Kaspersky Security Bulletin 2020. Статистика

kaspersky

Содержание

Цифры года . . . 4
Финансовые угрозы . . . 5
Количество пользователей, атакованных банковскими зловредами . . . 5
География атак . . . 6
TOP 10 семейств финансового вредоносного ПО . . . 7
Вредоносные программы-шифровальщики . . . 8
Количество пользователей, атакованных троянцами-шифровальщиками . . . 8
География атак . . . 9
Программы-майнеры . . . 11
Количество пользователей, атакованных майнерами . . . 11
География атак . . . 12
Уязвимые приложения, используемые злоумышленниками в ходе кибератак . . . 13
Атаки на macOS . . . 15
География угроз . . . 16
Атаки на IoT . . . 18
Статистика IoT-угроз . . . 18
Угрозы, загружаемые в ловушки . . . 20
Атаки через веб-ресурсы . . . 21
Страны — источники веб-атак . . . 21
Страны, в которых пользователи подвергались наибольшему риску заражения через интернет . . . 22
TOP 20 вредоносных программ, наиболее активно используемых в онлайн-атаках . . . 24
Локальные угрозы . . . 26
TOP 20 вредоносных объектов, обнаруженных на компьютерах пользователей . . . 26
Страны, в которых компьютеры пользователей подвергались наибольшему риску локального заражения . . . 27

kaspersky

Цифры года

- В течение года 10,18% компьютеров интернет-пользователей в мире хотя бы один раз подверглись веб-атаке **класса Malware**.
- Решения «Лаборатории Касперского» отразили **666 809 967** атак, которые проводились с интернет-ресурсов, размещенных в различных странах мира.
- Зафиксировано **173 335 902** уникальных вредоносных URL, на которых происходило срабатывание веб-антивируса.
- Наш веб-антивирус заблокировал **33 412 568** уникальных вредоносных объектов.
- Атаки шифровальщиков отражены на компьютерах **549 301** уникального пользователя.
- За отчетный период майнеры атаковали **1 523 148** уникальных пользователей.
- Попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на устройствах **668 619** пользователей.

Статистика по мобильным угрозам будет представлена в отчете «Мобильная вирусология 2020»

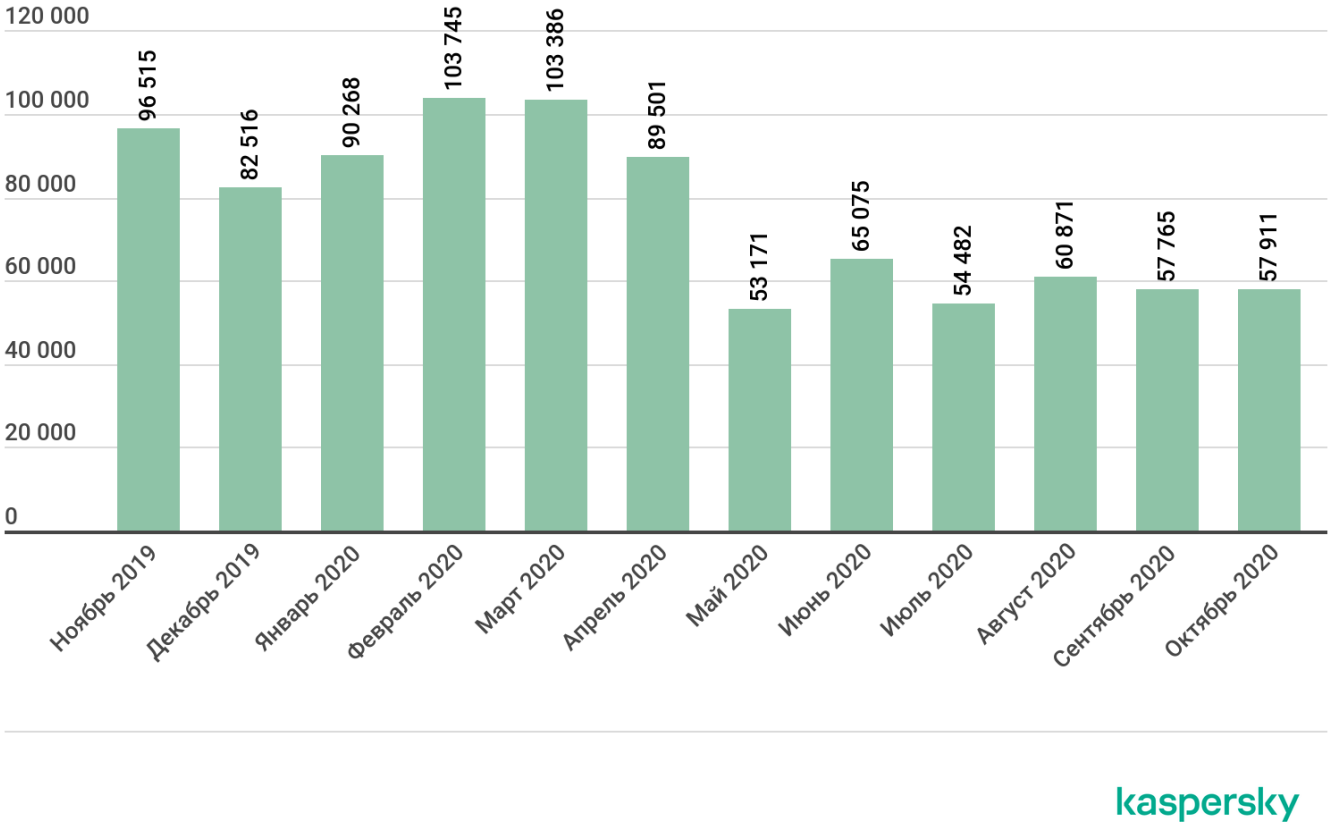
Все статистические данные, использованные в этом отчете, получены с помощью глобальной облачной сети Kaspersky Security Network (KSN), куда поступает информация от различных компонентов наших защитных решений. Данные получены от пользователей, давших свое согласие на передачу этой информации в KSN. В глобальном обмене сведениями о вредоносной активности принимают участие миллионы пользователей продуктов «Лаборатории Касперского» по всему миру. Собранная статистика охватывает период с ноября 2019 по октябрь 2020 года включительно.

Финансовые угрозы

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 **668 619** пользователей.

