Kaspersky Security Bulletin 2023

Kaspersky Security Bulletin 2023. Статистика

kaspersky bring on the future

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» по всему миру. Собранная статистика охватывает период с ноября 2022 по октябрь 2023 года включительно.

Цифры года

За отчетный период решения «Лаборатории Касперского»:

- Отразили **437 414 681** вредоносную атаку, которые проводились с интернет-ресурсов, размещенных в различных странах мира.
- Обнаружили **106 357 530** уникальных вредоносных URL, на которых происходило срабатывание веб-антивируса.
- Заблокировали с помощью веб-антивируса **112 922 612** уникальных вредоносных объектов.
- Отразили атаки шифровальщиков на компьютерах **193 662** уникальных пользователей.
- Предотвратили атаки майнеров на **1 140 573** уникальных пользователей.
- Заблокировали попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на устройствах **325 225** уникальных пользователей.

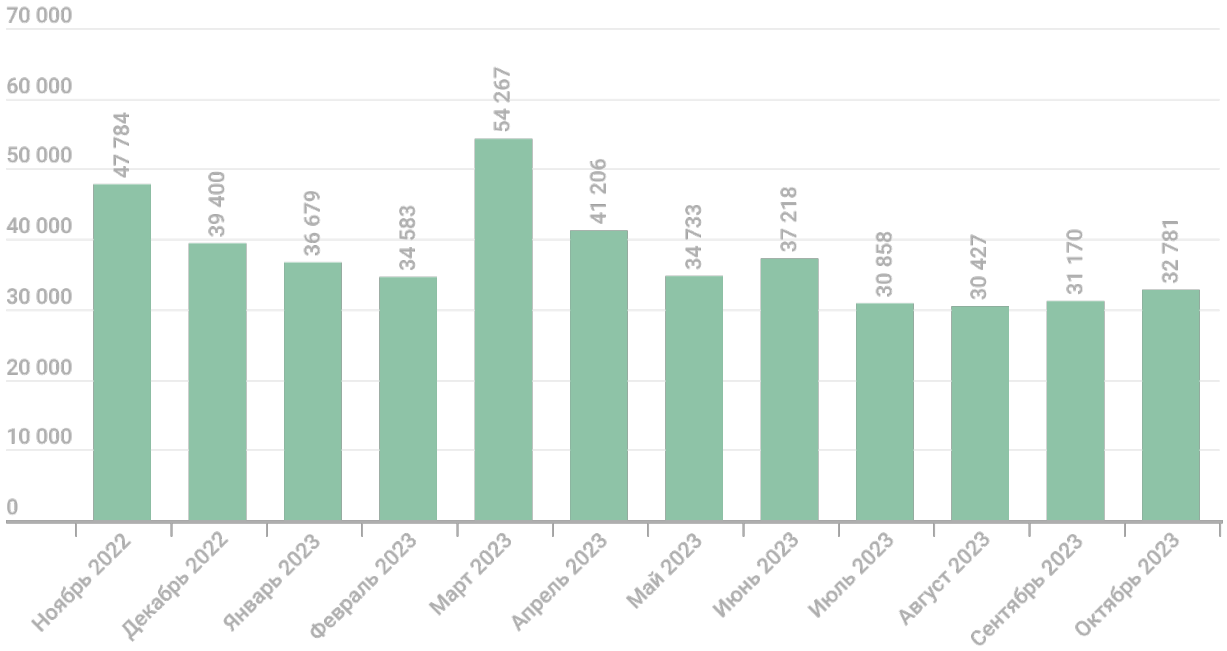
Статистика по мобильным угрозам будет представлена в отчете «Ландшафт мобильных угроз в 2023 году»

Финансовые угрозы

Представленная статистика включает не только банковские угрозы, но также вредоносные программы для банкоматов и терминалов оплаты.

Количество пользователей, атакованных финансовыми зловредами

За отчетный период решения «Лаборатории Касперского» отразили попытки запуска одного или нескольких финансовых зловредов на компьютерах **325 225** пользователей.



Количество пользователей, атакованных финансовым вредоносным ПО,
ноябрь 2022 года — октябрь 2023 года

География атак

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

TOP 10 стран и территорий по доле атакованных пользователей

	Страны и территории*	%**
1	Афганистан	6,2
2	Туркменистан	5,4
3	Таджикистан	4,0
4	Китай	3,3
5	Судан	2,6
6	Мавритания	2,6
7	Швейцария	2,5
8	Йемен	2,4
9	Египет	2,2
10	Парагвай	2,2

* При расчетах мы исключили те страны и территории, где 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.

