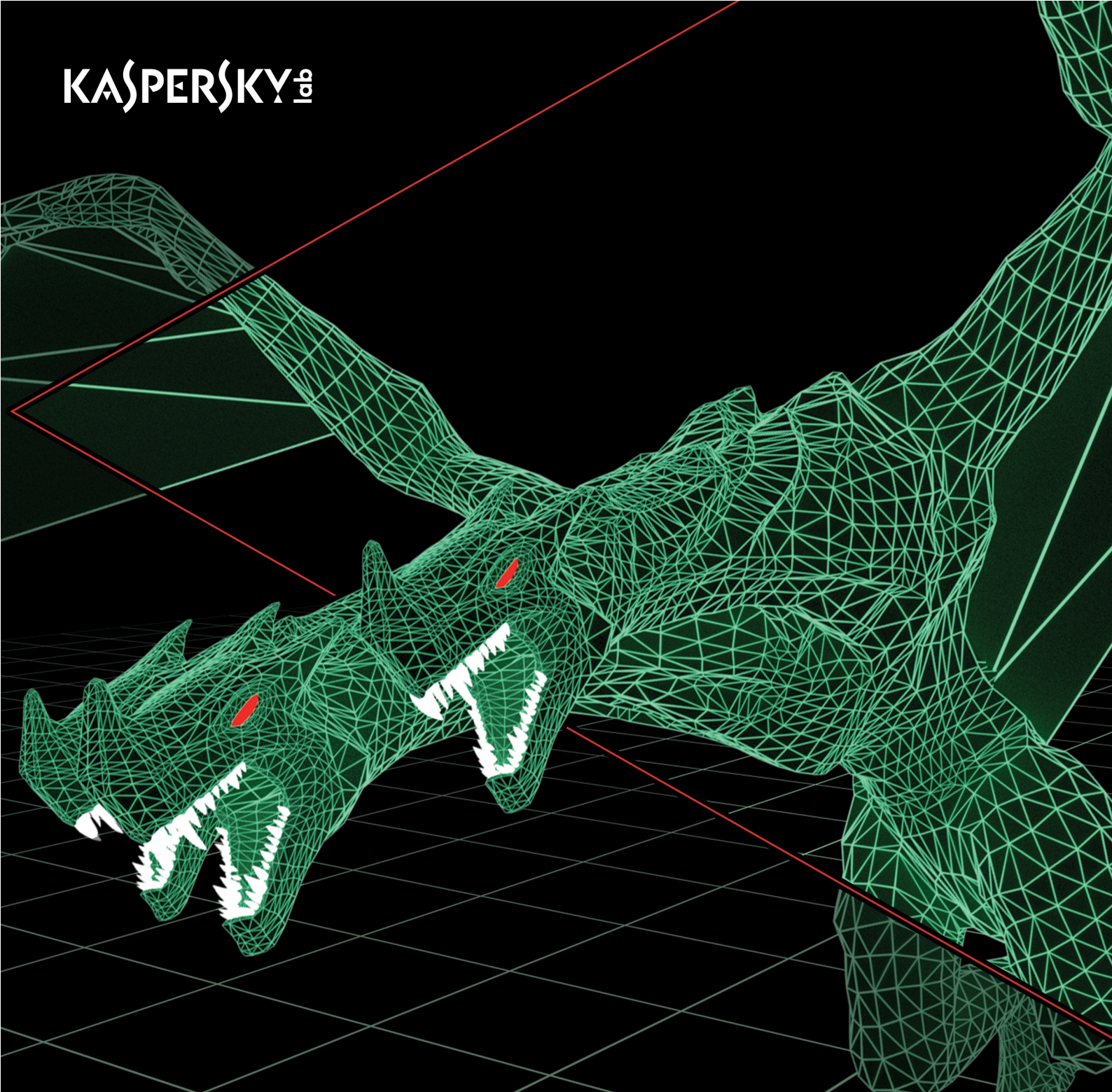
KASPERSKY lab



Kaspersky Security Bulletin 2016

СТАТИСТИКА

Мария Гарнаева, Федор Синицын, Юрий Наместников,
Денис Макрушин, Александр Лискин

GREAT

СОДЕРЖАНИЕ

Все статистические данные, использованные в отчете, получены с помощью распределенной антивирусной сети Kaspersky Security Network (KSN) как результат работы различных компонентов защиты от вредоносных программ. Данные получены от тех пользователей KSN, которые подтвердили свое согласие на их передачу. В глобальном обмене информацией о вредоносной активности принимают участие миллионы пользователей продуктов «Лаборатории Касперского» из 213 стран и территорий мира.

ЦИФРЫ ГОДА

- В 2016 году при серфинге в интернете веб-атакам вредоносных объектов класса Malware хотя бы раз подверглись **31,9%** компьютеров пользователей интернета.
- По данным KSN, решения «Лаборатории Касперского» отразили **758 044 650** атак, которые проводились с интернет-ресурсов, размещенных по всему миру.
- Зафиксировано **261 774 932** уникальных URL, на которых происходило срабатывание веб-антивируса.
- **29,1%** веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США.
- Нашим веб-антивирусом было обнаружено **69 277 289** уникальных детектируемых объектов (скрипты, эксплойты, исполняемые файлы и т.д.).
- Атаки шифровальщиков отражены на компьютерах **1 445 434 уникальных** пользователей.
- Попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам отражены на компьютерах **2 871 965** пользователей.
- Нашим файловым антивирусом зафиксировано **4 071 588** уникальных вредоносных и потенциально нежелательных объектов.

Статистика по мобильным угрозам представлена в отчете «Развитие мобильных угроз в 2016 году».

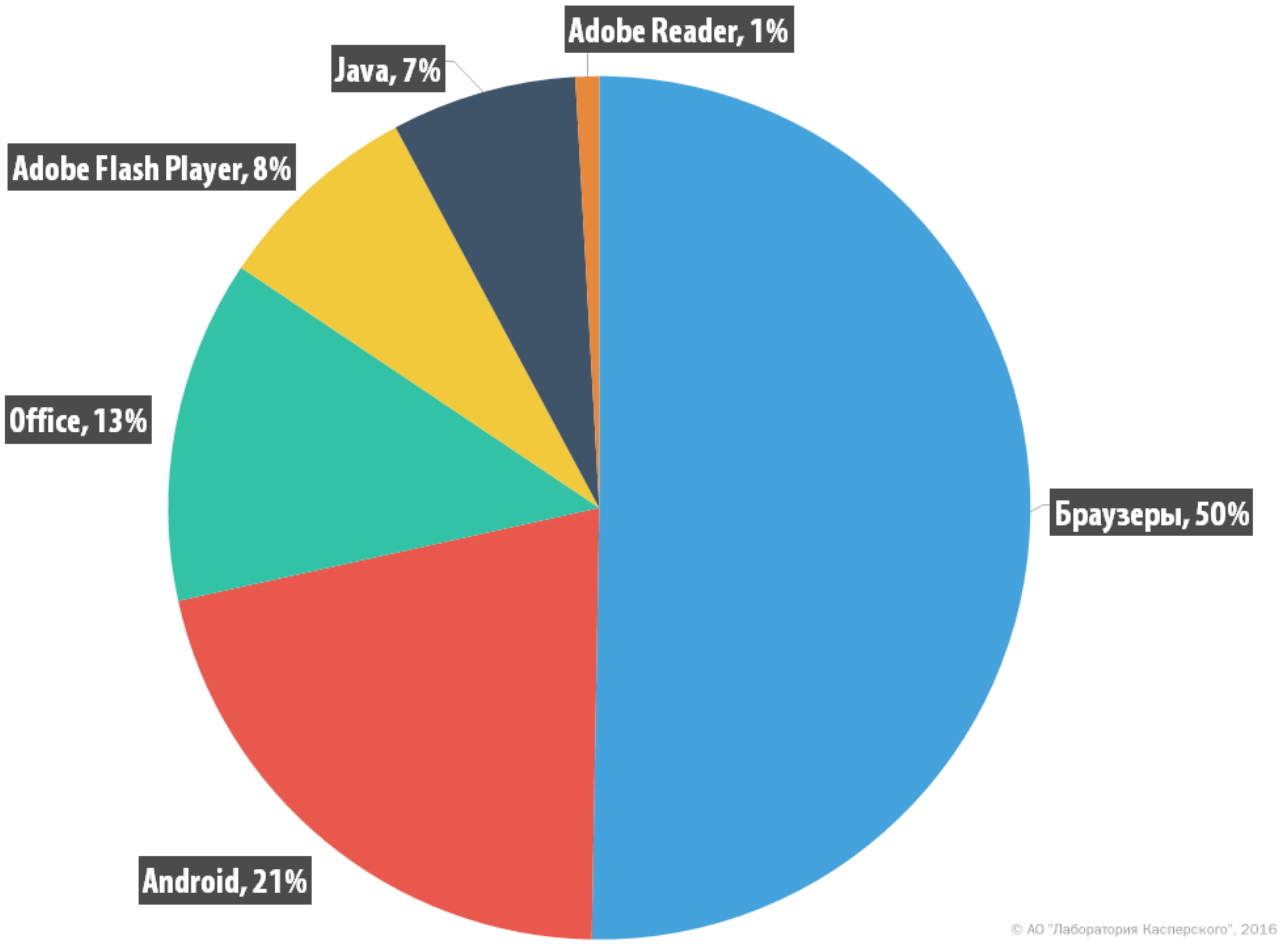
УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ

В 2016 году многие крупные игроки покинули рынок эксплойт-паков. Во втором квартале ушли такие гиганты, как Angler и Nuclear, которые в течение нескольких лет оставались бессменными лидерами рынка. Это означает, что киберпреступникам пришлось переключиться на другие эксплойт-паки, и в этом же квартале был зафиксирован небывалый рост популярности пака Neutrino. Однако уже в третьем квартале этот эксплойт тоже покинул рынок. На конец 2016 года активными остаются паки RIG и Magnitude. RIG был особенно заметен: он занял нишу, освободившуюся после Neutrino, и использовался все чаще.

