Kaspersky Security Bulletin ‘19

Статистика

kaspersky

Содержание

Цифры года . . . 3

Банковское вредоносное ПО . . . 4

Количество пользователей, атакованных банковскими зловредами . . . 4

География атак . . . 4

TOP 10 семейств банковского вредоносного ПО . . . 5

Вредоносные программы-шифровальщики . . . 6

Количество пользователей, атакованных троянцами-шифровальщиками . . . 6

География атак . . . 7

Программы-майнеры . . . 8

Количество пользователей, атакованных майнерами . . . 8

География атак . . . 8

Уязвимые приложения, используемые злоумышленниками в ходе кибератак . . . 9

Атаки через веб-ресурсы . . . 12

Страны — источники веб-атак . . . 12

Страны, в которых пользователи подвергались наибольшему риску заражения через интернет . . . 13

TOP 20 вредоносных программ, наиболее активно используемых в онлайн-атаках . . . 14

Локальные угрозы . . . 16

TOP 20 вредоносных объектов, обнаруженных на компьютерах пользователей . . . 16

Страны, в которых компьютеры пользователей подвергались наибольшему риску локального заражения . . . 17

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 203 стран и территорий по всему миру. Собранная статистика охватывает период с ноября 2018 по октябрь 2019 года включительно.

Цифры года

- В течение года 19,8% компьютеров интернет-пользователей в мире хотя бы один раз подверглись веб-атаке **класса Malware**.
- Решения «Лаборатории Касперского» отразили **975 491 360** атак, которые проводились с интернет-ресурсов, размещенных в различных странах мира.
- Зафиксировано **273 782 113** уникальных URL, на которых происходило срабатывание веб-антивируса.
- Наш веб-антивирус заблокировал **24 610 126** уникальных вредоносных объектов.
- Атаки шифровальщиков отражены на компьютерах **755 485** уникальных пользователей.
- За отчетный период майнеры атаковали **2 259 038** уникальных пользователей.
- Попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на устройствах **766 728** пользователей.

Статистика по мобильным угрозам будет представлена в отчете «Мобильная вирусология 2019».

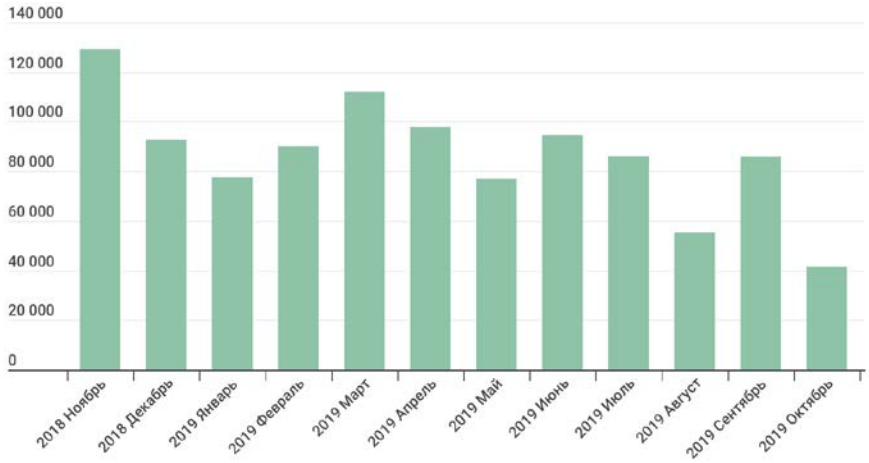
kaspersky

Банковское вредоносное ПО

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

Количество пользователей, атакованных банковскими зловредами

За отчетный период решения «Лаборатории Касперского» отразили попытки запуска одной или нескольких вредоносных программ, предназначенных для кражи денежных средств с банковских счетов, на компьютерах **766 728** пользователей.

