

РАЗВИТИЕ ИНФОРМАЦИОННЫХ УГРОЗ В ТРЕТЬЕМ КВАРТАЛЕ 2015 ГОДА

Дэвид Эмм
Мария Гарнаева
Роман Унучек
Денис Макрушин
Антон Иванов

ОГЛАВЛЕНИЕ

ЦИФРЫ КВАРТАЛА	3
ОБЗОР СИТУАЦИИ	4
Целевые атаки и кампании по распространению вредоносного ПО	4
Turla: использование спутникового интернета	4
Darkhotel расширяет список «гостей»	5
Blue Termite	6
Вредоносные истории	7
Конец пути для CoinVault?	7
Змей в обнесенном стеной саду Apple	8
Кибербанда Gaza	8
СТАТИСТИКА	9
Мобильные угрозы	9
Количество новых мобильных угроз	10
Распределение детектируемых мобильных программ по типам	11
TOP 20 мобильных вредоносных программ	12
География мобильных угроз	13
Мобильные банковские троянцы	14
Уязвимые приложения, используемые злоумышленниками	17
Вредоносные программы в интернете (атаки через веб-ресурсы)	18
Онлайн-угрозы в финансовом секторе	18
TOP 20 детектируемых объектов в интернете	22
Страны – источники веб-атак: TOP 10	24
Страны, в которых пользователи подвергались наибольшему риску заражения через интернет	24
Локальные угрозы	26
Детектируемые объекты, обнаруженные на компьютерах пользователей: TOP 20	26
Страны, в которых компьютеры пользователей подвергались наибольшему риску локального заражения	27

ЦИФРЫ КВАРТАЛА

- По данным KSN, решения «Лаборатории Касперского» отразили **235 415 870** атак, которые проводились с интернет-ресурсов, размещенных в разных странах мира;
- Зафиксировано **75 408 543** уникальных URL, на которых происходило срабатывание веб-антивируса.
- Нашим веб-антивирусом было обнаружено **38 233 047** уникальных детектируемых объектов (скрипты, эксплойты, исполняемые файлы и т.д.).
- Было зарегистрировано **5 686 755** уведомлений о попытках заражения вредоносным ПО для кражи денежных средств через онлайн-доступ к банковским счетам.
- Нашим файловым антивирусом зафиксировано **145 137 553** уникальных вредоносных и потенциально нежелательных объектов.
- Продуктами «Лаборатории Касперского» для защиты мобильных устройств было обнаружено:
 - **1 583 094** вредоносных установочных пакета;
 - **323 374** новых мобильных вредоносных программ;
 - **2516** мобильных банковских троянцев.

ОБЗОР СИТУАЦИИ

Целевые атаки

Turla: использование спутникового интернета

За последние полтора года мы писали о Turla несколько раз (наш [первый отчет](#), [последующий анализ](#) и [обзор вредоносной кампании](#) можно найти на сайте Securelist). Группировка, стоящая за этой кибершпионской кампанией, активна уже больше восьми лет. За это время заражены сотни компьютеров более чем в 45 странах. В число жертв атак вошли государственные ведомства, посольства, военные, образовательные и научные организации, а также фармацевтические компании.

Группировка Turla отбирает жертв определенного «профиля», применяя на начальном этапе атаки типа watering hole. При этом, как описано в нашем [последнем по времени отчете](#), в своих дальнейших действиях группа использует спутниковую связь для управления трафиком своих командных серверов.

У большинства людей спутниковая связь ассоциируется с телевещанием, однако она также используется и для доступа в интернет. Такое применение характерно для удаленных районов, где другие способы доступа в интернет не обеспечивают достаточно высокой скорости и устойчивости соединения или попросту отсутствуют. Один из наиболее распространенных и наименее затратных видов спутникового интернет-доступа – задействование спутниковой связи только для входящего трафика.

Способ, используемый группировкой Turla для взлома нисходящих спутниковых каналов, не требует подписки на спутниковый интернет. Ключевое преимущество этого метода для киберпреступников состоит в его анонимности – атакующих очень сложно вычислить. Спутниковый приемник может находиться в любом месте зоны покрытия спутника, которая обычно довольно велика, и выявить фактическое местонахождение командного сервера и физически захватить оборудование сложно. Кроме того, этот метод дешевле, чем покупка подписки на спутниковый интернет, и проще, чем перехват сетевого трафика между жертвой и оператором спутниковой связи и внедрение своих пакетов.

При атаке на спутниковые интернет-каналы тарелки законных пользователей и злоумышленников направлены на определенный спутник, который передает трафик. Злоумышленники пользуются тем, что пакеты не зашифрованы. После определения IP-адреса, на который маршрутизируется трафик через нисходящий спутниковый канал, злоумышленники начинают прослушивать сеть в ожидании пакетов, передаваемых через интернет на этот IP-адрес. При обнаружении такого пакета они идентифицируют источник и передают ему подмененный ответный пакет через обычную линию интернет-связи. При этом законный пользователь канала просто игнорирует этот пакет, так как он приходит на закрытый порт (например, 80 или 10080). Схему, наглядно показывающую, как Turla использует каналы спутниковой связи, можно найти [здесь](#).

Группировка Turla, как правило, выбирает провайдеров спутникового интернета, расположенных на Ближнем Востоке и в Африке, в том числе в Конго, Ливане,

Ливии, Нигере, Нигерии, Сомали и ОАЭ. Спутниковый сигнал, передаваемый на эти страны, как правило, не принимается в странах Европы и Северной Америки, что значительно усложняет для экспертов по безопасности анализ подобных атак.



Использование спутникового интернета киберпреступниками – интересный новый ход. Взлом полосы частот нисходящих спутниковых каналов обходится недорого (около 1000 долларов первоначальных инвестиций и примерно такая же сумма в год на текущее обслуживание), прост в реализации и обеспечивает высокий уровень анонимности. с другой стороны, данный метод не всегда так же надежен, как абьюзоустойчивый хостинг, несколько уровней прокси и взломанные веб-сайты – все эти методы Turla тоже использует, – что уменьшает вероятность его применения для организации крупных ботнетов. Тем не менее, если этот метод получит распространение среди АРТ-группировок или киберпреступников, это создаст серьезную проблему для индустрии IT-безопасности и правоохранительных органов.

Darkhotel расширяет список «гостей»

В ноябре 2014 года мы опубликовали [аналитический отчет](#) об АРТ-кампании Darkhotel. Для этих атак характерно злонамеренное использование ворованных сертификатов, внедрение HTA-файлов различными способами и проникновение в гостиничные Wi-Fi сети с целью загрузки бэкдоров на компьютеры жертв.

