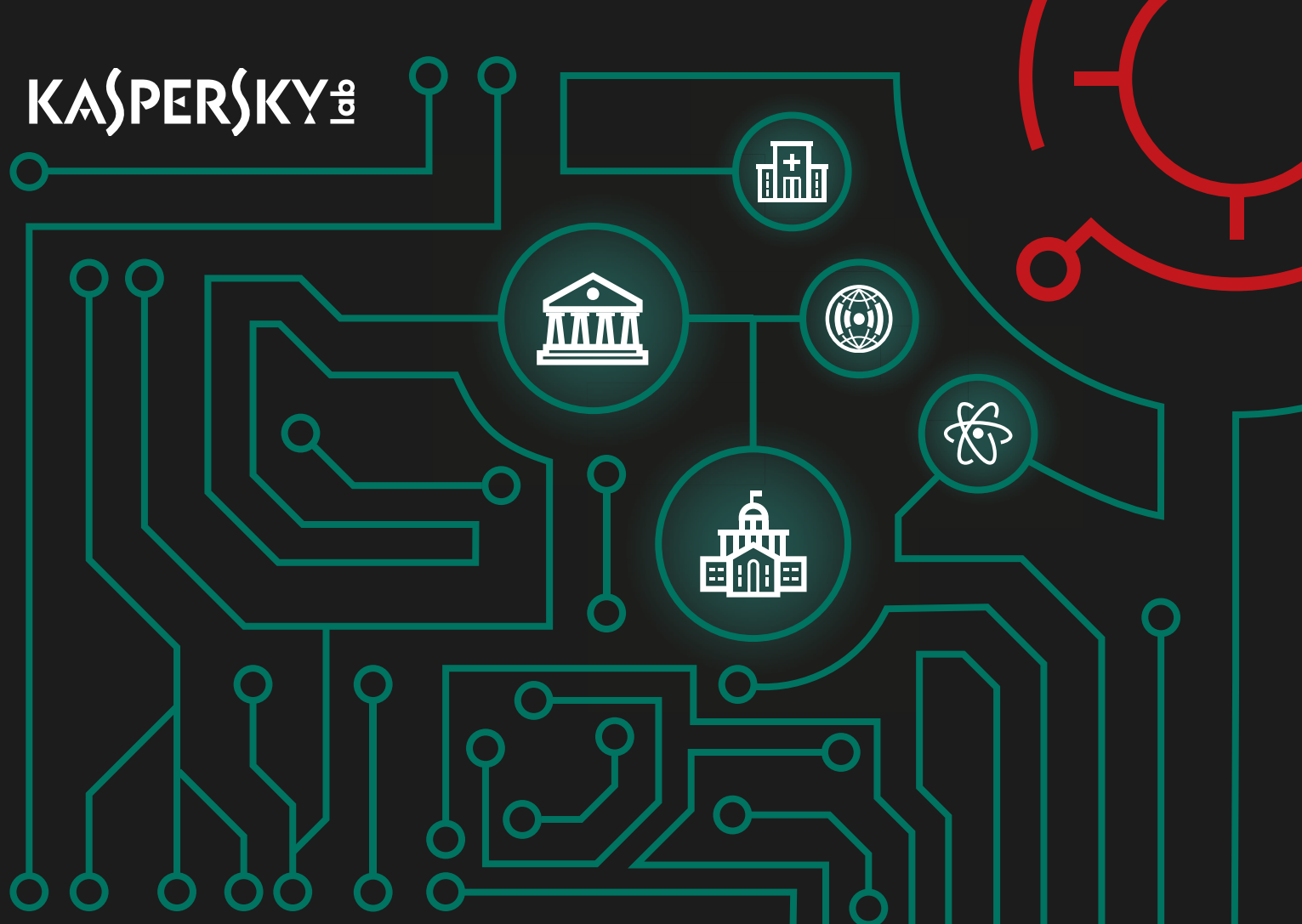
KASPERSKY lab

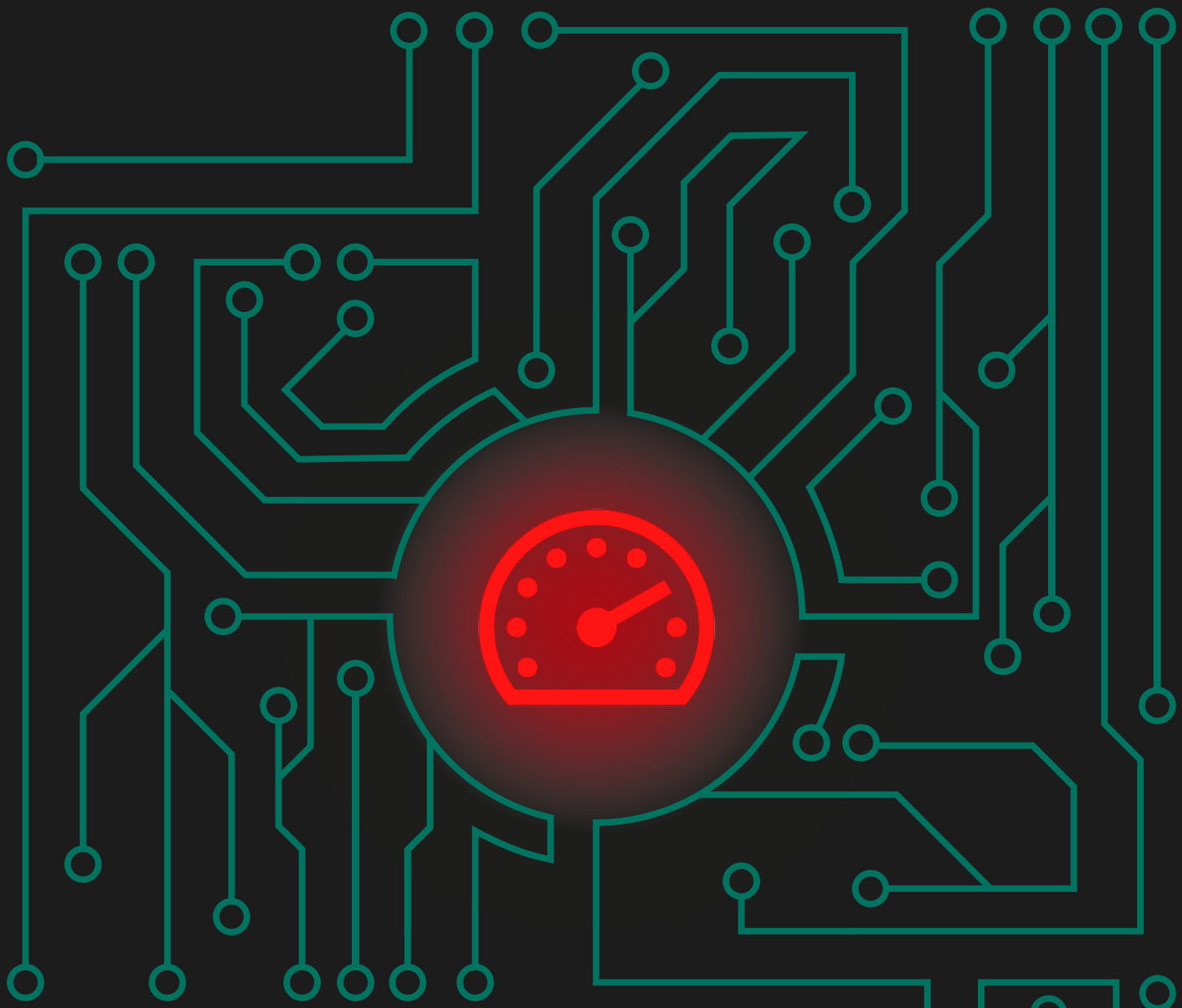


Kaspersky Security Bulletin:

# OVERALL STATISTICS FOR 2017

# CONTENTS

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.