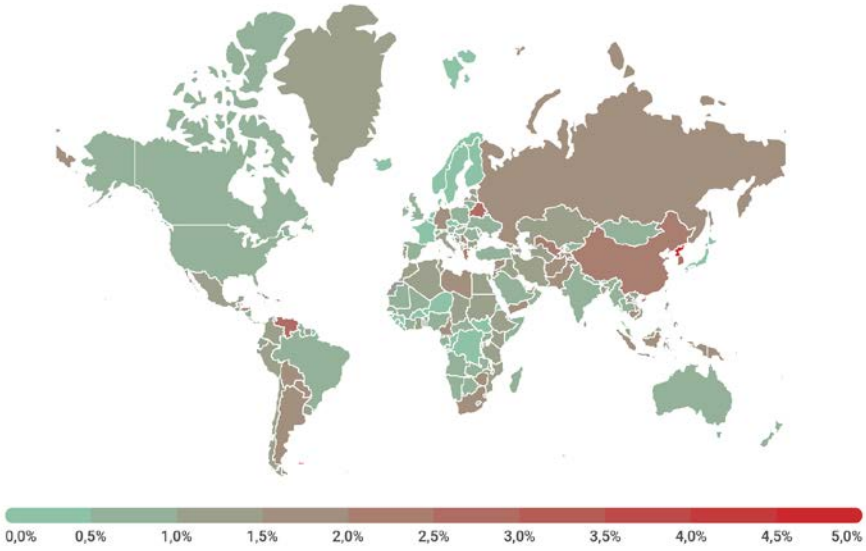


Количество пользователей, атакованных финансовым вредоносным ПО, ноябрь 2018 года — октябрь 2019 года

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.

kaspersky



География атак банковского вредоносного ПО, ноябрь 2018 года — октябрь 2019 года

TOP 10 стран по доле атакованных пользователей

	Страна*	%**
1	Беларусь	2,8
2	Южная Корея	2,6
3	Венесуэла	2,6
4	Китай	2,4
5	Греция	2,1
6	Мальдивские острова	2,0
7	Узбекистан	2,0
8	Камерун	1,9
9	Сербия	1,9
10	Афганистан	1,8

* 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 отчетный период.

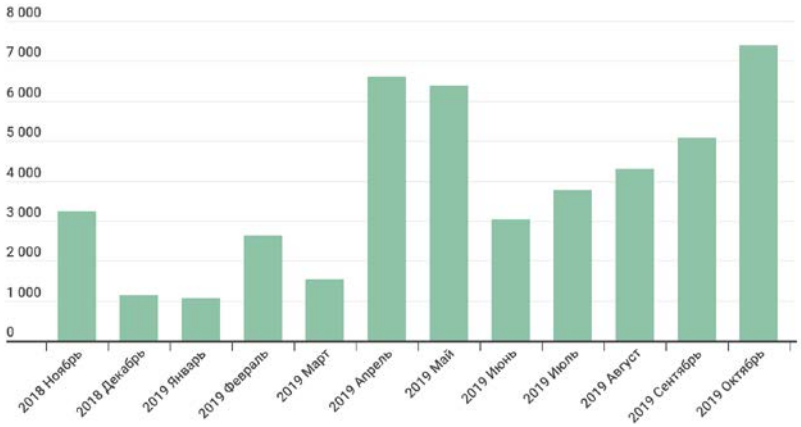
	Название	%*
1	Trojan.Win32.Zbot	23,10
2	Trojan-Banker.Win32.RTM	21,60
3	Backdoor.Win32.Emotet	12,30
4	Backdoor.Win32.SpyEye	7,10
5	Trojan.Win32.Nymaim	5,80
6	Trojan-Banker.Win32.Trickster	4,80
7	Trojan-Banker.Win32.Ramnit	4,40
8	Trojan.Win32. Neurevt	3,10
9	Trojan-Banker.Win32.CliptoShuffler	1,90
10	Trojan-Banker.Win32.Danabot	1,30