Как и в 2015, в этом году наиболее востребованными у злоумышленников были эксплойты для уязвимостей в Adobe Flash Player. Четыре новые уязвимости были добавлены в распространенные эксплойт-паки:

- CVE-2015-8651 (Adobe Flash)
- CVE-2016-1001 (Adobe Flash)
- CVE-2016-0034 (Microsoft Silverlight)
- CVE-2015-2419 (Internet Explorer)
- CVE-2016-4117 (Adobe Flash)
- CVE-2016-4171 (Adobe Flash)

Поскольку на рынке традиционно доминировали паки для уязвимостей в Adobe Flash Player, доля эксплойтов для Flash существенно увеличилась по сравнению с прошлым годом — с 3% до 8%.



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений*, 2016 год

* Рейтинг уязвимых приложений построен на основе данных о заблокированных нашими продуктами эксплойтах, используемых злоумышленниками как в веб-атаках, так и при взломе локальных приложений, в том числе на мобильных устройствах пользователей.

В течение года мы также наблюдали рост использования эксплойтов для уязвимостей в приложениях Microsoft Office — с 4% в прошлом году до 13% в этом. Причиной этому послужил всплеск вредоносного спама, содержащего эксплойты для Microsoft Office. Однако к концу года его количество снизилось.

Доля эксплойтов для Android увеличилась на 7 п.п. по сравнению с прошлым годом и составила 21%. Это произошло из-за появления все большего количества эксплойтов, которые могут пользоваться правами суперпользователя на мобильных устройствах.

Итак, в 2016 году долгосрочная тенденция имела свое продолжение: эксплойты для Adobe Flash Player, Microsoft Office и Internet Explorer по-прежнему остаются наиболее популярными у киберпреступников. На диаграмме выше эксплойты для Internet Explorer классифицируются как «Браузеры» (50% от всех эксплойтов), как и выявленные лендинг-страницы, которые распространяют эксплойты.

ВРЕДОНОСНЫЕ ПРОГРАММЫ В ИНТЕРНЕТЕ (АТАКИ ЧЕРЕЗ ВЕБ-РЕСУРСЫ)

Статистические данные в этой главе получены по результатам работы веб-антивируса, который защищает пользователей в момент загрузки вредоносных объектов с вредоносной/зараженной веб-страницы. Злоумышленники специально создают вредоносные сайты; заражены могут быть веб-ресурсы, контент которых создается пользователями (например, форумы), а также взломанные легитимные ресурсы.

В 2016 году нашим веб-антивирусом было обнаружено **69 277 289** уникальных объектов (скрипты, эксплойты, исполняемые файлы и т.д.), и зафиксировано **261 774 932** уникальных URL, на которых происходило срабатывание веб-антивируса. Решения «Лаборатории Касперского» отразили **758 044 650** атак, которые проводились с интернет-ресурсов, размещенных в 212 странах мира.

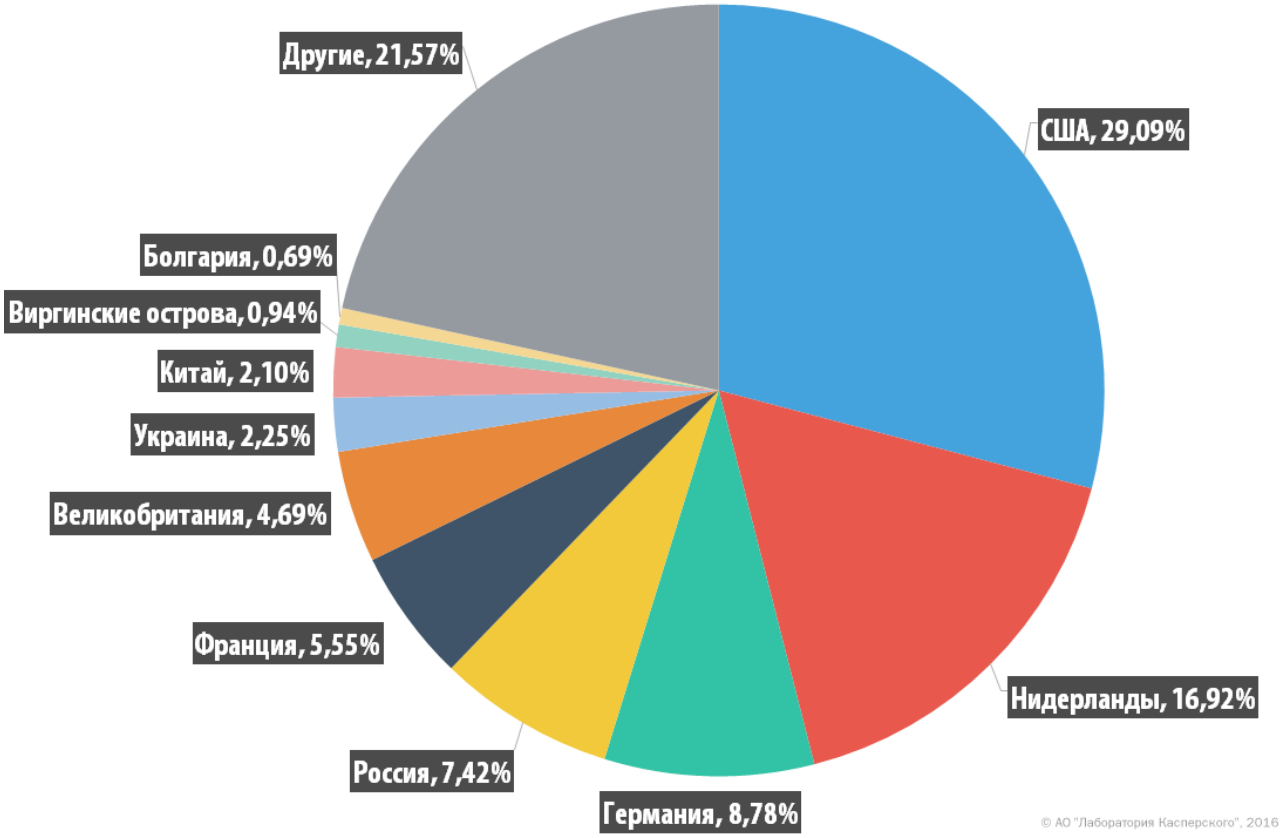
Страны — источники веб-атак: TOP 10

Данная статистика показывает распределение по странам источников заблокированных продуктами «Лаборатории Касперского» интернет-атак на компьютеры пользователей (веб-страницы с переадресацией на эксплойты, сайты с эксплойтами и другими вредоносными программами, командные серверы и т.п.). Отметим, что каждый уникальный хост мог быть источником одной и более 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).

В 2016 году решения «Лаборатории Касперского» отразили **758 044 650** атак, которые проводились с интернет-ресурсов, размещенных в разных странах мира. Зафиксировано **3 014 685** уникальных URL, на которых происходило срабатывание веб-антивируса.

78% нотификаций о заблокированных веб-атаках были получены с веб-ресурсов, расположенных в десяти странах мира.



Распределение источников веб-атак по странам (ноябрь 2015 — октябрь 2016)

Девятка стран — основных источников веб-атак не изменилась по сравнению с предыдущим годом. Нидерланды и Германия поменялись местами, как и Китай и Виргинские острова. Швеция выбыла из TOP 10, а новичок рейтинга Болгария заняла девятое место.

Угрозы в интернете: TOP 20

В 2016 году нашим веб-антивирусом было обнаружено **69 277 289** уникальных объектов (сэмплы, которым соответствуют уникальные хэши (включая скрипты, эксплойты, исполняемые файлы и т.д.).

В течение года рекламные программы и их компоненты были зафиксированы на 15,6% всех компьютеров пользователей, на которых сработал наш веб-антивирус.

Мы определили 20 вредоносных программ, которые наиболее часто использовались для атак на компьютеры пользователей в 2016 году.

На эти программы пришлось 96,6% атак вредоносных программ.

