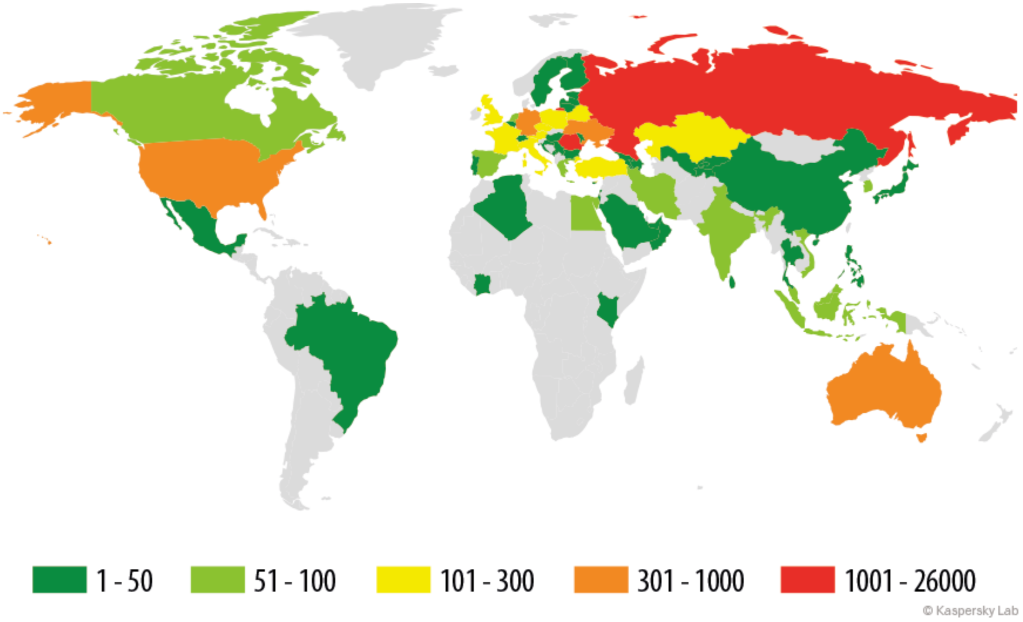
Although Australia is included in the Top 5 most secure countries, when it comes to mobile malware infections the situation is not as safe as would be expected: in the third quarter of 2015, users in Australia were attacked by mobile banker Trojans more often than users in other countries (see below.).

Mobile banker Trojans

In Q3 2015, we detected 2,516 mobile banker Trojans, which is a four-fold increase on the previous quarter.



Number of mobile banker Trojans detected by Kaspersky Lab's solutions (Q4 2014 – Q3 2015)



Geography of mobile banking threats in Q3 2015 (number of users attacked)

The number of attacked users depends on the overall number of users within each individual country. To assess the risk of a mobile banker Trojan infection in each country, and to compare it across countries, we made a country ranking according to the percentage of users attacked by mobile banker Trojans.

Top 10 counties attacked by mobile banker Trojans (ranked by percentage of users attacked)

	Country*	% of users attacked by mobile bankers**
1	Australia	0.85
2	Republic of Korea	0.40
3	Russia	0.32
4	Cyprus	0.32
5	Czech Republic	0.31
6	Austria	0.27
7	Kyrgyzstan	0.26
8	Bulgaria	0.24
9	Romania	0.23
10	Uzbekistan	0.23

* We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.

** Percentage of unique users in each country attacked by mobile banker Trojans, relative to all users of Kaspersky Lab's mobile security product in the country.

Australia, which was ranked eighth in the previous quarter, took the lead in Q3 2015. The percentage of users attacked by mobile bankers in Australia increased six-fold (from 0.14% to 0.85%). Such significant growth was caused by fraudsters making active use of

Trojan-Banker.AndroidOS.Agent.ad. This Trojan steals credentials used to enter the online banking system of one of Australia's largest banks. It also tries to steal users' credit card details (cardholder's name, card number, CVV, card expiry date).

At the same time, Korea, which topped the Q2 rating, saw its share decrease six-fold (from 2.37% to 0.4%) and dropped to second place in the ranking.

Top 10 countries by the percentage of users attacked by mobile bankers relative to all attacked users

An indication of how popular mobile banker Trojans are with cybercriminals in each country can be provided by the percentage of users who were attacked at least once by mobile banker Trojans during the quarter, relative to all users in the same country whose mobile security product was activated at least once in the reporting period. This ranking differs from the one above:

	Country*	% of users attacked by mobile bankers, relative to all attacked users **
1	Australia	24.31
2	Austria	7.02
3	Montenegro	5.92
4	Republic of Korea	5.69
5	France	5.66
6	Cyprus	5.56
7	Russia	5.09
8	Czech Republic	4.98
9	Sweden	4.81
10	Finland	4.56

* We eliminated countries from this ranking where the number of users of Kaspersky Lab's mobile security product is lower than 10,000.