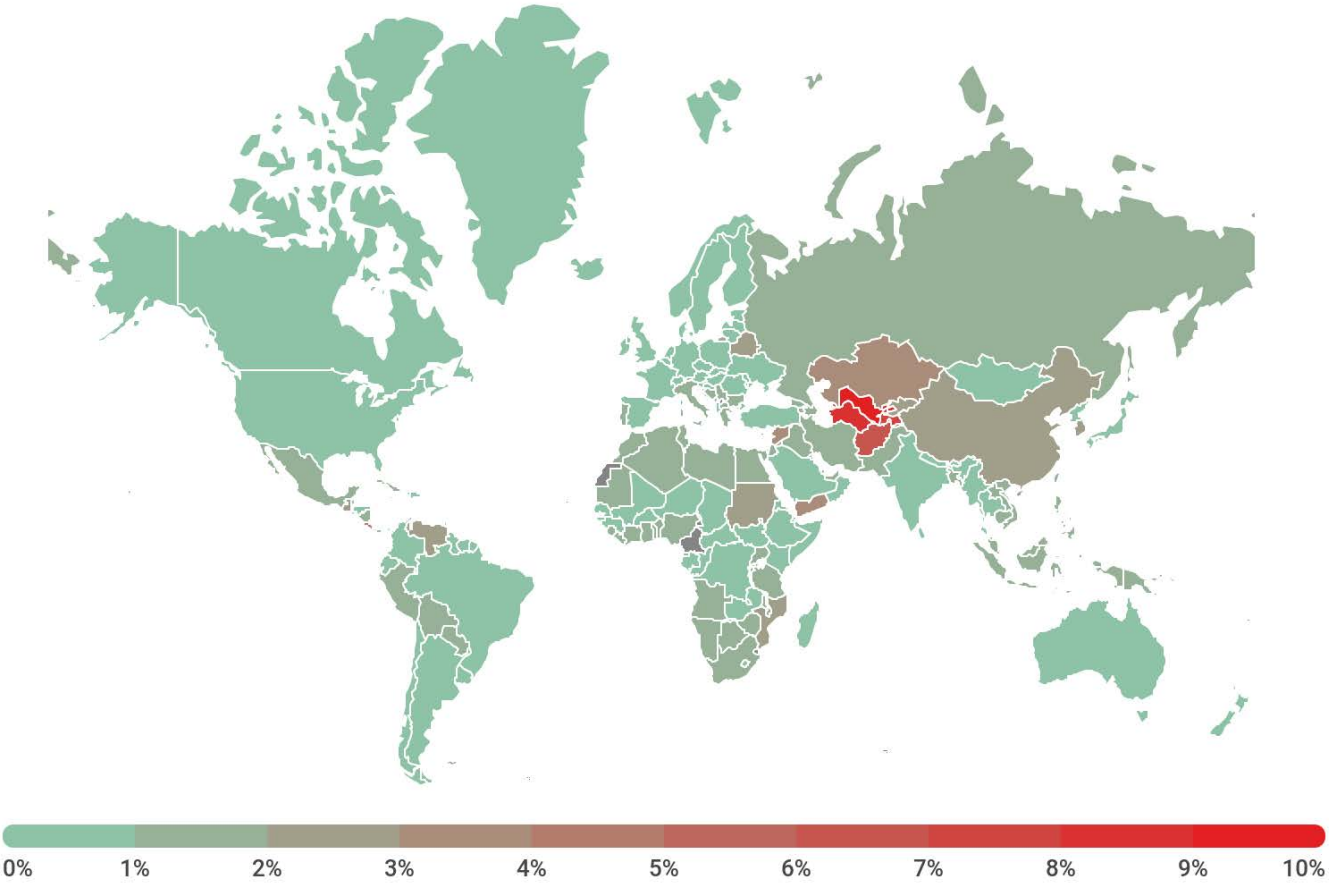


Количество пользователей, атакованных финансовым вредоносным ПО, ноябрь 2019 года — октябрь 2020 года

kaspersky

География атак

Чтобы оценить и сравнить степень риска заражения банковскими троянцами и ATM/PoS-зловредами, которому подвергаются компьютеры пользователей в разных странах мира, мы подсчитали в каждой из стран долю пользователей продуктов «Лаборатории Касперского», столкнувшихся с финансовой угрозой в отчетный период, от всех атакованных пользователей наших продуктов в заданной стране.



География атак банковского вредоносного ПО, ноябрь 2019 года — октябрь 2020 года

kaspersky

TOP 10 стран по доле атакованных пользователей

	Страна*	%**
1	Узбекистан	10,4
2	Туркменистан	8,6
3	Таджикистан	7,5
4	Афганистан	6,6
5	Коста-Рика	4,0
6	Йемен	3,9
7	Казахстан	3,5
8	Сирия	3,3
9	Гватемала	2,8
10	Южная Корея	2,7

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

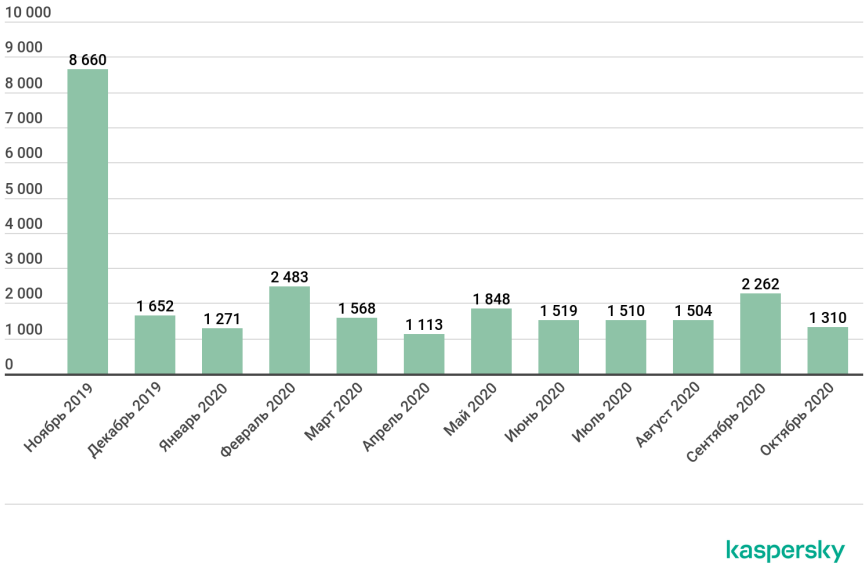
TOP 10 семейств финансового вредоносного ПО

	Название	%*
1	Zbot	21,6
2	Emotet	15,1
3	CliptoShuffler	15
4	RTM	11,1
5	Trickster	5,1
6	Nimnul	4,2
7	Neurevt	3,3
8	Danabot	3,2
9	SpyEye	3,2
10	Nymaim	2,1

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

Вредоносные программы-шифровальщики

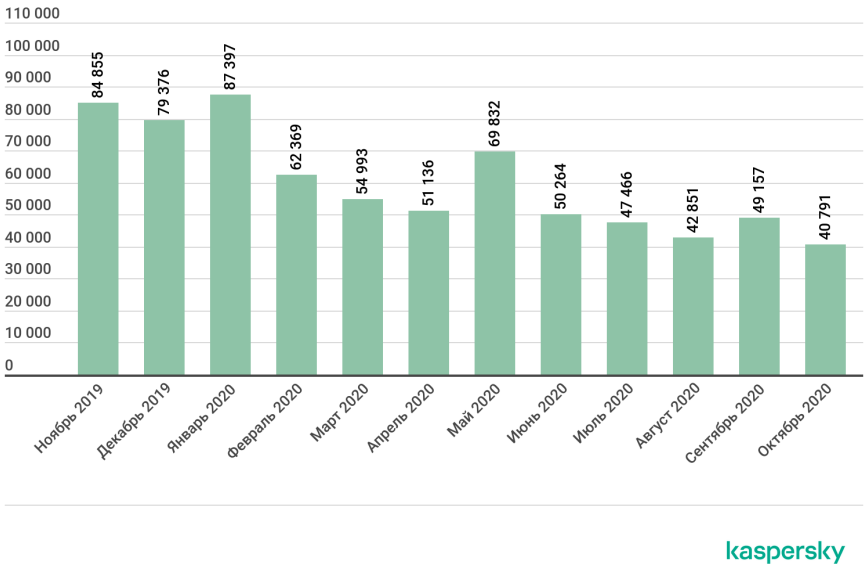
За отчетный период мы выявили более **26 700** модификаций шифровальщиков и обнаружили **21** новое семейство. Отметим, что не под каждый новый шифровальщик мы создавали отдельное семейство. Большей части угроз этого типа присваивался generic-вердикт, который мы используем при обнаружении новых и неизвестных образцов.