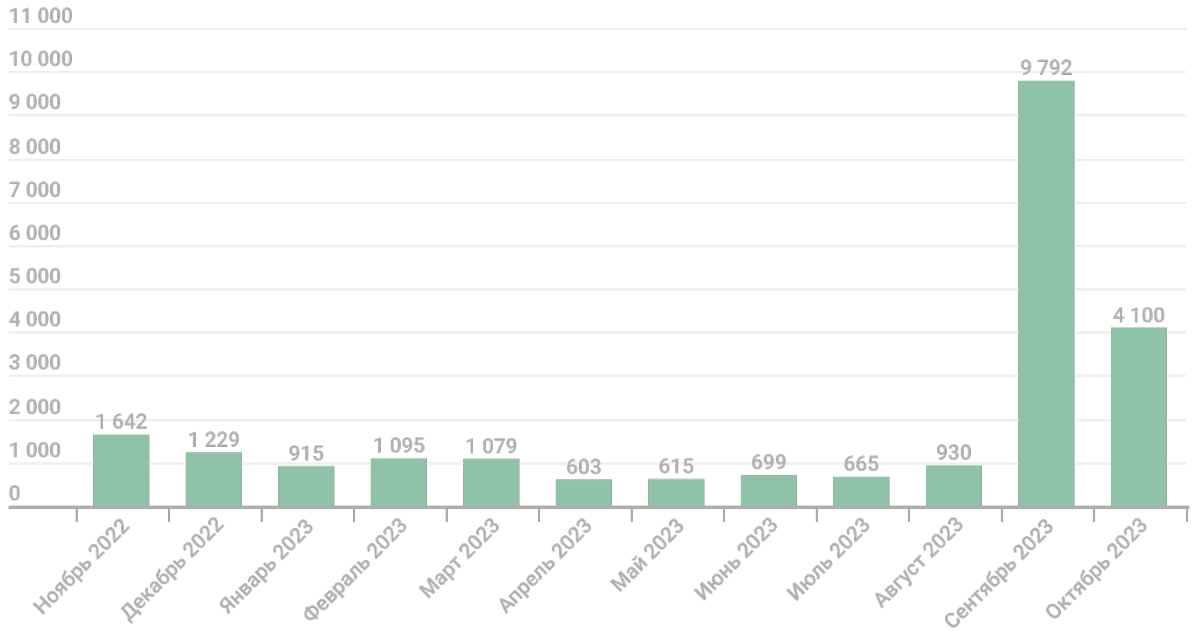
TOP 10 семейств финансового вредоносного ПО

	Название	Вердикт	%*
1	Ramnit/Nimnul	Trojan-Banker.Win32.Nimnul	30,4
2	Zbot/Zeus	Trojan-Spy.Win32.Zbot	18,9
3	Emotet	Trojan-Banker.Win32.Emotet	16,1
4	CliptoShuffler	Trojan-Banker.Win32.CliptoShuffler	6,1
5	RTM	Trojan-Banker.Win32.RTM	2,2
6	Danabot	Trojan-Banker.Win32.Danabot	1,9
7	Qbot/Qakbot	Trojan-Banker.Win32.Qbot	1,8
8	IcedID	Trojan-Banker.Win32.IcedID	1,3
9	Tinba/TinyBanker	Trojan-Banker.Win32.Tinba	1,2
10	BitStealer	Trojan-Banker.Win32.BitStealer	1,0

