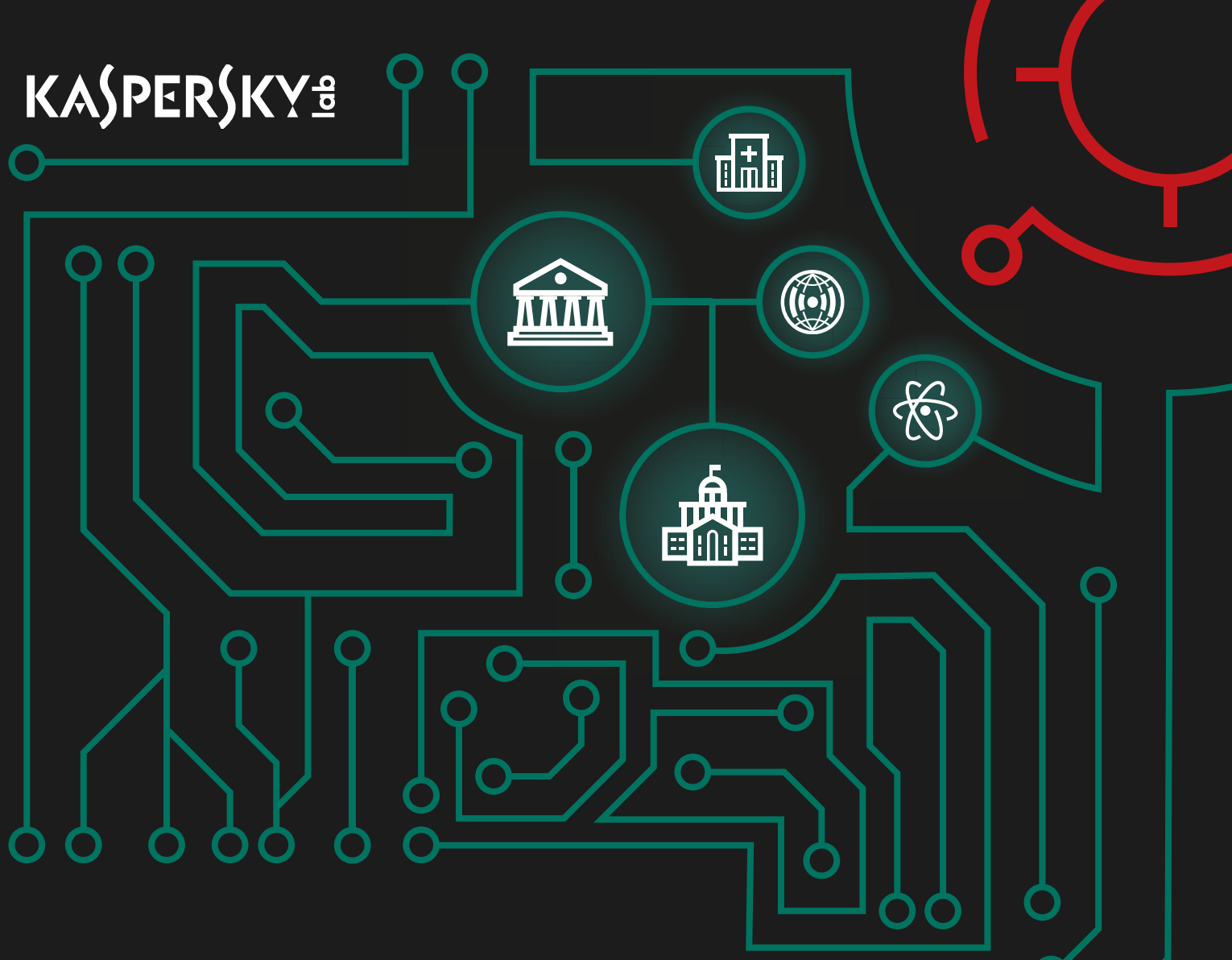
KASPERSKY lab



# Kaspersky Security Bulletin:
# СТАТИСТИКА 2017

# СОДЕРЖАНИЕ

Все статистические данные, использованные в этом отчете, получены с помощью глобальной облачной сети Kaspersky Security Network (KSN), куда поступает информация от различных компонентов наших защитных решений. Данные получены от пользователей, давших свое согласие на передачу этой информации в KSN. В глобальном обмене сведениями о вредоносной активности принимают участие миллионы пользователей продуктов «Лаборатории Касперского» из 213 стран и территорий по всему миру.

# ЦИФРЫ ГОДА

В течение года **29,4%** компьютеров интернет-пользователей в мире хотя бы один раз подверглись веб-атаке **класса Malware**.

Решения «Лаборатории Касперского» отразили **1 188 728 338** атак, которые проводились с интернет-ресурсов, размещенных в разных странах мира.