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

kaspersky

Вредоносные программы-шифровальщики

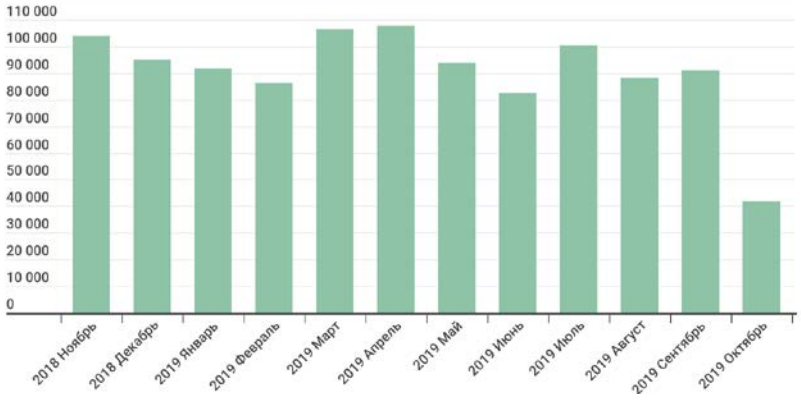
За отчетный период мы выявили более **46 156** модификаций шифровальщиков и обнаружили **22** новых семейства. Отметим, что не под каждый новый шифровальщик мы создавали отдельное семейство. Большей части угроз этого типа присваивается generic-вердикт, который мы используем при обнаружении новых и неизвестных образцов.



Количество новых модификаций шифровальщиков, ноябрь 2018 года — октябрь 2019 года

Количество пользователей, атакованных троянцами-шифровальщиками

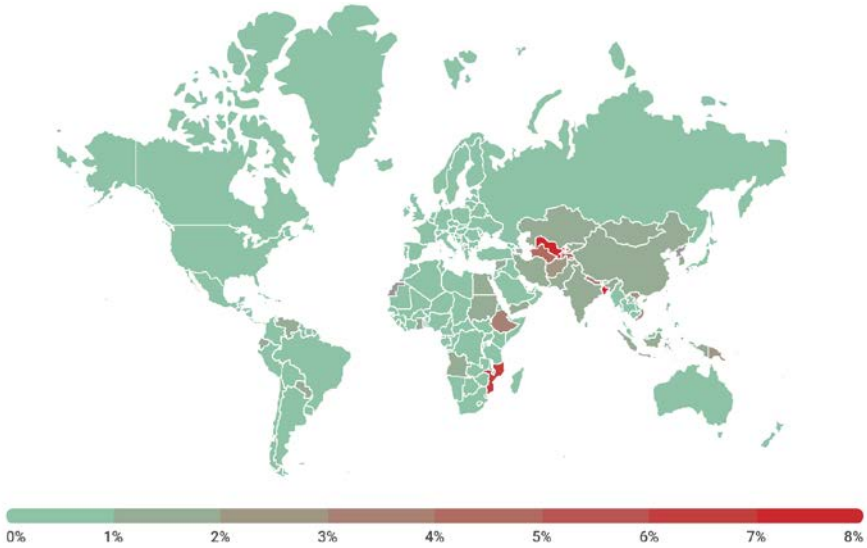
За отчетный период троянцы-шифровальщики атаковали **755 485** уникальных пользователей, в том числе 209 679 корпоративных пользователей (за вычетом SMB) и 22 440 пользователей, связанных с малым и средним бизнесом.



Количество пользователей, атакованных троянцами-шифровальщиками, ноябрь 2018 года — октябрь 2019 года

kaspersky

География атак



География атак троянцев-шифровальщиков, ноябрь 2018 года — октябрь 2019 года

TOP 10 стран, подвергшихся атакам троянцев-шифровальщиков

	Страна*	%**
1	Бангладеш	13,78
2	Узбекистан	7,20
3	Мозамбик	6,08
4	Туркменистан	4,23
5	Эфиопия	3,97
6	Непал	3,86
7	Афганистан	2,45
8	Вьетнам	2,34
9	Китай	1,94
10	Индия	1,91

* 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	23,56
2	(generic verdict)	Trojan-Ransom.Win32.Phny	16,81
3	GandCrab	Trojan-Ransom.Win32.GandCrypt	12,17
4	(generic verdict)	Trojan-Ransom.Win32.Gen	6,26
5	(generic verdict)	Trojan-Ransom.Win32.Crypmod	5,08
6	(generic verdict)	Trojan-Ransom.Win32.Encoder	4,65
7	Shade	Trojan-Ransom.Win32.Shade	2,66
8	PolyRansom/ VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.Win32.PolyRansom	2,43
9	(generic verdict)	Trojan-Ransom.Win32.Crypren	2,28
10	Stop	Trojan-Ransom.Win32.Stop	1,94