Количество новых модификаций шифровальщиков, ноябрь 2019 года — октябрь 2020 года

Количество пользователей, атакованных троянцами-шифровальщиками

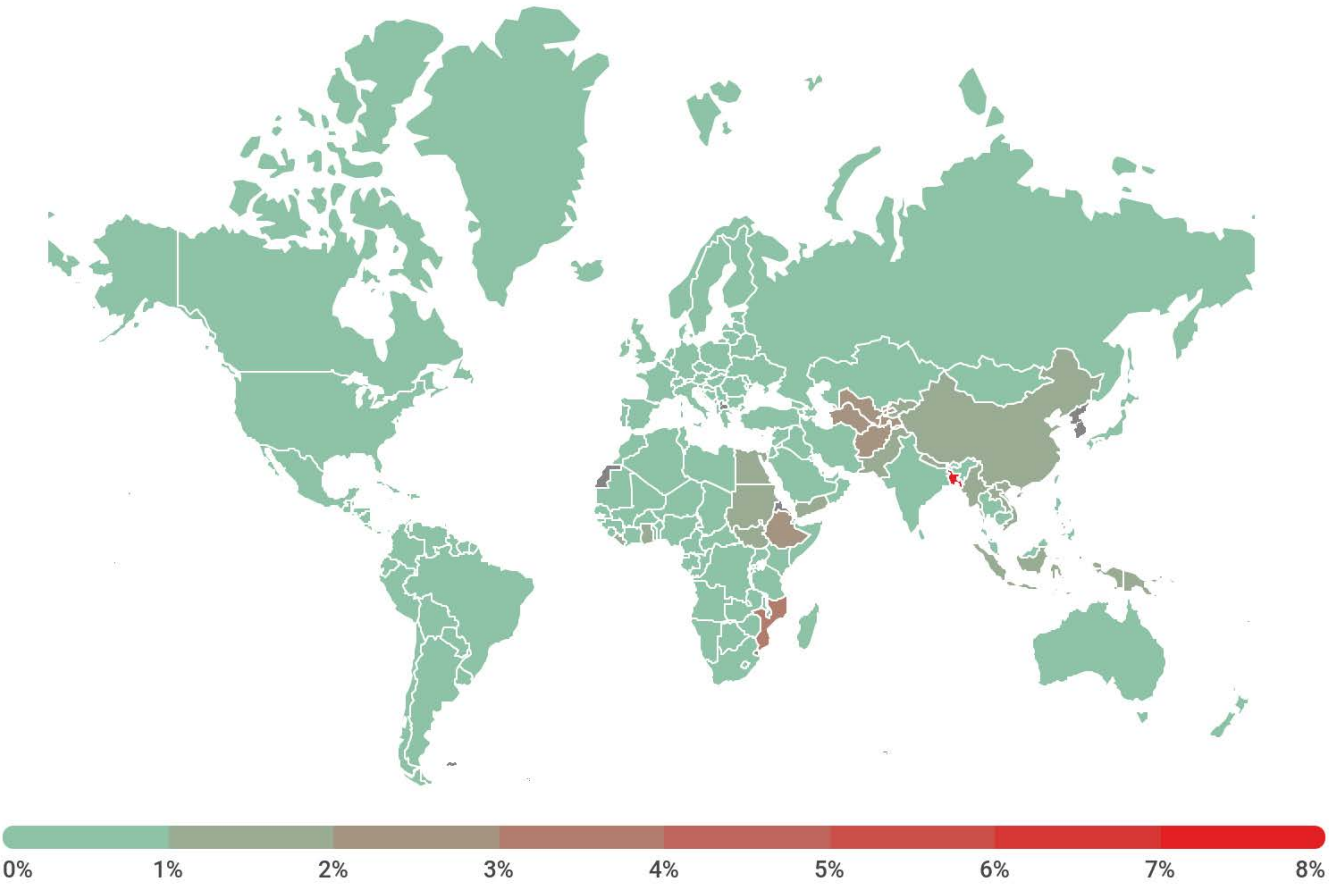
За отчетный период троянцы-шифровальщики атаковали **549 301** уникального пользователя, в том числе 123 630 корпоративных пользователей (за вычетом SMB) и 15 940 пользователей, связанных с малым и средним бизнесом.



Количество пользователей, атакованных троянцами-шифровальщиками, ноябрь 2019 года — октябрь 2020 года

kaspersky

География атак



География атак троянцев-шифровальщиков,
ноябрь 2019 года — октябрь 2020 года

kaspersky

TOP 10 стран, подвергшихся атакам троянцев-шифровальщиков

	Страна*	%**
1	Бангладеш	8,12
2	Мозамбик	3,13
3	Туркменистан	2,65
4	Гаити	2,47
5	Узбекистан	2,39
6	Эфиопия	2,10
7	Афганистан	2,06
8	Непал	1,97
9	Судан	1,92
10	Киргизия	1,77

* 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

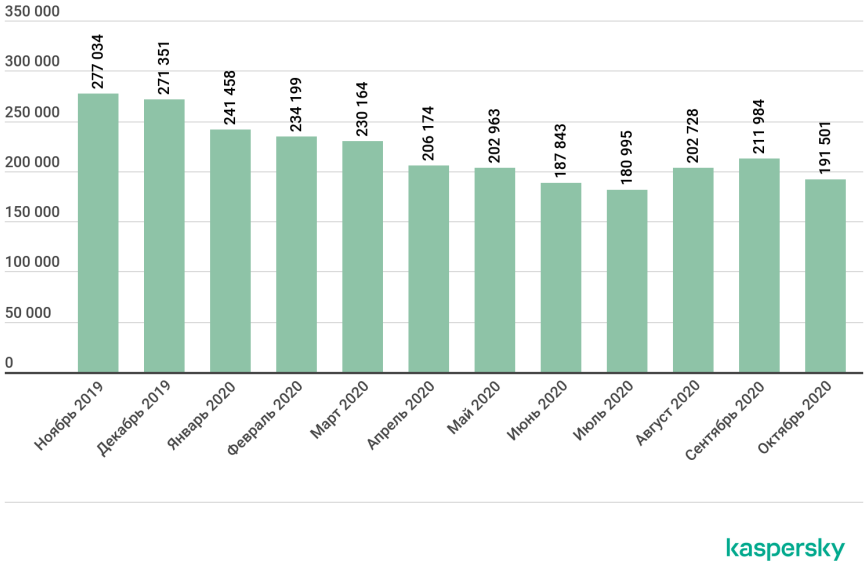
	Название	Вердикт	%*
1	WannaCry	Trojan-Ransom.Win32.Wanna	16,56
2	(generic verdict)	Trojan-Ransom.Win32.Phny	11,56
3	(generic verdict)	Trojan-Ransom.Win32.Gen	11,37
4	Stop	Trojan-Ransom.Win32.Stop	7,76
5	(generic verdict)	Trojan-Ransom.Win32.Encoder	6,66
6	(generic verdict)	Trojan-Ransom.Win32.Generic	4,77
7	(generic verdict)	Trojan-Ransom.Win32.Crypren	4,07
8	PolyRansom/VirLock	Virus.Win32.PolyRansom Trojan-Ransom.Win32.PolyRansom	2,54
9	Crysis/Dharma	Trojan-Ransom.Win32.Crusis	2,21
10	(generic verdict)	Trojan-Ransom.Win32.Crypmod	1,83

* 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 обнаружили попытки установки майнера на компьютерах **1 523 148** уникальных пользователей. В общем объеме атак доля майнеров составила 2,49%, а среди всех программ типа Risktool — 13,82%