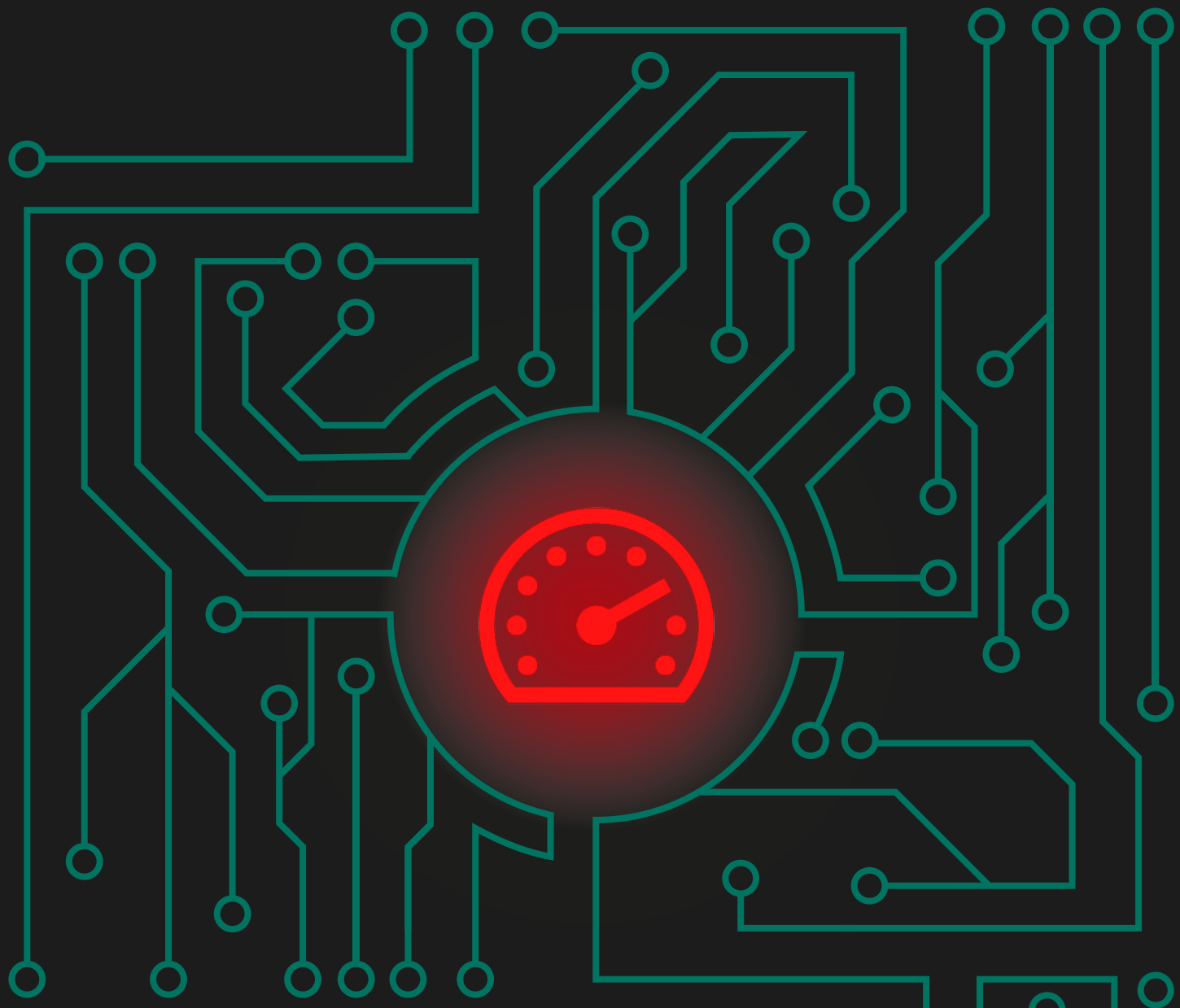
Зафиксировано **199 455 606** уникальных URL, на которых происходило срабатывание веб-антивируса.

Нашим веб-антивирусом зафиксировано **15 714 700** уникальных вредоносных объектов.

Атаки шифровальщиков отражены на компьютерах **939 722** уникальных пользователей.

Попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на устройствах **1 126 701** пользователей.

***Статистика по мобильным угрозам представлена в отчете «Мобильная вирусология 2017»***



# УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ

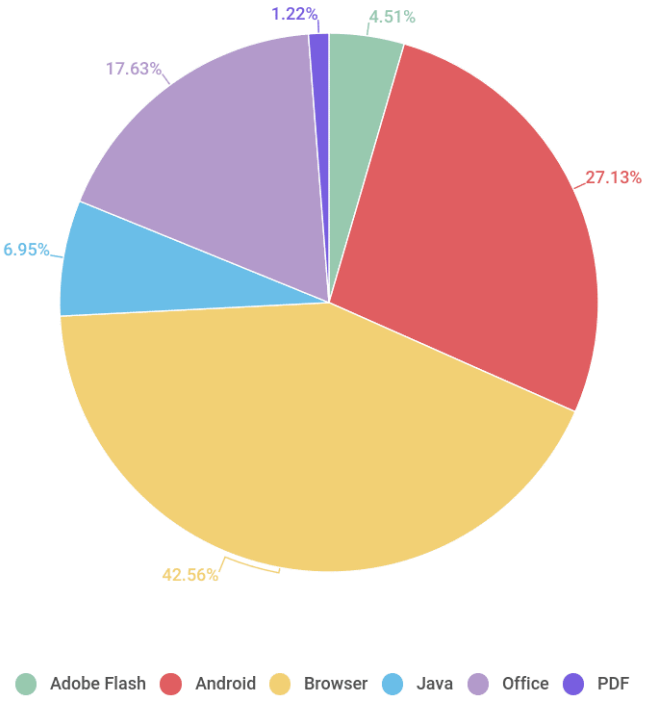
В 2017 году уязвимости нулевого дня активно использовались не только в целевых атаках на организации, но и в атаках на рядовых пользователей. В отличие от прошлого года количество эксплойтов к уязвимостям в Adobe Flash Player и Internet Explorer снижалось, а их место занимали эксплойты к Microsoft Office. Создание надежных эксплойтов для Flash Player стало слишком трудоемким и дорогостоящим для среднего киберпреступника. Теперь нужно не просто обнаружить и использовать уязвимости в самом Flash Player, а еще и обойти функции защиты в современных веб-браузерах. А поскольку все основные создатели наборов эксплойтов в 2017 году покинули рынок, теперь только очень высококвалифицированные киберпреступники способны разработать эксплойт для Flash Player.

Поскольку рынок наборов эксплойтов, на котором традиционно доминировали эксплойты для браузеров и Flash Player, находится в упадке, мы наблюдаем значительный рост атак, нацеленных на пользователей Microsoft Office. В течение года количество атакованных пользователей офисного пакета от Microsoft составило 4% или впечатляющие 14% за последние два года. Основная причина этому – многочисленные уязвимости нулевого дня, обнаруженные в Microsoft Office за последние 12 месяцев. Уязвимости, связанные с повреждением памяти – CVE-2017-0261, CVE-2017-0262, CVE-2017-11826, – использовались злоумышленниками в APT-атаках, но не применялись ими для проведения массовых кампаний по рассылке вредоносного спама, главным образом из-за сложности и низкой надежности эксплойтов. Эксплойты для трех «логических» уязвимостей – CVE-2017-0199, CVE-2017-8570 и CVE-2017-8759 – в этом году применялись в большинстве атак с использованием целевого фишинга. Согласно статистике, полученной из KSN, в 90% случаев в обнаруженных документах Microsoft Office, содержащих эксплойт, использовались именно эксплойты для CVE-2017-0199 или CVE-2017-8759, что делает их самыми популярными. Интересно отметить, что в 2017 году многие документы, содержащие эксплойт к Microsoft Office, также содержали фишинговый компонент на тот случай, если уязвимость на компьютере-мишени закрыта и встроенный в документ эксплойт не сработал.

Количество экспойтов для Android за год увеличилось на 6% и составило 27% от всех эксплойтов. Прошлогодний быстрый рост продолжился в основном из-за увеличения числа эксплойтов, используемых для повышения привилегий до уровня суперпользователя (root) на мобильных устройствах Android.