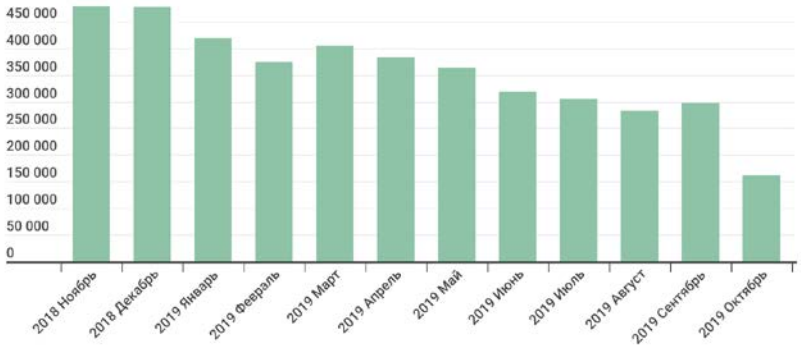
* Доля уникальных пользователей «Лаборатории Касперского», подвергшихся атакам определенного семейства троянцев-вымогателей, от всех пользователей, подвергшихся атакам троянцев-вымогателей.

kaspersky

Программы-майнеры

Количество пользователей, атакованных майнерами

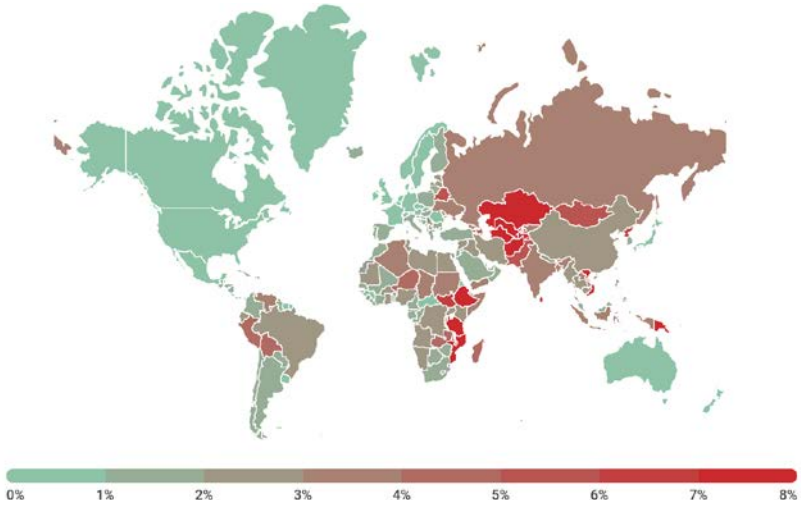
За отчетный период мы зафиксировали попытки установки майнера на компьютерах **2 259 038** уникальных пользователей. В общем объеме атак доля майнеров составила 3,64%, а среди всех программ типа Risktool — 6,94%.



Количество пользователей, атакованных майнерами, ноябрь 2018 года — октябрь 2019 года

Чаще других в отчетный период продукты «Лаборатории Касперского» обнаруживали Trojan.Win32.Miner.bbb — на его долю пришлось 13,45% от общего количества пользователей, атакованных майнерами. Следом идут Trojan.Win32.Miner.ays (11,35%), Trojan.JS.Miner.m (11,12%) и Trojan.Win32.Miner.gen (9,32%).

География атак



География атак с участием майнеров, ноябрь 2018 года — октябрь 2019 года

kaspersky

Уязвимые приложения, используемые злоумышленниками в ходе кибератак

Отчетный период запомнился нам большим количеством целевых атак с использованием эксплойтов для уязвимостей нулевого дня. За этот год эксперты «Лаборатории Касперского» обнаружили:

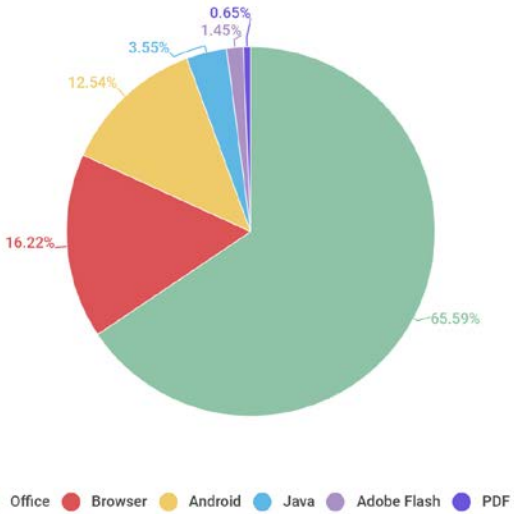
- Уязвимость **CVE-2018-8611**, исправленную в декабрьском наборе патчей. Ее использовали как минимум две хакерские группы — FruityArmor и SandCat. На момент обнаружения эксплойта для этой уязвимости FruityArmor уже была довольно известной группировкой, использовавшей не один эксплойт нулевого дня, а SandCat, наоборот, — относительно новой. Найденная уязвимость оказалась очень серьезной, так как позволяла получить привилегии системы и исполнять код на уровне ядра во всех версиях операционных систем Windows, включая самую последнюю на тот момент версию Windows 10 RS4. Кроме того, уязвимость находилась в драйвере Kernel Transaction Manager, что позволяло эксплойту обходить песочницы веб-браузеров.
- Уязвимость **CVE-2019-0797**. Ее обнаружили в феврале и исправили в мартовском наборе патчей. Как и CVE-2018-8611, новую уязвимость могли использовать различные группировки, включая FruityArmor и SandCat. Она стала четвертой активно эксплуатируемой уязвимостью нулевого дня, которую «Лаборатория Касперского» обнаружила в первом полугодии 2019 года. Как и предыдущие обнаруженные уязвимости, находка использовалась для повышения прав в ОС Windows, но в отличие от CVE-2018-8611 уязвимым компонентом выступал драйвер win32k.sys, отвечающий за графику и интерфейс.
- Активно эксплуатируемую уязвимость **CVE-2019-0859**. Она позволяла повышать права в Windows благодаря очередной ошибке в драйвере win32k.sys. Довольно специфическая полезная нагрузка, предоставляемая вместе с шелл-кодом, может свидетельствовать о том, что эксплойт использовался одной из киберпреступных групп, нацеленных на финансовый сектор.
- Уязвимость **CVE-2019-13720**. Ее выявили в конце октября после серии атак на свежие версии Google Chrome. После того как мы сообщили об этой активно используемой уязвимости в Google, компания выпустила обновленную версию браузера Chrome версии 78.0.3904.87. Атакам на CVE-2019-13270 мы дали имя Operation WizardOpium, так как, несмотря на некоторое сходство в коде, нам не удалось установить точную связь с другими группировками.

Если говорить об общем количестве активно используемых эксплойтов нулевого дня, которые обнаружили мы и наши партнеры из индустрии, то в 2019 году их было больше, чем в предыдущем.

В отчетный период мы наблюдали снижение количества эксплойтов для уязвимостей в Adobe Flash Player, поддержка которого должна прекратиться в конце следующего года. Доля эксплойтов для веб-браузеров также незначительно снизилась, даже несмотря на появление нескольких новых публично эксплуатируемых уязвимостей нулевого дня. То же самое можно сказать и про Android, доля эксплойтов для которого в этом отчетном периоде снизилась до 12%. Доля эксплойтов для PDF, напротив, незначительно возросла.

На протяжении прошлого отчетного периода мы наблюдали стремительный рост количества пользователей, атакованных эксплойтами для Microsoft Office, и в четвертом квартале 2018 года эксплойты для этого пакета стали лидерами по количеству атак. В этот отчетный период Microsoft Office остается на первой строчке в рейтинге самых атакуемых приложений. Но в отличие от предыдущих лет, в этом году инструментарий злоумышленников не претерпел значительных изменений, и наиболее часто по-прежнему используются эксплойты для CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 и CVE-2017-0199. Несмотря на отсутствие значительных изменений в ассортименте эксплойтов, злоумышленники продолжают находить новые техники для обфускации документов и обхода статических техник детектирования, но освещение этой темы требует отдельного обзора на Securelist.