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

Вредоносные программы-шифровальщики

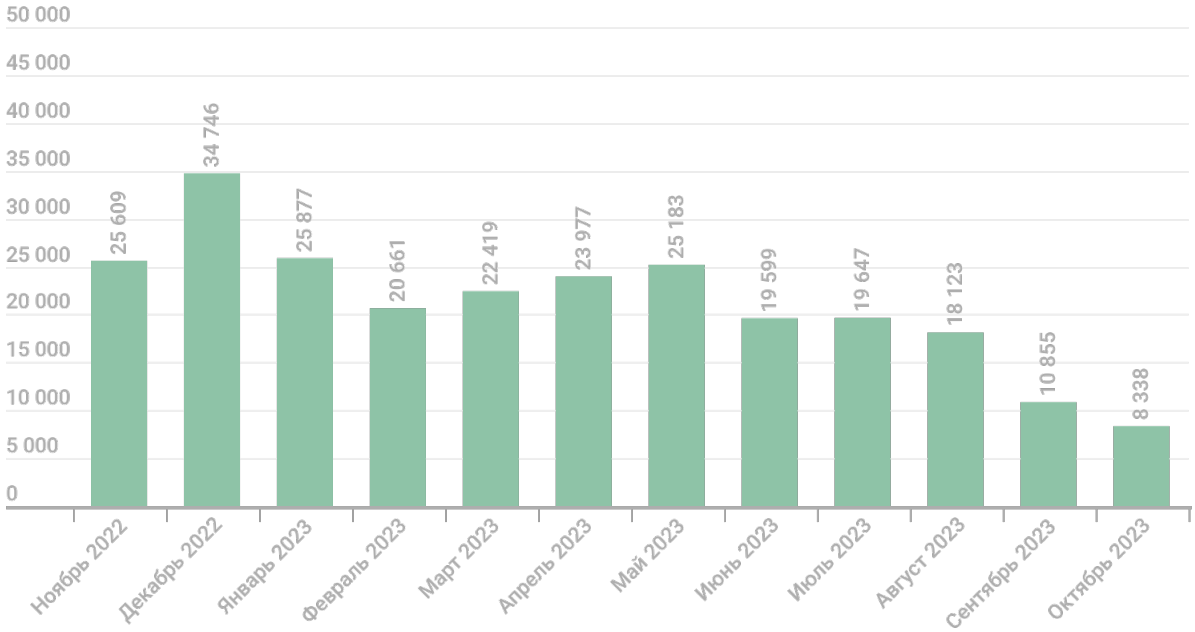
За отчетный период мы выявили **23 364** модификации шифровальщиков и обнаружили **43** новых семейства. Отметим, что отдельное семейство мы создавали не для каждого нового шифровальщика. Большей части угроз этого типа присваивался generic-вердикт, который мы используем при обнаружении новых и неизвестных образцов.



Количество новых модификаций шифровальщиков,
ноябрь 2022 года — октябрь 2023 года

Количество пользователей, атакованных троянцами-шифровальщиками

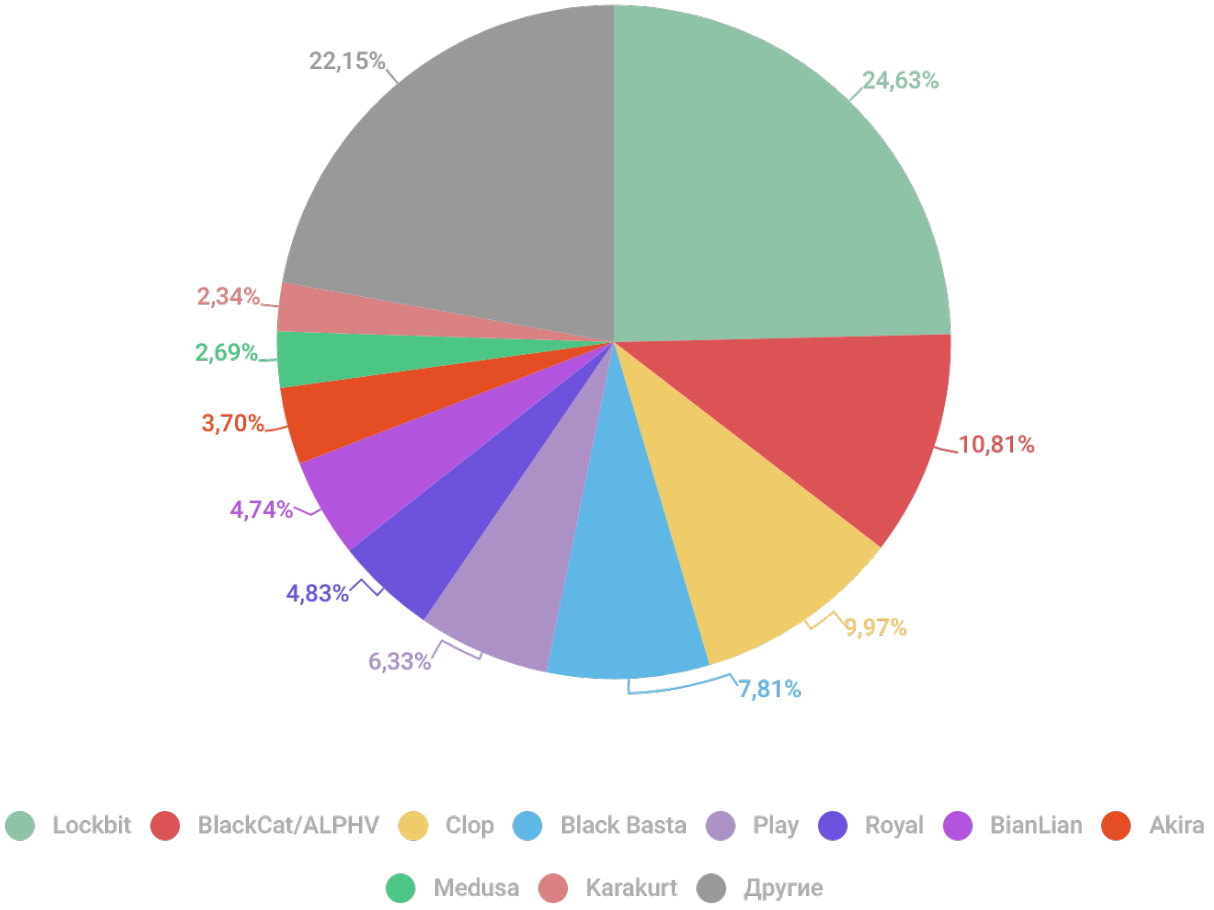
За отчетный период троянцы-шифровальщики атаковали **193 662** уникальных пользователей, в том числе **52 999** корпоративных пользователей (за вычетом SMB) и **6351** пользователя, связанного с малым и средним бизнесом.