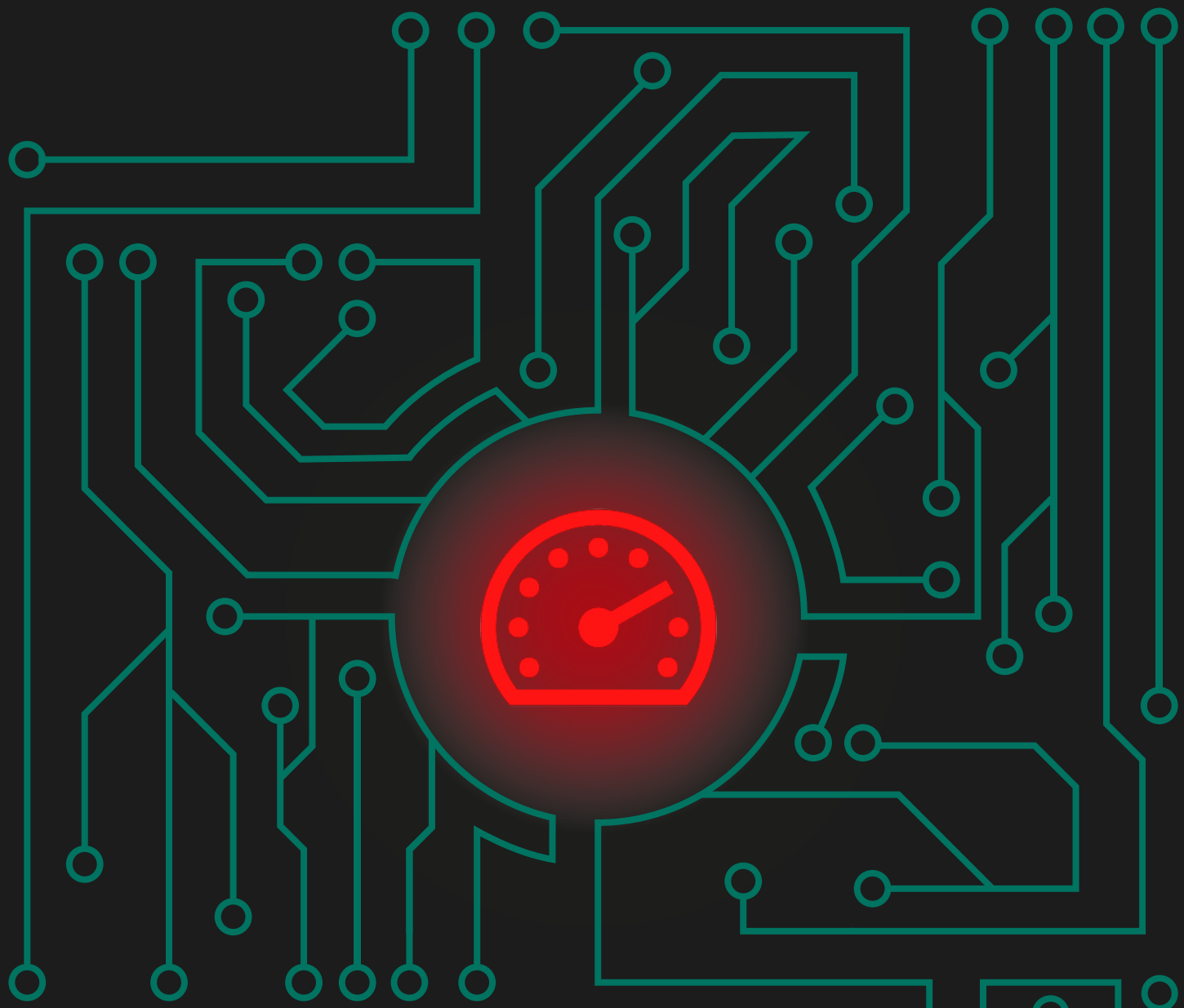
Но главным событием не только второго квартала, а всего 2017 года оказалась публикация хакерской группировкой Shadow Brokers архива Lost In Translation. Архив содержал большое количество сетевых эксплойтов для различных версий Windows. И даже несмотря на то, что большая часть указанных уязвимостей не являлась уязвимостями «нулевого дня» и была закрыта обновлением MS17-010 за месяц до слива, публикация привела к ужасающим последствиям. Ущерб от червей, троянцев и шифровальщиков, распространяющихся по сети при помощи СМБ-эксплойтов EternalBlue и EternalRomance, как и количество зараженных пользователей, не поддается подсчету. Согласно годовой статистике по сетевым атакам, заблокированным нашим компонентом IDS, вердикт Intrusion.Win.MS17-010.* всего за несколько месяцев стал одним из самых популярных сетевых эксплойтов.

Рейтинг уязвимых приложений основывается на вердиктах продуктов «Лаборатории Касперского» для заблокированных эксплойтов, используемых киберпреступниками как в сетевых атаках, так и в уязвимых локальных приложениях, в том числе на мобильных устройствах пользователей.




Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, ноябрь 2016 года – октябрь 2017 года

Итак, 2017 год прервал длительно существовавшую на рынке эксплойтов тенденцию, сместив акцент с Internet Explorer и Adobe Flash Player на Microsoft Office. Киберпреступники все чаще используют методы социальной инженерии, поскольку такой подход является более дешевым, а временами и более надежным, чем использование «традиционных» эксплойтов. Глобальные атаки троянцев-вымогателей WannaCry и ExPetr продемонстрировали, насколько катастрофически опасным может быть сетевой червь, даже если он использует уязвимость, которая давным-давно была исправлена.



# ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ (АТАКИ ЧЕРЕЗ ВЕБ-РЕСУРСЫ)

Статистические данные в этой главе получены на основе работы веб-антивируса, который защищает пользователей от загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Вредоносные сайты специально создаются злоумышленниками; зараженными могут быть веб-ресурсы, контент которых создается пользователями (например, форумы), а также взломанные легитимные ресурсы.

