KASPERSKY lab

Kaspersky Security Bulletin 2018

СТАТИСТИКА

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. Статистика 2018 года охватывает период с ноября 2017 по октябрь 2018 года.

ЦИФРЫ ГОДА

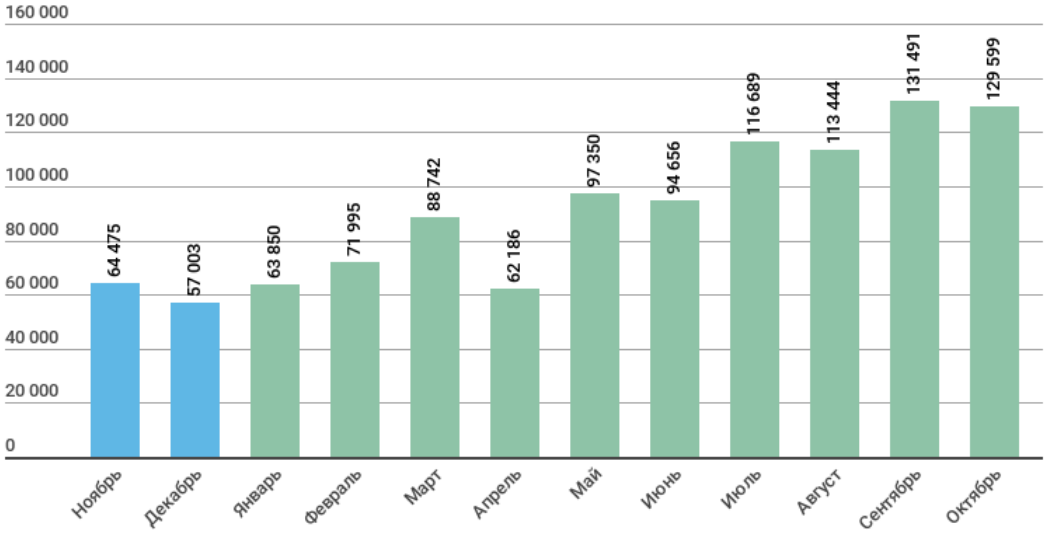
- В течение года 30,01% компьютеров интернет-пользователей в мире хотя бы один раз подверглись веб-атаке **класса Malware**.
- Решения «Лаборатории Касперского» отразили **1 876 998 691** атаку, которые проводились с интернет-ресурсов, размещенных в различных странах мира.
- Зафиксирован **554 159 621** уникальный URL, на которых происходило срабатывание веб-антивируса.
- Нашим веб-антивирусом зафиксировано **21 643 946** уникальных вредоносных объектов.
- Атаки шифровальщиков отражены на компьютерах **765 538** уникальных пользователей.
- За отчетный период майнерами были атакованы **5 638 828** уникальных пользователей.
- Попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на устройствах **830 135** пользователей.

БАНКОВСКОЕ ВРЕДОНОСНОЕ ПО

Представленная статистика включает не только банковские угрозы, но также вредоносные программы для банкоматов и терминалов оплаты. Статистика по аналогичным мобильным угроза представлена в отдельном отчете.

Количество пользователей, атакованных банковскими зловредами

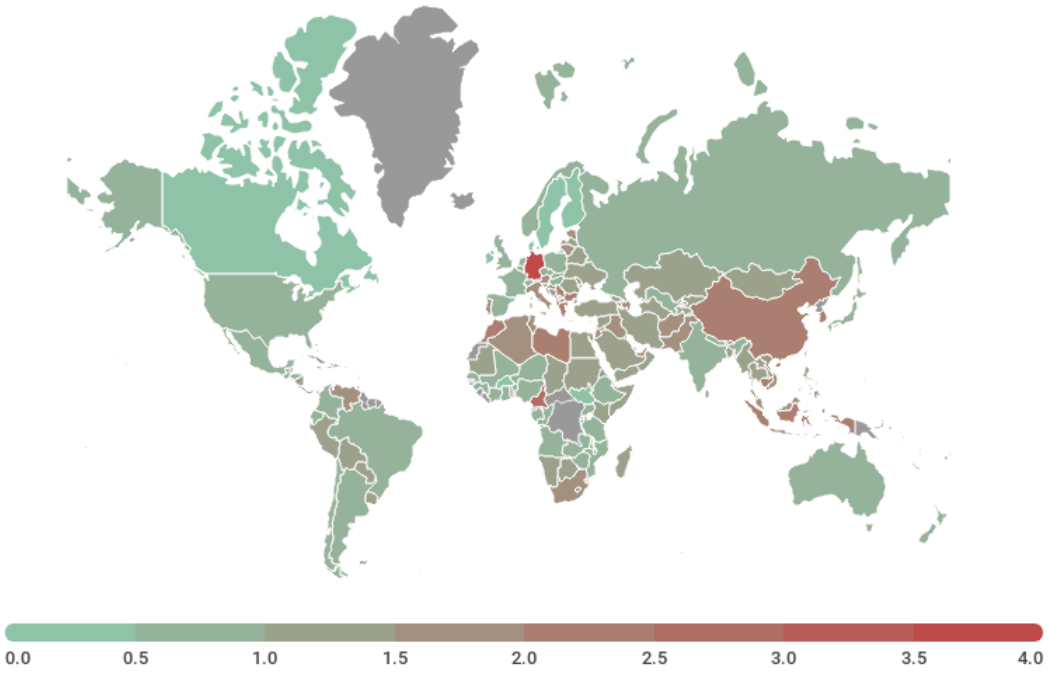
В 2018 году решения «Лаборатории Касперского» отразили попытки запуска одной или нескольких вредоносных программ, предназначенных для кражи денежных средств с банковских счетов, на компьютерах **830 135** пользователей.