Недавно мы опубликовали [новые сведения](#) о Darkhotel. Продолжая применять упомянутые выше методы, злоумышленники, стоящие за этой АРТ-кампанией, расширили свой арсенал. В частности, они стали уделять большее внимание

адресным фишинговым атакам на отобранных ими жертв. В дополнение к использованию HTA-файлов они также распространяют зараженные RAR-файлы, применяя механизм RTLO (right to left override) для маскировки настоящих расширений файлов. Злоумышленники также используют эксплойты для Flash, в том числе эксплойт нулевого дня, украденный при [взломе Hacking Team](#).

В 2015 году кампания Darkhotel расширила свой географический охват: ее жертвы располагались, в частности, в Северной Корее, России, Южной Корее, Японии, Бангладеш, Таиланде, Индии, Мозамбике и Германии.

Blue Termite

В августе мы писали об APT-группировке Blue Termite, целевые атаки которой были направлены на кражу информации у японских организаций. В число жертв группировки вошли правительственные ведомства, местные органы управления, группы общественных активистов, университеты, банки, провайдеры финансовых сервисов, а также компании, работающие в таких отраслях как энергетика, связь, тяжелая, химическая и автомобильная промышленность, производство электрооборудования, новостные СМИ, информационные услуги, здравоохранение, недвижимость, пищевая промышленность, полупроводники, робототехника, строительство, страхование, транспорт и др. Одной из наиболее заметных жертв группировки стала пенсионная служба Японии.



Вредоносное ПО модифицируется с учетом особенностей каждой конкретной жертвы. В коде бэкдора Blue Termite прописаны данные о нем, включая командные серверы, имя API, строки для защиты от анализа вредоносного кода, значения мьютексов, а также контрольные суммы (MD5) команд бэкдора и информация

о внутреннем прокси-сервере. Данные хранятся в зашифрованном виде, что усложняет анализ вредоносного ПО – для расшифровки каждого образца требуется уникальный ключ.

Основной метод заражения, как и во многих других кампаниях, построенных на целевых атаках, – адресная рассылка фишинговых электронных писем. Однако мы обнаружили и другие методы заражения, в том числе drive-by загрузки с применением эксплойта для Flash (CVE-2015-5119) – одного из эксплойтов, украденных при взломе Hacking Team. Таким образом взломано несколько японских сайтов. Мы также обнаружили атаки типа watering hole, в том числе с использованием сайта, принадлежащем видному представителю правительства Японии.

Вредоносные истории

Конец пути для CoinVault?

14 сентября 2015 года полиция Нидерландов арестовала двух мужчин по подозрению в причастности к атакам с использованием программы-вымогателя CoinVault. Это стало результатом совместных усилий «Лаборатории Касперского», компании Panda Security и национального подразделения полиции Нидерландов по расследованию высокотехнологичных преступлений (National High Tech Crime Unit, NHTCU). Это наглядный пример пользы, которую приносит сотрудничество между полицией и экспертами в области IT-безопасности. Данная вредоносная кампания началась в мае 2014 года и захватила часть текущего года. Ее жертвы находятся более чем в 20 странах, причем большинство – в Нидерландах, Германии, США, Франции и Великобритании. Злоумышленникам удалось зашифровать файлы на более чем 1500 компьютерах под управлением Windows, а плату за расшифровку данных от жертв требовали в биткойнах.

Преступники, стоящие за этой кампанией кибервымогательства, изменяли свои творения несколько раз, чтобы они могли поражать все новых жертв. Мы опубликовали результаты [первоначального анализа](#) CoinVault в ноябре 2014 года, вскорости после обнаружения первого образца вредоносной программы. Затем кампания пропала с экранов радаров до апреля 2015 года, когда мы обнаружили новый образец. В тот же месяц «Лаборатория Касперского» и NHTCU Голландии запустили [веб-сайт, действующий как репозиторий для ключей расшифровки](#). Кроме того, мы разместили в интернете [инструмент для расшифровки файлов](#), чтобы помочь жертвам вернуть свои файлы, не выплачивая выкуп кибервымогателям.

После открытия сайта с «Лабораторией Касперского» связалась компания Panda Security, которой удалось обнаружить информацию о дополнительных образцах вредоносной программы. Нам удалось получить подтверждение, что эти образцы также относятся к CoinVault. Мы передали эту информацию NHTCU Нидерландов.

Наш анализ разнообразных ухищрений, на которые пошли авторы CoinVault, можно найти [здесь](#).

Программы-вымогатели стали заметной частью ландшафта угроз. В то время как данный случай показывает, что сотрудничество между экспертами и правоохранительными органами может привести к положительным результатам,

чрезвычайно важно, чтобы и индивидуальные, и корпоративные пользователи принимали меры для нейтрализации риска, связанного с данным типом вредоносного ПО. Применение программ-вымогателей имеет смысл, только если жертвы готовы платить за расшифровку своих данных. В дополнение к защите от вредоносного ПО важно регулярно создавать резервные копии своих данных, чтобы избежать потери информации, которая приведет к необходимости платить выкуп.

Змей в обнесенном стеной саду Apple

Недавнее появление [вредоносных приложений в App Store](#) показало со всей ясностью, что, вопреки распространенному мнению, операционная система iOS не является неуязвимой для вредоносного ПО.

Вредоносная программа, получившая название Xcodeghost, заразила десятки приложений, в том числе WeChat, программу загрузки музыки сервиса NetEase, сканер визитных карточек CamCard и приложение для вызова автомобиля в рамках сервиса Didi Kuaidi. Также заражены китайские версии игры Angry Birds 2.

Злоумышленники не взломали App Store, а разместили в интернете вредоносную версию созданного Apple инструментария Xcode – бесплатного набора инструментов, с помощью которого разработчики создают приложения для iOS. Он официально распространяется Apple, но кроме того, его неофициально распространяют третьи лица. Кто-то разместил на своем веб-сервере в Китае версию Xcode, содержащую вредоносный код XcodeGhost. Некоторые китайские разработчики предпочитают загружать подобные средства разработки с местных серверов, поскольку так получается гораздо быстрее.

Любые приложения, созданные с помощью модифицированной версии Xcode, будут заражены. Зараженные приложения крадут данные у жертв и отправляют их злоумышленникам. Первоначально считалось, что процедуру проверки Apple обошли 39 зараженных приложений, которые были успешно загружены в App Store. Apple удалила зараженные приложения. Однако взломанная версия Xcode доступна уже около шести месяцев, поэтому общее число зараженных приложений, возможно, значительно больше – не в последнюю очередь потому, что [исходный код XcodeGhost был опубликован на Github](#).