** Percentage of unique users in each country attacked by mobile banker Trojans, relative to all unique users attacked by mobile malware in the country.

In Australia, which topped the ranking, slightly less than a quarter of all users attacked by mobile malware were targeted by mobile bankers.

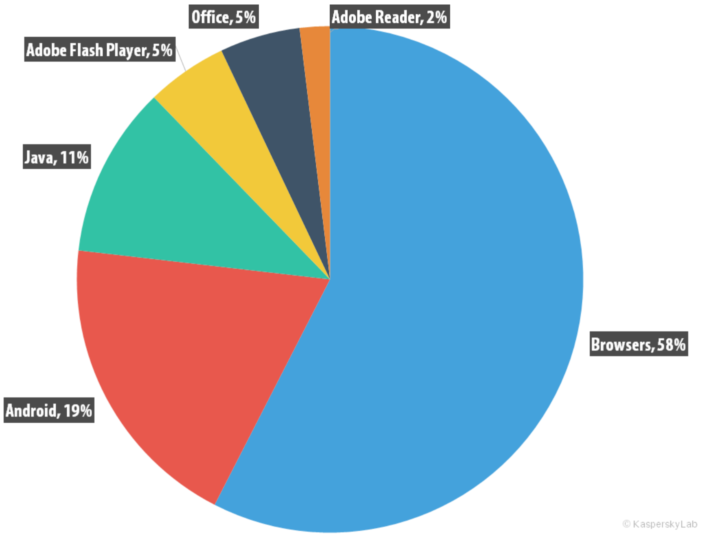
The share of bankers among all mobile malware attacks in Russia halved – from 10.35% to 5.09%. This was due to a significant drop in the activity of the Trojan-Banker.AndroidOS.Marcher family which was one of the most popular in the country. In the third quarter the number of attacks using this malware fell almost ten-fold compared to the previous quarter.

Vulnerable applications used by cybercriminals

The ranking of vulnerable applications below is based on information about the exploits blocked by our products. These exploits were used by cybercriminals in Internet attacks and in attempts to compromise local applications, including those installed on mobile devices.

Compared to Q2 2015, the following changes have taken place:

- The proportion of Adobe Flash Player exploits has risen by 2 percentage points (p.p.).
- The proportion of Adobe Reader exploits has decreased by 5 p.p.



Distribution of exploits used in attacks by type of application attacked, Q3 2015

In Q3, just like the rest of the year, exploits for Adobe Flash Player were in demand. Their share was only 5%, but there are more of them ‘in the wild’ and at the current time nearly all exploit packs are using vulnerabilities in this software. As was the case in the previous quarter, the share of Java exploits (11%) has continued to decrease in Q3. We have not observed any exploits for this software included in recent exploit packs.

In Q3, the most common exploit packs included exploits for the following vulnerabilities:

- CVE-2015-5560 (Adobe Flash; this exploit was described in a Kaspersky Lab article)
- CVE-2015-2419 (Internet Explorer)
- CVE-2015-1671 (Silverlight)

The previous quarter saw a dramatic increase in the number of spam messages containing malicious PDF documents. This quarter, the number of these messages decreased significantly, so the proportion of Adobe Reader exploits also decreased.

The overall trend so far for 2015 has continued in Q3: exploits for Adobe Flash Player and Internet Explorer are most popular with cybercriminals. In the pie chart above, the latter falls into the ‘Browsers’ category; the landing pages from which the exploits spread are also classified here.

Online threats (Web-based attacks)

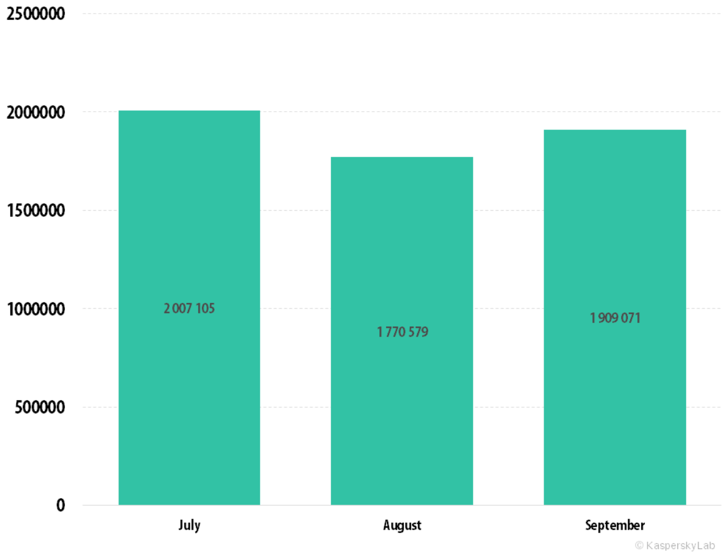
The statistics in this section were derived from web antivirus components that protect users from attempts to download malicious objects from a malicious/infected website. Malicious websites are created deliberately by malicious users; infected sites include those with user-contributed content (such as forums), as well as compromised legitimate resources.