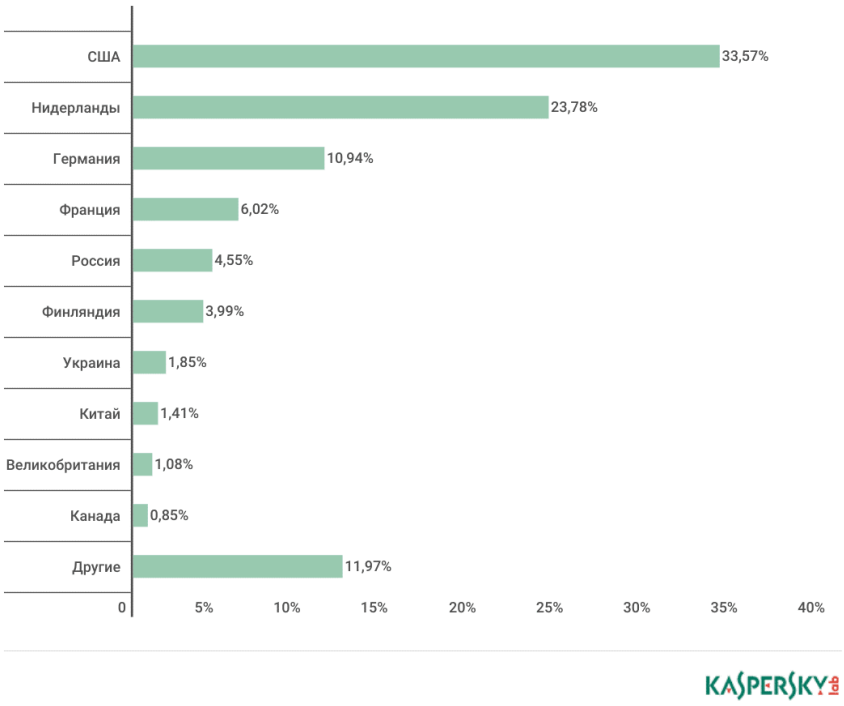
В 2017 году веб-антивирус «Лаборатории Касперского» выявил **15 714 700** уникальных вредоносных объектов (скриптов, эксплойтов, исполняемых файлов и т.д.) и **199 455 606** уникальных URL, на которых происходило срабатывание веб-антивируса. Решения «Лаборатории Касперского» отразили **1 188 728 338** атак, которые проводились с интернет-ресурсов, находящихся в 206 странах мира.

# СТРАНЫ – ИСТОЧНИКИ ВЕБ-АТАК: TOP 10

Данная статистика показывает распределение по странам онлайн-источников заблокированных продуктами «Лаборатории Касперского» атак на компьютеры пользователей (веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами и т.д.). Каждый уникальный хост мог быть источником одной и более веб-атак. Для определения географии источников веб-атак использовалась методика сопоставления доменного имени с реальным IP-адресом, на котором размещен данный домен, и установления географического местоположения данного IP-адреса (GEOIP).

В 2017 году решения «Лаборатории Касперского» отразили 1 188 728 338 атак, которые проводились с интернет-ресурсов, размещенных в разных странах мира.

88,03% уведомлений об атаках, заблокированных антивирусными компонентами, были получены с онлайн-ресурсов, расположенных в 10 странах.




Распределение источников веб-атак по странам, ноябрь 2016 года – октябрь 2017 года

Тройка лидеров по количеству срабатываний веб-антивируса осталась прежней: США (33,57%), Нидерланды (23,78%) и Германия (10,94%). Франция (6,02%) поменялась местами с Россией (4,55%) и заняла четвертое место. Вредоносные веб-ресурсы, расположенные на Виргинских островах и в Болгарии выбыли из TOP 10, вместо них появились ресурсы из Финляндии (3,99%) и Канады (0,85%).

# ТОП 20 ВРЕДОНОСНЫХ ПРОГРАММ, НАИБОЛЕЕ АКТИВНО ИСПОЛЬЗУЕМЫХ В ОНЛАЙН-АТАКАХ

В 2017 году веб-антивирус «Лаборатории Касперского» выявил 15 714 700 уникальных вредоносных объектов: скриптов, эксплойтов, исполняемых файлов и т.д.

В течение года рекламные программы и их компоненты были зарегистрированы на 22% компьютеров пользователей, на которых происходило срабатывание веб-антивируса.

Мы определили 20 вредоносных программ, наиболее активно используемых в онлайн-атаках на компьютеры пользователей в 2017 году.

| | Название* | % от всех атак** |
|---|---|---|
| 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%** |

| | Название* | % от всех атак** |
|---|---|---|
| 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%** |

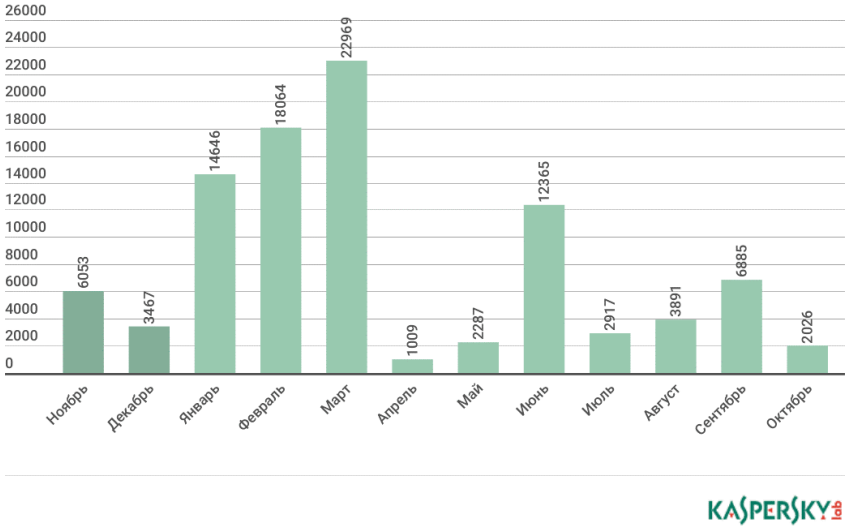
В настоящее время веб-эксплойты гораздо менее популярны, но на десятом месте рейтинга по-прежнему присутствует Exploit.Script.Generic.

Другие скрипты выполняют разные вредоносные действия. Например, Trojan.JS.Small.ci агрессивно внедряет в трафик сторонние рекламные объявления, Trojan.JS.Miner.d является веб-майнером, а Trojan.JS.Agent.sileof детектируется как мошеннический ресурс, который блокирует браузеры с помощью постоянно генерируемых поддельных сообщений о заражении.

* Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса. Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.
** Процент всех веб-атак класса Malware, зарегистрированных на компьютерах уникальных пользователей продуктов «Лаборатории Касперского».

# ВРЕДОНОСНЫЕ ПРОГРАММЫ-ШИФРОВАЛЬЩИКИ

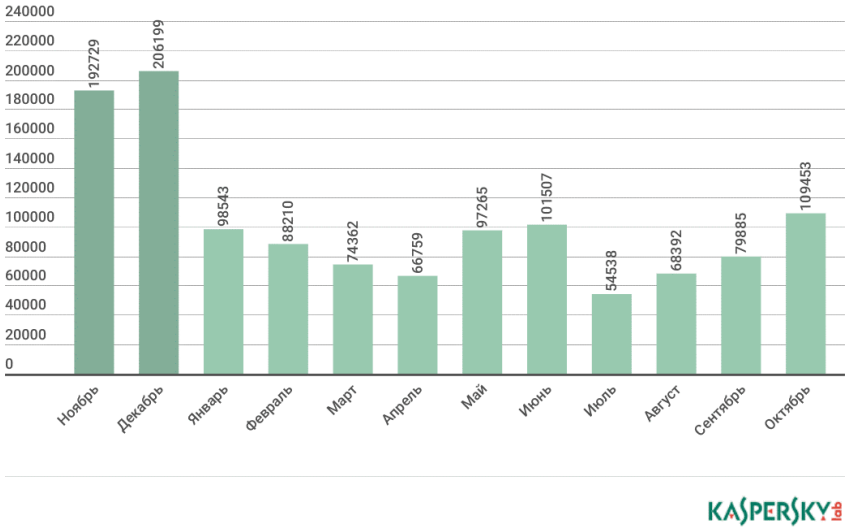
В 2017 году мы выявили более **96 000** модификаций криптовымогателей и обнаружили **38** новых семейств шифровальщиков.