Количество пользователей, атакованных банковским вредоносным ПО, ноябрь 2017 года – октябрь 2018 года

География атак

Чтобы оценить и сравнить степень риска заражения банковским зловредом, которому подвергаются компьютеры пользователей в разных странах мира, мы подсчитали в каждой стране долю пользователей продуктов «Лаборатории Касперского», которые столкнулись с этой угрозой в отчетный период, от всех пользователей наших продуктов в стране.



География атак банковского вредоносного ПО, ноябрь 2017 года – октябрь 2018 года

TOP 10 стран по доле атакованных пользователей

	Страна*	%**
1	Германия	4,0
2	Камерун	2,6
3	Южная Корея	2,4
4	Мальдивские острова	2,4
5	Республика Того	2,3

	Страна*	%**
6	Индонезия	2,2
7	Ливия	2,2
8	Объединенные Арабские Эмираты	2,1
9	Греция	2,1
10	Китай	2,0

** При расчетах мы исключили страны, в которых количество пользователей «Лаборатории Касперского» относительно мало (меньше 10 тысяч).*

*** Доля уникальных пользователей, чьи компьютеры подверглись атакам банковского вредоносного ПО, от всех пользователей, атакованных всеми видами вредоносного ПО.*

TOP 10 семейств банковского вредоносного ПО

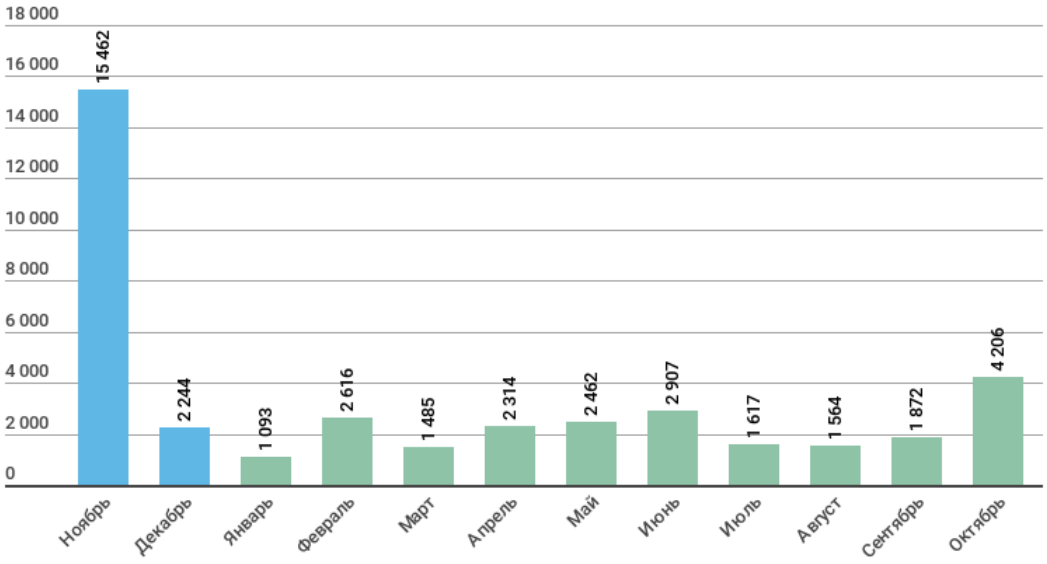
TOP 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга в 2018 году.

	Название	%*
1	Trojan.Win32.Zbot	26,3
2	Trojan.Win32.Nymaim	19,8
3	Backdoor.Win32.SpyEye	14,7
4	Backdoor.Win32.Caphaw	5,2
5	Trojan-Banker.Win32.RTM	5,2
6	Backdoor.Win32.Emotet	4,9
7	Trojan.Win32. Neurevt	3,9
8	Trojan-Banker.Win32.Tinba	1,9
9	Trojan.Win32.Gozi	1,8
10	Trojan-Banker.Win32.Trickster	1,5

** Доля уникальных пользователей, атакованных данным зловредом, от всех пользователей, атакованных банковским вредоносным ПО.*