Анализ XcodeGhost, подготовленный экспертами Palo Alto Networks, можно найти [здесь](#).

Описанный выше инцидент высвечивает опасность заражения программ на этапе создания в случае взлома инструментов, применяемых разработчиками.

Кибербанда Gaza

В конце сентября мы писали о еще одной региональной АРТ-группировке – [кибербанде Gaza](#). Это политически мотивированная арабская группировка, действующая на Ближнем Востоке и в Северной Африке. Сфера ее интересов охватывает прежде всего Египет, ОАЭ и Йемен. Группировку интересуют государственные ведомства – особенно посольства, где работа IT-инфраструктуры и безопасность не всегда находится на должном уровне. Кибербанда Gaza действует с 2012 года, однако она значительно активизировалась во втором квартале 2015 года.

Банда активно рассылает вредоносное ПО персоналу, отвечающему за информационные технологии (IT) и реагирование на инциденты (IR) в организациях, выбранных в качестве целей, причем имена рассылаемых файлов соответствуют названиям приложений и инструментов, применяемых IT-специалистами и используемых при расследовании кибератак. В этом нет ничего удивительного: IT-специалисты, как правило, имеют более высокий уровень прав доступа, чем остальные сотрудники, поскольку они отвечают за управление работой корпоративной IT-инфраструктуры. Специалисты по реагированию на инциденты зачастую имеют доступ к конфиденциальным данным, касающимся текущих киберрасследований, и пользуются расширенными правами доступа, позволяющими выявлять подозрительную активность в сети организации. Таким образом, злоумышленники получают возможность не только проникнуть в сеть атакуемой организации, но и взять ее под свой контроль.

Основные модули заражения, применяемые группировкой, – это популярные троянские программы, предназначенные для удаленного доступа к системе жертвы (remote access Trojans, RATs): XtremeRAT и PoisonIvy. Злоумышленники активно задействуют приемы социальной инженерии. Они используют имена файлов, связанные с информационными технологиями и расследованием инцидентов, а также контент и доменные имена, которые могут с большой степенью вероятности заинтересовать жертв (например, .gov.uae.kim).

СТАТИСТИКА

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.

Мобильные угрозы

Основной способ монетизации мобильных угроз остается прежним — показ рекламы пользователям. Продолжается рост количества программ, навязчиво демонстрирующих рекламу на мобильных устройствах (AdWare), в третьем квартале они составили более половины всех обнаруженных мобильных детектируемых объектов.

В то же время мы наблюдаем рост количества программ, которые используют рекламу как основное средство монетизации и при этом применяют методы из арсенала вирусописателей. Они часто рутируют устройство жертвы и пользуются правами суперпользователя, что делает борьбу с ними очень сложной, если не невозможной. В третьем квартале 2015 года такие троянцы составили больше половины из 20 самых популярных мобильных вредоносных программ.

В качестве способа монетизации по-прежнему актуальны и SMS-троянцы, особенно для России. Напомним, что эти программы отправляют с зараженного устройства платные сообщения без ведома пользователя. Хотя их доля в общем

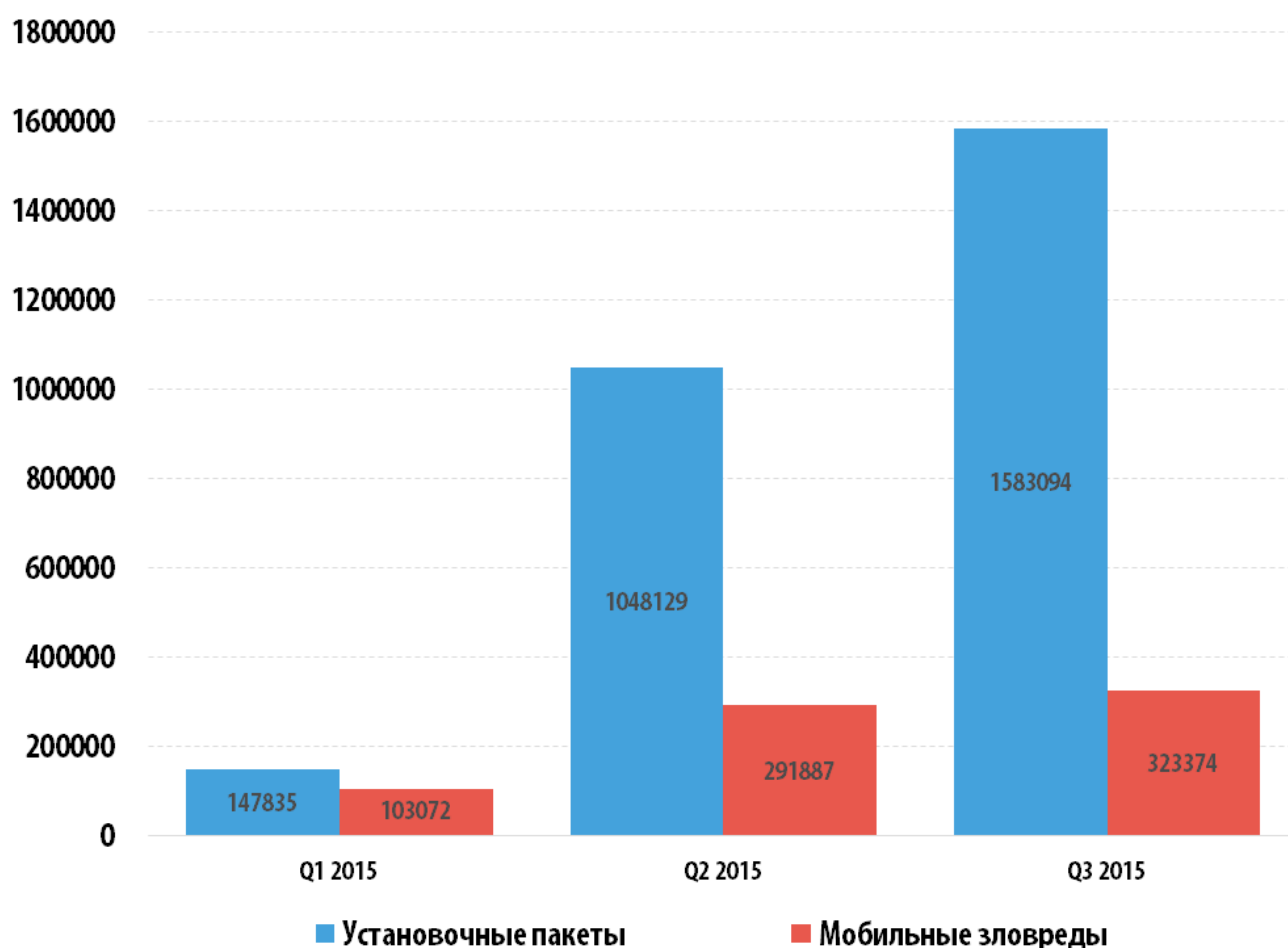
потоке мобильных угроз продолжает уменьшаться, среди вредоносных мобильных программ Trojan-SMS все еще лидируют по количеству обнаруженных за квартал новых образцов.