Online threats in the banking sector

These statistics are based on the detection verdicts returned by the antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.

In Q3 2015, Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on the **625,669** computers. This number is 17.2 p.p. lower than in Q2 2015 (**755,642**). A year ago, in Q3 2014 this number was 591,688.

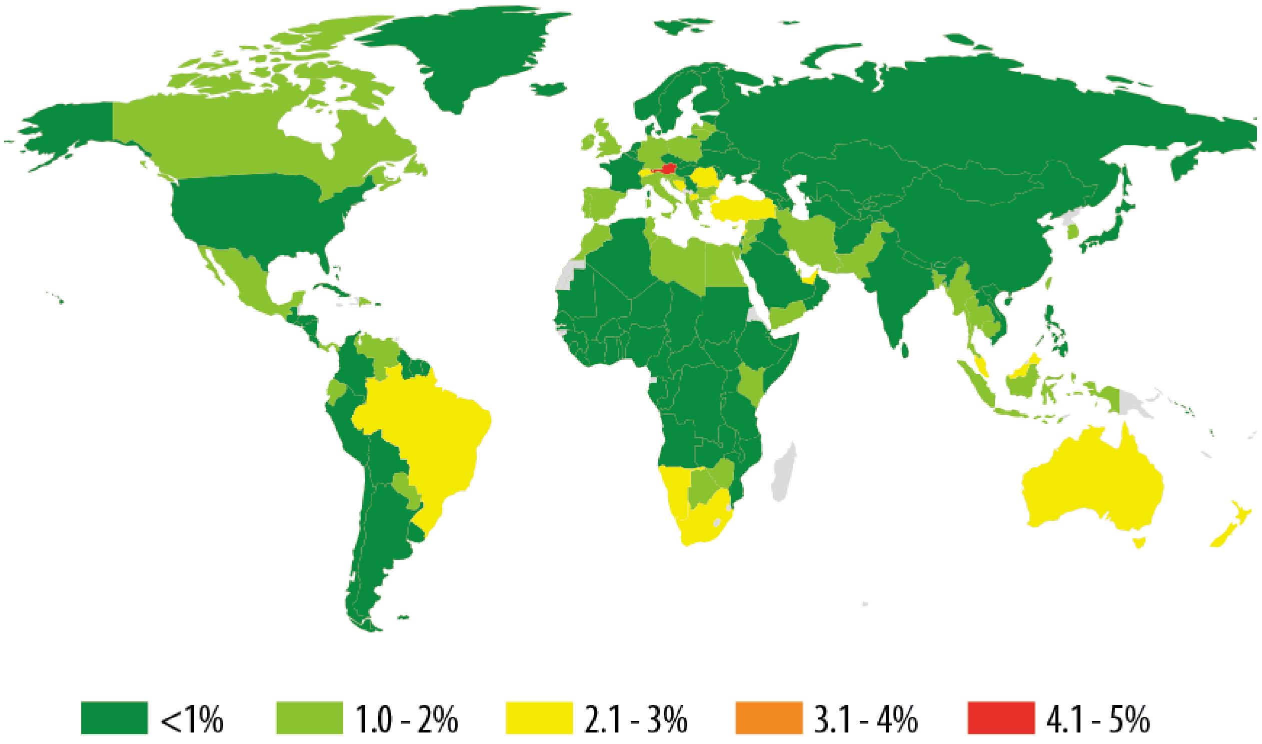
Kaspersky Lab's solutions produced a total of **5,686,755** notifications about attempted malware infections aimed at stealing money via online access to bank accounts in Q3 2015.



Number of attacks by financial users, Q3 2015

Geography of attacks

To evaluate and compare the degree of risk of being infected by banking Trojans which user computers are exposed to worldwide, we calculate the percentage of Kaspersky Lab product users who encountered this type of threat during the reporting period in the country, relative to all users of our products in the county.