	Название*	% от всех атак**
1	Malicious URL	77,26
2	Trojan-Clicker.HTML.Iframe.dg	8,15
3	Trojan.Script.Generic	6,74
4	Trojan.Script.Iframer	3,14
5	Trojan-Downloader.Script.Generic	0,35
6	Exploit.Script.Generic	0,20
7	Packed.Multi.MultiPacked.gen	0,15
8	Trojan.JS.FBook.bh	0,13
9	Exploit.Script.Blocker	0,11
10	Trojan-Downloader.JS.Iframe.div	0,11
11	Trojan.JS.Redirector.ns	0,09
12	Trojan-Dropper.VBS.Agent.bp	0,08
13	Trojan-Downloader.JS.Agent.hjc	0,08
14	Trojan.JS.Iframe.ako	0,07
15	Trojan.Win32.Generic	0,06
16	Trojan.Win32.Generic	0,06
17	Trojan.JS.Agent.ckf	0,05
18	Trojan-Spy.HTML.Fraud.gen	0,05
19	Trojan.Win32.Invader	0,04
20	Exploit.SWF.Agent.gen	0,04

* Статистика основана на детектирующих вердиктах модуля веб-антивируса на компьютерах пользователей продуктов «Лаборатории Касперского», подтвердивших свое согласие на передачу статистических данных.

** Процент от всех веб-атак вредоносных программ, которые были зафиксированы на компьютерах уникальных пользователей.

В TOP 20 представлены большей частью вердикты, которые присваиваются объектам, использующимся, как правило, в drive-by атаках. Они детектируются эвристически как Trojan.Script.Generic, Expoit.Script.Blocker, Trojan-Downloader.Script.Generic и другие.

На первом месте Malicious URL — вердикт для ссылок из нашего черного списка (ссылки на веб-страницы с переадресацией на эксплойты, сайты с эксплойтами и другими вредоносными программами, командные серверы, сайты-вымогатели и т.д.).

Под вердиктом Trojan.JS.FBook.bh детектируется скрипт, который получает ссылку с командного сервера, находящегося по определенному адресу, и обновляет статус пользователя Facebook, добавляя ссылку в статус и отмечая всех друзей пользователя. Ссылка предназначена для установки расширения для веб-браузера, которое получает доступ к аккаунту пользователя на Facebook и может выполнять любые действия от имени пользователя, в том числе внедрять эту схему распространения.

Trojan-Downloader.JS.Agent.hjc является «динамическим» кликером, который соединяется с командным сервером и считывает файл конфигурации. Этот файл содержит ссылку, которая будет включена в плавающий фрейм, и пользователь будет переходить по ней, кликнув на страницу сайта.

Trojan-Spy.HTML.Fraud.gen — вердикт фишинговой HTML-страницы, которая имитирует страницу интернет-магазина или банка и рассылается в фишинговом электронном сообщении и т.п.

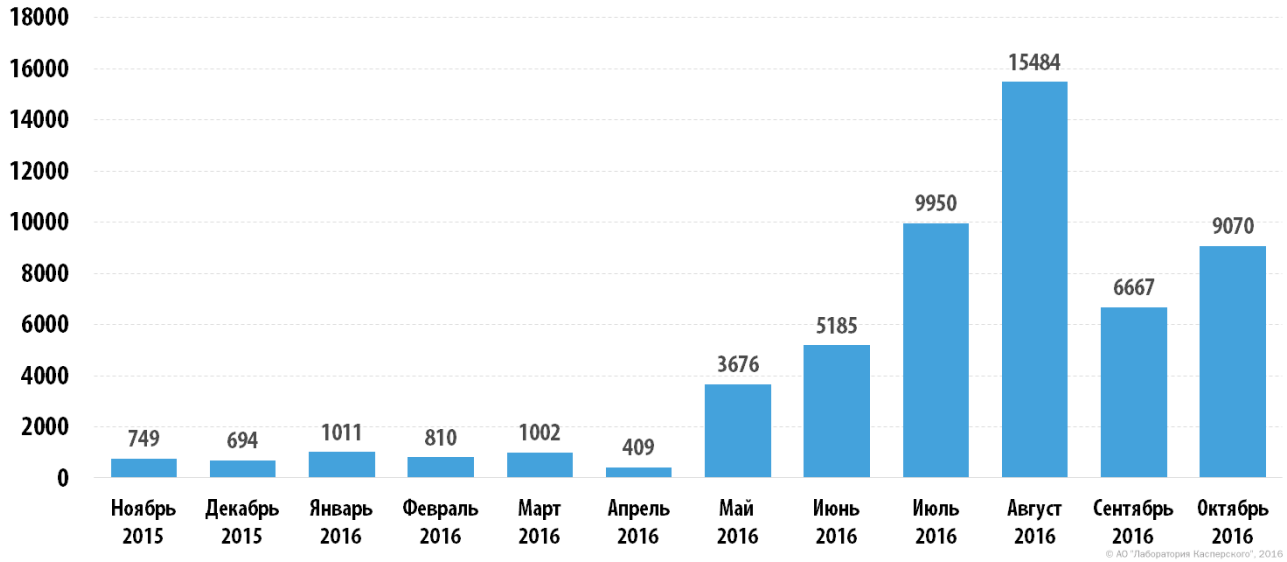
Вредоносные программы-шифровальщики

Угроза, которую представляют шифровальщики, продолжает расти: со второй половины года мы наблюдаем существенное увеличение количества и новых семейств, и новых модификаций этих вредоносных программ. Новые троянцы продолжают появляться с пугающей скоростью, и хотя большинство из них оказывается не слишком удачными экспериментами не слишком знающих разработчиков, некоторые, например Locky, Cerber и CryptXXX, создали серьезные проблемы как отдельным пользователям, так и предприятиям.

Тем временем хорошо знакомые шифровальщики, такие как CTB-Locker, CryptoWall и TorrentLocker продолжают активно действовать, а киберпреступники, стоящие за ними, не имеют ни малейшего желания видеть свои кампании закрытыми, как в случае с TeslaCrypt.

Количество новых модификаций шифровальщиков

В 2016 году мы обнаружили более **54 000 новых модификаций** шифровальщиков и **62 новых семейства**.

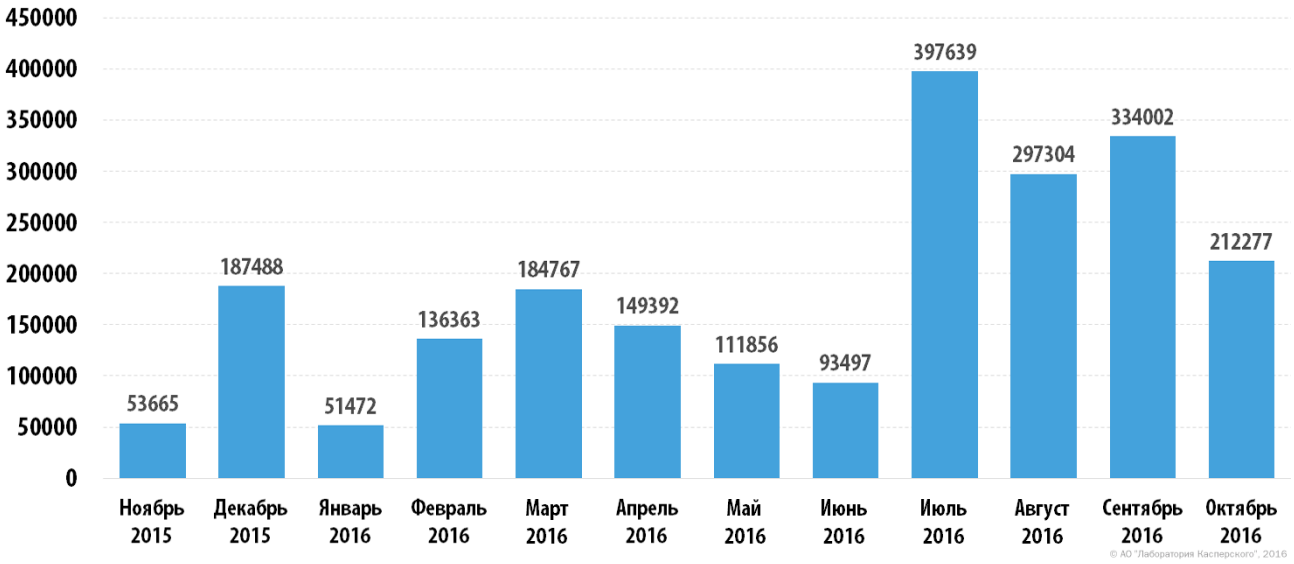


Количество новых модификаций шифровальщиков, ноябрь 2015 — октябрь 2016)

На сегодняшний день общее число модификаций шифровальщиков в нашей коллекции составило не менее **65 000**.