В погоне за наживой злоумышленники не ограничиваются показом рекламы и отправкой платных SMS. Их весьма интересуют банковские счета пользователей. По итогам квартала в потоке новых мобильных угроз суммарная доля мобильных банков и программ-шпионов, ворующих персональную информацию пользователей, на 0,7 п.п. превысила долю SMS-троянцев.

Количество новых мобильных угроз

В третьем квартале 2015 года «Лабораторией Касперского» было обнаружено **323 374** новых мобильных вредоносных программ – в 1,1 раза больше, чем во втором квартале 2015 года, и в 3,1 раза больше, чем в первом квартале 2015 года.

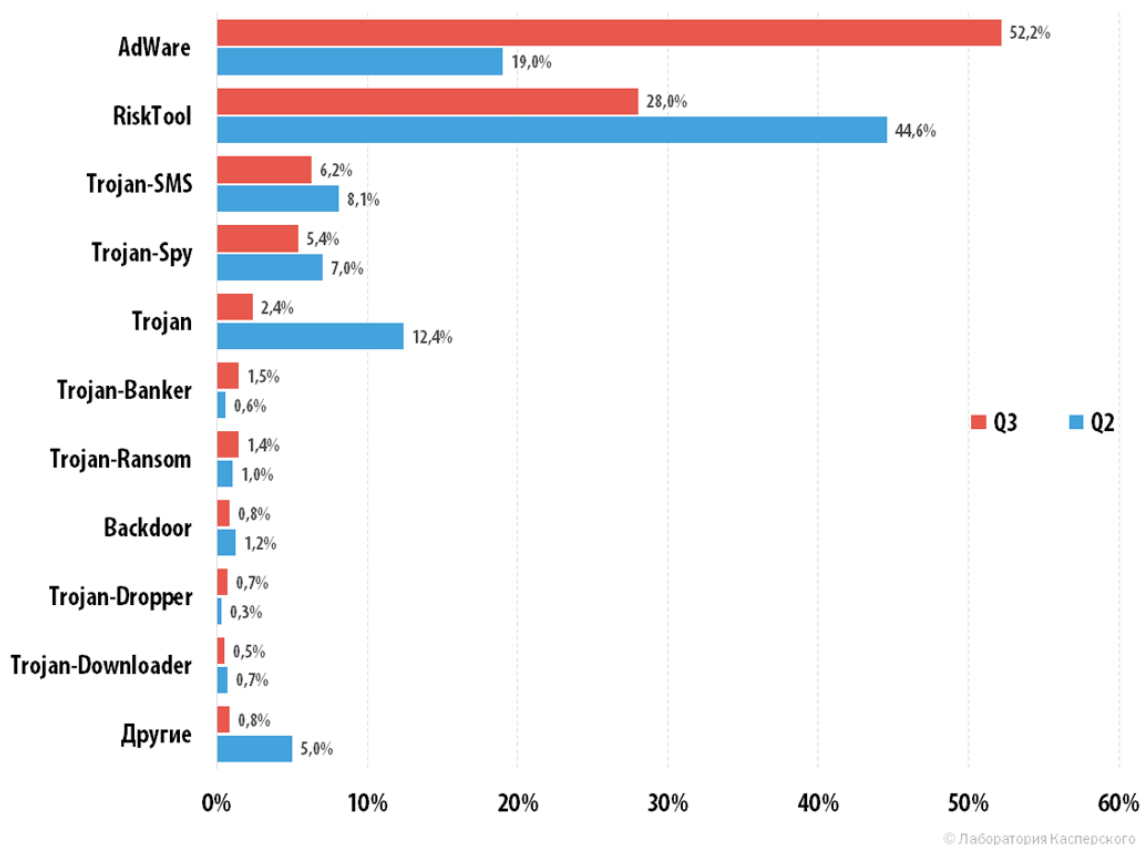
При этом количество обнаруженных вредоносных установочных пакетов составило **1 583 094** – это в 1,5 раза больше, чем в предыдущем квартале.



© Лаборатория Касперского

*Количество обнаруженных вредоносных установочных пакетов
и новых мобильных угроз (Q1 2015 – Q3 2015)*

Распределение детектируемых мобильных программ по типам



Распределение новых детектируемых мобильных программ по типам, второй и третий кварталы 2015 года

В рейтинге обнаруженных в третьем квартале 2015 года детектируемых объектов для мобильных устройств лидируют потенциально нежелательные рекламные приложения (Adware). Еще в прошлом квартале они были на втором месте с 19%, но за этот квартал их доля значительно увеличилась — до 52,2%.

На втором месте расположились RiskTool — легальные приложения, которые потенциально опасны для пользователей. Их использование злоумышленником или неаккуратное использование владельцем смартфона может привести к финансовым потерям. Доля Risktool упала на 16,6 п.п. по сравнению с прошлым кварталом, и они уступили первое место в рейтинге.

Доля Trojan-SMS в общем потоке мобильных угроз уменьшилась еще на 1,9 п.п. и составила 6,2%, однако они все еще лидируют среди вредоносных мобильных программ.

Trojan-Spy следуют сразу за SMS-троянцами с показателем 5,4%. Такие программы воруют персональные данные пользователей, в том числе входящие SMS (mTAN) от банков.

Среди вредоносных мобильных программ в третьем квартале самые высокие темпы роста зафиксированы у Trojan-Banker, доля которых увеличилась более чем в два раза и составила 1,5% против 0,6% во втором квартале. В прошлом квартале было обнаружено 630 таких программ, а в этом квартале — более 2500, т.е. в 4 раза больше.

ТОР 20 мобильных вредоносных программ

В рейтинг вредоносных программ, приведенный ниже, не входят потенциально опасные или нежелательные программы, такие как RiskTool и рекламные программы.