Количество пользователей, атакованных троянцами-шифровальщиками,
ноябрь 2022 года — октябрь 2023 года

Наиболее активные группировки

В этом разделе мы рассматриваем группировки вымогателей, которые занимаются так называемым двойным вымогательством — шифрованием файлов и кражей конфиденциальных данных. Такие группировки в большинстве своем атакуют крупные компании и часто ведут свой сайт (data leak site, DLS), где публикуют список атакованных организаций.



Наиболее активные группировки вымогателей, ноябрь 2022 года — октябрь 2023 года

На диаграмме указана доля жертв конкретной группировки (по данным сайта DLS конкретной группировки) среди жертв всех группировок, опубликованных на всех рассмотренных сайтах DLS.

География атак

TOP 10 стран и территорий, подвергшихся атакам троянцев-шифровальщиков

	Страны и территории*	%**
1	Бангладеш	2,41
2	Йемен	1,85
3	Тайвань	1,62
4	Южная Корея	1,47
5	Судан	1,15
6	Мозамбик	1,09
7	Палестина	0,97
8	Афганистан	0,97
9	Пакистан	0,88
10	Туркменистан	0,63

* При расчетах мы исключили те страны и территории, где число пользователей «Лаборатории Касперского» относительно мало (меньше 50 тысяч).

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

TOP 10 наиболее распространенных семейств троянцев-шифровальщиков

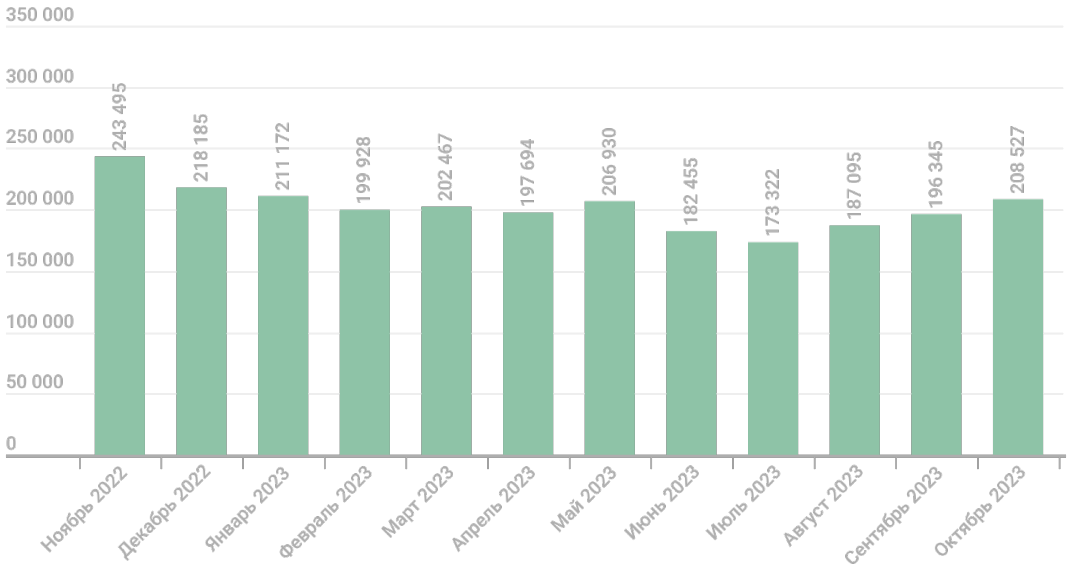
	Название	Вердикт	%*
1	Magniber	Trojan-Ransom.Win64.Magni	17,14
2	(generic verdict)	Trojan-Ransom.Win32.Gen	12,39
3	WannaCry	Trojan-Ransom.Win32.Wanna	11,46
4	(generic verdict)	Trojan-Ransom.Win32.Encoder	9,43
5	Stop/Djvu	Trojan-Ransom.Win32.Stop	6,39
6	(generic verdict)	Trojan-Ransom.Win32.Phny	5,69
7	(generic verdict)	Trojan-Ransom.Win32.Crypren	4,54
8	PolyRansom/VirLock	Virus.Win32.PolyRansom / Trojan-Ransom.Win32.PolyRansom	3,13
9	(generic verdict)	Trojan-Ransom.Win32.Agent	2,91
10	(generic verdict)	Trojan-Ransom.MSIL.Crypmodng	1,75

* Доля уникальных пользователей «Лаборатории Касперского», столкнувшихся с атаками определенного семейства троянцев-вымогателей, от всех пользователей, столкнувшихся с атаками троянцев-вымогателей.