© Kaspersky Lab

Geography of banking malware attacks in Q2 2015 (the percentage of users attacked)

Top 10 countries by the percentage of attacked users

	Country*	% attacked users**
1	Austria	4.98
2	Singapore	4.23
3	Turkey	3.04
4	Namibia	2.91
5	New Zealand	2.86
6	Hong Kong	2.81
7	Australia	2.78
8	Lebanon	2.60
9	United Arab emirates	2.54
10	Switzerland	2.46

* We excluded those countries in which the number of Kaspersky Lab product users is relatively small (less than 10,000).

** Unique users whose computers have been targeted by web attacks as a percentage of all unique users of Kaspersky Lab products in the country.

In Q3 2015, Austria became the leader in terms of the percentage of Kaspersky Lab users who were attacked by banking Trojans. Singapore, last quarter's leader, is now in second place. It should be noted that most countries in the Top 10 have significant numbers of online banking users, and this attracts the cybercriminals.

In Russia, 0.71% of users encountered a banking Trojan at least once in Q3; this number is little different from the Q2 figure of 0.75%. In the US, the figure was 0.59%, which is 0.3 p.p. lower than in Q2. The countries of Western Europe also saw a small decrease in the percentages of users attacked by banking malware compared to Q2: Spain stood at 1.95%, or 0.07 p.p. less than in Q2; the UK (1.24%) was down 0.34 p.p.; Italy (1.16%) saw a decrease of 0.41 p.p.; while Germany (1.03%) was 0.13 p.p. lower.

The TOP 10 banking malware families

The table below shows the Top 10 malware families most commonly used in Q3 2015 to attack online banking users:

	Name*	Percentage of attacks**
1	Trojan-Downloader.Win32.Upatre	63.13
2	Trojan-Spy.Win32.Zbot	17.86
3	Trojan-Banker.JS.Agent	1.70
4	Trojan-Banker.Win32.ChePro	1.97
5	Backdoor.Win32.Caphaw	1.14
6	Trojan-Banker.Win32.Banbra	1.93
7	Trojan-Banker.AndroidOS.Faketoken	0.90

8	Trojan-Banker.AndroidOS.Agent	0.57
9	Trojan-Banker.Win32.Tinba	1.93
10	Trojan-Banker.AndroidOS.Marcher	0.55

*These statistics are based on the detection verdicts returned by Kaspersky Lab's products, received from users of Kaspersky Lab products who have consented to provide their statistical data.

**Unique users whose computers have been targeted by the malicious program, as a percentage of all unique users targeted by financial malware attacks.

The majority of the Top 10 malicious programs work by injecting random HTML code in the web page displayed by the browser and intercepting any payment data entered by the user in the original or inserted web forms.

The Trojan-Downloader.Win32.Upatre family of malicious programs remains at the top of the ranking. The malware is no larger than 3.5 KB in size, and is limited to downloading the payload to the victim computer, most typically a banker Trojan from the Dyre/Dyzap/Dyreza family. The first malicious program from this family was detected in June 2014, and its main aim is to steal the user's payment details. Dyre does this by intercepting the data from a banking session between the victim's browser and the online banking web app. In the summer of 2015, however, Trojan-Downloader.Win32.Upatre was spotted on compromised home routers, which is a testimony to how cybercriminals make use of this multiple-purpose malware.

Trojan-Spy.Win32.Zbot, in second place, has become a permanent resident of this ranking, and it is no coincidence that it consistently occupies a leading position. The Trojans of the Zbot family were among the first to use web injections to compromise the payment details of online banking users and to modify the contents of banking web pages. They encrypt their configuration files at several levels; the decrypted configuration file is never stored in the memory in its entirety, but is instead loaded in parts. This gives the Trojans of the Trojan-Spy.Win32.Zbot family a technological edge over other malware programs.

Third place in the Q3 ranking was occupied by the Trojan-Banker.JS.Agent family. This is the malicious JavaScript code that results from an injection into an online banking page. The aim of this code is to intercept payment details that the user enters into online banking forms.

Of particular interest is the fact that three families of mobile banking Trojans are present in this ranking: Trojan-Banker.AndroidOS.Faketoken, Trojan-Banker.AndroidOS.Marcher (we wrote about these two in the Q2 report), and a newcomer to this ranking – Trojan-Banker.AndroidOS.Agent. The malicious programs belonging to the latter family steal payment details from Android devices.

The Top 10 operating systems attacked by banker Trojans

In Q3, users of Windows operating systems encountered the largest number of financial malware attacks (which comes as no surprise given how widespread Windows devices are). That said, users of Windows 7 x64 Edition encountered banking Trojans more often, accounting for **42.2%** of all banking Trojan attacks. Android also made it into the list of attacked operating systems.