Количество новых модификаций шифровальщиков, ноябрь 2016 года – октябрь 2017 года

## Количество пользователей, атакованных троянцами-шифровальщиками

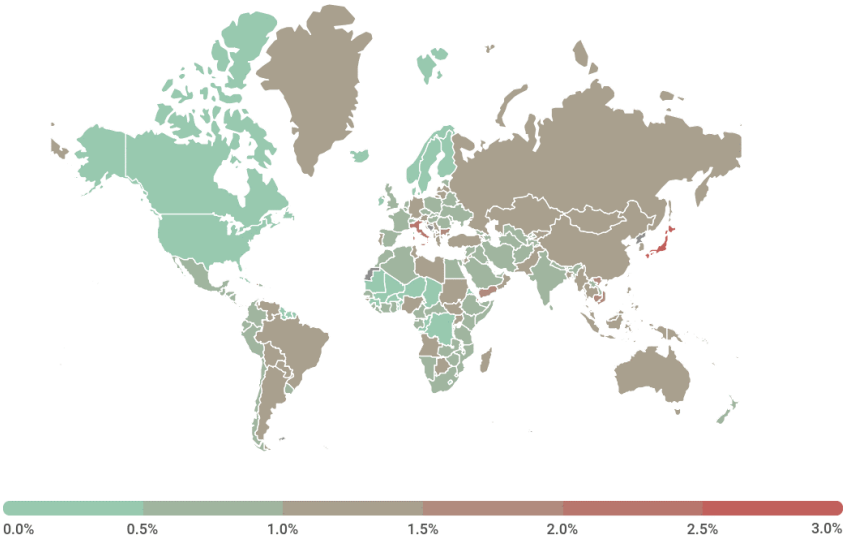
В 2017 году троянцами-шифровальщиками были атакованы **939 722** уникальных пользователей KSN, в том числе **200 000** корпоративных пользователей.




Количество пользователей, атакованных троянцами-шифровальщиками, ноябрь 2016 года – октябрь 2017 года

Важно помнить, что реальное число инцидентов выше: статистика отражает только результаты сигнатурного и эвристического обнаружения, тогда как новые и неизвестные вредоносные образцы троянцев-шифровальщиков детектируются продуктами «Лаборатории Касперского», основываясь на поведенческой модели.

## География атак




География атак троянцев-шифровальщиков в 2017 году (по проценту атакованных пользователей)

### TOP 10 стран, подвергшихся атакам троянцев-шифровальщиков

| | Страна* | % пользователей, атакованных шифровальщиками** |
|---|---|---|
| 1 | Япония | 2,83 |
| 2 | Италия | 2,37 |
| 3 | Вьетнам | 1,95 |
| 4 | Болгария | 1,68 |
| 5 | Тайвань | 1,59 |
| 6 | Камбоджа | 1,53 |
| 7 | Хорватия | 1,48 |
| 8 | Ливан | 1,44 |
| 9 | Бразилия | 1,42 |
| 10 | Индонезия | 1,35 |

* При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (менее 50 000).
** Процент уникальных пользователей, компьютеры которых были атакованы троянцами-шифровальщиками, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.

## TOP 10 most widespread encryptor families

| | Название | Вердикт* | % Процент атакованных пользователей** |
|---|---|---|---|
| 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** |

Эпидемия WannaCry затронула сотни тысяч компьютеров по всему миру. Неудивительно, что это семейство шифровальщиков стало самым распространенным в 2017 году.

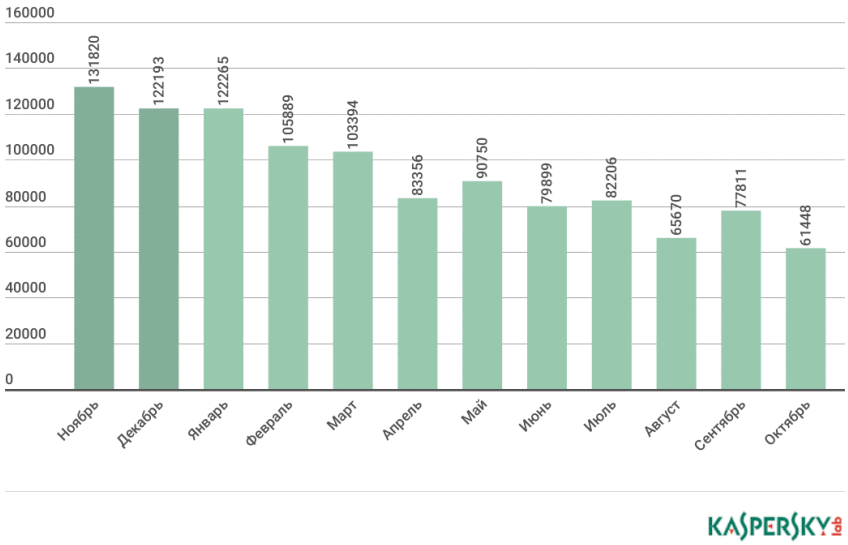
Более подробно о ситуации с троянцами-вымогателями можно узнать, прочитав наш отчет «Kaspersky Security Bulletin 2017. Сюжет года: Шифровальщики атакуют».

* Статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского». Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.
** Процент уникальных пользователей «Лаборатории Касперского», подвергшихся атакам конкретного семейства троянцев-вымогателей, от всех пользователей, подвергшихся атакам троянцев-вымогателей.

# ОНЛАЙН-УГРОЗЫ В ФИНАНСОВОМ СЕКТОРЕ

Настоящая статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского», полученных от пользователей, подтвердивших свое согласие на передачу статистических данных. Статистика 2017 года охватывает период с ноября 2016 по октябрь 2017 года и включает вредоносные программы для банкоматов и терминалов оплаты, но не включает мобильные угрозы.