Программы-майнеры

Количество пользователей, атакованных майнерами

За отчетный период мы зафиксировали попытки установки майнера на компьютерах **1 140 573** уникальных пользователей. В общем объеме атак доля майнеров составила 3,12%, а среди всех программ типа Risktool — 17,09%.



Количество пользователей, атакованных майнерами, ноябрь 2022 года — октябрь 2023 года

Чаще других за отчетный период продукты «Лаборатории Касперского» обнаруживали Trojan.Win32.Miner.gen — на его долю пришлось 25,12% от общего количества атакованных майнерами пользователей. Следом идут Worm.NSIS.BitMin.d (12,39%), Trojan.Win32.Miner.ays (10,41%) и Trojan.Win64.Miner.all (8,51%).

География атак

TOP 10 стран и территорий, подвергшихся атакам майнеров

	Страны и территории*	%**
1	Туркменистан	10,38
2	Афганистан	7,67
3	Казахстан	3,77
4	Таджикистан	3,33
5	Узбекистан	2,92
6	Монголия	2,83
7	Мозамбик	2,82
8	Беларусь	2,80
9	Судан	2,65
10	Кыргызстан	2,61

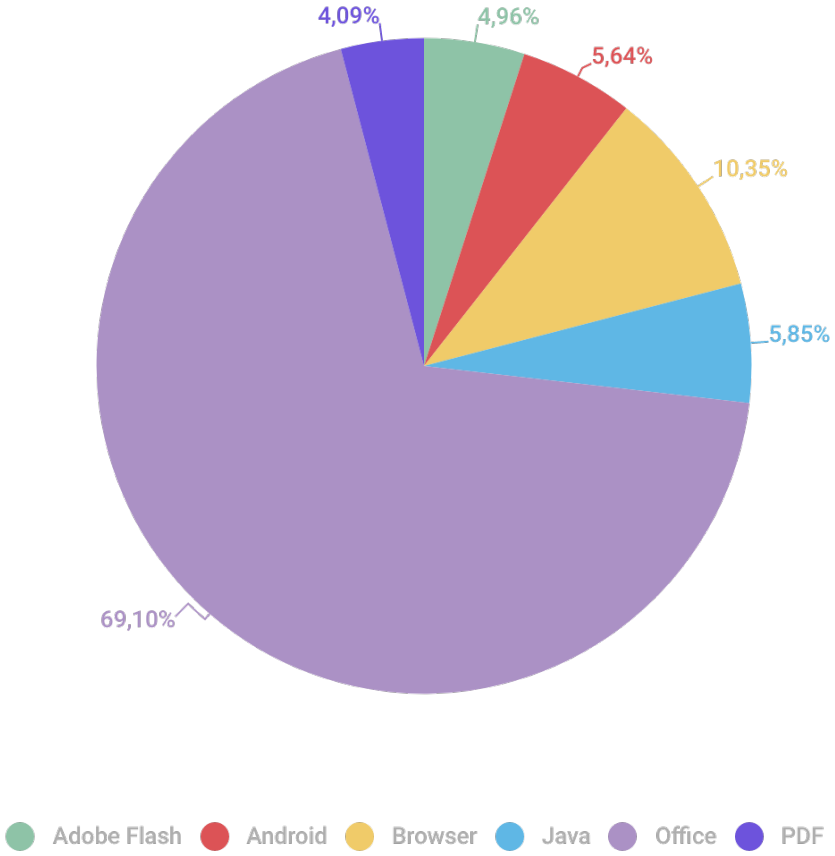
* При расчетах мы исключили страны и территории, где число пользователей «Лаборатории Касперского» относительно мало (меньше 50 тысяч).

** Доля уникальных пользователей, компьютеры которых были атакованы майнерами, от всех уникальных пользователей продуктов «Лаборатории Касперского» в определенном регионе.

Уязвимые приложения, используемые злоумышленниками в ходе кибератак

Отчетный период запомнился появлением ряда громких уязвимостей в бизнес-приложениях, например CVE-2023-34362, CVE-2023-35036 и CVE-2023-35708 в MOVEit Transfer или CVE-2023-23397 в Microsoft Outlook.