	Operating system	Percentage of attacks*
1	Windows 7 x64 Edition	42.2
2	Windows 7	11.6
3	Windows 7 Home x64 Edition	5.5
4	Windows XP Professional	7.0
5	Windows 8.1 Home x64 Edition	3.7
6	Windows 8.1 x64 Edition	2.3
7	Windows 7 Home	1.3
8	Windows 10 x64 Edition	1.2
9	Android 4.4.2	0.6
10	Windows NT 6.3 x64 Edition	0.7

*These percentage numbers are relative to all financial malware attacks detected on the computers of unique users who have consented to provide their statistical data.

It should be noted that although the family of Mac OS X operating systems did not make it to the Top 10, users of this operating system should not see themselves as being immune: in Q3 2015, computers running under Mac OS X were attacked **12,492** times.

TOP 20 malicious objects detected online

In the third quarter of 2015, Kaspersky Lab's web antivirus detected **38,233,047** unique malicious objects (scripts, exploits, executable files, etc.) and reported **75,408,543** unique URLs as malicious.

Of all malicious or potentially unwanted objects, we identified the 20 most active. These 20 accounted for 95% of all attacks on the Internet.

Top 20 malicious objects detected online

	Name*	% of all attacks**
1	Malicious URL	53.63
2	AdWare.JS.Agent.bg	16.71
3	AdWare.Script.Generic	7.14
4	Trojan.Script.Generic	6.30
5	Trojan.Script.Iframer	3.15
6	Trojan.Win32.Generic	1.52
7	AdWare.Win32.SoftPulse.heur	1.31
8	AdWare.JS.Agent.bt	1.09
9	AdWare.Win32.OutBrowse.heur	0.84
10	Trojan-Downloader.Win32.Generic	0.63
11	AdWare.NSIS.Vopak.heur	0.46
12	Exploit.Script.Blocker	0.46

13	Trojan-Downloader.JS.Iframe.diq	0.30
14	AdWare.Win32.Amonetize.aqxd	0.30
15	Trojan-Downloader.Win32.Genome.tqbx	0.24
16	AdWare.Win32.Eorezo.abyb	0.23
17	Hoax.HTML.ExtInstall.a	0.19
18	Trojan-Clicker.HTML.Iframe.ev	0.17
19	AdWare.Win32.Amonetize.bgnd	0.15
20	Trojan.Win32.Invader	0.14

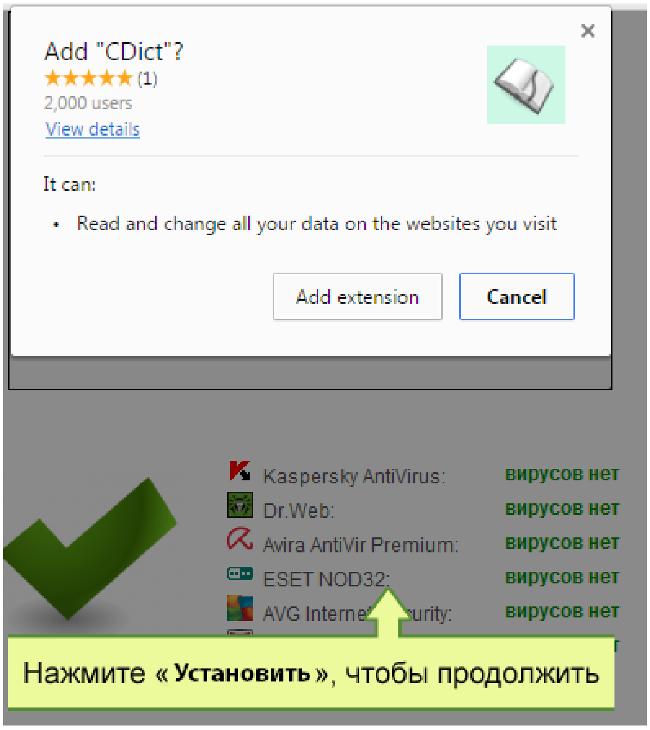
* These statistics represent the detection verdicts of the web antivirus module. Information was provided by users of Kaspersky Lab products who consented to share their local statistical data.

** The percentage of all web attacks recorded on the computers of unique users.

The Top 20 is largely made up of verdicts assigned to objects used in drive-by attacks, as well as adware programs. This quarter, adware verdicts occupied nine positions in this ranking.

Of interest is the verdict Hoax.HTML.ExtInstall.a, assigned to a web page which blocks the browser and urges the user to install a Chrome extension. When the user tries to close the page, the voice file 'voice.mp3' is often played – "Click on the 'Add' button to close this page".

The extensions that are offered do not cause any harm to users. However, the prompt is very intrusive and it is practically impossible for the user to reject it. This is why Kaspersky Lab products detect the corresponding web page with its popup window as malicious. There is a partnership program that uses this method to distribute the extension.