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 2018 года — ноябрь 2019 года

kaspersky

В этом отчетном периоде сетевые атаки по-прежнему остались одним из распространенных типов атак. Можно с уверенностью сказать, что 2019 год запомнится обнаружением множественных уязвимостей в подсистеме удаленного рабочего стола для различных версий операционных систем Windows. Эти уязвимости получили общие названия BlueKeep и DejaBlue. В данный момент мы не наблюдаем активной эксплуатации этих уязвимостей, что можно объяснить сложностью процесса. В топе сетевых атак, как и в предыдущие годы, различные вариации эксплойтов для уязвимостей в протоколе SMB, известных под именами EternalBlue, EternalRomance и др. Также нельзя не отметить, что большую долю вредоносного сетевого трафика составляют запросы, нацеленные на перебор паролей в популярных сетевых службах и серверах, таких как Remote Desktop Protocol и Microsoft SQL Server соответственно.

Атаки через веб-ресурсы

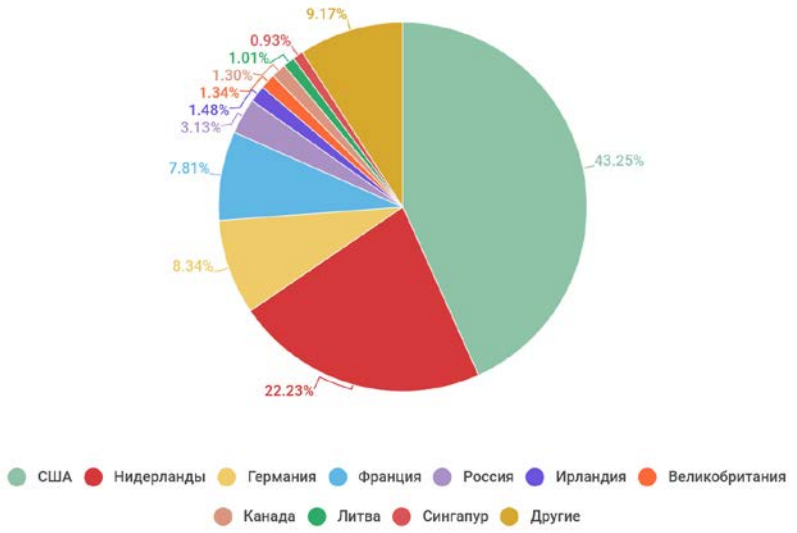
Статистические данные в этой главе получены на основе работы веб-антивируса, который защищает пользователей от загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Вредоносные сайты специально создаются злоумышленниками; зараженными могут быть веб-ресурсы, контент которых создается пользователями (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 **975 491 360** атак, которые проводились с интернет-ресурсов, размещенных в разных странах мира. При этом 90,83% от общего количества этих интернет-ресурсов были расположены всего в 10 странах.



Распределение источников веб-атак по странам, ноябрь 2018 года — октябрь 2019 года

kaspersky

По сравнению с результатами предыдущего года распределение источников веб-атак не сильно изменилось. На первом месте США (43,25%), следом идут Нидерланды (22,23%) и Германия (8,34%).

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 **78%** компьютеров пользователей, на которых происходило срабатывание веб-антивируса.

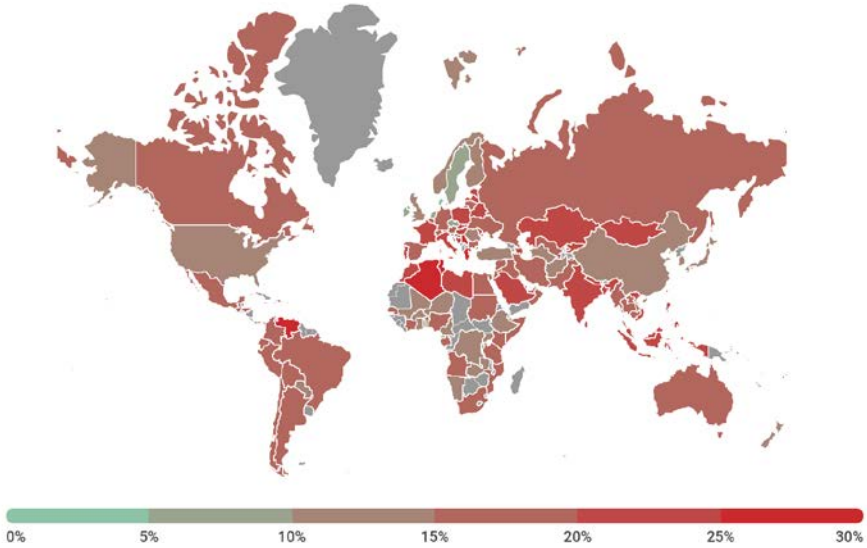
TOP 20 стран, в которых пользователи подвергались наибольшему риску заражения через интернет