# THE YEAR IN FIGURES

# THE YEAR IN FIGURES

**29.4%** of user computers were subjected to at least one **Malware-class** web attack over the year.

Kaspersky Lab solutions repelled **1 188 728 338** attacks launched from online resources located all over the world.

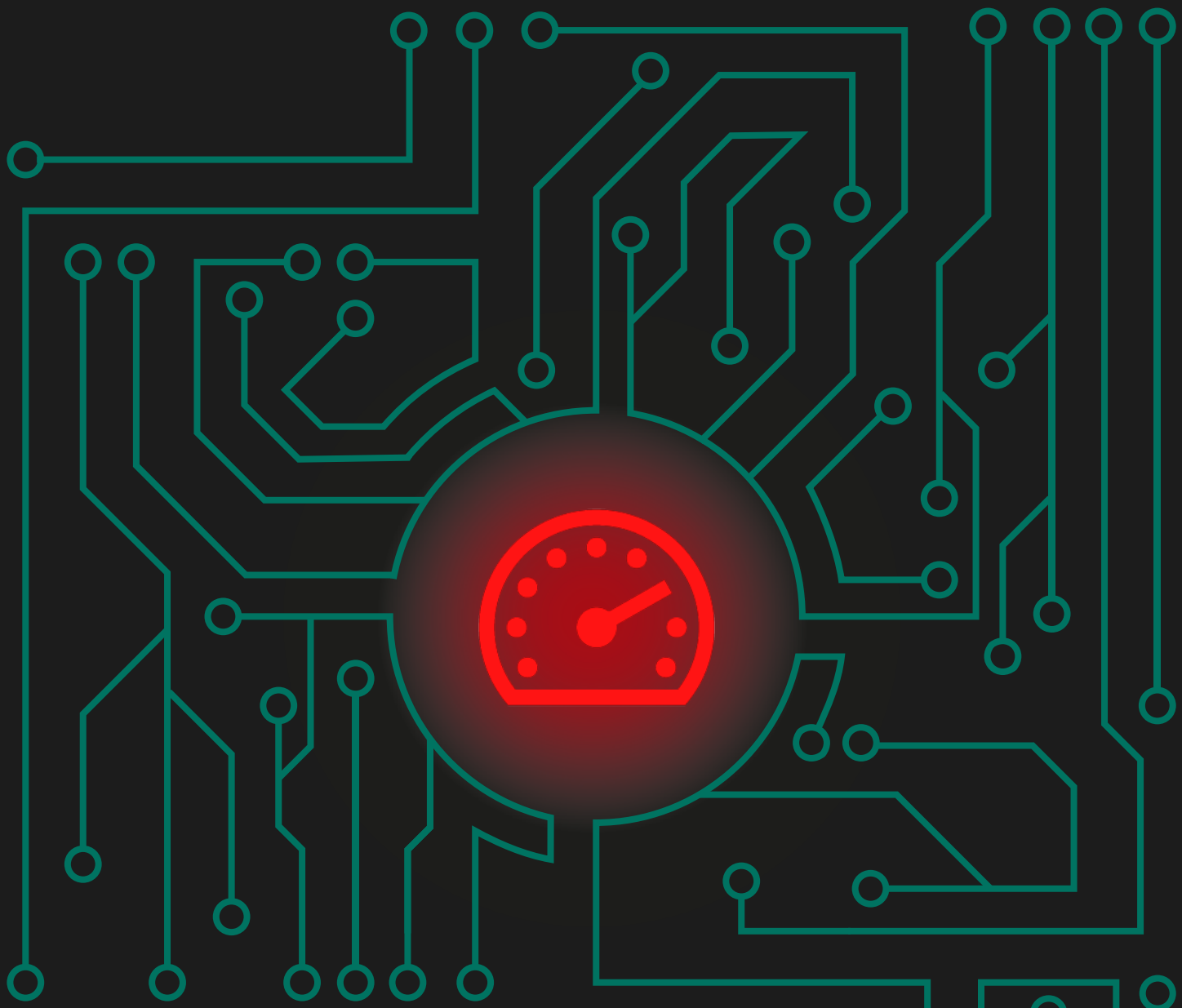
**199 455 606** unique URLs were recognized as malicious by web antivirus components.

Kaspersky Lab's web antivirus detected **15 714 700** unique malicious objects.

**939 722** computers of unique users were targeted by encryptors.

Kaspersky Lab solutions blocked attempts to launch malware capable of stealing money via online banking on **1 126 701** devices.

***Mobile threat statistics can be found in the report 'Mobile malware evolution 2017'.***



# VULNERABLE APPLICATIONS USED IN CYBERATTACKS

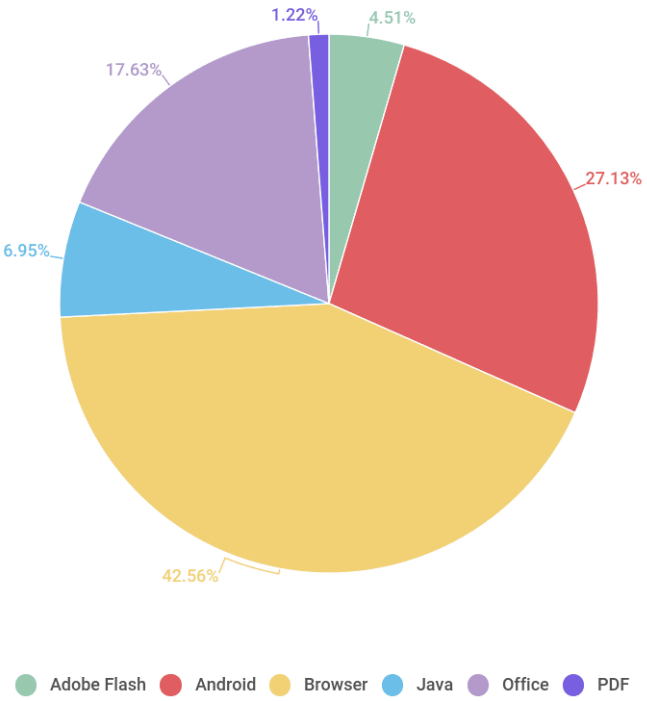
2017 saw lots of zero-day vulnerabilities actively exploited not only in targeted attacks but also against mass users. Unlike last year's statistics, exploits for Adobe Flash Player and Internet Explorer vulnerabilities have been in decline, replaced by Microsoft Office exploits. Creating reliable exploits for Flash Player has become too laborious and costly for the average cybercriminal. It's not just a case of finding and exploiting a vulnerability in Flash Player itself – the security features in today's web browsers have to be bypassed. And with all the major exploit kit players leaving the market in 2017, only a highly sophisticated attacker is capable of developing an exploit for Flash Player.