	Название	% атакованных пользователей*
1	DangerousObject.Multi.Generic	46,6
2	Trojan.AndroidOS.Rootnik.d	9,9
3	Trojan-SMS.AndroidOS.Podec.a	7,4
4	Trojan-Downloader.AndroidOS.Leech.a	6,0
5	Trojan.AndroidOS.Ztorg.a	5,5
6	Exploit.AndroidOS.Lotoor.be	4,9
7	Trojan-Dropper.AndroidOS.Gorpo.a	3,3
8	Trojan-SMS.AndroidOS.Opfake.a	3,0
9	Trojan.AndroidOS.Guerrilla.a	2,9
10	Trojan-SMS.AndroidOS.FakeInst.fz	2,6
11	Trojan-Ransom.AndroidOS.Small.o	2,3
12	Trojan-Spy.AndroidOS.Agent.el	2,1
13	Trojan.AndroidOS.Ventica.a	1,9
14	Trojan.AndroidOS.Ztorg.b	1,9
15	Trojan.AndroidOS.Ztorg.pac	1,8
16	Trojan.AndroidOS.Fadeb.a	1,6
17	Trojan-SMS.AndroidOS.Smapps.a	1,5
18	Trojan.AndroidOS.Iop.a	1,5
19	Trojan.AndroidOS.Guerrilla.b	1,5
20	Trojan-SMS.AndroidOS.FakeInst.fi	1,4

* Процент пользователей, атакованных данным зловредом, от всех атакованных пользователей.

На 1-м месте в рейтинге – DangerousObject.Multi.Generic (46,6%). Так новые вредоносные приложения детектируются облачными технологиями Kaspersky Security Network, которые позволяют нашим продуктам быстро реагировать на новые и неизвестные угрозы. Отметим, что доля DangerousObject.Multi.Generic в общем потоке выросла практически в три раза: с 17,5% в прошлом квартале до 46,6% в этом.

По сравнению с предыдущим кварталом в TOP 20 значительно выросло количество троянцев, которые используют рекламу в качестве основного средства монетизации. Если во втором квартале в TOP 20 попали шесть таких программ, то в третьем квартале — одиннадцать: три программы семейства Trojan.AndroidOS.Ztorg, две программы семейства Trojan.AndroidOS.Guerrilla, Trojan.AndroidOS.Rootnik.d,

Trojan-Downloader.AndroidOS.Leech.a, Trojan-Dropper.AndroidOS.Gorpo.a, Trojan-Spy.AndroidOS.Agent.el, Trojan.AndroidOS.Ventica.a и Trojan.AndroidOS.Fadeb.a.

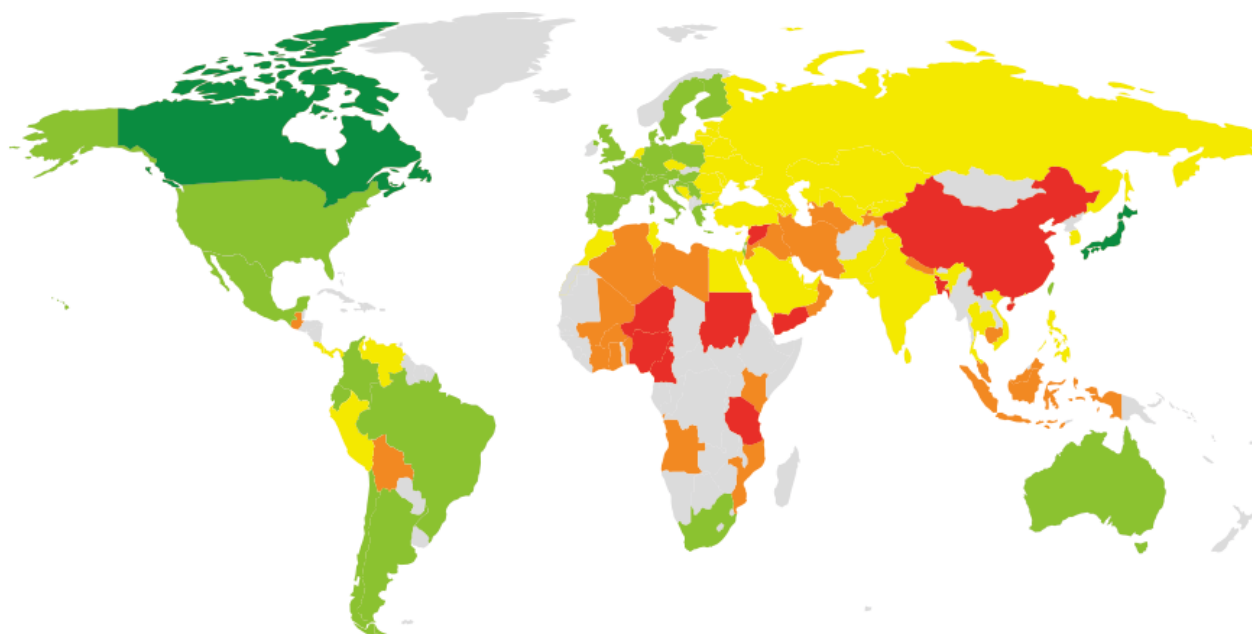
В отличие от обычных рекламных модулей эти программы не несут никакого полезного функционала. Их цель – доставить пользователю как можно больше рекламы различными способами, в том числе за счет установки новых рекламных программ. Эти троянцы [могут воспользоваться правами суперпользователя](#) для того, чтобы скрыться в системной папке, откуда удалить их будет очень сложно.

Среди этого списка хочется выделить Trojan-Spy.AndroidOS.Agent.el – он встречается даже в официальных прошивках некоторых производителей.

[Trojan-SMS.AndroidOS.Podec.a](#) (7,4%) входит в TOP 3 вредоносных мобильных угроз уже четыре квартала подряд, что обусловлено его активным распространением. Хочется отметить, что функциональность последних версий этого троянца поменялась, в них не предусмотрена возможность отправлять SMS. Теперь этот троянец полностью сконцентрировался на платных подписках, используя для этого распознавание CAPTCHA.

На 17 месте расположился троянец Trojan-SMS.AndroidOS.Smapps.a. Некоторые его версии умеют рассылать спам по команде с сервера через приложение Viber, если оно установлено у жертвы. Для этого троянцу не требуются никакие специальные разрешения или действия со стороны пользователя.

География мобильных угроз



 <3%  3,1 - 5%  5,1 - 10%  10,1 - 15%  >15%

© Лаборатория Касперского

*Карта попыток заражений мобильными зловредами в третьем квартале 2015 года
(процент атакованных пользователей в стране)*

ТОР 10 стран по проценту пользователей, атакованных мобильными зловредами:

	Страна*	% атакованных пользователей**
1	Бангладеш	22,57
2	Китай	21,45
3	Нигерия	16,01
4	Танзания	15,77
5	Иран	13,88
6	Малайзия	13,65
7	Алжир	12,73
8	Непал	12,09
9	Кения	11,17
10	Индонезия	10,82

* Из рейтинга мы исключили страны, где количество пользователей мобильного антивируса ЛК относительно мало (менее 10000).