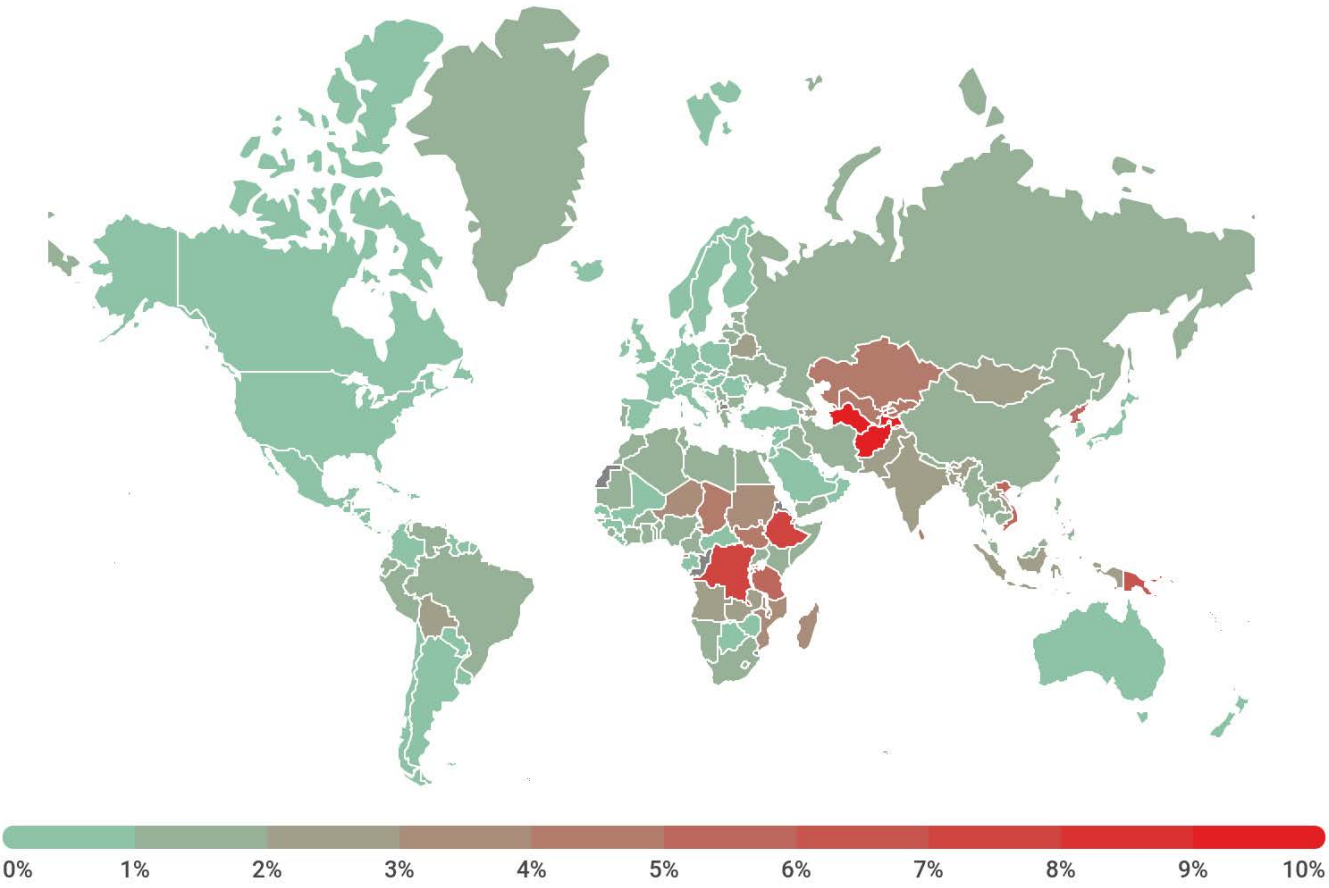


Количество пользователей, атакованных майнерами, ноябрь 2019 года — октябрь 2020 года

Чаще других за отчетный период продукты «Лаборатории Касперского» обнаруживали Trojan.Win32.Miner.bbb — на его долю пришлось 17,53% от общего количества пользователей, атакованных майнерами. Следом идут Trojan.Win32.Miner.ays (10,86%), Trojan.JS.Miner.m (10,28%) и Trojan.Win32.Miner.gen (8,00%).

kaspersky

География атак



География атак с участием майнеров,
ноябрь 2019 года — октябрь 2020 года

kaspersky

Уязвимые приложения, используемые злоумышленниками в ходе кибератак

В 2020 году большинство уязвимостей были найдены исследователями до того, как их смогли бы использовать злоумышленники. Однако без уязвимостей нулевого дня все же не обошлось: в частности, эксперты «Лаборатории Касперского» обнаружили две.

- Уязвимость CVE-2020-1380, представляющую собой возможный сценарий use-after-free в компоненте Jscript9 браузера Microsoft Internet Explorer, вызванный недостаточными проверками во время генерации оптимизированного JIT-кода. Данная уязвимость, вероятно, использовалась APT-группой DarkHotel на первой стадии компрометации систем, тогда как на следующих стадиях работу полезной нагрузки обеспечивал дополнительный эксплойт, повышающий привилегии злоумышленников в системе.
- Уязвимость CVE-2020-0986 в компоненте GDI Print/Print Spooler операционной системы Microsoft Windows, позволяющая манипулировать памятью процесса для получения возможности исполнять произвольный код в контексте служебного процесса системы. Эксплуатация этой уязвимости может привести к обходу песочницы, например в браузере.

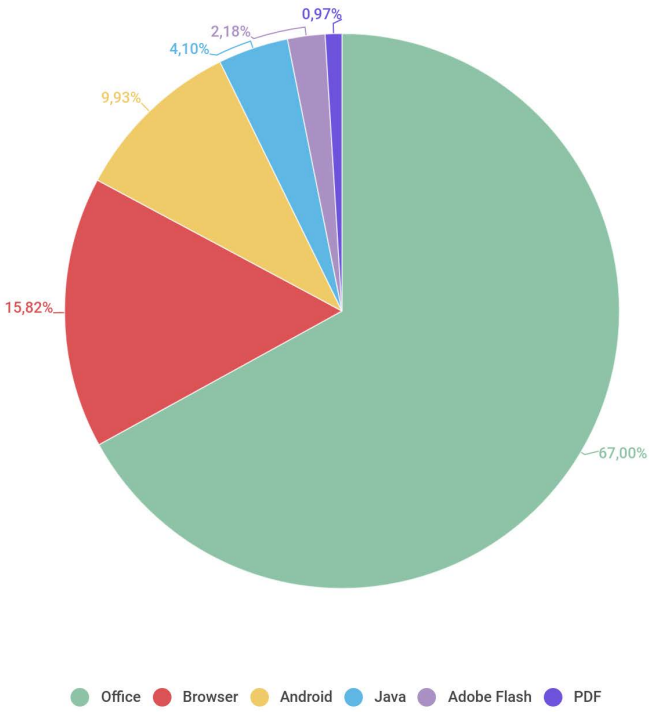
Также стоит сказать о тех уязвимостях, которые были найдены нашими партнерами:

- Четыре уязвимости нулевого дня в Google Chrome: CVE-2020-16010, CVE-2020-16009, CVE-2020-15999 и CVE-2020-6418. Все они были использованы для компрометации систем и давали возможность злоумышленникам запустить код в целевой системе. Так, например, уязвимость CVE-2020-15999 представляет собой ошибку в популярной библиотеке libfreetype2, возникающую во время обработки PNG-изображений, встроенных внутрь шрифтов TrueType. В теории эксплуатация уязвимости возможна и в других продуктах, где используется эта библиотека.
- Три уязвимости нулевого дня в Mozilla Firefox (CVE-2020-6820, CVE-2020-6819, CVE-2019-17026), также дающие возможность компрометации пользовательских систем.
- Уязвимость нулевого дня в Microsoft Internet Explorer (CVE-2020-0674), которая предположительно использовалась APT-группой DarkHotel. Ее суть заключается в возможном сценарии use-after-free, когда сборщик мусора в определенной ситуации переставал отслеживать объекты, переданные в качестве аргументов в функцию обратного вызова при использовании операции сортировки массивов.
- Четыре уязвимости нулевого дня в Microsoft Windows (CVE-2020-0938, CVE-2020-1020, CVE-2020-1027, CVE-2020-17087). CVE-2020-17087 — ошибка в криптографическом драйвере ядра, кроющаяся в недостаточных проверках входных данных при обращении к вызовам IOCTL на пользовательском уровне. Она позволяла злоумышленникам обойти песочницу Google Chrome и внедриться в систему.

Вероятно, что в будущем году мы еще услышим об атрибуции и инструментах, которые использовали эти уязвимости.