Если говорить об атаках на пользовательские системы, то здесь стоит отметить уязвимости «нулевого дня» CVE-2023-4863, CVE-2023-5217 и CVE-2023-4762 в Google Chrome, а также CVE-2023-28252 в ОС Windows. Традиционно мы видели попытки эксплуатировать хорошо известные уязвимости в Equation Editor (например, CVE-2017-11882 и CVE-2018-0802) и других компонентах пакета MS Office.



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, ноябрь 2022 года — октябрь 2023 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.

Атаки на macOS

За отчетный период появились несколько интересных зловредов для macOS:

- Шпион, похищающий Keychain.
- Распространяющийся под видом игр шпион для кражи различных данных из браузеров, мессенджеров и криптокошельков.
- Зараженный Xcode-проект, который загружает бэкдор.
- Продающиеся в Telegram троянцы MacStealer и AMOS для кражи паролей и файлов.
- Supply-chain атака на 3CX с загрузкой бэкдора.
- Бэкдоры на Rust от APT-группы BlueNoroff, которые распространялись под видом просмотрщиков PDF.

Решения "Лаборатории Касперского" детектируют эти и другие угрозы для macOS.

TOP 20 угроз для macOS

	Вердикт	%*
1	AdWare.OSX.Pirrit.ac	11,21
2	AdWare.OSX.Agent.ai	10,47
3	AdWare.OSX.Amc.e	8,83
4	AdWare.OSX.Pirrit.j	7,92
5	AdWare.OSX.Agent.gen	7,34
6	AdWare.OSX.Bnodlero.ax	6,77
7	AdWare.OSX.Pirrit.ae	5,83
8	Trojan-Downloader.OSX.Agent.h	4,85
9	Monitor.OSX.HistGrabber.b	4,70
10	Hoax.OSX.MacBooster.a	4,32

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

География угроз

TOP 10 стран и территорий по доле атакованных пользователей

	Страны и территории*	%**
1	Франция	2,41
2	Китай	2,38
3	Италия	2,38
4	Испания	2,23
5	США	2,16
6	Индия	2,16
7	Мексика	2,12
8	Канада	1,99
9	Австралия	1,85
10	Великобритания	1,84

* Из рейтинга мы исключили те страны и территории, где количество пользователей защитных решений «Лаборатории Касперского» для macOS относительно мало (меньше 5 тысяч).

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

Атаки на IoT

Статистика IoT-угроз

За отчетный период большинство устройств, атаковавших ловушки «Лаборатории Касперского», использовали протокол Telnet.

Telnet	83,85%
SSH	16,15%

Таблица распределения атакуемых сервисов по числу уникальных IP-адресов устройств, проводивших атаки, ноябрь 2022 года — октябрь 2023 года

Что касается распределения количества сессий, то тут также превалирует Telnet — более 98% всех рабочий сессий осуществлялись по этому протоколу.

Telnet	98,60%
SSH	1,40%

Таблица распределения рабочих сессий киберпреступников с ловушками «Лаборатории Касперского», ноябрь 2022 года — октябрь 2023 года

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

	Страны и территории*	%**
1	Китай	35,99
2	Индия	18,01
3	Бразилия	4,57
4	Россия	4,18
5	США	3,45
6	Южная Корея	2,35
7	Венесуэла	2,31
8	Тайвань	2,11
9	Аргентина	1,85
10	Иран	1,84

* Доля устройств, с которых осуществлялись атаки в определенном регионе, от общего количества атакующих устройств.

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

	Страны и территории*	%**
1	Китай	18,44
2	США	11,64
3	Южная Корея	6,36
4	Индия	5,25
5	Сингапур	4,65
6	Германия	4,50
7	Бразилия	4,34
8	Россия	3,62
9	Тайвань	3,01
10	Вьетнам	2,83

* Доля устройств, с которых осуществлялись атаки в определенном регионе, от общего количества атакующих устройств.

Угрозы, загружаемые в ловушки

	Вердикт	%*
1	Trojan-Downloader.Linux.NyaDrop.b	36,46
2	Backdoor.Linux.Mirai.b	18,67
3	Backdoor.Linux.Mirai.cw	8,23
4	Backdoor.Linux.Mirai.ba	7,12
5	Backdoor.Linux.Mirai.fg	3,64
6	Trojan.Linux.Agent.nx	3,12
7	Backdoor.Linux.Mirai.es	2,90
8	Backdoor.Linux.Gafgyt.a	2,36
9	Trojan-Downloader.Shell.Agent.p	2,04
10	Backdoor.Linux.Mirai.ew	1,83