Because the exploit kit market – traditionally dominated by browser and Flash Player exploits – is in decline, we are seeing a substantial growth in attacks targeting Microsoft Office users. It was 4% over the year, or a stunning 14% over the past two years. The main reason for that was the numerous zero-day vulnerabilities found in Office over the last 12 months. Binary memory corruption vulnerabilities CVE-2017-0261, CVE-2017-0262, CVE-2017-11826 were used in APT attacks, though have not been used more widely in malicious spam campaigns by cybercriminals, mainly due to the complexity and low reliability of the exploits. Exploits for three 'logical' vulnerabilities – CVE-2017-0199, CVE-2017-8570, and CVE-2017-8759 – have been the go-to exploit for most spear-phishing attacks this year – according to KSN statistics, over 90% of detected Microsoft Office documents with an exploit contained exploits for either CVE-2017-0199 or CVE-2017-8759, making them extremely prevalent amongst other exploits. It's interesting to note that a lot of the documents containing an exploit for Microsoft Office in 2017 also came with a phishing component appended, in case the target was already patched against the vulnerability.

Exploits for Android also showed a 6% year-to-year increase, accounting for 27% of all exploits. Last year's rapid growth continues, mostly due to an increasing number of exploits that facilitate root privilege escalation on Android mobile devices.

However, the main event, not only of Q2 but of 2017 overall, was the public release of the 'Lost In Translation' archive by the Shadow Brokers hacker group. The archive contained multiple network exploits for various Windows versions. And even though most of those vulnerabilities weren't actually zero-day vulnera-

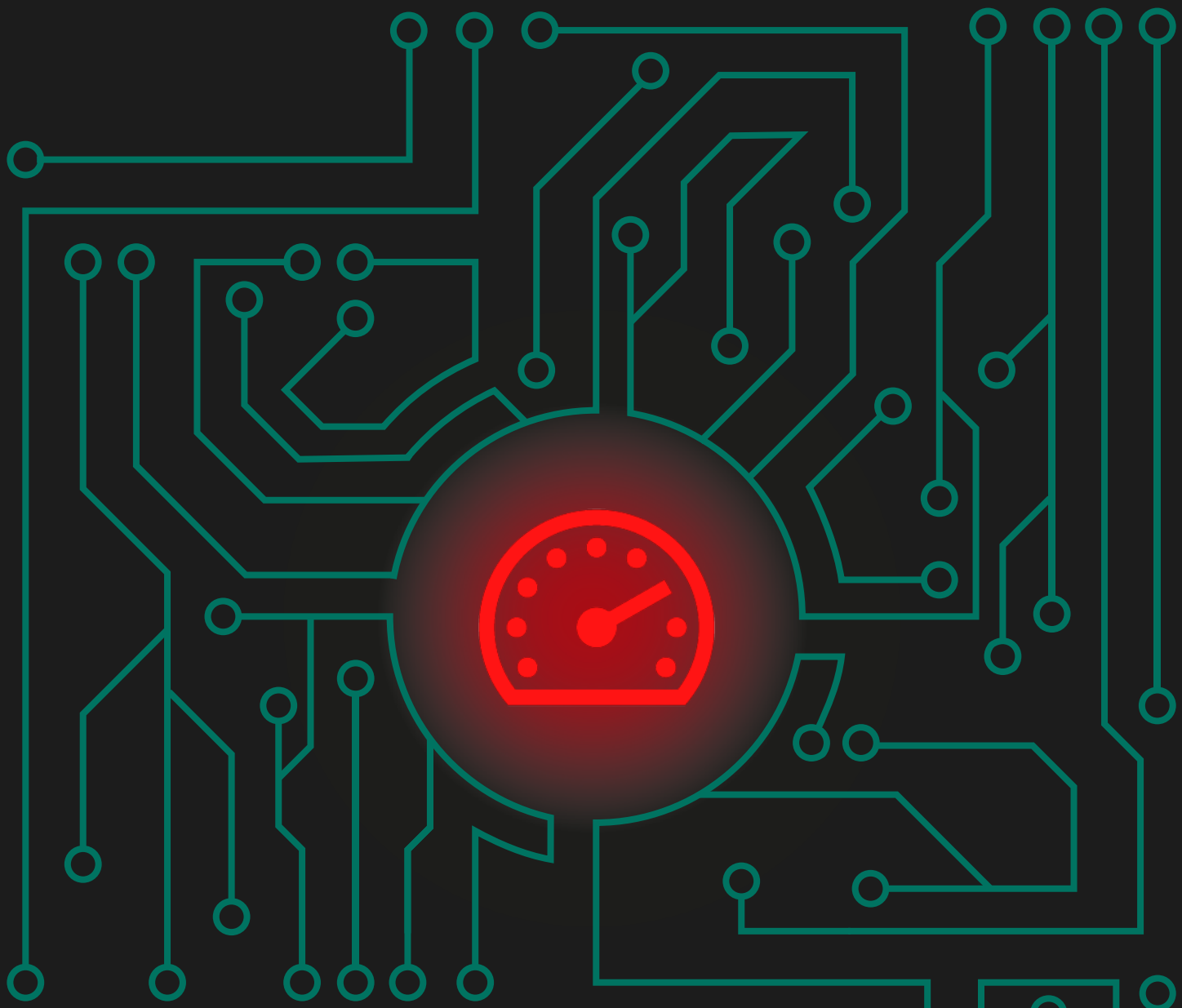
bilities and had already been patched in the MS17-010 update by Microsoft a month before the leak, the publication still had terrible consequences. The damage caused by network worms, Trojans and ransomware cryptors being distributed via the network with the help of EternalBlue and EternalRomance SMB exploits, as well as the number of users infected, is incalculable. In the yearly statistics for network attacks blocked by our IDS component, we saw the Intrusion.Win.MS17-010.* verdict become one of the most exploited network vulnerabilities in the space of just a few months.




Distribution of exploits used in cyberattacks, by type of application attacked, November 2016 – October 2017

Vulnerable applications are ranked based on Kaspersky Lab product reports of blocked exploits used by cybercriminals both in web-borne attacks and in compromised local applications, including those on users' mobile devices.

To sum up, 2017 broke a long going trend in the exploit kit market, with a shift of focus from Internet Explorer and Adobe Flash Player to Microsoft Office. It is more and more common for cybercriminals to utilize social engineering techniques, as it becomes much cheaper and at times even more reliable than using 'traditional' exploits. The global WannaCry and ExPetr ransomware attacks demonstrated just how dangerous and disastrous a network worm can be, even if it utilizes a vulnerability that was patched a long time ago.