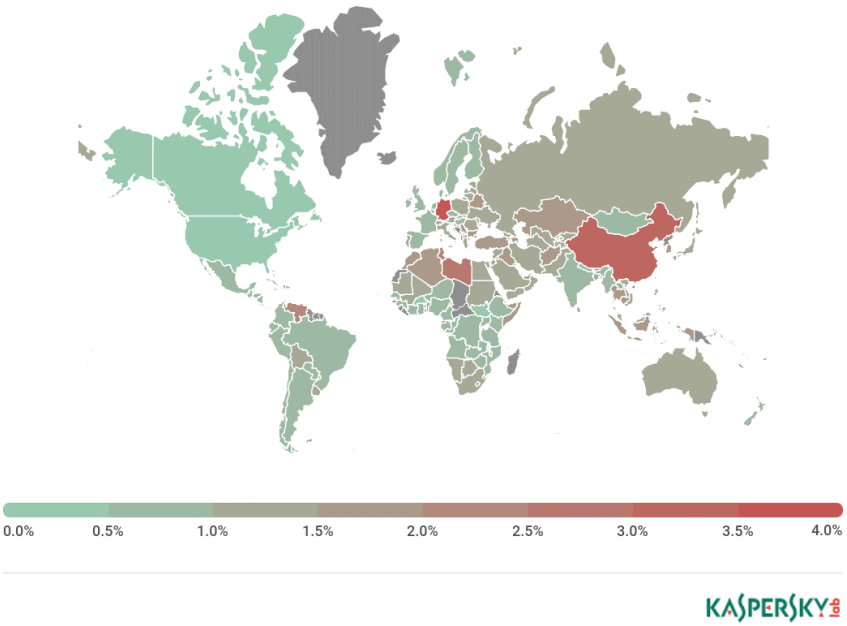
В 2017 году решения «Лаборатории Касперского» отразили попытки запуска одной или нескольких вредоносных программ для кражи денежных средств с банковских счетов на компьютерах **1 126 701** пользователей.




Число пользователей, атакованных финансовым вредоносным ПО, ноябрь 2016 года-октябрь 2017 года

## География атак

Чтобы оценить и сравнить степень риска заражения банковскими троянцами и зловредами для банкоматов и платежных терминалов в разных странах мира, мы подсчитали в каждой стране процент пользователей продуктов «Лаборатории Касперского», которые столкнулись с этой угрозой в отчетный период, от всех пользователей наших продуктов в стране.




География атак банковского вредоносного ПО в 2017 году

## TOP-10 стран по проценту атакованных пользователей

| | Country* | % attacked users** |
|---|---|---|
| 1 | Германия | **4,44** |
| 2 | Того | **3,17** |
| 3 | Китай | **3,05** |
| 4 | Ливия | **2,81** |
| 5 | Ливан | **2,45** |
| 6 | Тунис | **2,21** |
| 7 | Тайвань | **2,15** |
| 8 | Объединенные Арабские Эмираты | **2,12** |
| 9 | Венесуэла | **2,06** |
| 10 | Иордания | **1,88** |

* При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (меньше 10 тысяч уведомлений об обнаружении банковского вредоносного ПО).
** Процент уникальных пользователей, чьи компьютеры подверглись атакам финансового вредоносного ПО, от всех пользователей, атакованных всеми видами вредоносного ПО.

## TOP 10 семейств банковского вредоносного ПО

TOP 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга в 2017 году (по проценту атакованных пользователей):

| | Название* | % атакованных пользователей** |
|---|---|---|
| 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 |

* Статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского». Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.
** Процент уникальных пользователей, атакованных данным зловредом, от всех пользователей, атакованных финансовым вредоносным ПО.

# СТРАНЫ, В КОТОРЫХ ПОЛЬЗОВАТЕЛИ ПОДВЕРГАЛИСЬ НАИБОЛЬШЕМУ РИСКУ ЗАРАЖЕНИЯ ЧЕРЕЗ ИНТЕРНЕТ

Чтобы оценить степень риска заражения вредоносными программами через интернет, которому подвергаются компьютеры пользователей в разных странах мира, мы подсчитали в каждой стране процент пользователей продуктов «Лаборатории Касперского», которые столкнулись со срабатыванием веб-антивируса в отчетный период. Полученные данные являются показателем агрессивности среды, в которой работают компьютеры в разных странах.

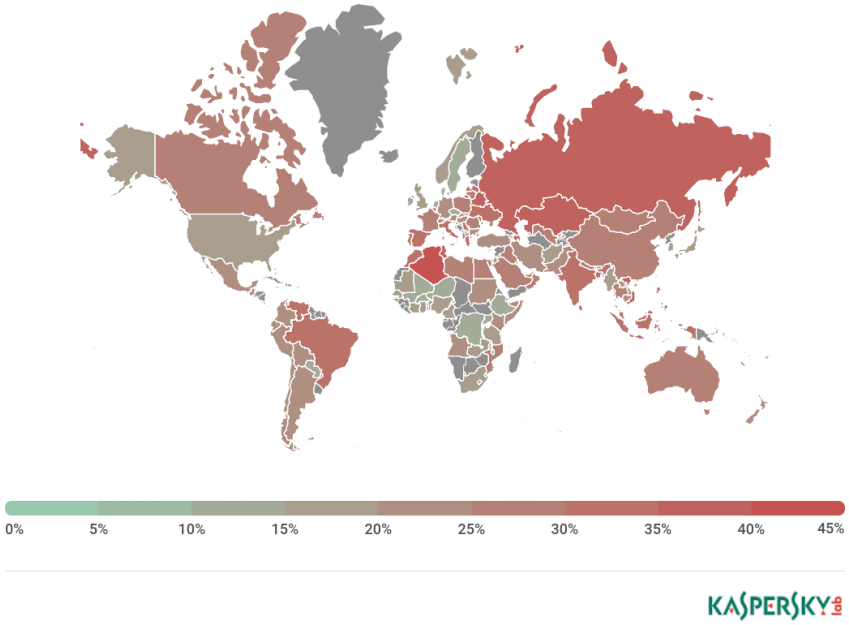
В рейтинге учитываются только атаки вредоносных объектов класса Malware. При подсчетах мы не учитывали срабатывания веб-антивируса на потенциально опасные и нежелательные программы, такие как RiskTool и рекламное ПО.