Количество пользователей, атакованных троянцами-шифровальщиками

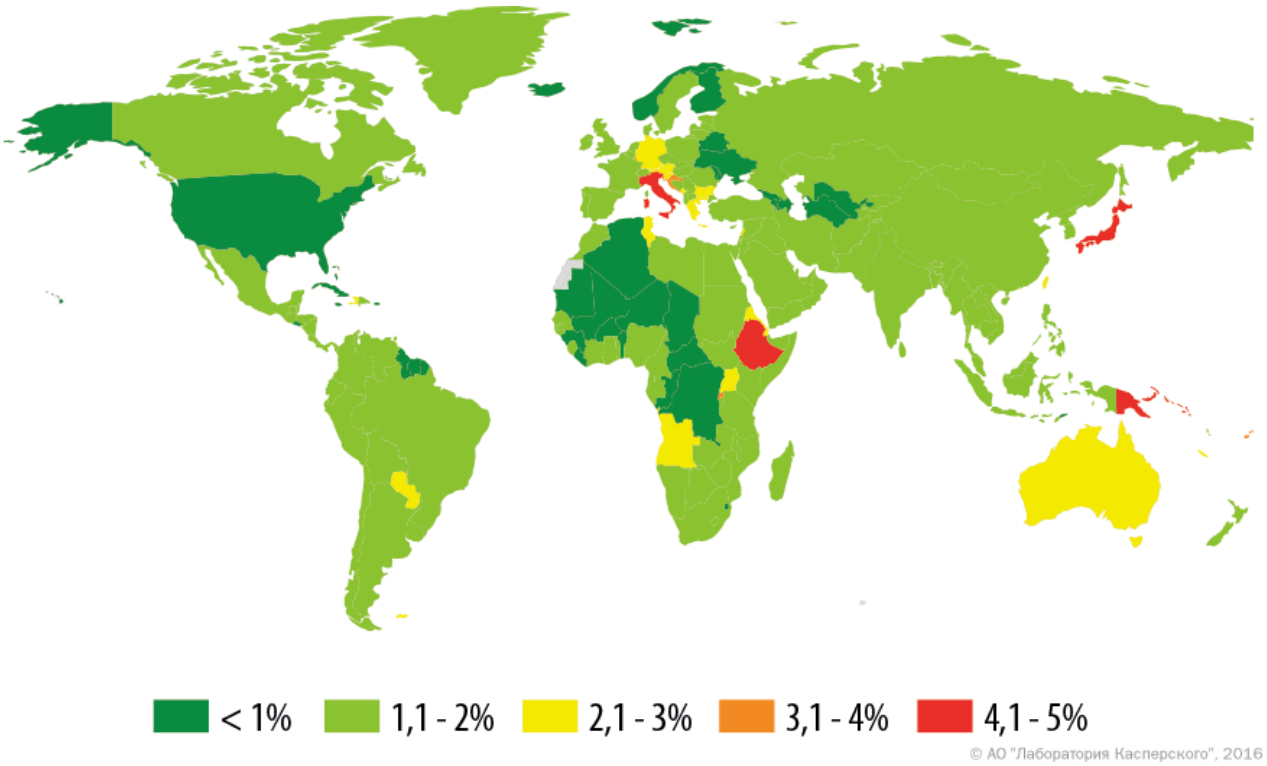
В 2016 году шифровальщиками было атаковано **1 445 434** компьютера **уникальных** пользователей KSN.



Количество уникальных пользователей, атакованных троянцами-шифровальщиками, ноябрь 2015 — октябрь 2016

Важно иметь в виду, что реальное число инцидентов гораздо больше: статистика отражает только результаты сигнатурных и эвристических обнаружений, тогда как в случае новых и неизвестных вредоносных программ продукты «Лаборатории Касперского» выявляют троянцев-шифровальщиков на основе моделей поведения..

География атак



География атак троянцев-шифровальщиков в 2016 году (процент атакованных пользователей)

TOP 10 стран, подвергшихся атакам троянцев-шифровальщиков

	Страна*	% пользователей, атакованных шифровальщиками**
1	Япония	4,46
2	Италия	4,17
3	Хорватия	3,23
4	Люксембург	3,15
5	Болгария	2,86
6	Уганда	2,55
7	Тунис	2,54
8	Австрия	2,45
9	Гонконг	2,43
10	Ливан	2,39

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

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

В России в течение года атаки Trojan-Ransom были зафиксированы на компьютерах 1,53% уникальных пользователей

TOP 10 наиболее распространенных семейств троянцев-шифровальщиков

	Название	Вердикт*	% атакованных пользователей**
1	CTB-Locker	Trojan-Ransom.Win32.Onion / Trojan-Ransom.NSIS.Onion	25,32
2	Locky	Trojan-Ransom.Win32.Locky / Trojan-Dropper.JS.Locky	7,07
3	TeslaCrypt	Trojan-Ransom.Win32.Bitman	6,54
4	Scatter	Trojan-Ransom.Win32.Scatter / Trojan-Ransom.BAT.Scatter / Trojan-Downloader.JS.Scatter / Trojan-Dropper.JS.Scatter	2,85
5	Cryakl	Trojan-Ransom.Win32.Cryakl	2,79
6	CryptoWall	Trojan-Ransom.Win32.Cryptodef	2,36
7	Shade	Trojan-Ransom.Win32.Shade	1,73
8	(generic verdict)	Trojan-Ransom.Win32.Snocry	1,26
9	Crysis	Trojan-Ransom.Win32.Crusis	1,15
10	Cryrar/ACCDFISA	Trojan-Ransom.Win32.Cryrar	0,90

* Статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского» на компьютерах пользователей, подтвердивших свое согласие на передачу статистических данных.

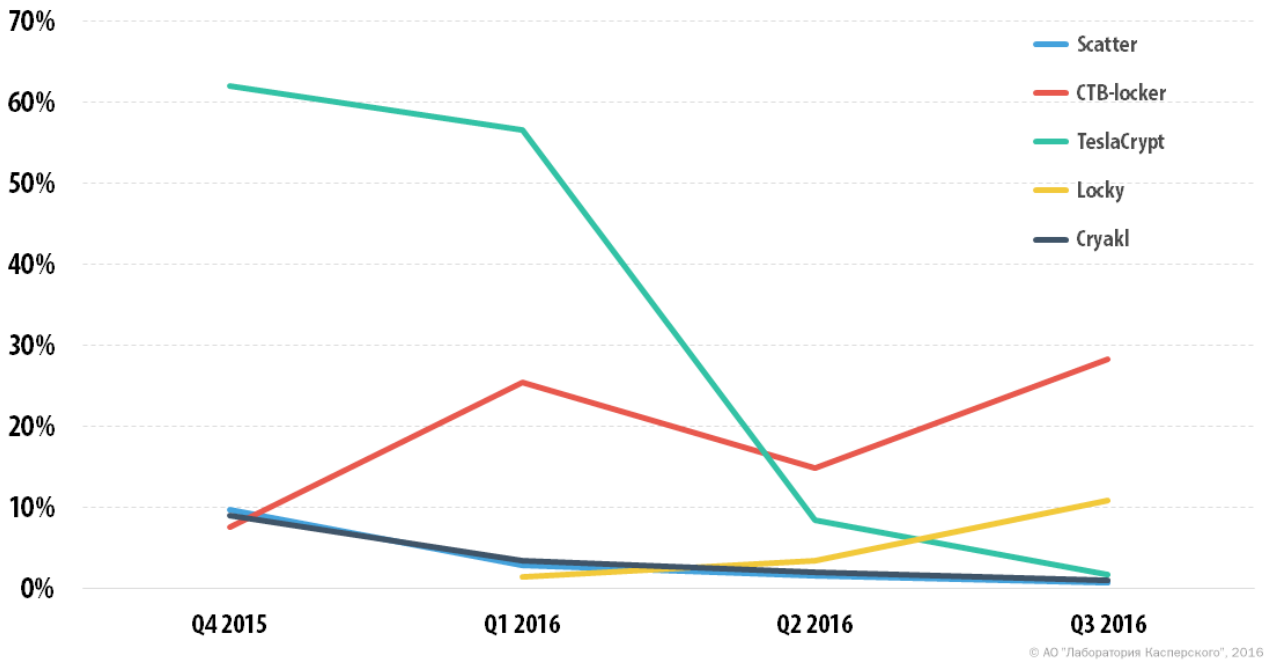
** Процент уникальных пользователей «Лаборатории Касперского», подвергшихся атакам конкретного семейства троянцев-вымогателей, от числа всех пользователей, подвергшихся атакам троянцев-вымогателей.

Большинство троянцев-шифровальщиков, входящих в TOP 10, известны давно. Это CTB-Locker, CryptoWall, Shade, Cryakl, TeslaCrypt, Scatter, Cryrar.

Два новых шифровальщика Locky и Crysis появились только в этом году, но уже получили широкое распространение.

Новые троянцы-шифровальщики, появившиеся в 2016 году, удивительным образом похожи на своих предшественников. Стандартные схемы шифрования, наиболее часто применяемые в этих вредоносных программах, хорошо известны, и преступникам не нужно придумывать новые, нетрадиционные подходы при создании новых шифровальщиков. В настоящее время их создатели, как правило, используют проверенные временем способы шифрования файлов и сосредотачивают свои усилия, главным образом, на новых методах противодействия реверс-инжинирингу и обхода обнаружения.

В то же время, мы обнаружили много новых шифровальщиков, созданных явно «неквалифицированными» разработчиками. Семейства этих троянцев, как правило, характеризуются низким качеством кода, большим количеством ошибок и недостатков в шифровании, использованием несложных алгоритмов и подходов, а иногда даже грамматическими ошибками в сообщениях с требованием выкупа. Такие программы редко получают широкое распространение, но количество таких новых семейств программ-вымогателей, созданных «любителями» не может остаться незамеченным. Очевидно, что получение легких денег путем вымогательства, а также широкое освещение зловредов этого типа в средствах массовой информации привлекает все больше преступников, специализирующихся на других видах мошенничества.



TOP 5 распространенных семейств троянцев-шифровальщиков, поквартально (процент атакованных пользователей)

Наблюдалось быстрое уменьшение доли пользователей, атакованных шифровальщиком TeslaCrypt, чего и следовало ожидать после его закрытия во втором квартале 2016 года.