Add "CDict"?

★★★★★ (1)

2,000 users

View details

It can:

- Read and change all your data on the websites you visit

Kaspersky AntiVirus: вирусов нет

Dr.Web: вирусов нет

Avira AntiVir Premium: вирусов нет

ESET NOD32: вирусов нет

AVG Interne urity: вирусов нет

Нажмите « Установить », чтобы продолжить

Web page urging users to install a Chrome extension (translation: "Press 'Add' to continue")

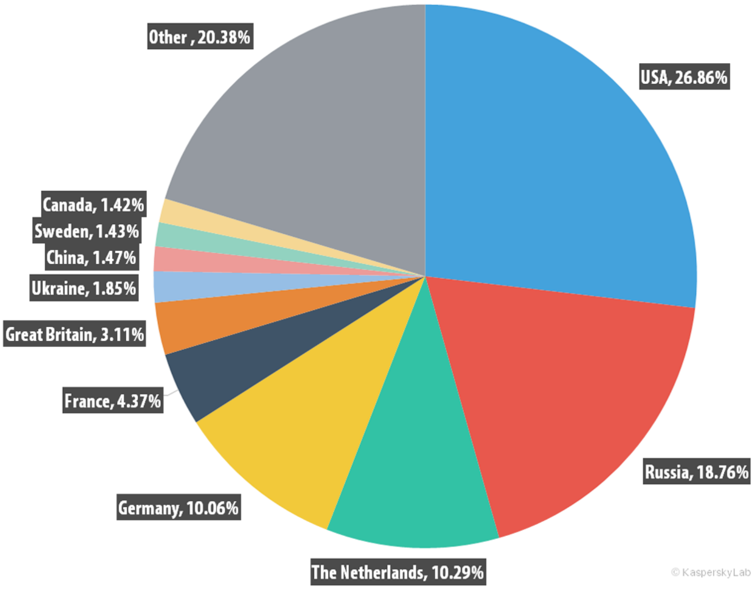
Top 10 countries where online resources are seeded with malware

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 could be the source of one or more web attacks.

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

In Q3 2015, Kaspersky Lab solutions blocked **235,415,870** attacks launched from web resources located in various countries around the world. 80% of notifications on blocked web attacks were triggered by attacks coming from web resources located in 10 countries.

Q3 saw the US take over first place (with 26.9%) from Russia (18.8%). The Virgin Islands and Singapore have fallen out of the Top 10, while there are two newcomers – Sweden (1.43%) and Canada (1.42%).



Distribution of web attack sources by country, Q3 2015

Countries where users faced the greatest risk of online infection

In order to assess the risk of online infection faced by users in different countries, we calculated the percentage of Kaspersky Lab users in each country who encountered detection verdicts on their machines during the quarter. The resulting data provide an indication of the aggressiveness of the environment in which computers work in different countries.

	Country*	% of unique users attacked **
1	Russia	38.20
2	Nepal	36.16
3	Kazakhstan	33.79
4	Ukraine	33.55
5	Syria	32.10
6	Azerbaijan	32.01
7	Belarus	30.68
8	Vietnam	30.26
9	China	27.82
10	Thailand	27.68
11	Armenia	27.65
12	Brazil	26.47
13	Algeria	26.16
14	Turkey	25.13
15	Mongolia	25.10
16	Kyrgyzstan	23.96
17	Macedonia	23.84
18	Lithuania	23.59

19	Bangladesh	23.56
20	Moldavia	23.36

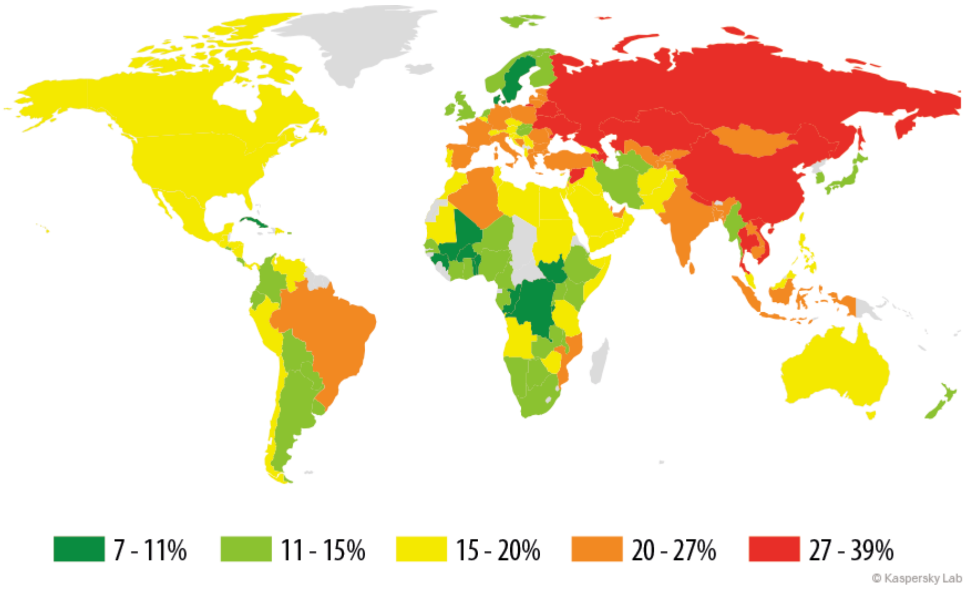
These statistics are based on the detection verdicts returned by the web antivirus module, received from users of Kaspersky Lab products who have consented to provide their statistical data.