	Страна*	%**
1	Алжир	33,02
2	Венесуэла	30,25
3	Тунис	29,50
4	Греция	26,07
5	Сербия	25,80
6	Бангладеш	24,95
7	Молдова	24,78
8	Азербайджан	24,74
9	Беларусь	24,52
10	Польша	24,13
11	Монголия	24,05
12	Филиппины	23,89
13	Марокко	23,87
14	Латвия	23,22
15	Катар	22,94
16	Вьетнам	22,57
17	Тайвань, провинция Китая	22,13
18	Франция	21,99
19	Португалия	21,97
20	Италия	21,96

* 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 за отчетный период **19,8%** компьютеров пользователей интернета в мире хотя бы один раз подвергались веб-атаке с участием ПО класса Malware.



География веб-атак вредоносного ПО, ноябрь 2018 года — октябрь 2019 года

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

За отчетный период веб-антивирус «Лаборатории Касперского» выявил **24 610 126** уникальных вредоносных объектов (скриптов, эксплойтов, исполняемых файлов и т. д.) и **273 782 113** уникальных вредоносных URL, на которых происходило срабатывание веб-антивируса. На основе собранных данных мы выделили 20 вредоносных программ, наиболее активно использовавшихся в онлайн-атаках на компьютеры пользователей.

	Вердикт	%*
1	Malicious URL	85,40
2	Trojan.Script.Generic	5,89
3	Trojan.Script.Miner.gen	3,89
4	Trojan-Clicker.HTML.Iframe.dg	0,65
5	Trojan.BAT.Miner.gen	0,26
6	Trojan-Downloader.JS.Inor.a	0,22
7	Trojan.PDF.Badur.gen	0,21
8	DangerousObject.Multi.Generic	0,21
9	Trojan-Downloader.Script.Generic	0,17
10	Trojan-PSW.Script.Generic	0,15
11	Trojan.Script.Agent.gen	0,15
12	Hoax.HTML.FraudLoad.m	0,13
13	Exploit.Script.Generic	0,08

kaspersky

	Вердикт	%*
14	Trojan.Script.Agent.bg	0,07
15	Trojan.Multi.Preqw.gen	0,06
16	Exploit.MSOffice.CVE-2017-11882.gen	0,06
17	Trojan-Downloader.JS.SLoad.gen	0,05
18	Hoax.Script.Loss.gen	0,05
19	Trojan.JS.Miner.m	0,05
20	Trojan-Downloader.VBS.SLoad.gen	0,04

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

Несмотря на то что в TOP 20 есть несколько вердиктов, относящихся к веб-майнерам, количество детектов JavaScript-майнеров и попыток подключения к веб-майнинговым сайтам значительно снизилось по сравнению с 2018 годом. Это отразилось как на общем количестве веб-детектов, так и на доле вердикта Malicious URL. Этот вердикт основывается на нашем черном списке, который содержит ссылки на веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами и т. д.

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 отчетном периоде чаще всего детектировались на компьютерах пользователей. В данный рейтинг не входят программы типа Riskware и рекламные программы.