ВРЕДОНОСНЫЕ ПРОГРАММЫ-ШИФРОВАЛЬЩИКИ

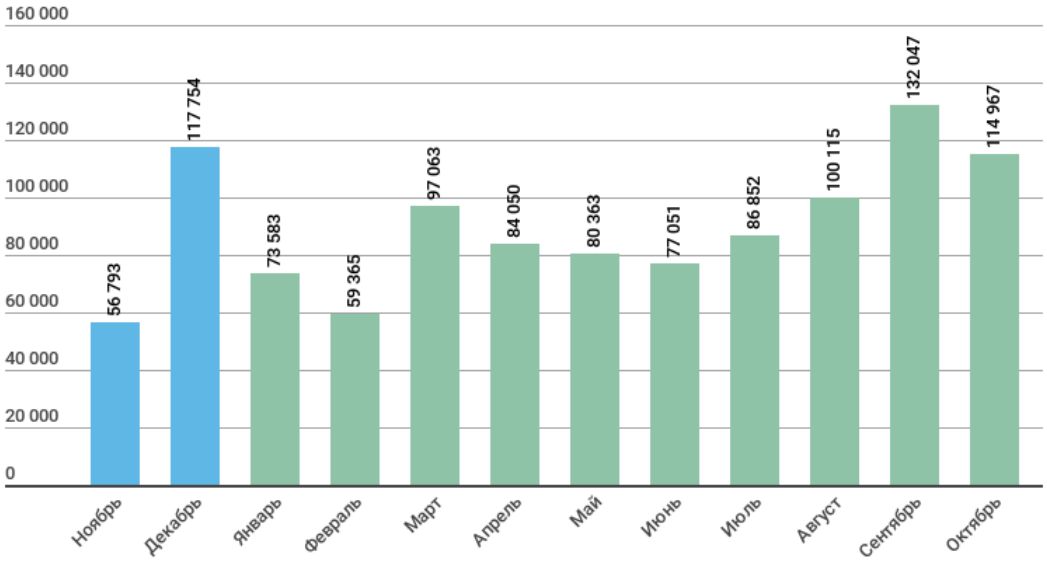
В 2018 году мы выявили более **39 842** модификаций шифровальщиков и обнаружили **11** новых семейств. Отметим, что не под каждый новый шифровальщик мы создавали новое семейство, большей части угроз этого типа присваивается generic-вердикт, который мы используем при обнаружении новых и неизвестных образцов.



Количество новых модификаций шифровальщиков, ноябрь 2017 года – октябрь 2018 года

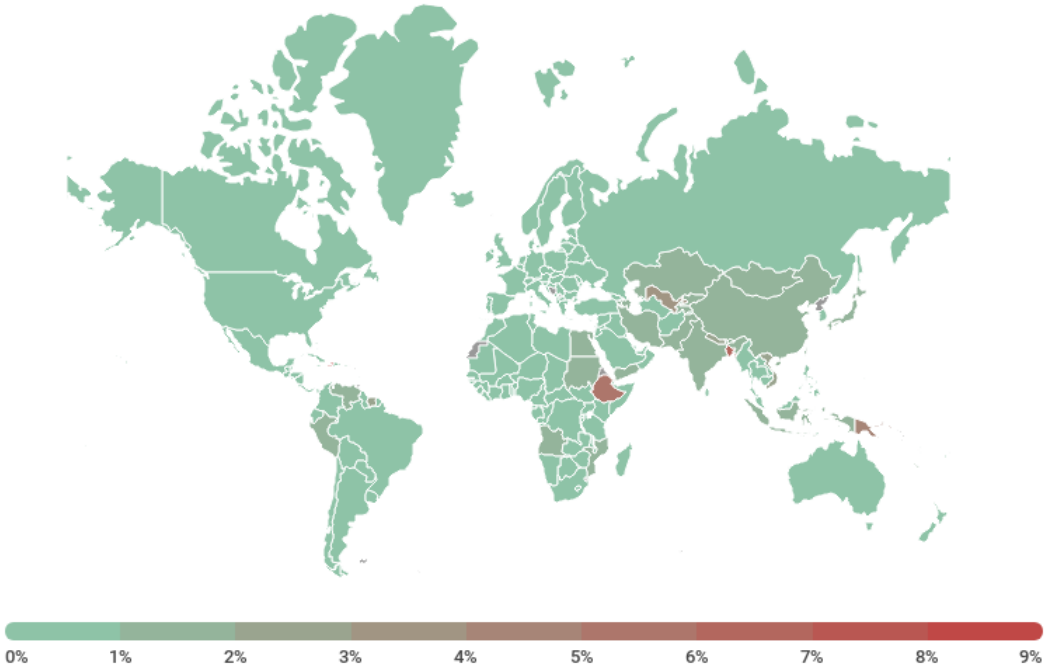
Количество пользователей, атакованных троянцами-шифровальщиками

В 2018 году троянцами-шифровальщиками были атакованы **765 538** уникальных пользователей, в том числе более 220 тысяч корпоративных пользователей и более 27 тысяч из числа малого и среднего бизнеса.



Количество пользователей, атакованных троянцами-шифровальщиками, ноябрь 2017 года – октябрь 2018 года

География атак



География атак троянцев-шифровальщиков, ноябрь 2017 года – октябрь 2018 года

TOP 10 стран, подвергшихся атакам троянцев-шифровальщиков

	Страна*	%**
1	Бангладеш	6,65
2	Эфиопия	5,25
3	Узбекистан	3,50
4	Непал	2,79
5	Вьетнам	2,12
6	Индонезия	1,95
7	Индия	1,87
8	Ангола	1,84

	Страна*	%**
9	Пакистан	1,78
10	Китай	1,72

** При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (менее 50 000).*

*** Доля уникальных пользователей, компьютеры которых были атакованы троянцами-шифровальщиками, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.*