*These calculations excluded countries where the number of Kaspersky Lab users is relatively small (fewer than 10,000 users).

**Unique users whose computers have been targeted by web attacks as a percentage of all unique users of Kaspersky Lab products in the country.

The leader of this ranking remained unchanged – it is still Russia with 38.2%. Since the previous quarter, Georgia, Croatia, Qatar, Bosnia and Herzegovina and Greece have left the Top 20. Newcomers to the ranking are Nepal, which went straight in at number two (36.16%), Brazil in 12th place (26.47%), Turkey in 14th (25.13%), Lithuania in 18th (23.59%), and Bangladesh (23.56%) in 19th.

The countries with the safest online surfing environments included Switzerland (17%), the Czech Republic (16%), the US (16.3%), Singapore (15%), Hungary (13.8%), Norway (13%), Ireland (12.2%), and Sweden (10.8%).



On average, 23.4% of computers connected to the Internet globally were subjected to at least one web attack during the three months. This is a 0.5 p.p. decrease on Q2.

Local threats

Local infection statistics for users computers are a very important indicator: they reflect threats that have penetrated computer systems using means other than the Internet, email, or network ports.

Data in this section is based on analyzing statistics produced by antivirus scans of files on the hard drive at the moment they were created or accessed, and the results of scanning removable storage media.

In Q3 2015, Kaspersky Lab's file antivirus modules detected **145,137,553** unique malicious and potentially unwanted objects.

Top 20 malicious objects detected on user computers

	Name*	% of unique users attacked**
1	DangerousObject.Multi.Generic	19.76
2	Trojan.Win32.Generic	14.51
3	Trojan.WinLNK.StartPage.gena	5.56
4	WebToolbar.JS.Condonit.a	4.98
5	AdWare.Script.Generic	4.97
6	WebToolbar.Win32.Agent.azm	4.48
7	RiskTool.Win32.GlobalUpdate.dx	3.63
8	WebToolbar.JS.AgentBar.e	3.63
9	WebToolbar.JS.CroRi.b	3.32
10	Downloader.Win32.Agent.bxib	3.20
11	AdWare.Win32.OutBrowse.heur	3.13
12	Adware.NSIS.ConvertAd.heur	3.08
13	AdWare.Win32.Generic	3.06
14	Downloader.Win32.MediaGet.elo	2.98
15	Trojan.Win32.AutoRun.gen	2.92
16	AdWare.Win32.BrowseFox.e	2.91
17	WebToolbar.Win32.MyWebSearch.si	2.82
18	AdWare.Win32.MultiPlug.heur	2.66
19	Virus.Win32.Sality.gen	2.61
20	RiskTool.Win32.BackupMyPC.a	2.57

*These statistics are compiled from malware detection verdicts generated by the on-access and on-demand scanner modules on the computers of those users running Kaspersky Lab products who have consented to submit their statistical data.

**The proportion of individual users on whose computers the antivirus module detected these objects as a percentage of all individual users of Kaspersky Lab products on whose computers a file antivirus detection was triggered.

In line with the established practice, this ranking represents the verdicts assigned to adware programs or their components, and to worms distributed on removable drives.

The only virus in the rankings – Virus.Win32.Sality.gen – continues to lose ground. The proportion of user machines infected by this virus has been diminishing for a long time. In Q3 2015, Sality was in 19th place with 2.61%, which is a 0.25 p.p. decrease on Q2.

Countries where users faced the highest risk of local infection

For each of the countries, we calculated the percentage of Kaspersky Lab product users on whose computers the file antivirus had been triggered during the quarter. These statistics reflect the level of personal computer infection in different countries.