# ONLINE THREATS (WEB-BASED ATTACKS)

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

In 2017, Kaspersky Lab's web antivirus detected **15 714 700** unique malicious objects (scripts, exploits, executable files, etc.) and **199 455 606** unique URLs were recognized as malicious by web antivirus components. Kaspersky Lab solutions detected and repelled **1 188 728 338** malicious attacks launched from online resources located in 206 countries all over the world.

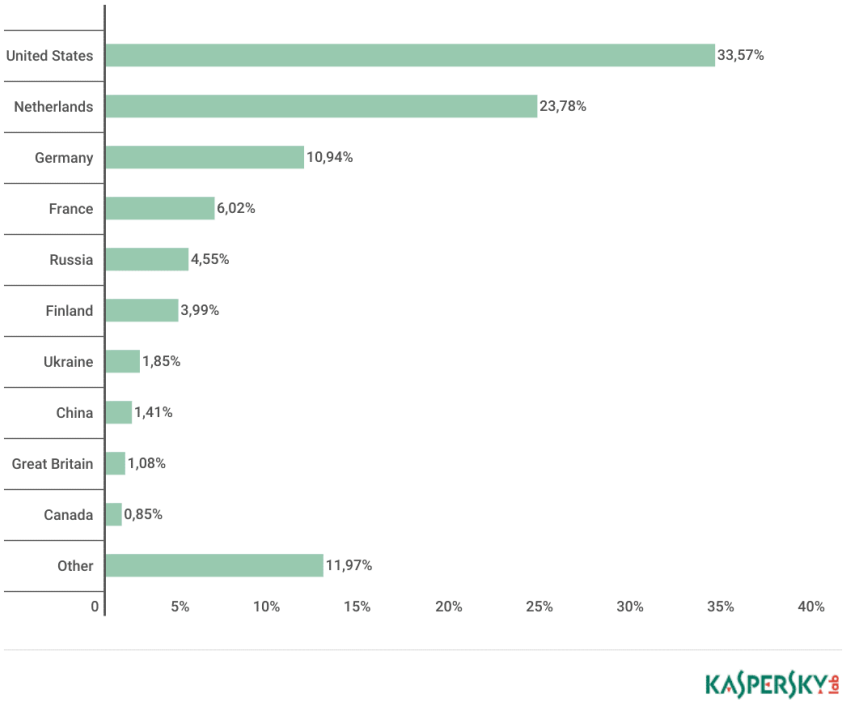
# TOP 10 COUNTRIES WHERE ONLINE RESOURCES ARE SEEDED WITH MALWARE

The following statistics are based on the physical location of the online resources 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 against their actual domain IP addresses, and then the geographical location of a specific IP address (GEOIP) is established.

In 2017, Kaspersky Lab solutions blocked 1 188 728 338 attacks launched from web resources located in various countries around the world.

88.03% of notifications about attacks blocked by antivirus components were received from online resources located in 10 countries.




Distribution of web attack sources by country, November 2016 – October 2017

The TOP 3 countries remained the same: the USA (33.57%), the Netherlands (23.78%) and Germany (10.94%). France (6.02%) swapped places with Russia (4.55%) and occupied fourth place. The Virgin Islands and Bulgaria left the TOP 10 rating, while Finland (3.99%) and Canada (0.85%) were newcomers.

# TOP 20 VERDICTS DETECTED ONLINE

Throughout 2017, Kaspersky Lab's web antivirus detected **15 714 700** unique malicious objects: scripts, exploits, executable files, etc.

During the year, advertising programs and their components were registered on 22% of user computers where our web antivirus was triggered.

We identified the 20 malicious programs most actively involved in online attacks launched against computers in 2017.

| | Name* | % of all attacks** |
|---|---|---|
| 1 | Malicious URL | **87.75%** |
| 2 | Trojan.Script.Generic | **6.69%** |
| 3 | Trojan.JS.Small.ci | **1.66%** |
| 4 | Trojan-Clicker.HTML.Iframe.dg | **1.44%** |
| 5 | Trojan.JS.Miner.d | **0.31%** |
| 6 | Trojan-Downloader.JS.Agent.npe | **0.25%** |
| 7 | Packed.Multi.MultiPacked.gen | **0.16%** |
| 8 | Trojan-Downloader.Script.Generic | **0.14%** |
| 9 | Trojan-Dropper.VBS.Agent.bp | **0.09%** |
| 10 | Exploit.Script.Generic | **0.07%** |
| 11 | Trojan.JS.Agent.dvu | **0.07%** |
| 12 | Trojan-Clicker.Script.Generic | **0.06%** |
| 13 | Trojan.JS.Agent.sileof | **0.05%** |
| 14 | Trojan-Downloader.JS.SLoad.gen | **0.05%** |
| 15 | Trojan-Downloader.JS.Redirector.a | **0.04%** |
| 16 | Hoax.HTML.FraudLoad.m | **0.03%** |
| 17 | Trojan.Script.Iframer.a | **0.03%** |
| 18 | Trojan.JS.AdInject.a | **0.03%** |
| 19 | Trojan.JS.Agent.ckf | **0.02%** |
| 20 | Trojan.Win32.Cometer.aj | **0.02%** |

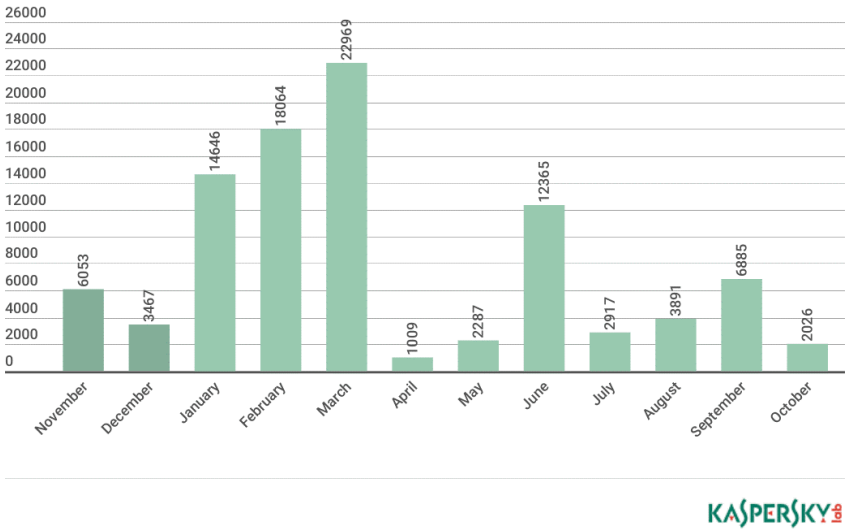
* These statistics represent detection verdicts from the web antivirus module. Information was provided by users of Kaspersky Lab products who consented to share their local data.
** The percentage of all malware web attacks recorded on the computers of unique users.

Web exploits are much less popular nowadays, but we still can see Exploit.Script.Generic in tenth place of this rating.