## TOP 20 стран, в которых пользователи подвергались наибольшему риску заражения через интернет

| | Страна* | % уникальных пользователей** |
|---|---|---|
| 1 | Алжир | 44,06 |
| 2 | Беларусь | 38,39 |
| 3 | Россия | 36,91 |
| 4 | Казахстан | 36,57 |
| 5 | Тунис | 36,51 |
| 6 | Вьетнам | 35,01 |
| 7 | Азербайджан | 34,70 |
| 8 | Катар | 34,20 |
| 9 | Португалия | 33,01 |
| 10 | Греция | 32,80 |
| 11 | Бразилия | 32,66 |
| 12 | Молдова | 32,42 |
| 13 | Индия | 32,34 |
| 14 | Марокко | 31,72 |
| 15 | Венесуэла | 31,52 |
| 16 | Испания | 31,20 |
| 17 | Шри-Ланка | 30,75 |
| 18 | Малайзия | 30,52 |
| 19 | Бангладеш | 30,37 |
| 20 | Украина | 30,27 |

Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса. Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

* При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского», относительно мало (меньше 50 000).
** Процент уникальных пользователей, подвергшихся веб-атакам вредоносных объектов класса Malware, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.



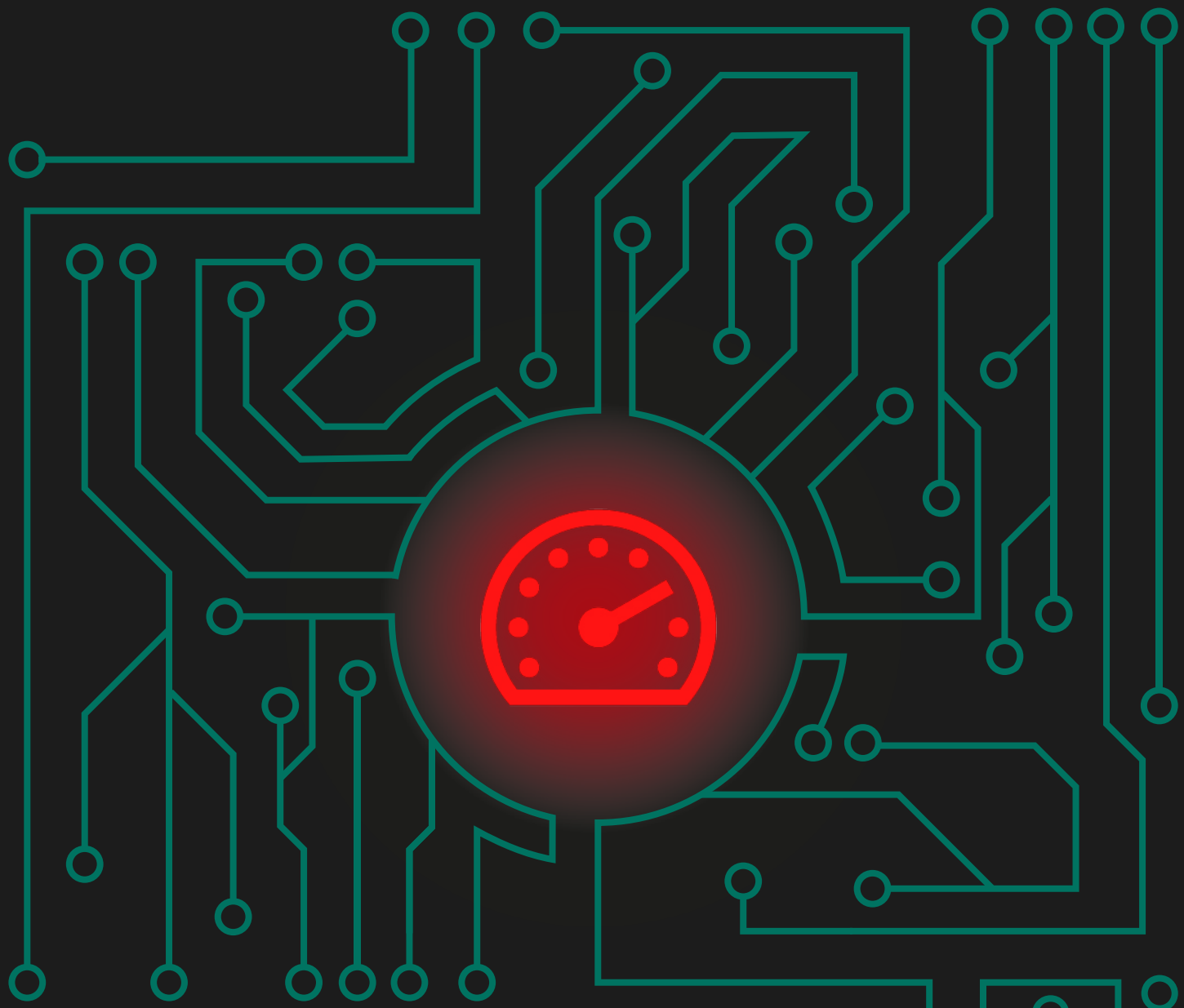

География веб-атак вредоносного ПО в 2017 году (процент атакованных пользователей)

По степени риска заражения при просмотре сайтов в интернете все страны можно распределить на три группы.

**1. Группа повышенного риска (выше 40%)**
В 2017 году в эту группу вошла только одна страна – Алжир.

**2. Группа риска (20-39,9%)**
В эту группу попали 75 стран, в том числе Беларусь (38,39%), Россия (36,91%), Казахстан (36,57%), Вьетнам (35,01%), Испания (31,19%), Румыния (29,5%), Ирак (26,85%), Ангола (24,22%), Германия (22,82%), Швейцария (21,55%), Кения (20,6%), Боливия (20,15%).

**3. Группа наиболее безопасных стран (0-19,9%)**
В числе самых безопасных с точки зрения просмотра веб-сайтов стран – Афганистан (19,55%), США (19,4%), Великобритания (19,22%), Япония (15,41%), Уганда (13,49%). В 2017 году 29,4% компьютеров интернет-пользователей в мире хотя бы один раз подверглись веб-атаке класса **Malware**.



# ЛОКАЛЬНЫЕ УГРОЗЫ

# ТОР 20 ВРЕДОНОСНЫХ ОБЪЕКТОВ, ОБНАРУЖЕННЫХ НА КОМПЬЮТЕРАХ ПОЛЬЗОВАТЕЛЕЙ

Статистика локальных заражений компьютеров пользователей является важным показателем. Сюда попадают объекты, которые проникли на компьютер путем заражения файлов или съемных носителей либо изначально попали на компьютер не в открытом виде (например, программы в составе сложных инсталляторов, зашифрованные файлы и т.д.). Кроме того, эти статистические данные включают объекты, обнаруженные на компьютерах пользователей после первой проверки системы с помощью антивирусной программы «Лаборатории Касперского».

В этом разделе мы анализируем статистические данные, полученные по итогам антивирусной проверки файлов на жестком диске в момент их создания или обращения к ним, и данные о проверке различных съемных носителей информации.