TOP 10 наиболее распространенных семейств троянцев-шифровальщиков

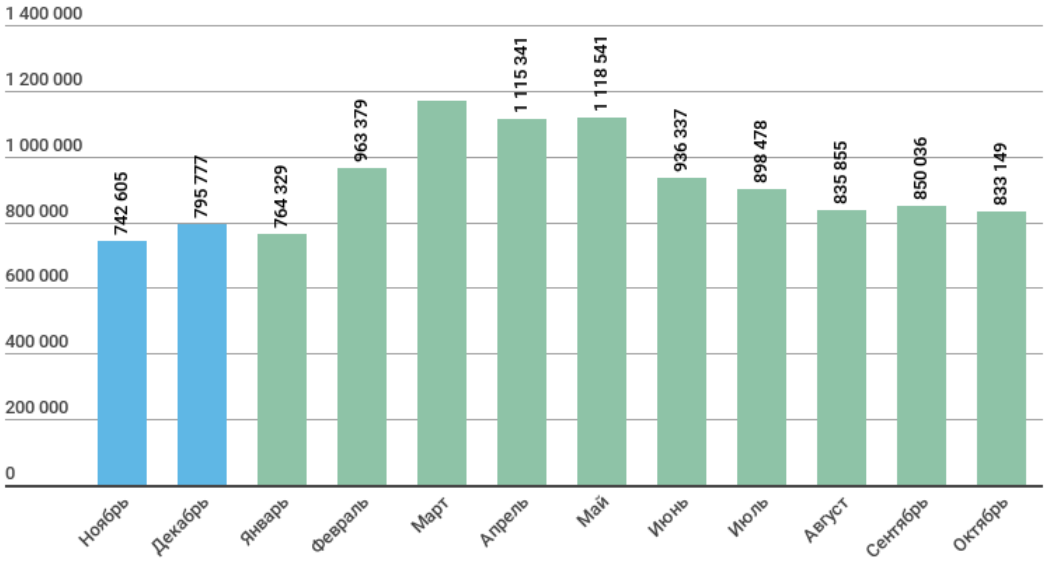
	Название	Вердикт	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	29,32
2	(generic verdict)	Trojan-Ransom.Win32.Phny	11,43
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	6,67
4	Cryakl	Trojan-Ransom.Win32.Cryakl	4,59
5	PolyRansom/VirLock	Virus.Win32.PolyRansom	2,86
6	(generic verdict)	Trojan-Ransom.Win32.Gen	2,40
7	Shade	Trojan-Ransom.Win32.Shade	2,29
8	Cerber	Trojan-Ransom.Win32.Zerber	2,20
9	Purgen/GlobeImposter	Trojan-Ransom.Win32.Purgen	1,82
10	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	1,72

** Доля уникальных пользователей «Лаборатории Касперского», подвергшихся атакам определенного семейства троянцев-вымогателей, от всех пользователей, подвергшихся атакам троянцев-вымогателей.*

ПРОГРАММЫ-МАЙНЕРЫ

Количество пользователей, атакованных майнерами

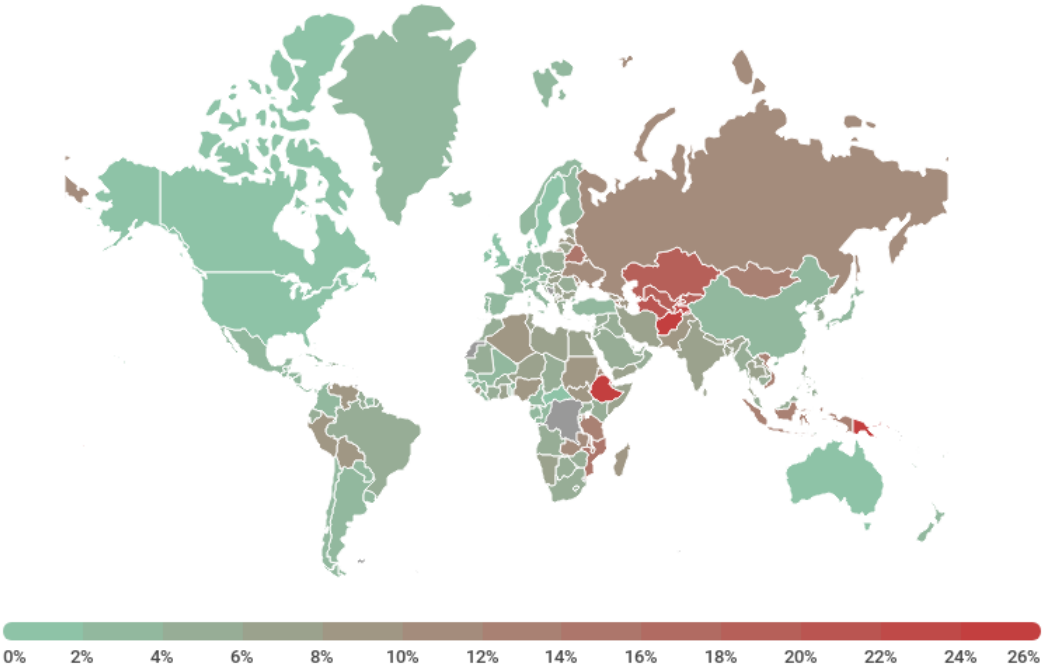
За отчетный период мы зафиксировали попытки установки майнера на компьютерах 5 638 828 уникальных пользователей. В общем объеме атак доля майнеров составила 8,50%, а среди всех программ типа Risktool – 16,88%.