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

Атаки через веб-ресурсы

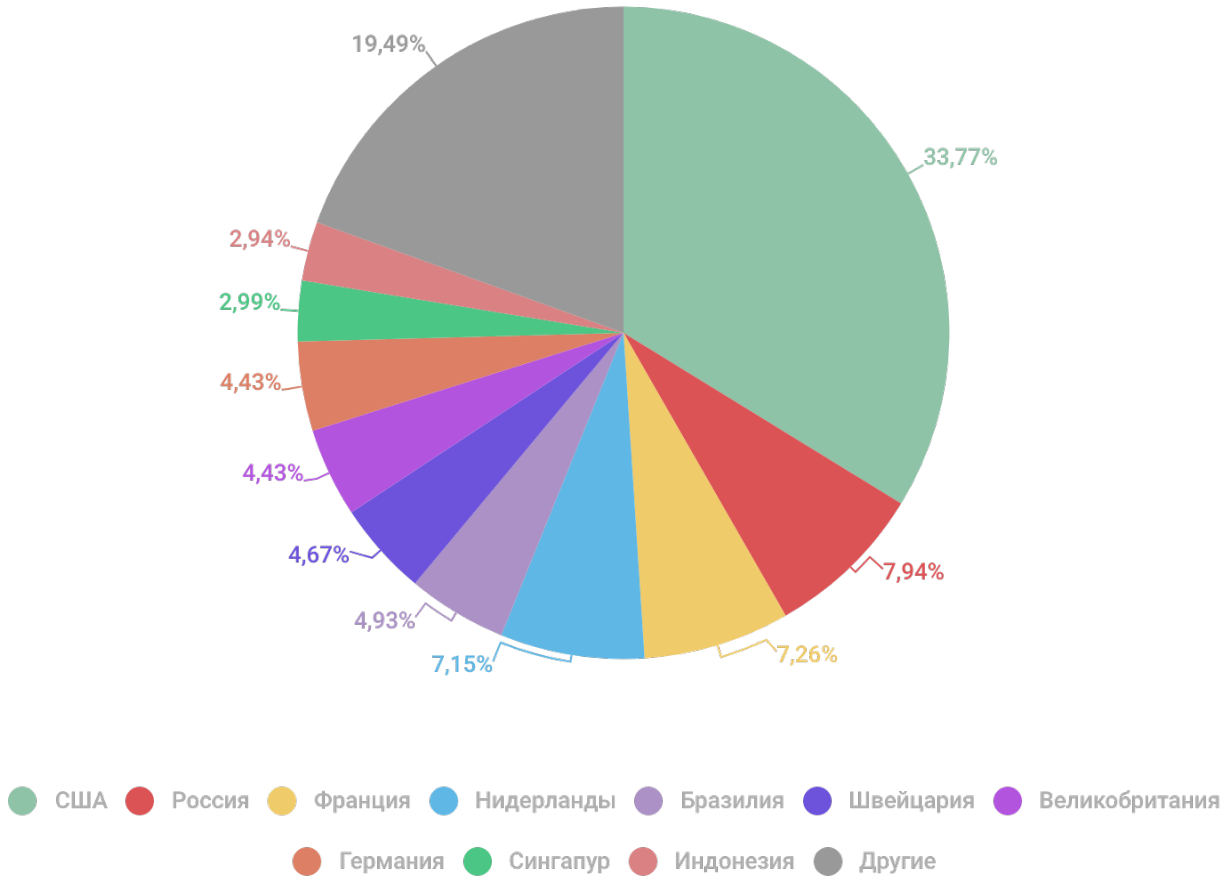
Статистические данные в этой главе получены на основе работы веб-антивируса, который защищает пользователей в момент загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Вредоносные сайты злоумышленники создают целенаправленно; зараженными могут быть веб-ресурсы, где контент создается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

Страны и территории — источники веб-атак

Данная статистика показывает распределение по странам и территориям 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 **437 414 681** вредоносную атаку, которые проводились с интернет-ресурсов, размещенных в разных странах мира. При этом **80,49%** от общего количества этих ресурсов были расположены всего в 10 странах.



Распределение источников веб-атак по странам,
ноябрь 2022 года — октябрь 2023 года

Страны и территории, где пользователи подвергались наибольшему риску заражения через интернет

Чтобы оценить риск заражения вредоносными программами через интернет, которому подвергаются компьютеры пользователей в разных странах и территориях мира, мы подсчитали в каждой долю 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 и территориях.

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 **88%** компьютеров пользователей, на которых происходило срабатывание веб-антивируса.