Other scripts perform different malicious activities. For example, Trojan.JS.Small.ci aggressively injects third-party ads into traffic, Trojan.JS.Miner.d is a web miner, Trojan.JS.Agent.sileof is the detection for fraudulent resources that lock browsers with constantly generated fake messages about infections.

# CRYPTO-RANSOMWARE

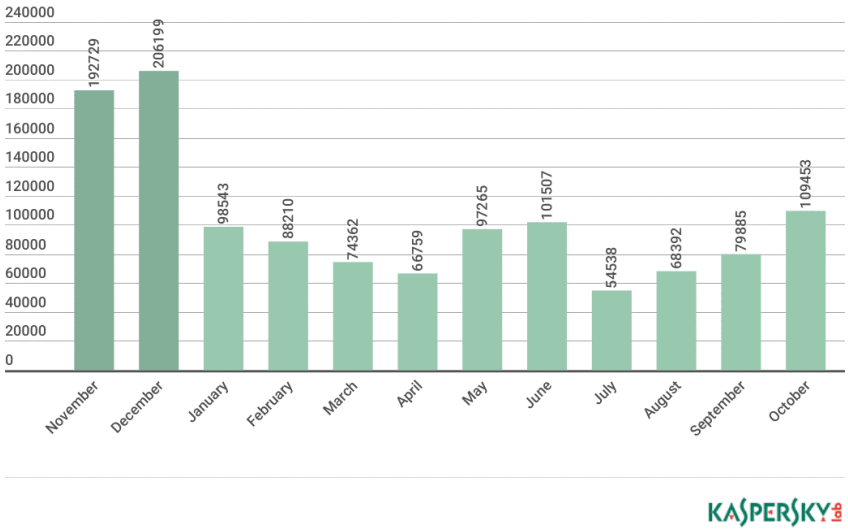
During the year, we detected more than **96 thousand modifications** of crypto-ransomware and discovered **38 new families.**




Number of new crypto-ransomware modifications, November 2016 – October 2017

## The number of users attacked by encryptors

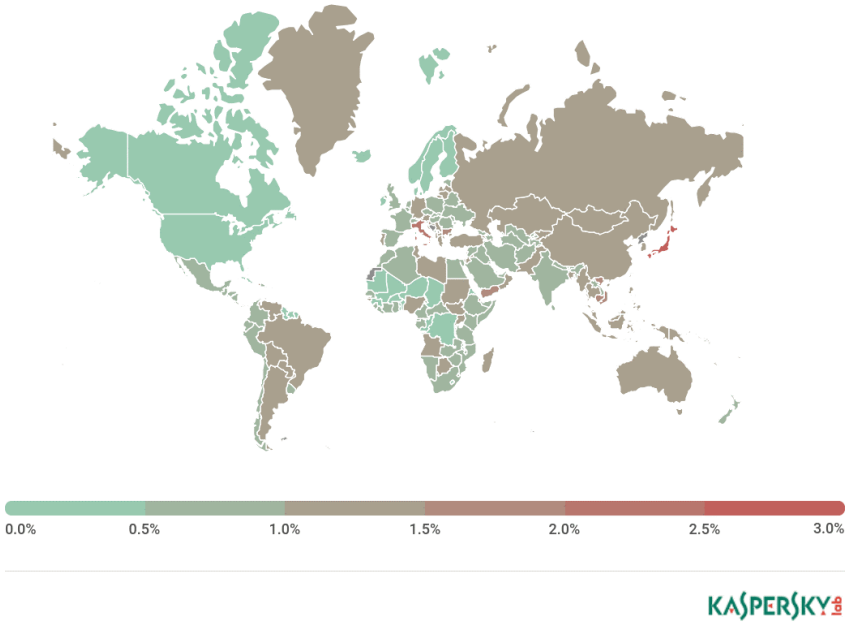
In 2017, **939 722 unique KSN users** were attacked by encryptors, including more than **240 thousand** corporate users.




Number of users attacked by crypto-ransomware (November 2016 – October 2017)

It is important to remember that the real number of incidents is higher: the statistics only reflect the results of signature-based and heuristic detections, while in the case of new and unknown malware samples Kaspersky Lab products detect encryption Trojans based on behavior recognition models.

## Geography of attacks




Geography of crypto-ransomware attacks in 2017 (percentage of attacked users)

## TOP 10 countries attacked by encryptors

| | Country* | % of users attacked by encryptors** |
|---|---|---|
| 1 | Japan | 2.83 |
| 2 | Italy | 2.37 |
| 3 | Vietnam | 1.95 |
| 4 | Bulgaria | 1.68 |
| 5 | Taiwan | 1.59 |
| 6 | Cambodia | 1.53 |
| 7 | Croatia | 1.48 |
| 8 | Lebanon | 1.44 |
| 9 | Brazil | 1.42 |
| 10 | Indonesia | 1.35 |

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (under 50,000).
** Unique users whose computers have been targeted by crypto-ransomware as a percentage of all unique users of Kaspersky Lab products in the country.

## TOP 10 most widespread encryptor families

| | Name | Verdict* | % of attacked users** |
|---|---|---|---|
| 1 | WannaCry | Trojan-Ransom.Win32.Wanna | **7.71** |
| 2 | Locky | Trojan-Ransom.Win32.Locky | **6.70** |
| 3 | Cerber | Trojan-Ransom.Win32.Zerber | **5.89** |
| 4 | Jaff | Trojan-Ransom.Win32.Jaff | **2.58** |
| 5 | Cryrar/ACCDFISA | Trojan-Ransom.Win32.Cryrar | **2.20** |
| 6 | Spora | Trojan-Ransom.Win32.Spora | **2.19** |
| 7 | Purgen/GlobeImposter | Trojan-Ransom.Win32.Purgen | **2.11** |
| 8 | Shade | Trojan-Ransom.Win32.Shade | **2.06** |
| 9 | Crysis | Trojan-Ransom.Win32.Crusis | **1.25** |
| 10 | CryptoWall | Trojan-Ransom.Win32.Cryptodef | **1.13** |

The WannaCry epidemic affected hundreds of thousands of computers around the globe. It comes as no surprise that it was the most widespread encryptor family in 2017.

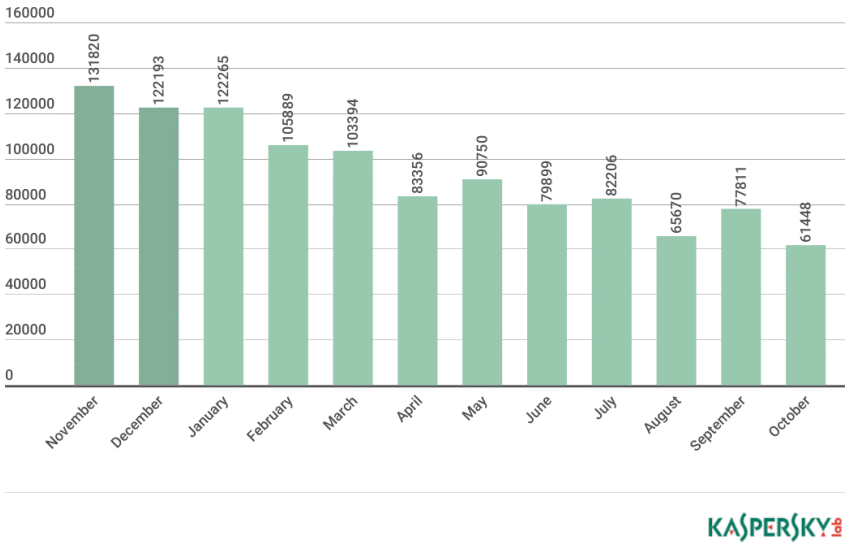
Read more about the ransomware situation in Kaspersky Security Bulletin – Story of the year 2017.