Top 20 countries with the highest levels of computer infection

	Country*	% of unique users**
1	Bangladesh	64.44
2	Vietnam	60.20
3	Nepal	60.19
4	Georgia	59.48
5	Somalia	59.33
6	Laos	58.33
7	Russia	57.79
8	Armenia	57.56
9	Afghanistan	56.42
10	Ethiopia	56.34
11	Rwanda	56.21
12	Syria	55.82
13	Mozambique	55.79
14	Yemen	55.17
15	Cambodia	55.12
16	Algeria	55.03
17	Iraq	55.01
18	Kazakhstan	54.83
19	Mongolia	54.65
20	Ukraine	54.19

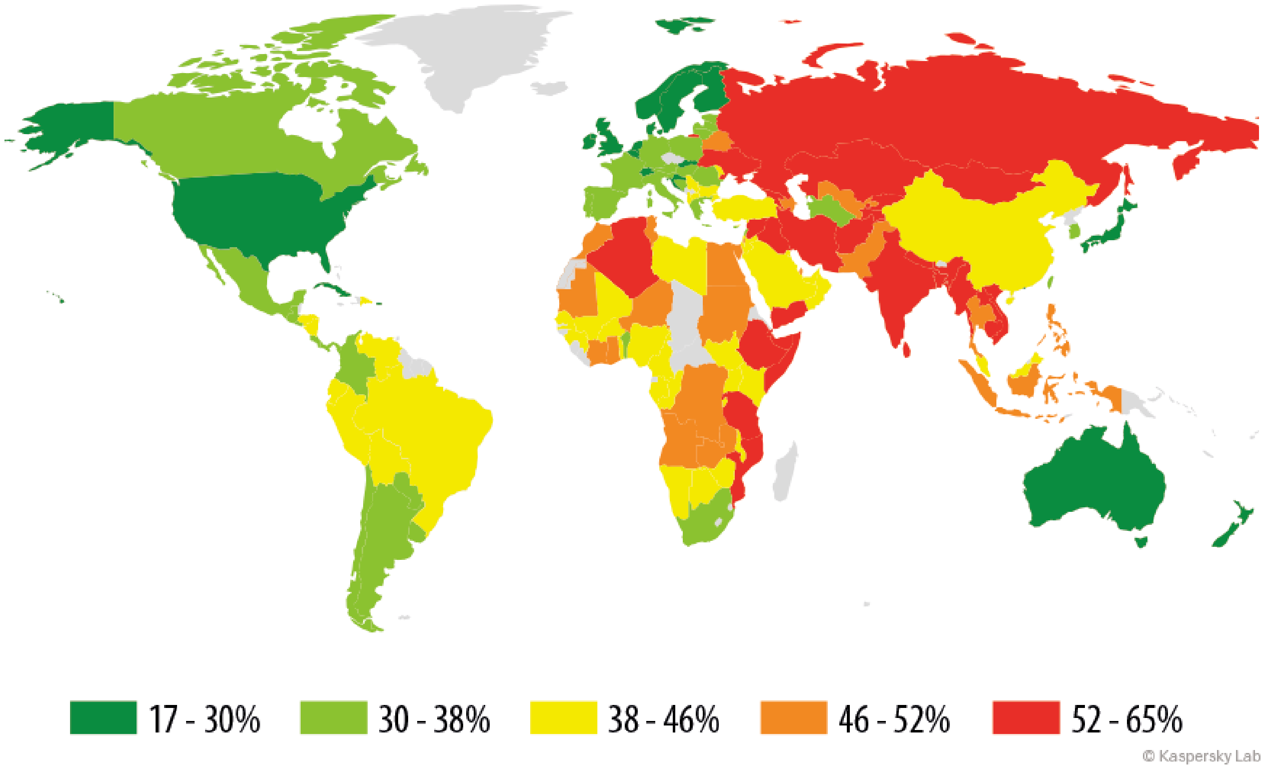
These statistics are based on the detection verdicts returned by on-access and on-demand antivirus modules, received from users of Kaspersky Lab products who have consented to provide their statistical data. The data include detections of malicious programs located on users' computers or on removable media connected to the computers, such as flash drives, camera and phone memory cards, or external hard drives.

* These calculations exclude countries where the number of Kaspersky Lab users is relatively small (fewer than 10,000 users).

** The percentage of unique users in the country with computers that blocked local threats as a percentage of all unique users of Kaspersky Lab products.

The newcomers to this ranking are Mozambique in 13th position (55.8%), and Yemen in 14th (55.2%).

The safest countries in terms of local infection risks were Sweden (21.4%), Denmark (19.8%) and Japan (18.0%).



An average of 42.2% of computers globally faced at least one local threat during Q3 2015, which is 2.2% p.p. more than in Q2 2015.

Securelist the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

Tel:	+7-495-797-8700
	+7-495-737-3412
Fax:	+7-495-797-8709