Количество пользователей, атакованных майнерами, ноябрь 2017 года – октябрь 2018 года

Чаще других продукты «Лаборатории Касперского» обнаруживали Trojan.JS.Miner.m – на его долю пришлось почти 22% от общего количества пользователей, атакованных майнерами. Следом с заметным отрывом идут представители семейства Trojan.Win32.Miner: Miner.gen (9,44%), Miner.ays (5,30%) и Miner.bbb (2,71%).

География атак



География атак с участием майнеров, ноябрь 2017 года – октябрь 2018 года

УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ В ХОДЕ КИБЕРАТАК

Отчетный период запомнился нам большим количеством целевых атак с использованием эксплойтов для уязвимостей нулевого дня. Были обнаружены:

- Эксплуатируемые злоумышленниками уязвимости в подходящем к концу своего жизненного цикла Adobe Flash (CVE-2018-4878, CVE-2018-5002);
- Первая за достаточно долгое время эксплуатируемая уязвимость в Acrobat Reader (CVE-2018-4990);
- Уязвимости в VBScript, одном из скриптовых движков Windows, использующемся в том числе в браузере Internet Explorer (CVE-2018-8174, CVE-2018-8373);
- Сразу несколько уязвимостей в драйвере графической подсистемы Windows - win32k.sys, которые использовались злоумышленниками как для повышения привилегий в ОС, так и совместно с другими уязвимостями для обхода "песочницы" (CVE-2018-8120, CVE-2018-8453, CVE-2018-8589).

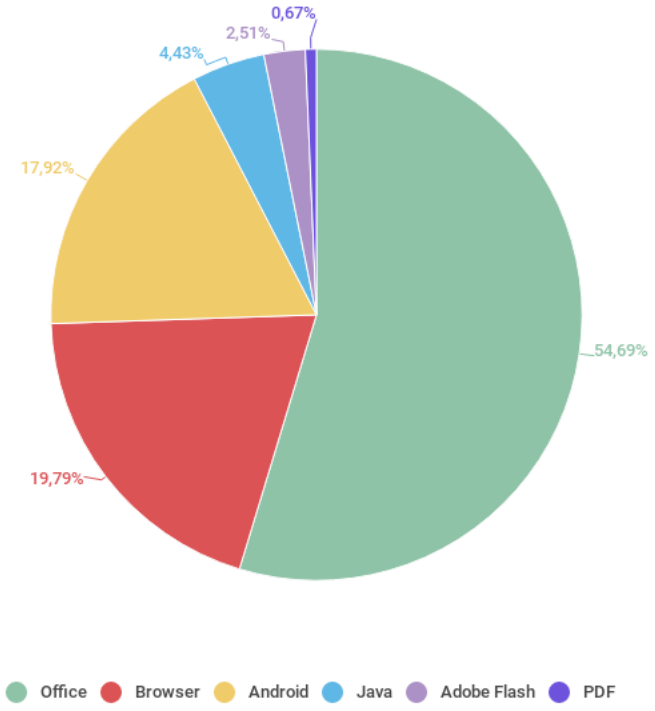
Как и в прошлом году доля пользователей, атакованных эксплойтами для уязвимостей в Adobe Flash Player и Internet Explorer снизилась, даже несмотря на появление нескольких новых публично эксплуатируемых уязвимостей нулевого дня в обоих продуктах. К примеру, уязвимость CVE-2018-4878 в Adobe Flash Player, proof-of-concept для которой был выложен исследователем в публичный доступ, была интегрирована во многие популярные эксплойт-паки менее чем через два месяца после выхода патча. Но даже несмотря на это, доля упомянутых платформ в ежегодной статистике уменьшилась более чем в два раза.

Доля платформы Android на нашем графике распределения эксплойтов упала до 18% (-9 п.п. по сравнению с прошлым годом), что подталкивает к выводу о росте безопасности ОС от Google. Отчасти причиной послужила более агрессивная политика обновления устройств до последних версий ОС. К примеру, по данным на октябрь 2018 года ОС Android 8.0+ Oreo установлена на устройствах 22% пользователей Android. Для сравнения, в октябре 2017-го года последняя на тот момент версия Android 7.0+ Nougat была установлена всего у 16% пользователей.

Одновременно с этим мы наблюдали резкий рост количества пользователей, атакованных эксплойтами для Microsoft Office, – четырехкратный по сравнению со средним показателем за 2017 год. Это привело к увеличению доли офисного пакета в нашей статистике – с 17,63% до казавшихся невероятным 55%. Причиной такого роста послужили массовые спам-рассылки, распространяющие документы с эксплойтами для уязвимостей

CVE-2017-11882 и CVE-2018-0802. Популярность среди киберпреступников эти уязвимости приобрели благодаря стабильности работы и простоте использования – для эксплуатация достаточно модифицировать выложенный в общий доступ скрипт билдера эксплойта. Немалую роль сыграла и возможность применения обфускаций для обхода обнаружения защитными решениями и широкий охват различных версий Microsoft Office – без соответствующего патча уязвимы все версии офисного пакета, вышедшие за последние 18 лет.