Locky, впервые появившийся в первом квартале 2016 года, наоборот, находится на подъеме. CTB-Locker продолжает занимать первое место по распространенности после закрытия Teslacrypt. Cryakl и Scatter, атакующие в основном пользователей в русскоязычных странах, неуклонно теряют свои позиции.

Программы-шифровальщики в корпоративном секторе

В 2016 году 22,6% пользователей, атакованных шифровальщиками, пришлось на корпоративный сектор. Десять наиболее распространенных семейств шифровальщиков практически те же, что и в рейтинге, о котором говорилось выше. Однако есть одно исключение, о котором следует сказать отдельно. Это Trojan-Ransom.Win32.Rakhni, затронувший 2,42% всех корпоративных пользователей, атакованных шифровальщиками.

Trojan-Ransom.Win32.Rakhni распространяется с помощью Trojan-Downloader.Win32.Rakhni. Этот загрузчик представляет собой исполняемый файл, встроенный в документ .docx, который обычно рассылается в виде вложения в спам-сообщения. Хозяева Rakhni явно нацелены на корпоративный сектор (а именно на отделы кадров) в русскоязычных странах, поскольку в формате .docx обычно создаются формы заявки о приеме на работу (например, «Резюме Жанна.docx»). Когда жертвы открывают .docx-файл, они видят иконку PDF Reader и, кликнув на нее, исполняют загрузку вредоносный программы. Чтобы не вызвать немедленных подозрений, троянец показывает резюме, которое выглядит вполне достоверно.

Менеджер по работе с клиентами

Общая информация

Заработная плата: **от 35 000 руб.**
Характер работы: На территории работодателя
График работы: Полный рабочий день

Образование: Высшее
Опыт работы: 11 лет 2 месяца
Возраст: 28 лет (11 февраля 1988)

Опыт работы 11 лет 9 месяцев

Период работы: сентябрь 2008 — по настоящее время
Должность: **Менеджер отдела прямых продаж**
Компания: ООО "Протек"
Обязанности: Оптово-розничная продажа дверей
стратегическое планирование и развитие продаж;
составление бюджетов продаж и расходов отдела;
анализ эффективности работы отдела;
разработка мероприятий по увеличению объемов продаж отдела;
оперативное управление отделом: организация работы, координация,
контроль выполнения плана продаж, составление отчетов;
контроль дебиторской задолженности, работа с просроченной задолженностью;

Период работы: август 2007 — сентябрь 2008 (1 год 2 месяца)
Должность: **Специалист по документообороту**
Компания: ООО Биокад
Обязанности: Прием и распределение тел звонков, работа с оргтехникой, архивация документов, деловая переписка, организация и планирование деловых встреч руководителей, контроль исполнения приказов и распоряжений.

Период работы: январь 2005 — август 2007 (2 года 8 месяцев)
Должность: **Ассистент менеджера**
Компания: ООО ПКФ Эрион
Обязанности: Ведение делопроизводства, оформление документов при закупке/продаже товаров.

Образование

Образование: Высшее
Окончание: 2010 год
Учебное заведение: МЭСИ
Факультет: Менеджмент организации
Специальность: Менеджер по конкурентоспособности

Дополнительная информация

Иностранные языки: Английский (Базовый)
Водительские права: Категория В
Владение компьютером: Эксперт
Возможность командировок: Есть
Навыки и умения: Высокие коммуникативные навыки, хорошие аналитические способности, умение работать в команде и с большим объемом информации, знание 1С программы "Управление торговлей 8.0"

Резюме, демонстрируемое жертве загрузчиком Trojan-Downloader.Win32.Rakhni

Тем временем троянец продолжает загружать основную вредоносную программу-шифровальщик Trojan-Ransom.Win32.Rakhni, который зашифровывает файлы и показывает сообщение с требованием выкупа.

Данные KSN убедительно доказывают, что киберпреступники, стоящие за Rakhni, не слишком заинтересованы в заражении отдельных пользователей, их цель — компании: это семейство не входит в TOP 10 наиболее распространенных программ-шифровальщиков, но является одним из самых популярных для использования в атаках на корпоративный сектор.

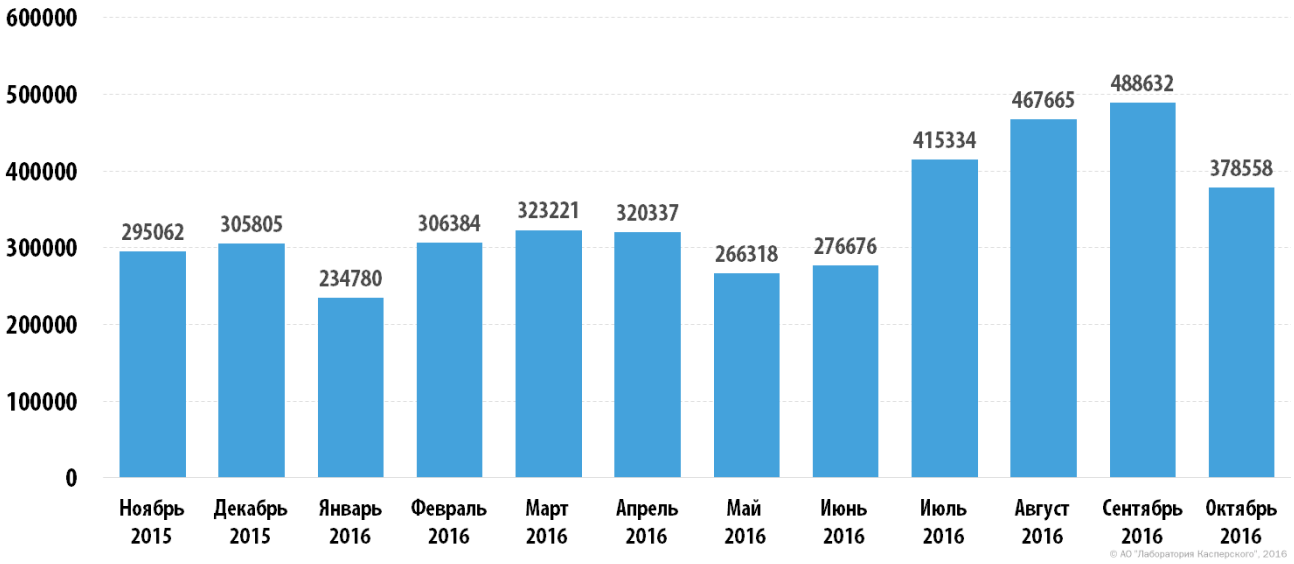
Онлайн-угрозы в банковском секторе

Настоящая статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского» на компьютерах пользователей, подтвердивших свое согласие на передачу статистических данных.

Годовая статистика за 2016 г. основана на данных, полученных в период с ноября 2015 г. по октябрь 2016 г.

В силу того что постоянно появляются новые представители банковских троянцев и происходят функциональные изменения в существующих банковских троянцах, во втором квартале 2016 г. мы значительно обновили список вердиктов, классифицируемых как банковские риски. Это означает, что число жертв финансовых зловредов значительно изменилось по сравнению с данными, опубликованными за прошлые годы. Для сравнения мы пересчитали статистику за прошлый год, учитывая все вредоносное ПО из обновленного списка.

В 2016 г. решения «Лаборатории Касперского» заблокировали попытки запуска вредоносного ПО, способного красть деньги через каналы онлайн-банкинга, на **2 871 965** устройствах.