* These statistics are based on detection verdicts received from users of Kaspersky Lab products who have consented to provide their statistical data.
** Unique users whose computers have been targeted by a specific crypto-ransomware family as a percentage of all users of Kaspersky Lab products attacked by crypto-ransomware.

# ONLINE THREATS IN THE FINANCIAL SECTOR

These statistics are based on detection verdicts of Kaspersky Lab products, received from users of Kaspersky Lab products who have consented to provide their statistical data. The annual statistics for 2017 are based on data received between November 2016 and October 2017 and included malicious programs for ATMs and POS terminals, but do not include mobile threats.

In 2017, Kaspersky Lab solutions blocked attempts to launch one or more malicious programs capable of stealing money via online banking on **1 126 701 computers**.



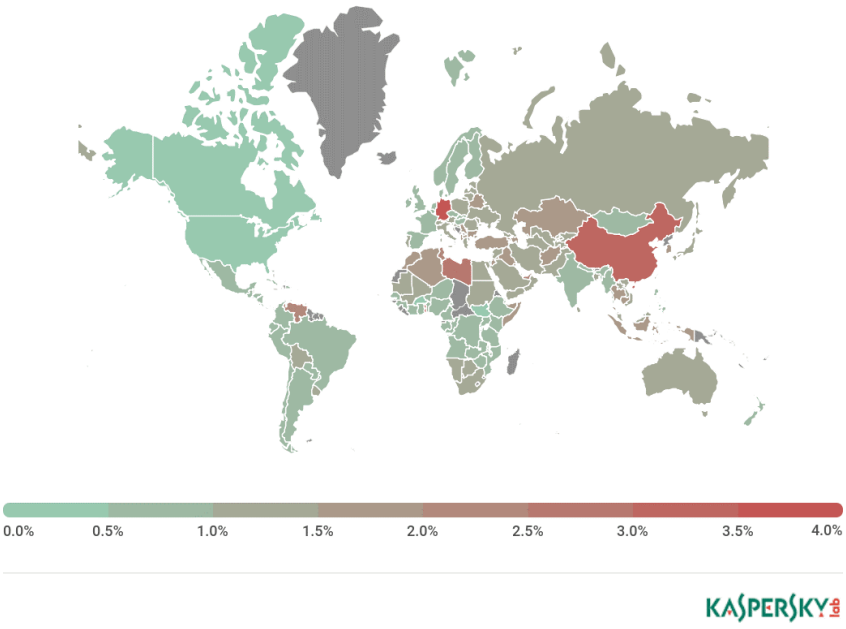

The number of users targeted by financial malware, November 2016-October 2017



KASPERSKY lab

## Geography of attacks

To evaluate and compare the risk of being infected by banking Trojans and ATM and POS malware worldwide, we calculate the percentage of Kaspersky Lab product users in the country who encountered this type of threat during the reporting period, relative to all users of our products in that country.




Geography of financial malware attacks in 2017

## TOP 10 countries by percentage of attacked users

| | Country* | % attacked users** |
|---|---|---|
| 1 | Germany | 4.44 |
| 2 | Togo | 3.17 |
| 3 | China | 3.05 |
| 4 | Libya | 2.81 |
| 5 | Lebanon | 2.45 |
| 6 | Tunisia | 2.21 |
| 7 | Taiwan | 2.15 |
| 8 | United Arab Emirates | 2.12 |
| 9 | Venezuela | 2.06 |
| 10 | Jordan | 1.88 |

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (less than 10,000).
** Unique users whose computers have been targeted by financial malware as a percentage of all users attacked by all types of malware.

## TOP 10 banking malware families

The table below shows the 10 malware families most commonly used in 2017 to attack banking users (as a percentage of users attacked):

| | Name* | % users attacked** |
|---|---|---|
| 1 | Trojan-Spy.Win32.Zbot | 39.2 |
| 2 | Trojan.Win32.Nymaim | 26.2 |
| 3 | Trojan.Win32.Neurevt | 5.9 |
| 4 | SpyEye | 5.8 |
| 5 | Trojan-Banker.Win32.Gozi | 4.3 |
| 6 | Emotet | 3.1 |
| 7 | Caphaw | 3.0 |
| 8 | Trickster | 2.8 |
| 9 | Cridex/Dridex | 2.7 |
| 10 | Backdoor.Win32.Shiz | 2.4 |

* 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.

# COUNTRIES WHERE USERS FACE THE GREATEST RISK OF ONLINE INFECTION

In order to assess the countries in which users most often face cyber-threats, we calculated how often Kaspersky Lab users encountered detection verdicts on their machines in each country. The resulting data characterizes the risk of infection that computers are exposed to in different countries across the globe, providing an indicator of the aggressiveness of the environment facing computers in different parts of the world.

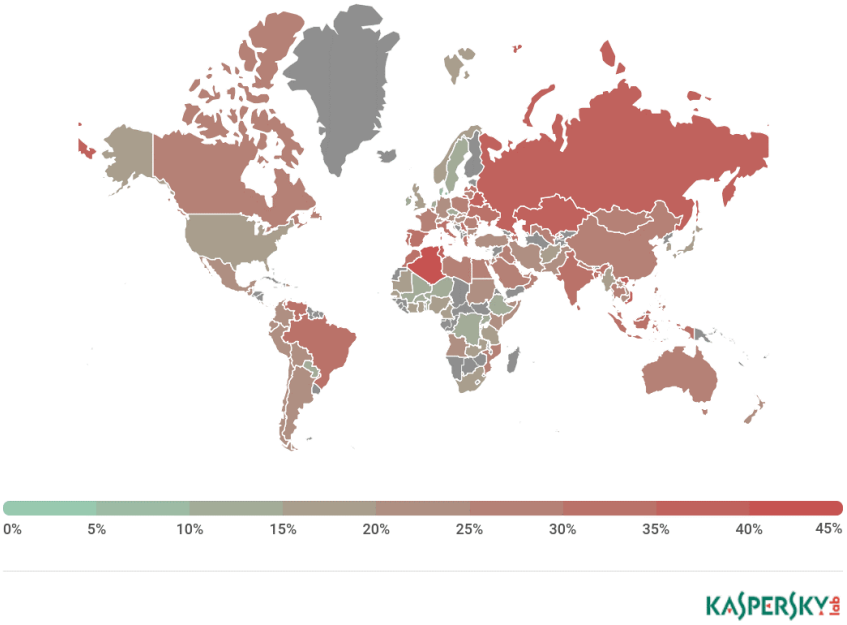
This rating only includes attacks by malicious programs that fall under the Malware class. The rating does not include web antivirus module detections of potentially dangerous or unwanted programs such as RiskTool or Adware.