На протяжении отчетного периода мы наблюдали незначительное снижение количества атак на приложения пакета Microsoft Office, но это не помешало им занять первое место по популярности. Злоумышленники продолжили модифицировать и обфусцировать эксплойты к уже известным уязвимостям CVE-2017-11882, CVE-2018-0802, CVE-2017-8570 и CVE-2017-0199, что позволяло им в течение определенного времени обходить защитные механизмы в некоторых антивирусных решениях.

В этом году подходит конец жизни продукта Adobe Flash, но наши данные показывают, что интерес злоумышленников к нему не ослабевает: количество атак, которые эксплуатируют ошибки Flash, выросло на 0,7 п. п. Веб-браузеры в отчетном периоде сохраняют показатели на отметке 15,82% и остаются одним из основных способов заражения незащищенных пользовательских систем. Доля атак на Android (9,93%) с использованием уязвимостей уменьшилась на 2,6 п. п. Незначительно изменилось количество эксплойтов, которые используют уязвимости Java-платформы (4,10%) и уязвимости в PDF (0,97%).



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, ноябрь 2019 года — ноябрь 2020 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.

Как и ранее, сетевые атаки были в 2020 году самым распространенным способом проникновения в системы, причем значительная их часть представляла собой перебор паролей для различных сетевых служб: RDP, MSSQL и т. п. Также этот отчетный период показал нам, что в операционной системе Windows все циклично и большинство обнаруженных уязвимостей существуют в одних и тех же сервисах, например в драйверах сетевых протоколов SMB (SMBGhost, SMBBleed), DNS (SigRed), ICMPv6 (BadNeighbor). Две критические уязвимости (CVE-2020-0609 и CVE-2020-0610) были найдены в службе Remote Desktop Gateway. Также была обнаружена интересная уязвимость в сетевом сервисе NetLogon, она получила название Zerologon. Наконец, несмотря на то, что эксплойты семейства EternalBlue и EternalRomance являются уже старыми, они все еще используются злоумышленниками.

Атаки на macOS

За отчетный период мы обнаружили не только модификации уже известных зловредов для macOS, но и несколько новых угроз. Среди них два бэкдора — Capip и Lador. Последний особо примечателен тем, что написан на языке Go, а его размер составляет 5,5 мегабайт, что в разы больше аналогичных зловредов, написанных на языке Objective C. Также из интересного — вымогатель с функцией саморепликации Virus.OSX.ThifQseut.a, он же EvilQuest.

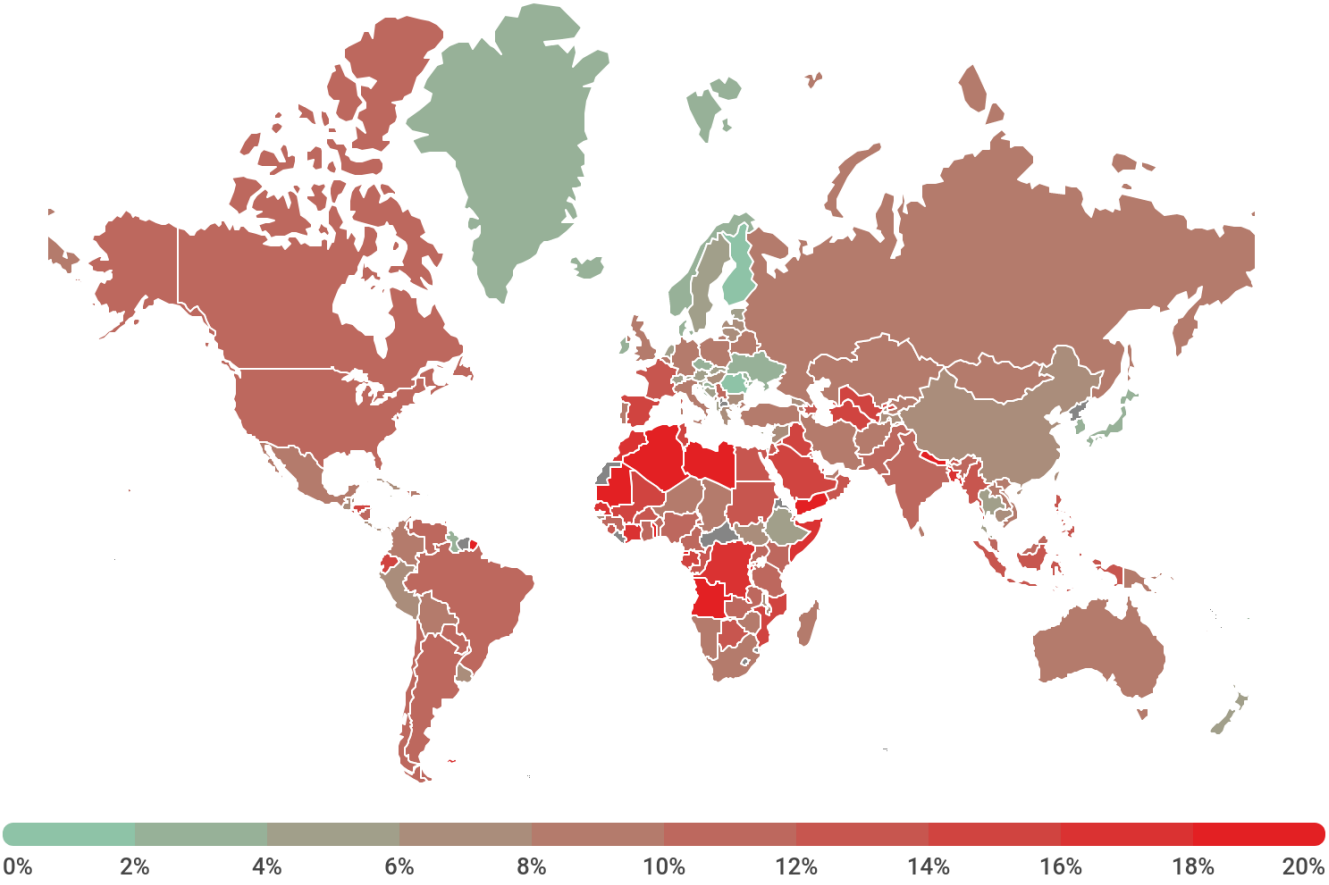
TOP 20 угроз для macOS

	Вердикт	%*
1	Trojan-Downloader.OSX.Shlayer.a	17,27
2	Monitor.OSX.HistGrabber.b	9,10
3	AdWare.OSX.Pirrit.j	8,08
4	AdWare.OSX.Cimpli.k	6,99
5	AdWare.OSX.Pirrit.x	6,93
6	AdWare.OSX.Bnodlero.at	6,33
7	AdWare.OSX.Pirrit.o	5,41
8	AdWare.OSX.Ketin.h	5,33
9	AdWare.OSX.Bnodlero.t	5,14
10	AdWare.OSX.Spc.a	4,95%

* Доля уникальных пользователей, столкнувшихся с данным зловредом, от всех атакованных пользователей защитных решений «Лаборатории Касперского» для macOS.

Большую часть нашего TOP 10 за отчетный период заняли рекламные программы. Однако на первом месте оказался троянец Shlayer, о котором мы писали еще в начале 2020 года.

География угроз



География угроз для macOS,
ноябрь 2019 года — октябрь 2020 года

kaspersky

TOP 10 стран по доле атакованных пользователей

	Страна*	%**
1	Испания	14,03
2	Франция	13,54
3	Канада	11,35
4	США	10,76
5	Индия	10,53
6	Бразилия	10,22
7	Мексика	9,86
8	Италия	9,80
9	Австралия	9,09
10	Великобритания	8,99

* Из рейтинга мы исключили страны, где количество пользователей защитных решений «Лаборатории Касперского» для macOS относительно мало (менее 5000).

** Доля уникальных атакованных пользователей в стране по отношению ко всем пользователям защитных решений для macOS «Лаборатории Касперского» в стране.