** Процент уникальных пользователей, атакованных в стране, по отношению ко всем пользователям мобильного антивируса ЛК в стране.

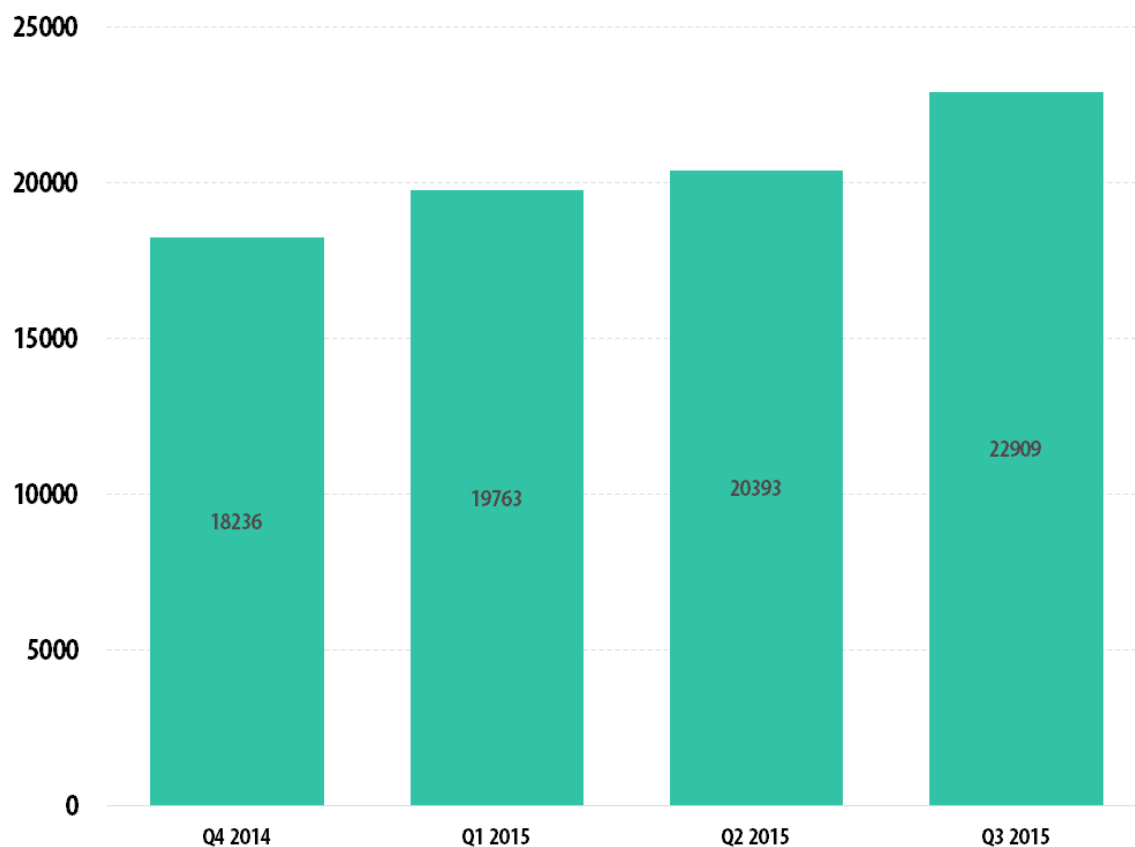
Самые безопасные страны по этому показателю:

	Страна	% атакованных пользователей**
1	Япония	1,13
2	Канада	2,87
3	Дания	3,20
4	Швеция	3,45
5	Австралия	3,48

Отметим, что хотя Австралия и попала и В ТОП 5 безопасных стран по вероятности заражения мобильными зловредами, ситуация в этой стране не столь безопасна, как хотелось бы: в третьем квартале австралийские пользователи чаще остальных подвергались атакам мобильных банковских троянцев (см. ниже).

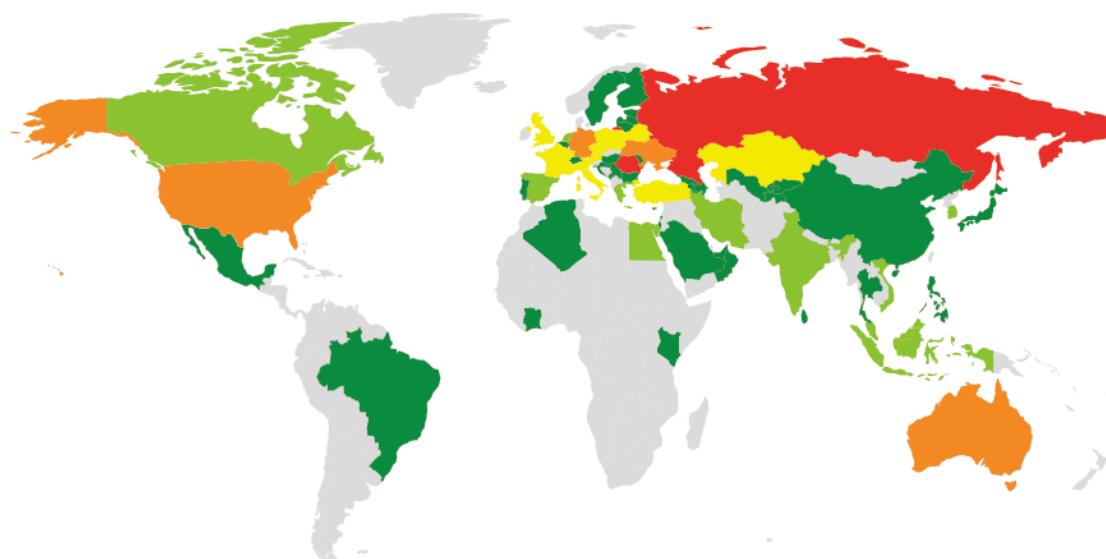
Мобильные банковские троянцы

За отчетный период мы обнаружили 2516 мобильных банковских троянцев, что практически в 4 раза больше, чем в прошлом квартале.