	Вердикт	%*
1	DangerousObject.Multi.Generic	26,43
2	Trojan.Multi.BroSubsc.gen	9,48
3	Trojan.Script.Generic	6,19
4	Trojan.Multi.GenAutorunReg.a	5,94
5	HackTool.Win64.HackKMS.b	4,40
6	HackTool.MSIL.KMSAuto.by	3,69
7	HackTool.Win32.KMSAuto.bu	3,54
8	Trojan.WinLNK.Agent.gen	3,45
9	HackTool.MSIL.KMSAuto.a	3,43
10	Trojan.WinLNK.Starter.gen	3,42
11	HackTool.MSIL.KMSAuto.dh	2,83
12	HackTool.Win32.KMSAuto.c	2,75
13	HackTool.MSIL.KMSAuto.di	2,65
14	Trojan.Win32.Generic	2,53
15	HackTool.Win32.KMSAuto.cb	2,50
16	HackTool.Win64.HackKMS.c	2,47
17	HackTool.MSIL.KMSAuto.bx	2,18
18	Trojan.Win32.AutoRun.gen	1,93
19	Virus.Win32.Sality.gen	1,90
20	HackTool.Win32.KMSAuto.m	1,90

* 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.

kaspersky

Первое место в нашем TOP 20 традиционно занял вердикт DangerousObject.Multi.Generic (26,43%), 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.

Второе место заняла сравнительно новая угроза, получившая широкое распространение в этом году, — Trojan.Multi.BroSubsc.gen (9,48%). Зловреды этого семейства скрытно устанавливаются в браузер после того, как жертва посетит вредоносный или рекламный сайт. Задачей Trojan.Multi.BroSubsc.gen является демонстрация рекламных сообщений даже в тех случаях, когда браузер жертвы не запущен.

В целом в отчетный период мы заметили снижение популярности майнеров — этот тип зловредов покинул TOP 20 угроз.

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.

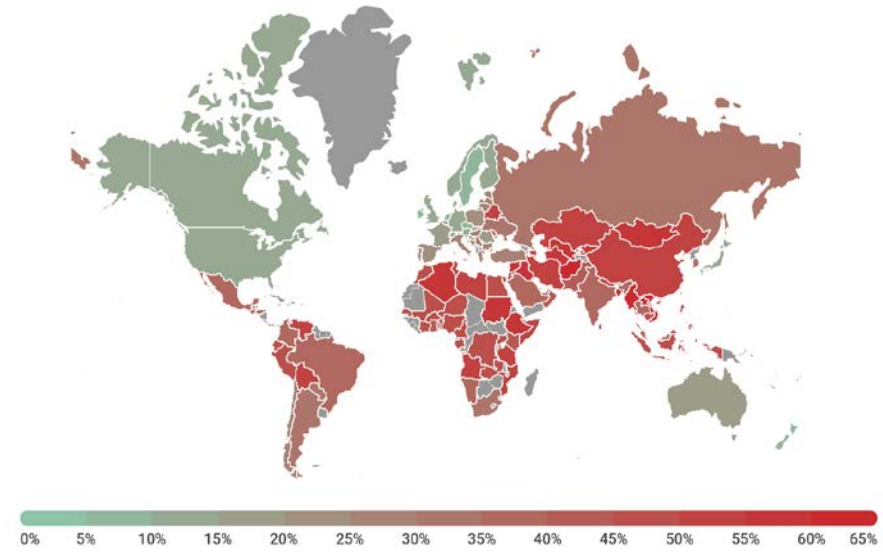
TOP 20 стран по уровню риска локального заражения

	Страна*	%**
1	Афганистан	65,55
2	Вьетнам	61,84
3	Лаос	61,95
4	Мьянма	60,80
5	Бангладеш	59,51
6	Монголия	59,41
7	Узбекистан	58,06
8	Туркменистан	57,57
9	Алжир	57,50
10	Ирак	57,33
11	Сирия	57,04
12	Судан	55,41
13	Киргизстан	55,15

* 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.

	Страна*	%**
14	Эфиопия	55,08
15	Боливия	54,85
16	Китай	54,64
17	Непал	54,57
18	Мозамбик	54,52
19	Ливия	54,36
20	Руанда	54,14



География локальных заражений вредоносным ПО, ноябрь 2018 года — октябрь 2019 года

В отчетный период хотя бы одна вредоносная программа была обнаружена в среднем на **34,05%** компьютеров, жестких дисков или съемных носителей, принадлежащих пользователям KSN.

kaspersky