Атаки на IoT

Статистика IoT-угроз

За отчетный период более 80% атак на ловушки «Лаборатории Касперского» проводились по протоколу Telnet.

Telnet	81,02%
SSH	18,98%

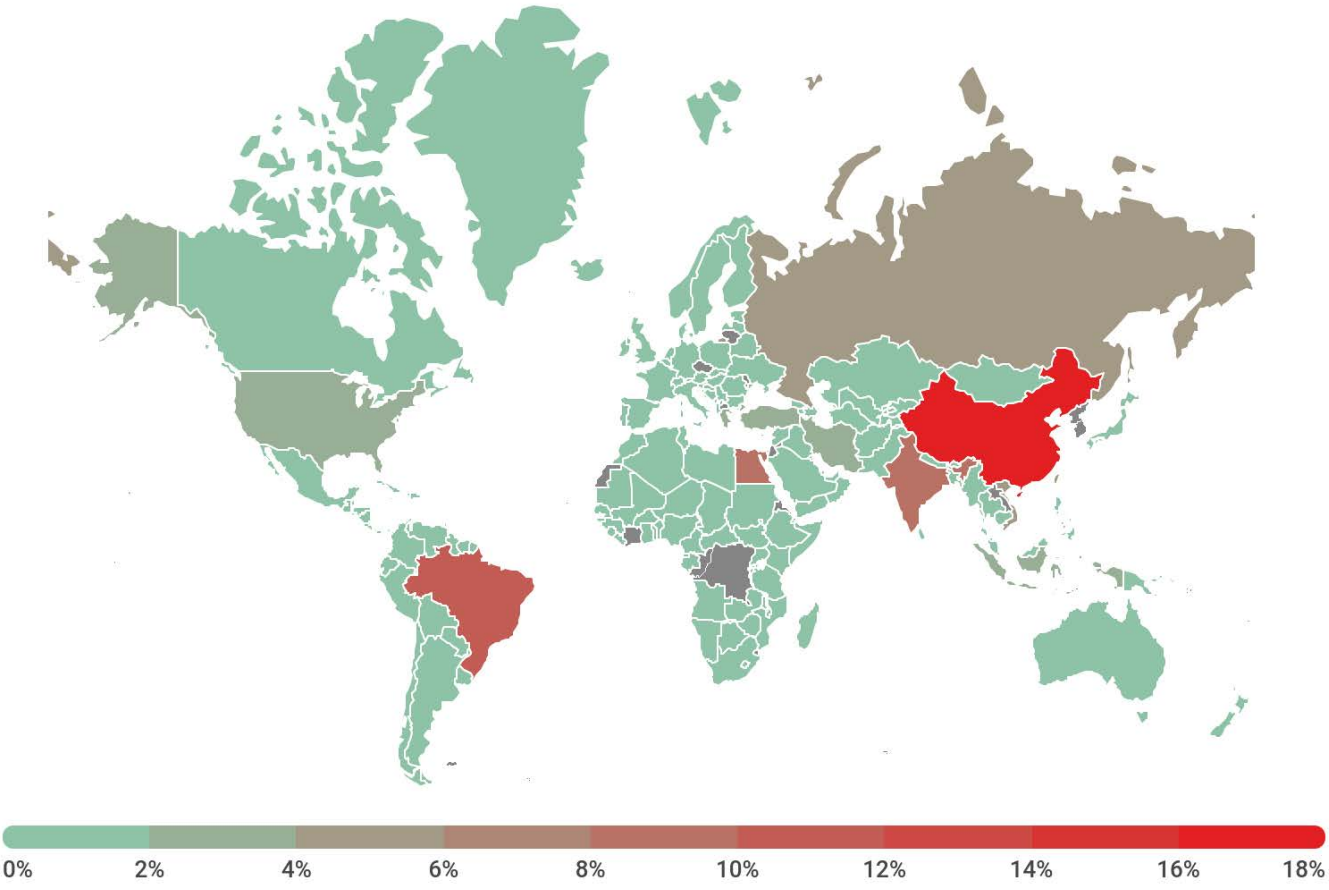
Таблица распределения атакуемых сервисов по числу уникальных IP-адресов устройств, проводивших атаки, ноябрь 2019 года — октябрь 2020 года

Что касается распределения количества сессий, то тут также превалирует Telnet — две трети всех рабочий сессий осуществлялись по этому протоколу.

Telnet	67,60%
SSH	32,40%

Таблица распределения рабочих сессий киберпреступников с ловушками «Лаборатории Касперского», ноябрь 2019 года — октябрь 2020 года

В результате именно устройства, осуществлявшие атаки по протоколу Telnet, были выбраны для построения карты распределения IP-адресов атакующих.



География IP-адресов устройств, с которых осуществлялись атаки на Telnet-ловушки «Лаборатории Касперского», ноябрь 2019 года — октябрь 2020 года

TOP 10 стран, где располагались устройства, с которых осуществлялись атаки на Telnet-ловушки «Лаборатории Касперского»

	Страна*	%**
1	Китай	17,95
2	Бразилия	10,35
3	Египет	9,26
4	Индия	8,51
5	Тайвань, провинция Китая	5,11
6	Вьетнам	4,94
7	Россия	4,00
8	Иран	3,96
9	Турция	2,46
10	США	2,42

* Доля устройств, с которых осуществлялись атаки, в определенной стране от общего количества устройств.

Угрозы, загружаемые в ловушки

	Вердикт	%*
1	Trojan-Downloader.Linux.NyaDrop.b	42,43
2	Backdoor.Linux.Mirai.b	27,01
3	Backdoor.Linux.Mirai.ba	10,09
4	Backdoor.Linux.Gafgyt.a	7,46
5	Backdoor.Linux.Gafgyt.bj	1,54
6	Trojan-Downloader.Shell.Agent.p	0,83
7	Backdoor.Linux.Mirai.cn	0,73
8	Backdoor.Linux.Mirai.cw	0,64
9	Backdoor.Linux.Mirai.h	0,53
10	Backdoor.Linux.Mirai.c	0,51

* Доля определенного зловреда от общего количества вредоносных программ, загруженных на IoT-устройства в результате успешной атаки.

Атаки через веб-ресурсы

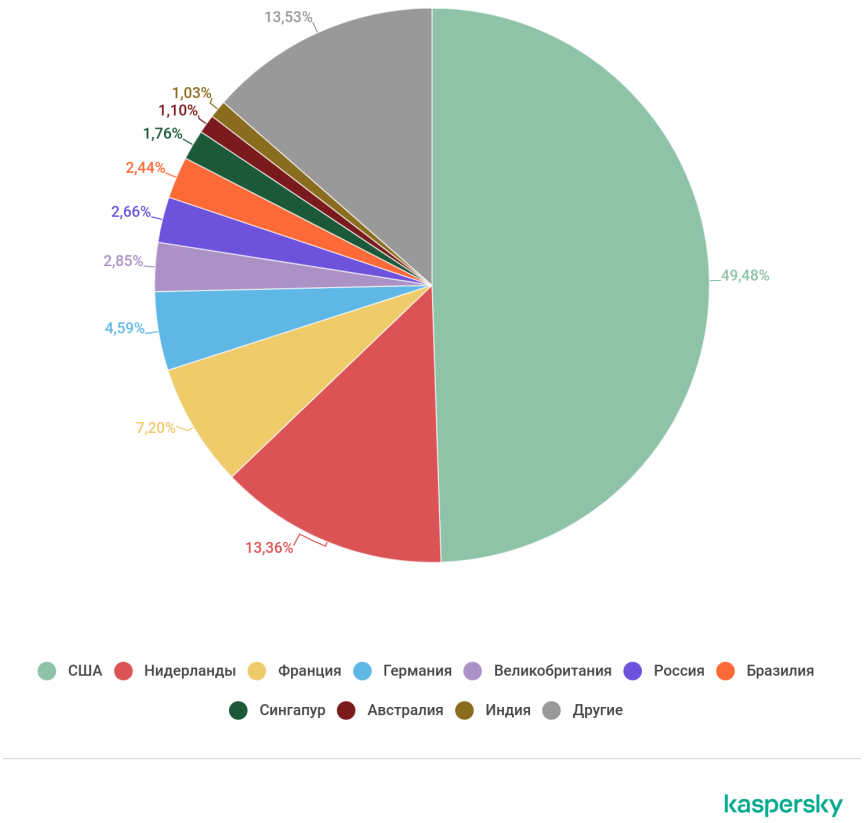
Статистические данные в этой главе получены на основе работы веб-антивируса, который защищает пользователей в момент загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Вредоносные сайты злоумышленники создают целенаправленно; зараженными могут быть веб-ресурсы, где контент создается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