© Лаборатория Касперского

Количество мобильных банковских троянцев в коллекции «Лаборатории Касперского»
(Q4 2014 – Q3 2015)



1 - 50 51 - 100 101 - 300 301 - 1000 1001 - 26000

© Лаборатория Касперского

География мобильных банковских угроз в третьем квартале 2015 года
(количество атакованных пользователей)

Количество атакованных пользователей зависит от общего числа пользователей в стране. Чтобы оценить и сравнить риск заражения мобильными банковскими троянцами в разных странах мы составили рейтинг стран по проценту атакованных мобильными банковскими троянцами пользователей.

ТОР 10 стран по проценту пользователей, атакованных мобильными банковскими троянцами

	Страна*	% атакованных банкерами пользователей**
1	Австралия	0,85
2	Республика Корея	0,40
3	Россия	0,32
4	Кипр	0,32
5	Чехия	0,31
6	Австрия	0,27
7	Киргизия	0,26
8	Болгария	0,24
9	Румыния	0,23
10	Узбекистан	0,23

* Из рейтинга мы исключили страны, где количество пользователей мобильного антивируса ЛК относительно мало (менее 10 000).

** Процент в стране уникальных пользователей, атакованных мобильными банковскими троянцами, по отношению ко всем пользователям мобильного антивируса ЛК в стране.

Австралия, которая в прошлом квартале занимала 8-е место, по итогам третьего квартала лидирует. Процент пользователей, атакованных мобильными банкерами, в Австралии вырос в 6 раз (с 0,14% до 0,85%). Такой значительный рост обусловлен активным использованием злоумышленниками Trojan-Banker.AndroidOS.Agent.ad. Этот троянец ворует логин и пароль для входа в систему онлайн-банкинга одного из крупнейших банков Австралии. Также он пытается украсть данные о банковской карте пользователя (имя владельца, номер карты, CVV, срок действия карты).

В то же время долевым показателем Кореи, которая во втором квартале занимала первое место, уменьшился почти в 6 раз (с 2,37% до 0,4%), и эта страна опустилась на вторую строчку рейтинга.

ТОР 10 стран по доле пользователей, атакованных мобильными банкерами, среди всех атакованных пользователей

Показателем популярности у злоумышленников мобильных банковских троянцев в каждой стране может быть отношение количества пользователей, атакованных хотя бы раз в течение квартала мобильными троянцами, ко всем пользователям в этой же стране, у которых хотя бы раз в квартал было зафиксировано срабатывание мобильного антивируса. Этот рейтинг отличается от приведенного выше:

	Страна*	% пользователей, атакованных банкерами, от всех атакованных пользователей**
1	Австралия	24,31
2	Австрия	7,02

3	Монтенегро	5,92
4	Республика Корея	5,69
5	Франция	5,66
6	Кипр	5,56
7	Россия	5,09
8	Чехия	4,98
9	Швеция	4,81
10	Финляндия	4,56

* Из рейтинга мы исключили страны, где количество пользователей мобильного антивируса «Лаборатории Касперского» относительно мало (менее 10000).

** Процент уникальных пользователей в стране, атакованных мобильными банковскими троянцами, по отношению ко всем атакованным мобильными зловредами уникальным пользователям в этой стране.

В России доля атак банкеров среди всех атак мобильных зловредов упала практически в два раза — с 10,35% до 5,09%. Это произошло из-за значительного снижения активности семейства банковских троянцев Trojan-Banker. AndroidOS.Marcher, которое было одним из самых распространенных в стране. В третьем квартале было зафиксировано практически в десять раз меньше атак с использованием этого зловреда, чем во втором.

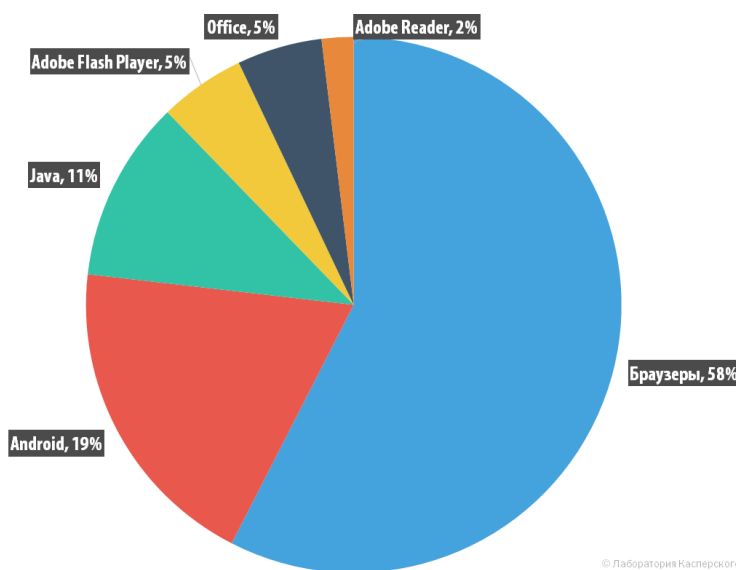
В Австралии, которая заняла первое место и в этом рейтинге, чуть менее четверти всех пользователей, атакованных мобильными зловредами, были атакованы в том числе мобильными банкерами.

Уязвимые приложения, используемые злоумышленниками

Приведенный ниже рейтинг уязвимых приложений построен на основе данных о заблокированных нашими продуктами эксплойтах, используемых злоумышленниками и в атаках через интернет, и при компрометации локальных приложений, в том числе на мобильных устройствах пользователей.

По сравнению со вторым кварталом 2015 года мы наблюдаем следующие изменения:

- Рост числа эксплойтов для Adobe Flash Player на 2 п.п.
- Снижение количества эксплойтов для Adobe Reader на 5 п.п.



Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, третий квартал 2015 года

В этом квартале, как и на протяжении всего года, были востребованы эксплойты для Adobe Flash Player. Их доля составила всего 5%, но «в дикой природе» их больше и на данный момент практически все актуальные эксплойт-паки используют уязвимости в данном ПО. Как и в предыдущем квартале, доля эксплойтов для Java (11%) в третьем квартале продолжила уменьшаться. На данный момент мы не фиксируем включение эксплойтов для данного ПО в эксплойт-паки.

В третьем квартале наиболее известные эксплойт-паки включали эксплойты для уязвимостей:

- CVE-2015-5560 (Adobe Flash; этот эксплойт [был описан в статье](#) от «Лаборатории Касперского»)
- CVE-2015-2419 (Internet Explorer)
- CVE-2015-1671 (Silverlight)

В предыдущем квартале мы выявили значительное увеличение потока спам-рассылок, содержащих вредоносные PDF-документы. В этом квартале число подобных рассылок значительно снизилось, поэтому доля эксплойтов для Adobe Reader уменьшилась.