Эксплойты для других популярных уязвимостей (CVE-2017-8570, CVE-2018-4878, CVE-2018-8174), распространяющиеся посредством документов MS Office, также сыграли свою роль в увеличении доли этого пакета в нашей статистике.



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, ноябрь 2017 года – октябрь 2018 года

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.

В 2018 году обошлось без происшествий, подобных прошлогодней публикации хакерской группировкой Shadow Brokers архива Lost In Translation, содержащего большое количество сетевых эксплойтов. Однако количество вредоносных файлов, использующих эксплойты из этого архива, как и количество атак с их использованием, продолжило расти: по сравнению с прошлым годом наш компонент обнаружения сетевых вторжений заблокировал на порядок больше попыток эксплуатации сетевого SMB-эксплойта EternalBlue.

АТАКИ ЧЕРЕЗ ВЕБ-РЕСУРСЫ

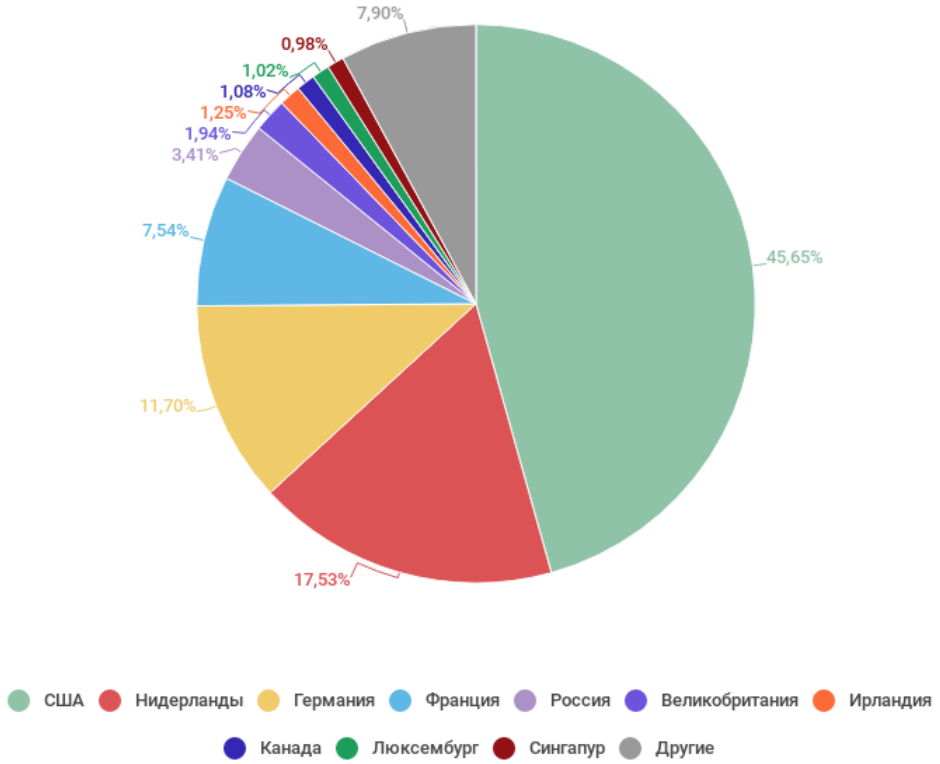
Статистические данные в этой главе получены на основе работы веб-антивируса, который защищает пользователей от загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Вредоносные сайты специально создаются злоумышленниками; зараженными могут быть веб-ресурсы, контент которых создается пользователями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

Страны – источники веб-атак

Данная статистика показывает распределение по странам онлайн-источников атак на компьютеры пользователей (веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами и т.д.), заблокированных продуктами «Лаборатории Касперского». 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).

За отчетный период решения «Лаборатории Касперского» отразили **1 876 998 691** атаку, которые проводились с интернет-ресурсов, размещенных в разных странах мира. При этом 92,1% от общего количества уведомлений об атаках, заблокированных антивирусными компонентами, был получен с онлайн-ресурсов, расположенных всего в 10 странах.



Распределение источников веб-атак по странам, ноябрь 2017 года – октябрь 2018 года

По сравнению с результатами предыдущего года распределение источников веб-атак не сильно изменилось. На первом месте по-прежнему США (45,65%), следом идут Нидерланды (17,53%) и Германия (11,70%). Первую десятку покинули Финляндия, Украина и Китай, их места заняли Ирландия (1,25%), Люксембург (1,02%) и Сингапур (0,98%).

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.

Напомним, что в этом 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 рекламные программы. В целом, за отчетный период рекламные программы и их компоненты были зарегистрированы на 53% компьютеров пользователей, на которых происходило срабатывание веб-антивируса.