Страны — источники веб-атак

Данная статистика показывает распределение по странам источников заблокированных продуктами «Лаборатории Касперского» интернет-атак на компьютеры пользователей (веб-страницы с редиректами на эксплойты, сайты с эксплойтами и другими вредоносными программами, центры управления ботнетами и т. д.). Отметим, что каждый уникальный хост мог быть источником одной или нескольких веб-атак.

Для определения географического источника 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 **666 809 967** атак, которые проводились с интернет-ресурсов, размещенных в разных странах мира. При этом 86,47% от общего количества этих ресурсов были расположены всего в 10 странах.



Распределение источников веб-атак по странам, ноябрь 2019 года — октябрь 2020 года

Как и в 2019 году, первое место среди стран-источников веб-атак занимают США (49,48%), их доля выросла на 6 п. п. Германия (4,59%) спустилась с третьей на четвертую позицию, а ее место заняла Франция (7,20%).

Страны, в которых пользователи подвергались наибольшему риску заражения через интернет

Чтобы оценить риск 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.

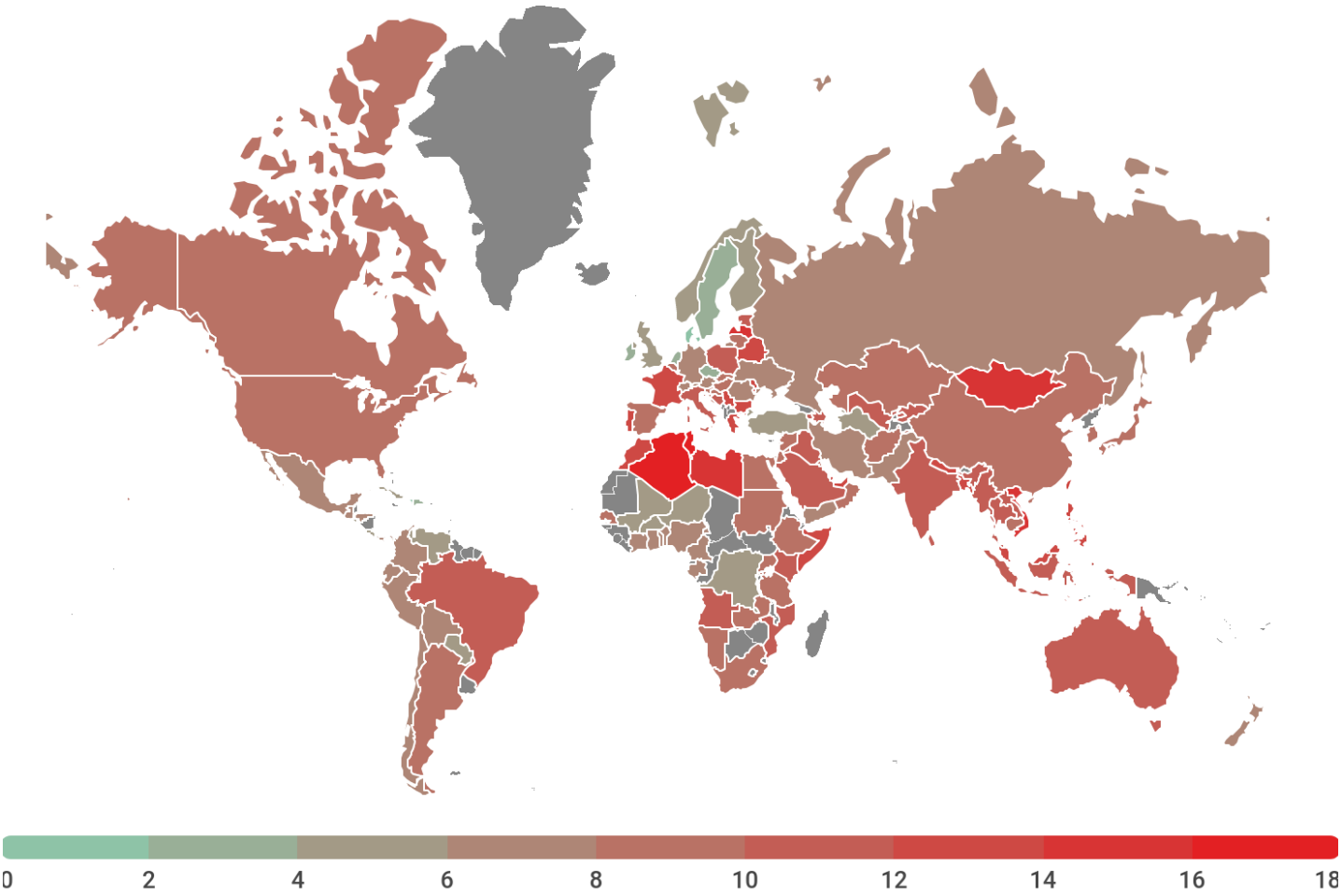
Напомним, что в этом рейтинге учитываются только атаки вредоносных объектов класса Malware; при подсчетах мы не учитывали срабатывания веб-антивируса на потенциально опасные и нежелательные программы, такие как RiskTool и рекламные программы. В целом за отчетный период рекламные программы и их компоненты 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	Тунис	18,27
2	Алжир	16,42
3	Монголия	15,94
4	Вьетнам	15,61
5	Латвия	14,73
6	Ливия	14,25
7	Греция	13,96
8	Бангладеш	13,75
9	Тайвань, провинция Китая	13,62
10	Франция	13,58
11	Болгария	13,37
12	Непал	13,15
13	Филиппины	12,99
14	Португалия	12,79
15	Катар	12,75
16	Марокко	12,71
17	Малайзия	12,55
18	Республика Молдова	12,55
19	Белоруссия	12,54
20	Сомали	12,45

* 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 **10,18%** компьютеров пользователей интернета в мире хотя бы один раз подвергались веб-атаке с участием ПО класса Malware.



kaspersky

**География веб-атак вредоносного ПО,
ноябрь 2019 года — октябрь 2020 года**

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

За отчетный период веб-антивирус «Лаборатории Касперского» выявил **33 412 568** уникальных вредоносных объектов (скриптов, эксплойтов, исполняемых файлов и т. д.) и **173 335 902** 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.

kaspersky

	Вердикт*	%**
1	Malicious URL	66,07
2	Trojan.Script.Generic	9,25
3	Trojan.Multi.Preqw.gen	6,10
4	Trojan.BAT.Miner.gen	3,57
5	Trojan.Script.Miner.gen	3,43
6	Hoax.HTML.FraudLoad.m	1,38
7	Trojan.PDF.Badur.gen	1,12
8	Backdoor.HTTP.TeviRat.gen	0,51
9	Trojan-Downloader.Script.Generic	0,50
10	Trojan-PSW.Script.Generic	0,47
11	Exploit.MSOffice.CVE-2017-11882.gen	0,38
12	DangerousObject.Multi.Generic	0,36
13	Trojan-Clicker.HTML.IFrame.dg	0,23
14	Trojan.Script.Redirector.gen	0,22
15	Hoax.Script.Loss.gen	0,19
16	Exploit.Script.Generic	0,17
17	Trojan.MSOffice.SAgent.gen	0,13
18	Trojan.Script.Agent.bg	0,13
19	Trojan-Downloader.JS.SLoad.gen	0,12
20	Trojan-Downloader.MSOffice.SLoad.gen	0,12

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

В отчетном периоде первое место традиционно занял вердикт Malicious URL (66,07%). Пользователи видят его, когда наши решения блокируют попытки перехода по уже известным опасным ссылкам, ведущим на ресурсы с эксплойтами и другим вредоносным ПО, C&C ботнетов, сайты вымогателей и т. д.