TOP 20 стран и территорий, где пользователи подвергались наибольшему риску заражения через интернет

	Страны и территории*	%**
1	Тайвань	24,41
2	Греция	24,12
3	Беларусь	22,65
4	Алжир	22,64
5	Турция	22,54
6	Сербия	22,09
7	Тунис	21,17
8	Молдавия	21,10
9	Непал	20,99
10	Бангладеш	20,81
11	Шри-Ланка	20,47
12	Босния и Герцеговина	20,20
13	Португалия	19,87
14	Катар	19,62
15	Марокко	19,50
16	Эквадор	19,02
17	Филиппины	18,55
18	Монголия	18,51
19	Перу	18,36
20	Россия	18,22

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

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

В среднем за отчетный период **16,31%** компьютеров пользователей интернета в мире хотя бы один раз подвергались веб-атаке с участием ПО класса Malware.

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

За отчетный период веб-антивирус «Лаборатории Касперского» выявил **112 922 612** уникальных вредоносных объектов (скриптов, эксплойтов, исполняемых файлов и т. д.) и **106 357 530** уникальных вредоносных URL. На основе собранных данных мы выделили 20 вредоносных программ, которые злоумышленники использовали в онлайн-атаках на компьютеры пользователей активнее всего.

	Вердикт*	%**
1	Malicious URL	47,62
2	Trojan.Script.Generic	26,21
3	Trojan.BAT.Miner.gen	4,57
4	Trojan.Script.Miner.gen	2,93
5	Hoax.HTML.Phish.gen	2,26
6	Trojan.PDF.Badur.gen	1,72
7	Trojan.Multi.Preqw.gen	1,53
8	Hoax.HTML.FraudLoad.m	1,16
9	Trojan.Script.Agent.gen	1,04
10	Trojan-Downloader.Script.Generic	1,01
11	Trojan.JS.Miner.gen	0,70
12	Trojan.JS.Agent.eqq	0,53
13	Trojan-PSW.Script.Generic	0,50
14	Exploit.Win32.CVE-2011-3402.a	0,44
15	DangerousObject.Multi.Generic	0,44
16	Exploit.Multi.Desert.gen	0,26
17	Trojan-Banker.PowerShell.CoinStealer.gen	0,23
18	Trojan.MSOffice.Generic	0,17
19	Exploit.MSOffice.CVE-2017-11882.gen	0,16
20	Trojan.MSOffice.Agent.gen	0,15

* Из списка исключены угрозы типа HackTool.

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

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 угрозы типа Riskware и рекламные программы.

	Вердикт*	%**
1	DangerousObject.Multi.Generic	17,87
2	Trojan.Multi.BroSubsc.gen	12,70
3	Trojan.Multi.Misslink.a	6,40
4	Trojan.Multi.GenAutorunReg.a	5,98
5	Trojan.Script.Generic	5,63
6	Trojan.Win32.Agent.gen	5,10
7	Trojan.Win32.SEPEH.gen	3,06
8	Trojan.WinLNK.Agent.gen	2,87
9	Trojan.Win32.Hosts2.gen	2,15
10	Trojan.Multi.GenBadur.gen	2,08
11	Trojan.Multi.Agent.gen	1,91
12	Virus.Win32.Pioneer.cz	1,78
13	Worm.Python.Agent.gen	1,65
14	Trojan.Win32.Agentb.bqyr	1,51
15	Trojan.Win32.Generic	1,48
16	Worm.Python.Agent.c	1,45
17	Trojan.Script.Agent.gen	1,41
18	VHO:Trojan.Win32.Sdum.gen	1,38
19	Trojan.Multi.Powesta.d	1,37
20	Trojan.MSIL.Agent.gen	1,34

* 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.

Страны и территории, где компьютеры пользователей подвергались наибольшему риску локального заражения

Для каждой из стран или территорий 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 и территориях мира.

TOP 20 стран и территорий по уровню риска локального заражения

	Страны и территории*	%**
1	Йемен	59,74
2	Туркменистан	59,71
3	Афганистан	58,74
4	Бангладеш	51,82
5	Мьянма	51,22
6	Алжир	49,40
7	Бенин	48,32
8	Руанда	48,19
9	Узбекистан	47,97
10	Гвинея	47,97
11	Камерун	47,08
12	Буркина-Фасо	47,05
13	Танзания	46,99
14	Ирак	46,13
15	Демократическая Республика Конго	45,94
16	Нигер	45,05
17	Венесуэла	44,70
18	Мали	44,64
19	Беларусь	44,57
20	Вьетнам	44,18

* При расчетах мы исключили страны и территории, где 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 определенном регионе.

В отчетном периоде хотя бы одна вредоносная программа была обнаружена в среднем на **26,33%** компьютеров, жестких дисков или съемных носителей, принадлежащих пользователям решений «Лаборатории Касперского».

kaspersky активируй будущее