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

| | Name* | % users attacked** |
|---|---|---|
| 1 | Algeria | **44.06** |
| 2 | Belarus | **38.39** |
| 3 | Russia | **36.91** |
| 4 | Kazakhstan | **36.57** |
| 5 | Tunisia | **36.51** |
| 6 | Vietnam | **35.01** |
| 7 | Azerbaijan | **34.70** |
| 8 | Qatar | **34.20** |
| 9 | Portugal | **33.01** |
| 10 | Greece | **32.80** |
| 11 | Brazil | **32.66** |
| 12 | Moldova | **32.42** |
| 13 | India | **32.34** |
| 14 | Morocco | **31.72** |
| 15 | Venezuela | **31.52** |
| 16 | Spain | **31.20** |
| 17 | Sri Lanka | **30.75** |
| 18 | Malaysia | **30.52** |
| 19 | Bangladesh | **30.37** |
| 20 | Ukraine | **30.27** |

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.

* We excluded those countries where the number of Kaspersky Lab product users is relatively small (less than 50,000).
** Unique users whose computers have been targeted by Malware-class web attacks as a percentage of all unique users of certain Kaspersky Lab products in the country.



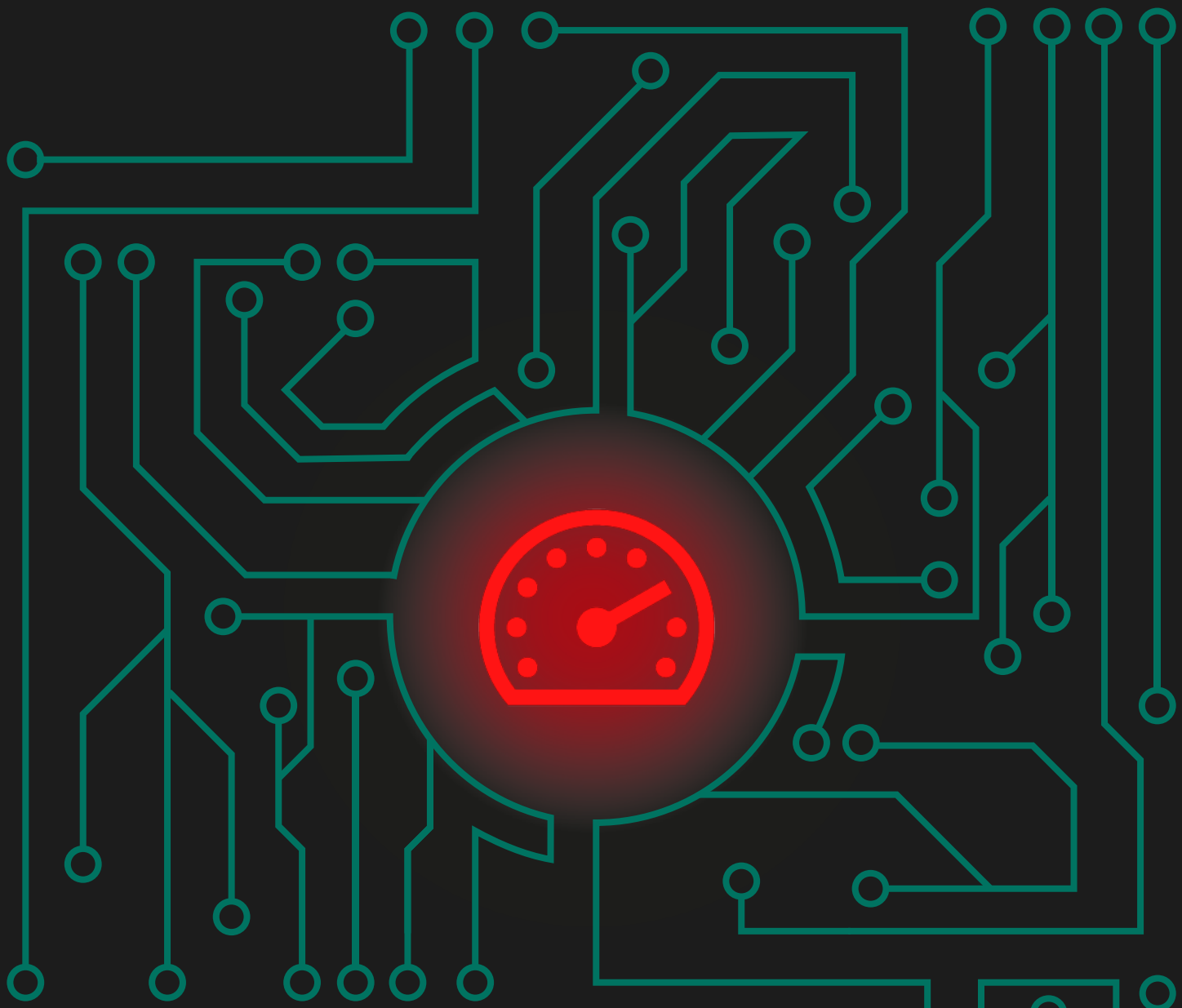

Geography of malicious web attacks in 2017 (ranked by percentage of users attacked)

The countries can be divided into three groups that reflect the different levels of infection risk.

**1. The high risk group (over 40%)**
In 2017, this group included only one country – Algeria.

**2. The medium risk group (20-39.9%)**
This group includes 75 countries; among them are Belarus (38.39%), Russia (36.91%), Kazakhstan (36.57%), Vietnam (35.01%), Spain (31.19%), Romania (29.5%), Iraq (26.85%), Angola (24.22%), Germany (22.82%), Switzerland (21.55%), Kenya (20.6%), Bolivia (20.15%).

**3. The low risk group (0-19.9%)**
The countries with the safest online surfing environments include Afghanistan (19.55%), United States (19.4%), United Kingdom (19.22%), Japan (15.41%), Uganda (13.49%), Ireland (12.15%).
In 2017, 29.4% of computers encountered at least one Malware-class web attack while online.



# LOCAL THREATS

# TOP 20 MALICIOUS OBJECTS DETECTED ON USER COMPUTERS

Local infection statistics for user computers are a very important indicator: they reflect threats that have penetrated computer systems by infecting files or removable media, or initially got on the computer in an encrypted format (for example, programs integrated in complex installers, encrypted files, etc.). In addition, these statistics include objects detected on user computers after the first scan of the system by Kaspersky Lab's file antivirus.

This section contains an analysis of the statistical data obtained based on antivirus scans of files on the hard drive at the moment they are created or accessed, and the results of scanning various removable data storages.