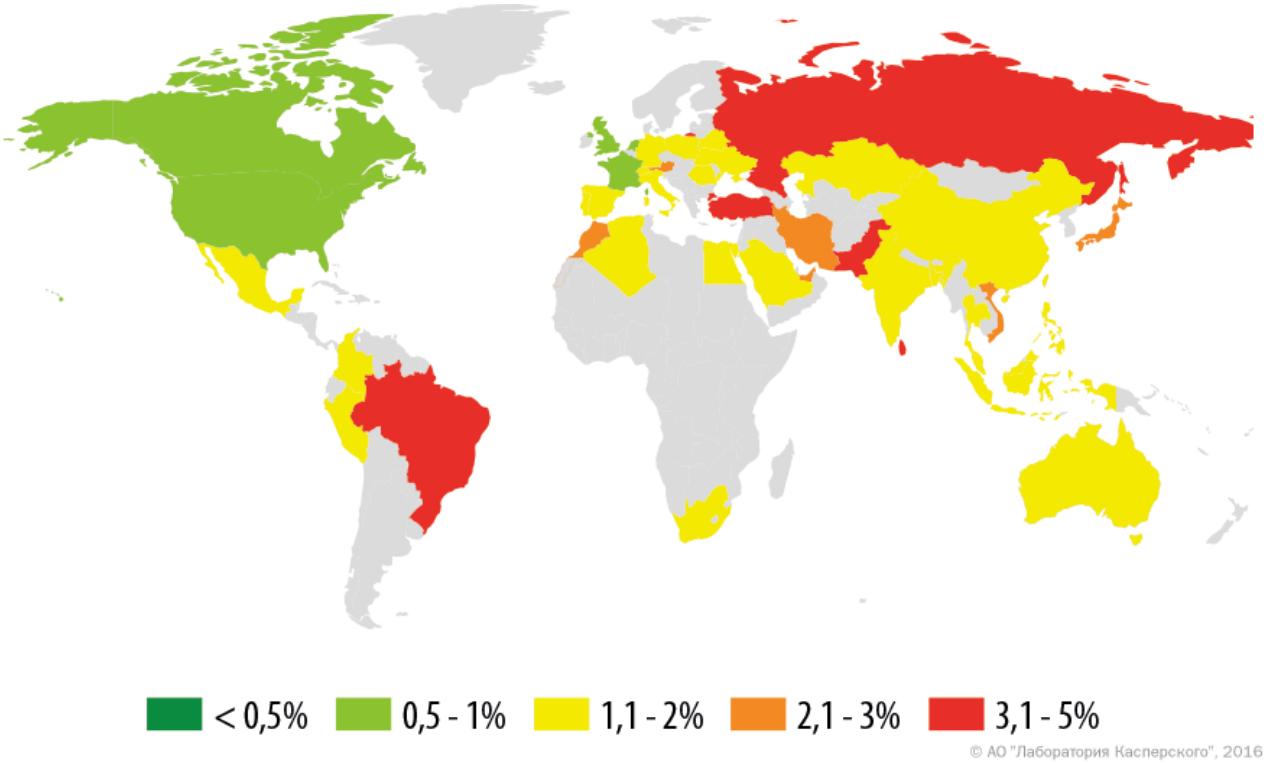


Число пользователей-мишеней финансовых зловредов, ноябрь 2015 — октябрь 2016

С конца 2015 г. мы наблюдали снижение числа устройств, подвергшихся атакам — это было связано с приостановкой деятельности ботнета Dyre (Dyreza). Однако с середины 2016 г. число атак стало постепенно расти, а в сентябре число атакованных устройств за месяц превысило максимальные месячные показатели и за 2014 г., и за 2015 г. — это произошло за счет роста числа атак на пользователей мобильного банкинга, в первую очередь владельцев Android-устройств.

География атак

Чтобы оценить популярность финансовых зловредов среди киберпреступников, а также риск заражения банковскими троянцами пользовательских компьютеров по всему миру, мы считаем долю пользователей защитных продуктов «Лаборатории Касперского» в соответствующей стране, которые столкнулись с этим типом угроз на протяжении отчетного периода, по отношению ко всем пользователям наших продуктов в стране.



География атак банковских зловредов в 2016 г. (процент атакованных пользователей в стране)

TOP 10 стран, подвергшихся атакам банковских троянцев

	Страна*	% пользователей, атакованных троянцем-вымогателем**
1	Российская Федерация	4,8
2	Бразилия	4,7
3	Турция	4,5
4	Шри Ланка	4,5
5	Пакистан	3,8
6	Австрия	2,6
7	Вьетнам	2,4
8	ОАЭ	2,3
9	Япония	2,2
10	Марокко	2,2

* При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского» относительно мало (менее 50 000, и менее 7000 уведомлений о заражениях банковским вредоносным ПО).

** Процент уникальных пользователей, компьютеры которых были атакованы банковскими троянцами, от числа всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.

В данном рейтинге на первом месте стоит Российская Федерация. Из всех российских пользователей «Лаборатории Касперского», атакованных вредоносным ПО, за год 4,8% стали мишенью хотя бы одного банковского троянца. Это отражает популярность в стране финансовых угроз по отношению ко всем видам угроз.

В Бразилии 4,7% атакованных в 2016 г. пользователей хотя бы раз столкнулись с банковским троянцем. В Турции таких пользователей было 4,5%, в Германии — 2%, в Швейцарии — 1,7%, во Франции — 1%.

TOP 10 банковских вредоносных программ

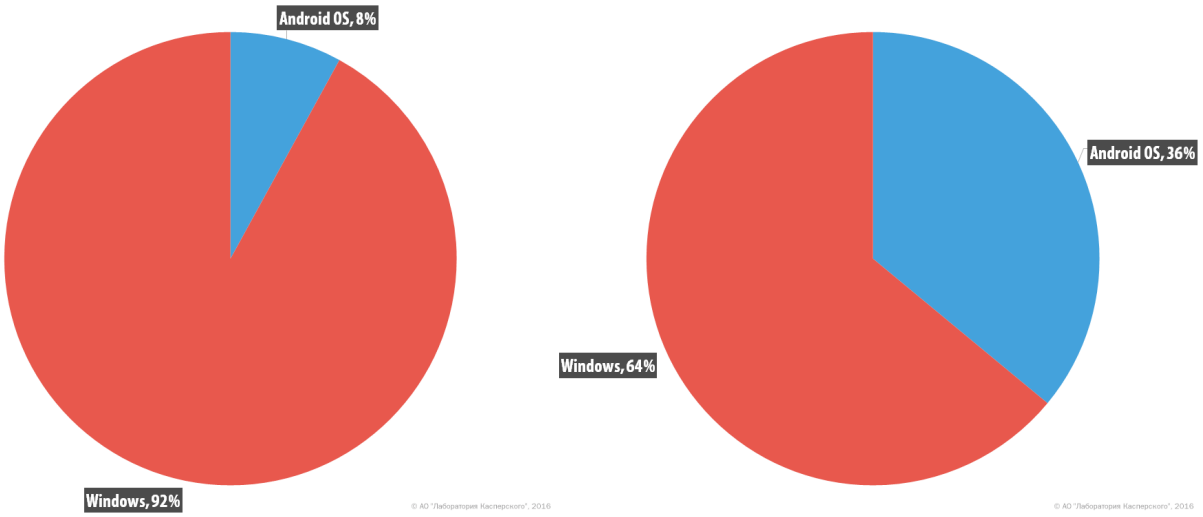
TOP 10 вредоносных программ, наиболее часто использовавшихся для атак на пользователей мобильного и онлайн-банкинга в 2016 году (по доле атакованных пользователей):

	Название*	% атакованных пользователей**
1	Trojan-Banker.AndroidOS.Svpeng.q	8,8
2	Trojan-Banker.Win32.Gozi.gr	5,7
3	Trojan.BAT.Qhost.abp	4,5
4	Trojan-Spy.Win32.Zbot.pef	3,5
5	Trojan-Banker.AndroidOS.Agent.ai	2,8
6	Trojan-Spy.Win32.Zbot.vho	2,5
7	Trojan-Banker.AndroidOS.Asacub.e	1,9
8	Trojan-Banker.AndroidOS.Svpeng.r	1,8
9	Trojan.Win32.Qhost.afes	1,4
10	Trojan-Banker.AndroidOS.Hqwar.t	1,2

* Данная статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского» на компьютерах пользователей, подтвердивших свое согласие на передачу статистических данных.

** Процент уникальных пользователей, атакованных данной вредоносной программой, от всех пользователей, атакованных финансовым вредоносным ПО.

Из десяти наиболее популярных банковских троянцев пять предназначены для кражи банковских данных с Android-устройств. По сравнению с 2015 годом доля атак на такие устройства увеличилась в 4,5 раза. Это говорит о том, что киберпреступники внимательно следят за поведением пользователей и переключаются с атак на сайты банков на подмену приложений для мобильного банкинга.



Процентное соотношение устройств, атакованных банковским вредоносным ПО в 2015 и 2016 гг.

Большинство вредоносных программ для Windows, попавших в TOP 10, используют внедрение HTML-кода в отображаемую браузером веб-страницу с последующим перехватом платежных данных, вводимых пользователем в оригинальные и добавленные троянцем веб-формы, тогда как мобильные банковские троянцы пытаются открывать фишинговые окна, отображаемые поверх окна программы мобильного банкинга, и красть одноразовые коды аутентификации, перехватывая входящие SMS-сообщения.

Самым популярным мобильным банковским троянцем в 2016 году стал Trojan-Banker.AndroidOS.Svpeng.q, благодаря активному распространению через рекламную сеть Google AdSense, которая используется многими (в том числе новостными) сайтами для показа пользователям таргетированной рекламы. Очевидно, авторы Svpeng разместили в этой сети вредоносную рекламу. Загрузка троянца происходит сразу же при загрузке рекламного объявления, независимо от того, тапнул пользователь по нему или нет. Банковские троянцы семейства Svpeng известны «Лаборатории Касперского» с 2013 года и обладают широким набором вредоносных функций. После установки и запуска вредоносная программа скрывается из списка установленных приложений и запрашивает права администратора устройства (чтобы усложнить свое удаление антивирусами и пользователем). Svpeng может красть информацию о банковских картах пользователя с помощью фишинговых окон, перехватывать, удалять и отправлять текстовые сообщения (это нужно для атаки на системы ДБО, использующие одноразовые коды аутентификации, отправляемые в SMS-сообщениях).

На втором месте представитель семейства Trojan-Banker.Win32.Gozi, который использует технику внедрения кода в работающие процессы популярных веб-браузеров для кражи платежной информации, вводимой на сайтах онлайн-банкинга. Некоторые варианты этого троянца могут заражать главную загрузочную запись (Master Boot Record, MBR) и сохранять свое присутствие в операционной системе даже в том случае, если она была переустановлена. Первые версии этого троянца появились 10 лет назад, и за это время он существенно изменился. В этом году создатели Gozi, помимо кражи банковских данных взялись за вымогательство с помощью троянцев-шифровальщиков. Мы обнаружили, что исходный код троянской программы Nymaim содержит фрагменты кода банковского троянца Gozi, который обеспечивает злоумышленникам удаленный доступ к зараженным компьютерам. Это означает, что если жертва программы-вымогателя использует онлайн-банкинг, то киберпреступники не только вымогают у жертвы деньги, но и крадут с ее банковского счета все имеющиеся на нем средства.