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

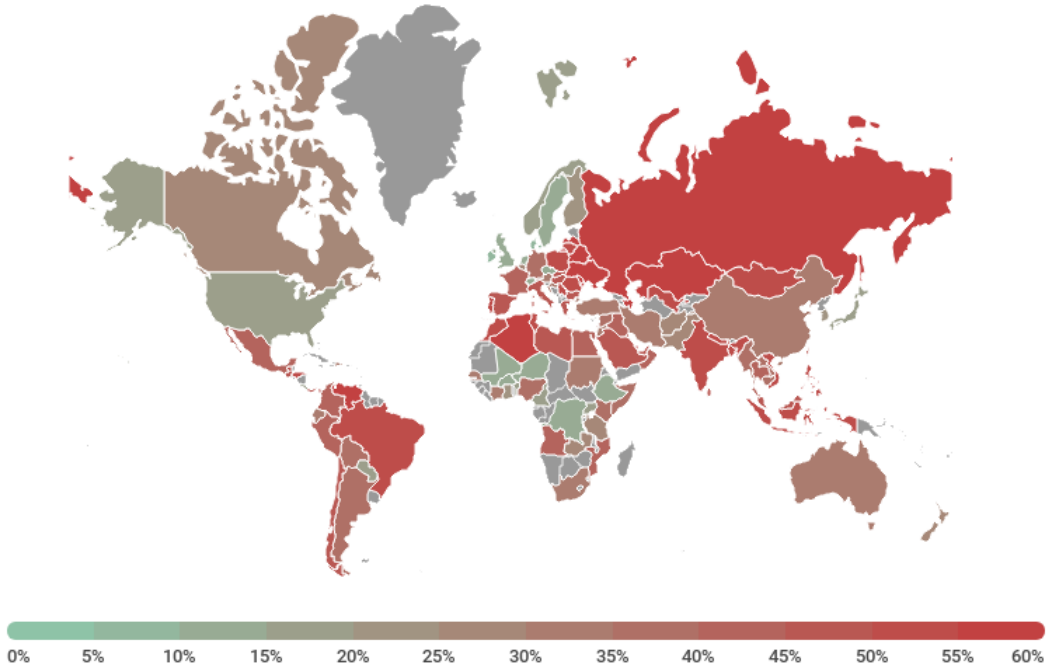
	Страна*	%**
1	Алжир	43,31
2	Беларусь	43,0
3	Венесуэла	39,48
4	Казахстан	37,76
5	Республика Молдова	37,39
6	Азербайджан	36,82
7	Россия	36,22
8	Украина	35,52
9	Латвия	34,63
10	Сербия	34,62
11	Вьетнам	34,45
12	Катар	34,37
13	Тунис	34,35
14	Индонезия	33,69
15	Румыния	33,09
16	Монголия	32,88
17	Филиппины	32,81

	Страна*	%**
18	Марокко	32,7
19	Бразилия	31,0
20	Непал	31,90

** При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского», относительно мало (меньше 50 000).*

*** Доля уникальных пользователей, подвергшихся веб-атакам вредоносных объектов класса Malware, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.*

В среднем в течение года **30,01%** компьютеров пользователей интернета в мире хотя бы один раз подвергались веб-атаке с участием ПО класса Malware.



География веб-атак вредоносного ПО, ноябрь 2017 года – октябрь 2018 года

TOP 20 вредоносных программ, наиболее активно используемых в онлайн-атаках

В 2018 году веб-антивирус «Лаборатории Касперского» выявил **21 643 946** уникальных вредоносных объектов (скриптов, эксплойтов, исполняемых файлов и т.д.) и **554 159 621** уникальный URL, на которых происходило срабатывание веб-антивируса. На основе собранных данных мы выделили 20 вредоносных программ, наиболее активно используемых в онлайн-атаках на компьютеры пользователей.

	Вердикт	%*
1	Malicious URL	89,50
2	Trojan.Script.Generic	6,19
3	Trojan.Script.Miner.gen	1,95
4	Trojan.Script.Agent.gen	0,38
5	Trojan.JS.Miner.m	0,27
6	Trojan-Clicker.HTML.Iframe.dg	0,26
7	Trojan.JS.Agent.eak	0,13
8	Trojan.JS.Miner.d	0,12
9	Hoax.HTML.FraudLoad.m	0,08
10	Trojan.Win32.Miner.ays	0,06
11	Trojan-Dropper.VBS.Agent.bp	0,05
12	Trojan-Downloader.Script.Generic	0,05
13	Trojan.Win64.Shelma.a	0,04
14	Packed.Multi.MultiPacked.gen	0,04
15	Trojan.JS.Miner.x	0,04
16	Trojan.JS.Miner.y	0,04
17	Hoax.Script.Generic	0,03

	Вердикт	%*
18	DangerousObject.Multi.Generic	0,03
19	Trojan.Script.Iframer	0,03
20	Trojan.JS.Agent.ecp	0,02

** Процент всех веб-атак класса Malware, зарегистрированных на компьютерах уникальных пользователей продуктов «Лаборатории Касперского».*

В этом году в TOP 20 вошло множество веб-майнеров, особенно старались представители семейства Trojan.JS.Miner – четыре места из двадцати. В то же время веб-эксплойты, собранные под вердиктом Exploit.Script.Generic и занявшие в прошлом году 10-ую позицию, в этот раз не попали в TOP 20.

ЛОКАЛЬНЫЕ УГРОЗЫ

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.

TOP 20 вредоносных объектов, обнаруженных на компьютерах пользователей

Мы выделили двадцать угроз, которые в 2018 году чаще всего детектировались на компьютерах пользователей. В данный рейтинг не входят программы типа Riskware и рекламные программы.