Мы выделили двадцать угроз, которые в 2017 году чаще всего детектировались на компьютерах пользователей. В данный рейтинг не входят программы классов Adware и Riskware.

| | Название* | % атакованных уникальных пользователей** |
|---|---|---|
| 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% |

Настоящая статистика основана на детектирующих вердиктах модулей OAS и ODS антивируса (проверка при доступе и по требованию). Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

Первое место (35,87%) в нашем TOP 20 занял вердикт DangerousObject.Multi.Generic, используемый для вредоносных программ, обнаруженных с помощью облачных технологий. Эти технологии работают, когда в антивирусных базах еще нет ни сигнатуры, ни эвристики для детектирования вредоносной программы, но в облачной антивирусной базе компании уже есть информация об этом объекте. Таким образом детектируются самые новые вредоносные программы.

Общая доля вредоносного ПО для Win32-платформ сократилась, наряду с увеличением числа обнаруженных скриптов для других платформ.

Доля Trojan.Win32.Generic снизилась, потому что в этом году некоторые представители этого семейства не были классифицированы как generic.

На пятом, шестом, седьмом и пятнадцатом местах в TOP 20 расположились несколько популярных модификаций WinLNK. Это вредоносное ПО может изменять настройки браузера или быть использовано для загрузки других вредоносных программ.

Двенадцатое место занял новичок Trojan.Multi.Powecod.a (2,59%). Это вредоносное ПО использует PowerShell для выполнения различных вредоносных действий.

* Детектирующие вердикты модулей OAS и ODS антивируса на компьютерах пользователей продуктов «Лаборатории Касперского», подтвердивших свое согласие на передачу статистических данных.
** Процент уникальных пользователей, на компьютерах которых файловый антивирус детектировал данный объект, от всех уникальных пользователей продуктов «Лаборатории Касперского», у которых происходило срабатывание антивируса на вредоносные программы.

# СТРАНЫ, В КОТОРЫХ КОМПЬЮТЕРЫ ПОЛЬЗОВАТЕЛЕЙ ПОДВЕРГАЛИСЬ НАИБОЛЬШЕМУ РИСКУ ЛОКАЛЬНОГО ЗАРАЖЕНИЯ

Для каждой из стран мы подсчитали, как часто ее пользователи сталкивались со срабатыванием файлового антивируса в течение года. Учитывались детектируемые объекты, найденные непосредственно на компьютерах пользователей или же на подключенных к ним съемных носителях (флешках, картах памяти фотоаппаратов и телефонов, внешних жестких дисках). Эта статистика отражает уровень зараженности персональных компьютеров в различных странах мира.

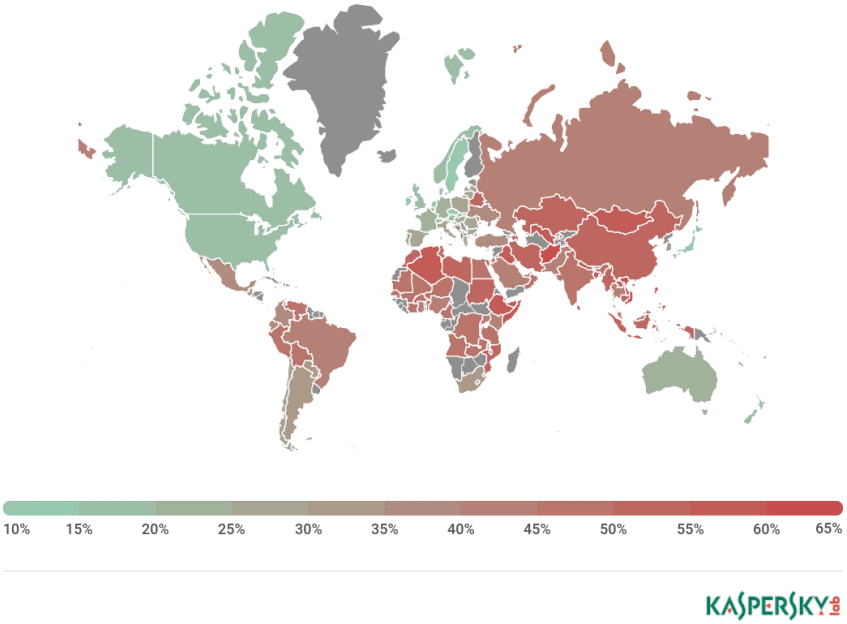
### TOP 20 стран по уровню зараженности компьютеров

| | Страна* | % уникальных пользователей** |
|---|---|---|
| 1 | Вьетнам | 67,41 |
| 2 | Афганистан | 63,03 |
| 3 | Алжир | 61,36 |
| 4 | Лаос | 61,08 |
| 5 | Монголия | 60,67 |
| 6 | Узбекистан | 58,86 |
| 7 | Руанда | 58,42 |
| 8 | Ирак | 58,39 |
| 9 | Эфиопия | 58,35 |
| 10 | Бангладеш | 58,09 |
| 11 | Сомали | 57,78 |
| 12 | Непал | 57,60 |
| 13 | Мозамбик | 56,12 |
| 14 | Ливия | 55,85 |
| 15 | Камбоджа | 55,79 |
| 16 | Казахстан | 54,87 |

| | Страна* | % уникальных пользователей** |
|---|---|---|
| 17 | Судан | **54,76** |
| 18 | Мьянма | **54,73** |
| 19 | Индонезия | **53,92** |
| 20 | Марокко | **53,48** |

Настоящая статистика основана на детектирующих вердиктах файлового антивируса. Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

* 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.




География локальных заражений вредоносным ПО в 2017 году (процент атакованных пользователей)

В отношении локальных угроз мы можем разделить все страны мира на несколько категорий.

**Максимальный уровень заражения (более 60%):** в эту группу вошли первые пять из TOP 20 стран, в которых компьютеры пользователей подвергались наибольшему риску локального заражения.

**Высокий уровень заражения (41-59,99%):** в эту группу попали Узбекистан (58,87%), Камбоджа (55,79%), Камерун (50,87%), Египет (49,12%), Уганда (45,12%), Россия (42,26%), Бразилия (41,94%).

**Средний уровень заражения (20-39,99%):** в группу вошли Украина (39,84%), Мексика (36,52%), Турция (35,91%), Сербия (32,02%), Чили (28,67%), Греция (26%), Израиль (24,4%), Венгрия (21,96%).

**Низкий уровень заражения (0-19.9%):** Австралия (19,55%), Сингапур (15,5%), Япония (12,5%), Ирландия (10,25%), Дания (8,88%).

В 2017 году хотя бы одна вредоносная программа была обнаружена в среднем на 36,8% компьютеров, жестких дисков или съемных носителей, принадлежащих пользователям KSN.

KASPERSKY lab