For this rating, we identified the 20 most frequently detected threats on user computers in 2017. This rating does not include the Adware and Riskware classes of program.

| | Name* | % of unique attacked users** |
|---|---|---|
| 1 | DangerousObject.Multi.Generic | 35.87% |
| 2 | Trojan.Script.Generic | 9.47% |
| 3 | Trojan.Multi.GenAutorunReg.a | 8.48% |
| 4 | HackTool.Win32.KMSAuto.i | 8.39% |
| 5 | Trojan.WinLNK.Runner.jo | 5.57% |
| 6 | Trojan.WinLNK.Agent.gen | 4.89% |
| 7 | Trojan.WinLNK.StartPage.gena | 4.14% |
| 8 | Trojan-Downloader.Script.Generic | 3.64% |
| 9 | Trojan.Win32.AutoRun.gen | 3.46% |
| 10 | HackTool.Win32.KMSAuto.c | 3.21% |
| 11 | Virus.Win32.Sality.gen | 3.16% |
| 12 | Trojan.Multi.Powecod.a | 2.59% |
| 13 | Trojan.Win32.Starter.yy | 2.21% |
| 14 | Worm.VBS.Dinihou.r | 2.18% |
| 15 | Trojan.WinLNK.Agent.ew | 2.14% |
| 16 | Trojan.Multi.StartPageTask.a | 2.02% |
| 17 | Trojan.Multi.StartPageTask.b | 1.94% |
| 18 | Trojan.Win32.Generic | 1.94% |
| 19 | HackTool.Win32.Kiser.fnawf | 1.69% |
| 20 | Trojan.Win32.Agentb.bqyr | 1.58% |

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 consented to submit their statistical data.

* Malware detection verdicts generated by the on-access and on-demand scanner modules on the computers of those users running Kaspersky Lab products who consented to submit their statistical data.
** The proportion of individual users on whose computers the file antivirus detected these programs as a percentage of all individual users of Kaspersky Lab products on whose computers a malicious program was detected.

The DangerousObject.Multi.Generic verdict, which is used for malware detected with the help of cloud technologies, is in first place (35.87%). Cloud technologies work when the antivirus databases do not yet contain either signatures or heuristics to detect a malicious program but the company's cloud antivirus database already has information about the object. In fact, this is how the very latest malware is detected.

The overall share of Win32 malware decreased due to a corresponding increase in various other script platform detections.

Trojan.Win32.Generic share decreased because some representatives of this detection were classified as less generic this year.

There are several widespread variations of WinLNK malware – in fifth, sixth, seventh and 15th places in our TOP 20. This malware can change browser settings or can be used for downloading the next stages of infection.

Twelfth place was taken by newcomer Trojan.Multi.Powecod.a (2.59%). This malware uses PowerShell for a variety of malicious actions.

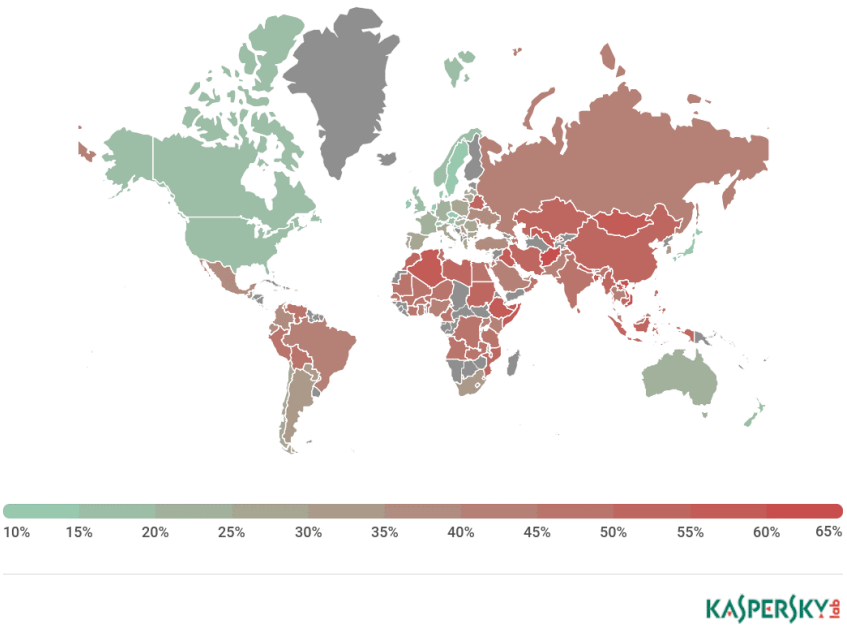
# COUNTRIES WHERE USERS FACE THE HIGHEST RISK OF LOCAL INFECTION

For each country, we calculated the number of file antivirus detections users faced during the year. The data includes malicious programs located on user computers or on removable media connected to computers, such as flash drives, camera and phone memory cards, or external hard drives. This statistic reflects the level of infected personal computers in different countries around the world.

| | Country* | % of unique users** |
|---|---|---|
| 1 | Vietnam | 67.41 |
| 2 | Afghanistan | 63.03 |
| 3 | Algeria | 61.36 |
| 4 | Laos | 61.08 |
| 5 | Mongolia | 60.67 |
| 6 | Uzbekistan | 58.86 |
| 7 | Rwanda | 58.42 |
| 8 | Iraq | 58.39 |
| 9 | Ethiopia | 58.35 |
| 10 | Bangladesh | 58.09 |
| 11 | Somalia | 57.78 |
| 12 | Nepal | 57.60 |
| 13 | Mozambique | 56.12 |
| 14 | Libya | 55.85 |
| 15 | Cambodia | 55.79 |
| 16 | Kazakhstan | 54.87 |
| 17 | Sudan | 54.76 |
| 18 | Myanmar | 54.73 |
| 19 | Indonesia | 53.92 |
| 20 | Morocco | 53.48 |

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

* When calculating, we excluded countries where there are fewer than 50,000 Kaspersky Lab users.
** The percentage of unique users in the country with computers that blocked Malware-class local threats as a percentage of certain unique users of Kaspersky Lab products.




Geography of malicious web attacks in 2017 (ranked by percentage of users attacked)

The countries can be divided into several risk categories that reflect the level of local threats.

**Maximum risk (over 60%):** five leading countries from the TOP 20.

**High risk (40-59.99%):** countries including Uzbekistan (58.87%), Cambodia (55.79%), Cameroon (50.87%), Egypt (49.12%), Uganda (45.12%), Russia (42.26%), Brazil (41.94%).

**Moderate local infection rate (20-39.99%):** countries including Ukraine (39.84%), Mexico (36.52%), Turkey (35.91%), Serbia (32.02%), Chile (28.67%), Greece (26%), Israel (24.4%), Hungary (21.96%).

**The low risk group (0-19.9%):** Australia (19.55%), Singapore (15.5%), Japan (12.5%), Ireland (10.25), Denmark (8.88%).

In 2017, at least one malicious program was found on an average of 36.8% of computers, hard drives or removable media belonging to KSN users.

株式会社カスペルスキー
PR-1045- 201712