	Вердикт	%*
1	DangerousObject.Multi.Generic	32,15
2	Trojan.Script.Generic	14,46
3	Trojan.Multi.GenAutorunReg.a	5,76
4	Trojan.WinLNK.Agent.gen	4,56
5	Trojan.WinLNK.Starter.gen	3,47
6	HackTool.Win32.KMSAuto.c	3,14
7	HackTool.Win64.HackKMS.b	2,69
8	Trojan.Win32.Generic	2,56
9	Trojan.Script.Miner.gen	2,44
10	Trojan.Win32.AutoRun.gen	2,43
11	Trojan-Downloader.Script.Generic	2,33
12	Virus.Win32.Sality.gen	2,30

	Вердикт	%*
13	HackTool.Win32.KMSAuto.m	2,05
14	Trojan.AndroidOS.Boogr.gsh	1,96
15	Trojan.Win32.Agentb.bqyr	1,48
16	Trojan.Win32.Miner.gen	1,41
17	Trojan.Multi.GenAutorunBITS.a	1,28
18	Trojan.Multi.Babits.genw	1,19
19	Virus.Win32.Nimnul.a	1,18
20	HackTool.MSIL.KMSAuto.ba	1,13

** Доля 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.*

Первое место в нашем TOP 20 традиционно занял вердикт DangerousObject.Multi.Generic (32,15%), 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.

По-прежнему распространены различные вариации WinLNK-зловредов: на четвертом месте Trojan.WinLNK.Agent.gen (4,56%), а сразу за ним Trojan.WinLNK.Starter.gen (3,47%). Это вредоносное ПО может менять настройки браузера жертвы или использоваться для загрузки других зловредов.

На 14 месте троянец Trojan.AndroidOS.Boogr.gsh (1,96%), он детектируется с использованием технологий машинного обучения для зловредов под ОС Android.

Trojan.Multi.GenAutorunBITS.a (1,28%) и Trojan.Multi.Babits.genw (1,19%) занимают 17 и 18 места соответственно. Эти зловреды, как и многие другие, используют компонент Background Intelligent Transfer Service для закрепления в системе.

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.

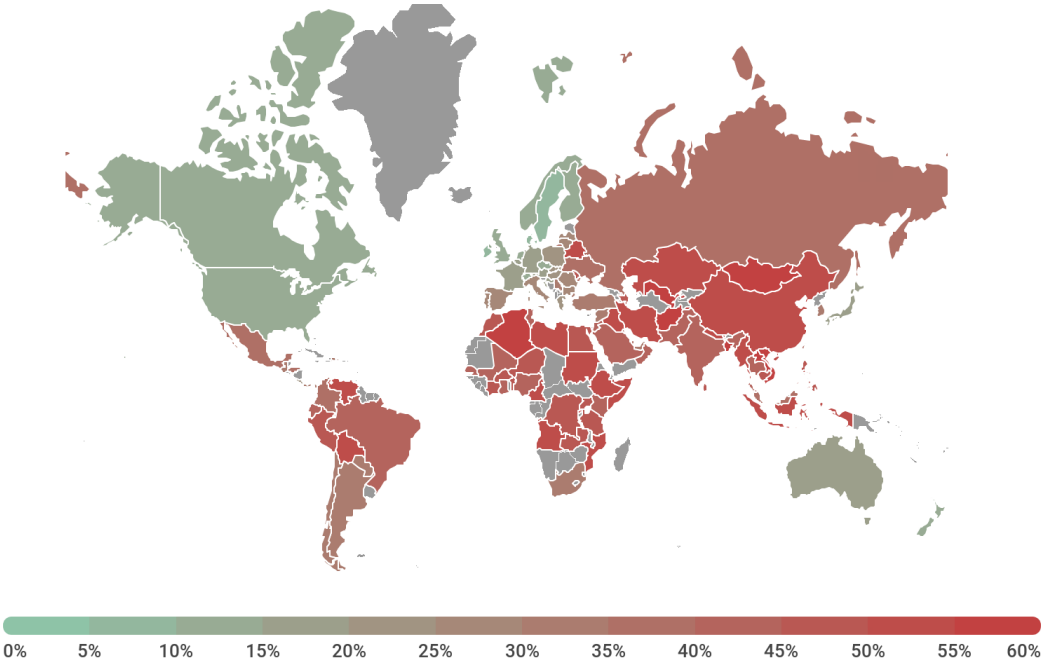
TOP 20 стран по уровню риска локального заражения

	Страна*	%**
1	Вьетнам	62,29
2	Афганистан	61,93
3	Узбекистан	60,22
4	Лаос	58,94
5	Монголия	58,35
6	Алжир	58,13
7	Бангладеш	56,58
8	Руанда	54,88
9	Сирия	54,76
10	Мьянма	54,03
11	Судан	53,77
12	Эфиопия	53,69
13	Ирак	53,50
14	Мозамбик	53,31
15	Казахстан	53,15
16	Непал	53,14
17	Беларусь	52,38

	Страна*	%**
18	Ливия	51,92
19	Венесуэла	51,18
20	Китай	51,17

** При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (меньше 50 тысяч).*

*** Доля уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы класса Malware, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.*



География локальных заражений вредоносным ПО, ноябрь 2017 года – октябрь 2018 года

В 2018 году хотя бы одна вредоносная программа была обнаружена в среднем на 35,06% компьютеров, жестких дисков или съемных носителей, принадлежащих пользователям KSN.