В течение долгого времени семейство троянских программ Zbot постоянно находилось в TOP 3 самого популярного банковского вредоносного ПО, но с появлением в рейтинге мобильных банковских троянцев ситуация в нем изменилась. Следует отметить, однако, что Zbot не исчез, он располагается на четвертом месте и используется в качестве основы для огромного количества других банковских троянцев, таких как Citadel, Kins и ZeusVM.

Третье и девятое места занимают представители семейства Qhost, одного из самых старых семейств банковских троянских программ, что никак не умаляет их эффективности. Эти два представителя семейства меняют содержимое файла hosts на компьютере жертвы таким образом, что все обращения к сайту банка проходят через вредоносный сервер, с которого можно «вмешаться в разговор» и подменить данные, которые пользователь видит в браузере, а также данные, передаваемые в банк.

Страны, в которых пользователи подвергались наибольшему риску заражения через интернет

Чтобы определить страны, в которых пользователи наиболее часто сталкиваются с интернет-угрозами, мы подсчитали для каждой страны процент пользователей продуктов «Лаборатории Касперского», которые столкнулись со срабатыванием веб-антивируса в отчетный период. Полученные данные характеризуют

уровень риска заражения компьютера в разных странах мира, т.е. являются показателем агрессивности среды, в которой работают компьютеры в разных регионах.

Отметим, что данный рейтинг учитывает только атаки вредоносных программ класса Malware, т.е. при подсчетах не учитываются срабатывания веб-антивируса на потенциально опасные и нежелательные программы, такие как RiskTool и рекламные программы (Adware).

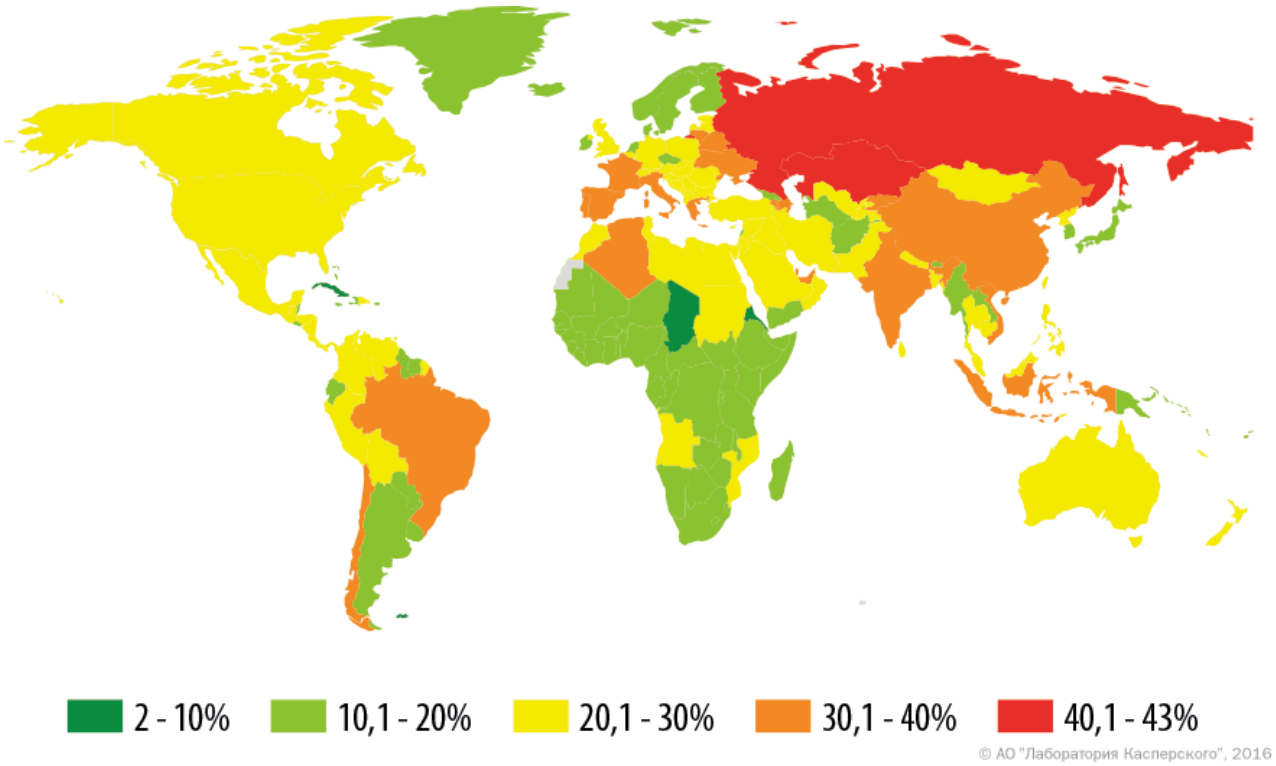
20 стран, в которых отмечен наибольший риск заражения компьютеров через интернет

	Страна*	% уникальных пользователей**
1	Россия	42,15
2	Казахстан	41,22
3	Италия	39,92
4	Украина	39,00
5	Бразилия	38,83
6	Азербайджан	38,81
7	Испания	38,21
8	Беларусь	38,04
9	Алжир	37,11
10	Вьетнам	36,77
11	Китай	36,53
12	Португалия	35,86
13	Франция	34,74
14	Армения	33,01
15	Греция	32,99
16	Чили	32,82
17	Индия	32,61
18	Катар	32,53
19	Индонезия	32,30
20	Молдова	31,42

Данная статистика основана на детектирующих вердиктах модуля веб-антивируса на компьютерах пользователей продуктов «Лаборатории Касперского», подтвердивших свое согласие на передачу статистических данных.

* Из расчетов были исключены страны, где число пользователей «Лаборатории Касперского» относительно мало (меньше 50 000).

** Процент уникальных пользователей, подвергшихся веб-атакам с применением вредоносного ПО, от всех уникальных пользователей определенных продуктов «Лаборатории Касперского» в стране.



Географическое распределение вредоносных атак через интернет в 2016 году
(процент атакованных пользователей)

По степени риска заражения все страны мира можно разделить на три группы.

1. **Группа высокого риска (более 40%)**
   В 2016 году в эту группу вошли первые две страны из TOP 20 — Россия и Казахстан.

2. **Группа среднего уровня риска (20–39,9%)**
   В эту группу попали 105 стран, в том числе: Турция (29,3%), Канада (29,5%), Польша (28,7%), Румыния (27,4%), Мексика (26,8%), Австралия (26,2%), Германия (26,2%), Бельгия (25,3%), Австрия (24,8%), США (24%), Швейцария (23,6%), Великобритания (22,13%), Венгрия (21,3%), Ирландия (20%).

3. **Группа наиболее безопасных стран (0–19,9%)**
   В эту группу вошли Чешская Республика (19,6%), Аргентина (19,5%), Япония (17,7%), Норвегия (15,9%), Швеция (15,2%), Грузия (14,6%), Нидерланды (14,5%), Дания (12,2%).

В 2016 году при работе в интернете веб-атакам с применением вредоносных объектов **класса Malware** хотя бы один раз подверглись **31,9%** компьютеров.

ЛОКАЛЬНЫЕ УГРОЗЫ

Статистика локальных заражений пользовательских компьютеров — важный показатель, формируемый вредоносными объектами, которые проникли на компьютер путем заражения файлов или съемных носителей либо изначально попали на компьютер в зашифрованном виде (например, программы в составе сложных инсталляторов, зашифрованные файлы и т.д.). Кроме того, в этой статистике учитываются объекты, которые были обнаружены на компьютерах пользователей после установки нашего продукта и первой проверки системы файловым антивирусом.

В этом разделе мы анализируем статистические данные, полученные при антивирусной проверке файлов на жестком диске в момент их создания или обращения к ним, а также при проверке различных съемных носителей данных.

Всего в 2016 году было зафиксировано **4 071 588** уникальных вредоносных и потенциально опасных программ (при этом за число уникальных программ принимается число уникальных вердиктов).

TOP 20 вердиктов на компьютерах пользователей

Мы выделили двадцать угроз, которые в 2016 году чаще всего детектировались на компьютерах пользователей. В данный рейтинг не входят программы классов Adware и Riskware.

	Название*	% уникальных атакованных пользователей**
1	DangerousObject.Multi.Generic	42,32
2	Trojan.Win32.Generic	9,23
3	Trojan.WinLNK.Agent.gen	7,78
4	Trojan.WinLNK.StartPage.gena	6,25
5	Trojan.Script.Generic	5,86
6	Trojan.Win32.AutoRun.gen	4,78
7	Virus.Win32.Sality.gen	4,34
8	Trojan.WinLNK.Runner.jo	4,17
9	Worm.VBS.Dinihou.r	3,58
10	Trojan.WinLNK.Agent.ew	3,13
11	Trojan.Win32.Starter.yy	2,93
12	Trojan-Downloader.Script.Generic	2,80
13	Trojan.Win32.Autoit.cfo	2,27
14	Trojan.Win32.Wauchos.a	2,03
15	Virus.Win32.Nimnul.a	2,02
16	Trojan-Proxy.Win32.Bunitu.avz	1,90
17	Worm.Win32.Debris.a	1,83
18	Trojan.Win32.Hosts2.gen	1,80
19	Trojan-Dropper.VBS.Agent.bp	1,34
20	Trojan.WinLNK.StartPage.ab	1,26

Данная статистика основана на детектирующих вердиктах модулей OAS и ODS антивируса на компьютерах пользователей продуктов «Лаборатории Касперского», подтвердивших свое согласие на передачу статистических данных.