Несколько веб-майнеров, таких как Trojan.Script.Miner.gen, все еще занимают места в нашем TOP 20, однако скрытый майнинг уже далеко не так популярен, как пару лет назад.

Детекты из нашего TOP 20, содержащие в названии MS Office или PDF, — это различные вредоносные документы, использующиеся в спам-рассылках. Как правило, их задачей является доставка полезной нагрузки, например банкера Emotet, и именно ее скачивание блокирует наш веб-антивирус.

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	26,59
2	Trojan.Multi.BroSubsc.gen	20,44
3	Trojan.Multi.GenAutorunReg.a	7,99
4	Trojan.Multi.Misslink.a	7,47
5	Trojan.Script.Generic	6,45
6	Trojan.WinLNK.Agent.gen	3,00
7	Trojan.Win32.SEPEH.gen	2,88
8	Trojan.Win32.Generic	2,53
9	Trojan.WinLNK.Starter.gen	2,45
10	Trojan.Multi.Agent.gen	2,12
11	Trojan.WinLNK.Runner.jo	2,02
12	Trojan.Win32.AutoRun.gen	1,91
13	Trojan.Multi.GenAutorunTask.c	1,91
14	Virus.Win32.Sality.gen	1,84
15	Trojan.Multi.GenAutorunTask.a	1,76
16	Trojan.Multi.GenAutorunTaskFile.a	1,73
17	Trojan-Downloader.Script.Generic	1,64
18	Trojan.AndroidOS.Boogr.gsh	1,59

	Вердикт*	%**
19	Trojan.Multi.GenBadur.gen	1,52
20	Virus.Win32.Pioneer.cz	1,51

* Из списка исключены угрозы типа HackTool.
** 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 отчетном периоде занял вердикт DangerousObject.Multi.Generic (26,59%), который мы используем для вредоносных программ, обнаруженных с помощью облачных технологий. Эти технологии срабатывают, когда в антивирусных базах еще нет данных для детектирования вредоносной программы, но в облаке антивирусной компании уже есть информация об объекте. По сути, так детектируются самые новые вредоносные программы.

Страны, в которых компьютеры пользователей подвергались наибольшему риску локального заражения

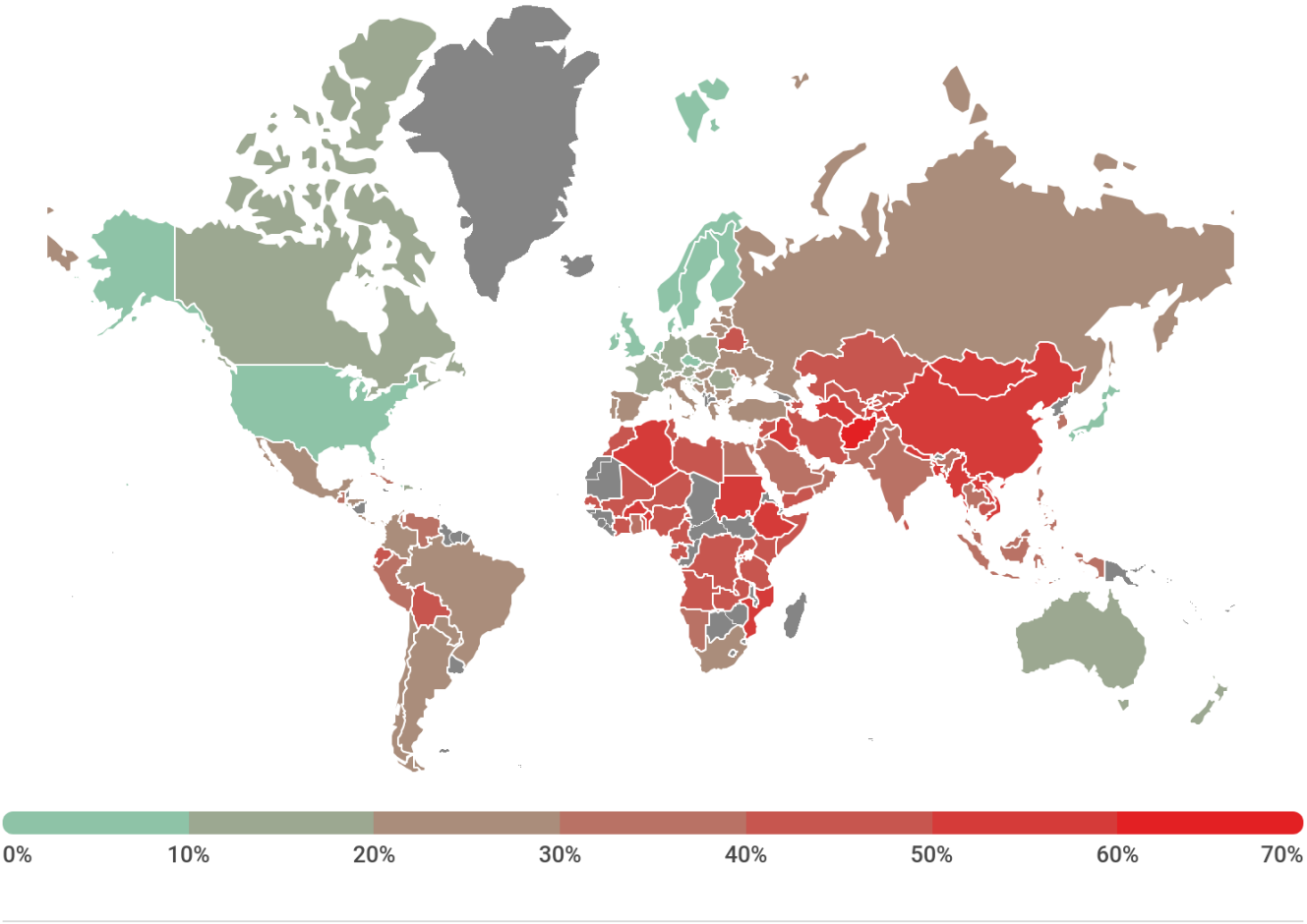
Для каждой из стран мы подсчитали, как часто ее пользователи сталкивались со срабатыванием файлового антивируса в течение года. Учитывались детектируемые объекты, найденные непосредственно на компьютерах пользователей или же на подключенных к ним съемных носителях (флешках, картах памяти фотоаппаратов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

TOP 20 стран по уровню риска локального заражения

	Страна*	%**
1	Афганистан	63,52
2	Мьянма	59,89
3	Лаос	57,40
4	Вьетнам	56,84
5	Монголия	55,11
6	Китай	54,81
7	Бангладеш	54,74
8	Эфиопия	54,67
9	Руанда	53,22
10	Буркина-Фасо	52,57
11	Туркменистан	52,47
12	Бенин	52,43
13	Таджикистан	52,29
14	Алжир	51,85
15	Ирак	51,73

	Страна*	%**
16	Мозамбик	50,98
17	Судан	50,88
18	Непал	50,07
19	Танзания	49,34
20	Кот-д'Ивуар	49,31

* 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 2019 года — октябрь 2020 года

В отчетный период хотя бы одна вредоносная программа была обнаружена в среднем на **28,65%** компьютеров, жестких дисков или съемных носителей, принадлежащих пользователям решений «Лаборатории Касперского».

kaspersky