* Детектирующие вердикты модулей OAS и ODS антивируса на компьютерах пользователей продуктов «Лаборатории Касперского», подтвердивших свое согласие на передачу статистических данных.

** Процент уникальных пользователей, на компьютерах которых файловый антивирус детектировал данный объект, от всех уникальных пользователей продуктов «Лаборатории Касперского», на компьютерах которых были обнаружены вредоносные программы.

Первое место занимает вердикт DangerousObject.Multi.Generic (42,32%), используемый для вредоносных программ, обнаруженных с помощью облачных технологий. Эти технологии срабатывают, когда в антивирусных базах еще отсутствует сигнатура или эвристический алгоритм для детектирования вредоносной программы, однако облачные антивирусные базы компании уже содержат информацию об объекте. Данный метод применяется для детектирования новейших вредоносных программ.

Продолжает падать доля вирусов: например, Virus.Win32.Sality.gen в прошлом году встречался у 5,53% пользователей, а в 2016 — у 4,34%. Показатель Virus.Win32.Nimnul.a в 2015 году — 2,37%, а в 2016 — 2,02%. Присутствующий в рейтинге на девятнадцатом месте вердикт Trojan-Dropper.VBS.Agent.bp представляет собой VBS-скрипт, который извлекает из себя и сохраняет на диск Virus.Win32.Nimnul.

Помимо эвристических вердиктов и вирусов в TOP 20 представлены вердикты для червей, распространяющихся через съемные носители, и их компонентов. Их попадание в двадцатку обусловлено характером их распространения и созданием множества копий. Червь может продолжать свое распространение на протяжении длительного времени, даже если его командные серверы уже не действуют.

Например, Trojan.Win32.Wauchos.a — новый вердикт в этом рейтинге — является компонентом семейства Worm.Win32.Debris, которое устанавливает эту троянскую программу на съемные носители. Этот зловред способен загружать другое вредоносное ПО с командных серверов. Так, например, были зафиксированы случаи загрузки новых версий Worm.Win32.Debris.

Trojan-Proxy.Win32.Bunitu.avz — нехарактерный для этого рейтинга вердикт, поскольку он принадлежит к классу Trojan-Proxy и не имеет механизма самораспространения.

Большинство представителей Trojan.Win32.Hosts2.gen в этом году — файлы hosts, блокирующие доступ к сайтам и серверам антивирусных компаний.

Страны, в которых компьютеры пользователей подвергались наибольшему риску локального заражения

Для каждой из стран мы подсчитали число срабатываний файлового антивируса в течение года. Учитывались вредоносные программы, обнаруженные непосредственно на компьютерах пользователей и на съемных носителях, подключенных к компьютерам, — флеш-накопителях, картах памяти фотоаппаратов и телефонов, внешних жестких дисках. Эта статистика отражает уровень зараженности персональных компьютеров в разных странах мира.

ТОП 20 стран по уровню зараженности компьютеров

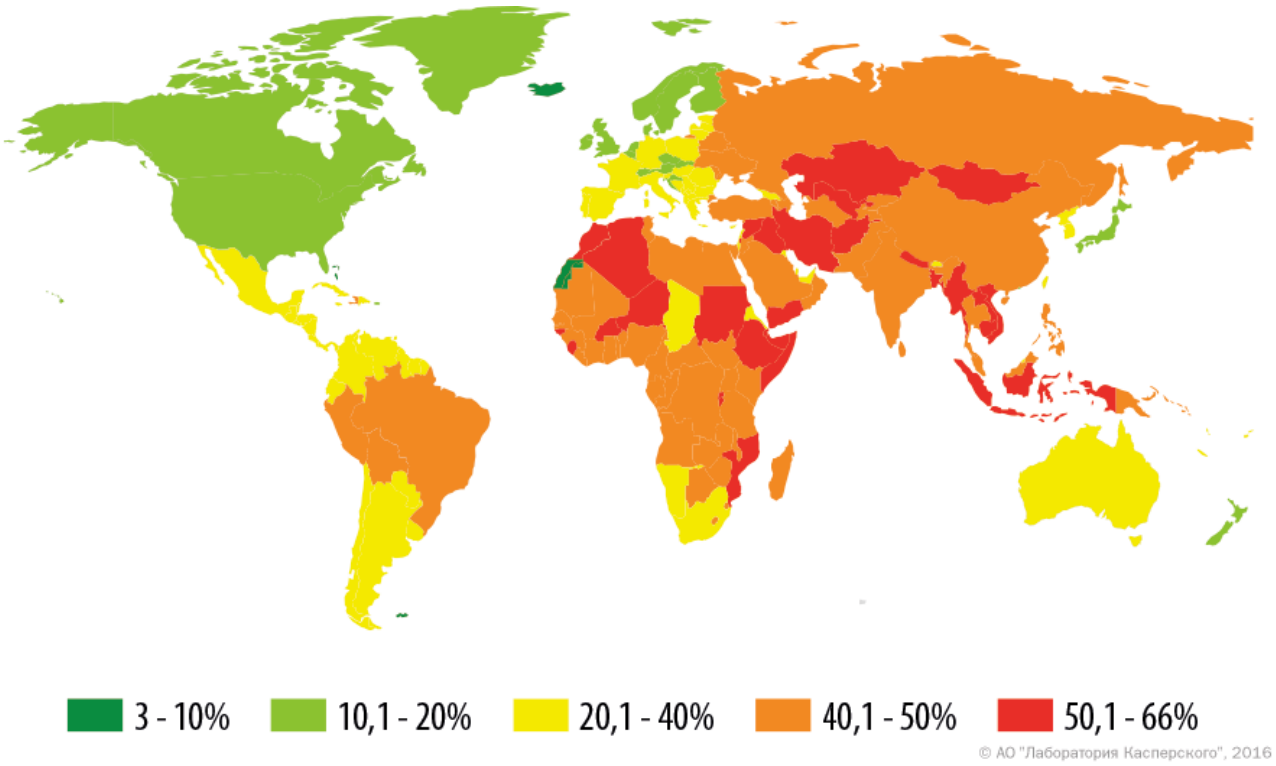
	Страна*	% уникальных пользователей**
1	Вьетнам	65,69
2	Сомали	63,90
3	Афганистан	61,05
4	Руанда	60,17
5	Алжир	59,80
6	Лаос	58,90
7	Эфиопия	57,75
8	Бангладеш	57,39
9	Непал	57,35
10	Монголия	56,89
11	Камбоджа	55,90
12	Индонезия	55,51
13	Мозамбик	54,95
14	Узбекистан	54,03
15	Ирак	53,97
16	Сирия	53,44
17	Марокко	53,39
18	Мьянма	53,11
19	Казахстан	53,02
20	Нигер	52,96

Данная статистика основана на детектирующих вердиктах файлового антивируса на компьютерах пользователей продуктов «Лаборатории Касперского», подтвердивших свое согласие на передачу статистических данных.

* Из расчетов были исключены страны, где число пользователей «Лаборатории Касперского» меньше 50 000.

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

В среднем в группе стран, входящих в TOP 20, вредоносный объект хотя бы один раз был обнаружен на компьютере — на жестком диске или на съемном носителе, подключенном к нему, — у 36,8% пользователей KSN.



Географическое распределение локальных заражений вредоносными программами в 2016 году (процент атакованных пользователей)

По уровню локальных угроз все страны мира можно разделить на несколько категорий.

- **Максимальный уровень риска (более 60%).** В эту группу вошли 4 страны из TOP 20.
- **Высокий уровень риска (41–60%).** В эту группу попали Иран (51,9%), Индия (50,4%), Беларусь (48,7%), Китай (48,6%), Украина (47,9%), Саудовская Аравия (44,04%), Россия (43,6%), Турция (42%), Бразилия (41,3%).
- **Средний уровень локального заражения (21–40,99%).** В группу вошли Молдова (40,8%), Армения (40,4%), Мексика (39,1%), Южная Африка (30,5%), Сербия (28,6%), Польша (29%), Болгария (27,4%), Испания (27%), Греция (26,2%), Италия (24,8%), Израиль (24,8%), Венгрия (23,4%), Франция (21,1%).

В десятку самых безопасных по уровню локального заражения стран попали:

	Страна	% уникальных пользователей
1	Дания	10,4
2	Швеция	13,0
3	Нидерланды	13,9
4	Япония	13,9
5	Норвегия	14,5
6	Ирландия	15,1
7	Чехия	15,2
8	Швейцария	15,75
9	США	16,48
10	Новая Зеландия	16,78

В среднем в десятке самых безопасных стран мира за год хотя бы по одному разу было атаковано 16% компьютеров пользователей.

Securelist

Ресурс экспертов «Лаборатории Касперского» с актуальной информацией о киберугрозах

Сайт «Лаборатории Касперского»

Блог Евгения Касперского

B2C блог «Лаборатории Касперского»

B2B блог «Лаборатории Касперского»

Новостная служба «Лаборатории Касперского»

Блог Kaspersky Academy