В целом в третьем квартале 2015 года сохранился тренд, который мы наблюдаем на протяжении всего 2015 года – спросом у злоумышленников в основном пользуются эксплойты для Adobe Flash Player и Internet Explorer. На нашем графике последний входит в категорию «Браузеры», куда попадают также детектирования лэндинг-страниц, которые «раздают» эксплойты.

Вредоносные программы в интернете (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 специально создаются злоумышленниками; зараженными могут быть веб-ресурсы, контент которых создается пользователями (например, форумы), а также взломанные легитимные ресурсы.

Онлайн-угрозы в финансовом секторе

Настоящая статистика основана на детектирующих вердиктах продуктов «Лаборатории Касперского», которые были предоставлены пользователями, подтвердившими свое согласие на передачу статистических данных.

В третьем квартале 2015 года решения «Лаборатории Касперского» отразили попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на **625 669** компьютерах пользователей. По сравнению с предыдущим кварталом (**755 642**) данный показатель уменьшился на 17,2 п.п. Год назад, в третьем квартале 2014 года он составлял 591 688 компьютеров пользователей.

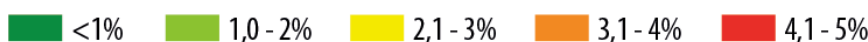
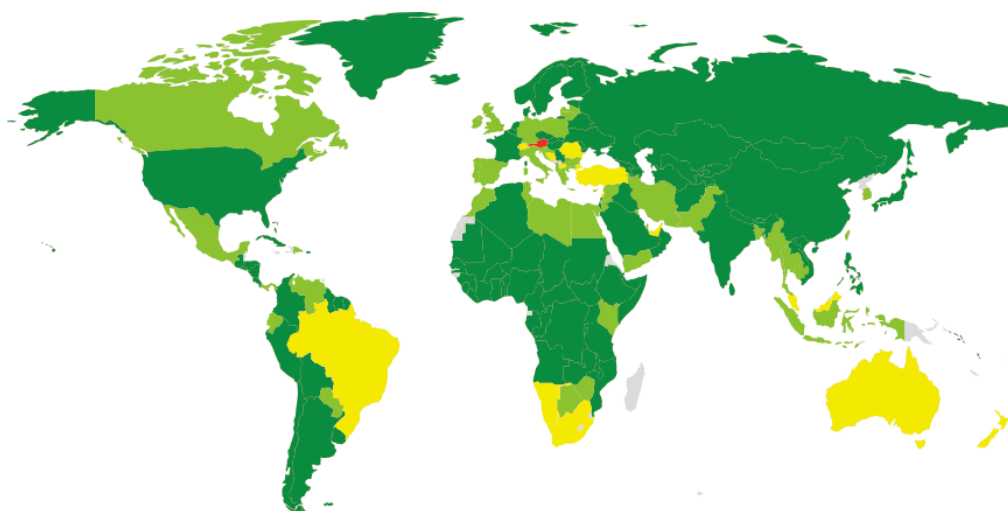
Всего защитными продуктами «Лаборатории Касперского» было зарегистрировано **5 686 755** уведомлений о попытках заражения вредоносными программами, предназначенными для кражи денежных средств через онлайн-доступ к банковским счетам.



Число атак на пользователей со стороны финансового вредоносного ПО, третий квартал 2015

География атак

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



© Лаборатория Касперского

*География атак банковского вредоносного ПО в третьем квартале 2015 года
(процент атакованных пользователей)*

ТОР-10 стран по проценту атакованных пользователей

	Страна*	% атакованных пользователей**
1	Австрия	4,98
2	Сингапур	4,23
3	Турция	3,04
4	Намибия	2,91
5	Новая Зеландия	2,86
6	Гонконг	2,81
7	Австралия	2,78
8	Ливан	2,60
9	ОАЭ	2,54
10	Швейцария	2,46

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

** Процент уникальных пользователей ЛК, подвергшихся атакам финансовых зловредов, от всех уникальных пользователей продуктов ЛК в стране.

В третьем квартале 2015 года лидером по доле пользователей «Лаборатории Касперского», атакованных банковскими троянками, стала Австрия. Лидер прошлого квартала (Сингапур) сместился на второе место. Отметим, что в большинстве стран из TOP 10 достаточно большое количество пользователей онлайн-банкинга, и это привлекает внимание киберпреступников.

В России с банковскими троянками хотя бы раз в течение квартала столкнулись 0,71% пользователей, этот показатель незначительно отличается от показателя предыдущего квартала (0,75%). В США (0,59%) данный показатель снизился в текущем квартале на 0,3 п.п. Небольшое уменьшение процента атакованных банкерами пользователей отмечено и в странах Западной Европы: в Испании (1,95%) – на 0,07 п.п., в Великобритании (1,24%) – на 0,34 п.п., в Италии (1,16%) – на 0,41 п.п., в Германии (1,03%) – на 0,13 п.п.

ТОР 10 семейств банковского вредоносного ПО

ТОР 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга в третьем квартале 2015 года:

	Название*	Процент атак**
1	Trojan-Downloader.Win32.Upatre	63,13
2	Trojan-Spy.Win32.Zbot	17,86
3	Trojan-Banker.JS.Agent	1,70
4	Trojan-Banker.Win32.ChePro	1,97
5	Backdoor.Win32.Caphaw	1,14
6	Trojan-Banker.Win32.Banbra	1,93

7	Trojan-Banker.AndroidOS.Faketoken	0,90
8	Trojan-Banker.AndroidOS.Agent	0,57
9	Trojan-Banker.Win32.Tinba	1,93
10	Trojan-Banker.AndroidOS.Marcher	0,55

* Детектирующие вердикты продуктов «Лаборатории Касперского». Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

** Процент от всех атак финансовых зловредов, которые были зафиксированы на компьютерах уникальных пользователей.

Подавляющее большинство зловредов семейств, попавших в TOP 10, используют классическую для банковских троянцев технику внедрения произвольного HTML-кода в отображаемую браузером веб-страницу и перехвата платежных данных, вводимых пользователем в оригинальные и вставленные веб-формы.

Зловреды семейства Trojan-Downloader.Win32.Upatre по-прежнему лидируют в рейтинге. Их размер не превышает 3,5 Кб, а функции ограничиваются загрузкой «полезной нагрузки» на зараженный компьютер – чаще всего это троянцы-банкеры семейства, известного как Dyre/Dyzap/Dyreza. Представитель этого семейства был впервые обнаружен в июне 2014 года, и его основной задачей является кража платежных данных пользователя. Для этого Dyre использует перехват данных банковской сессии между браузером жертвы и веб-приложением онлайн-банкинга. Однако летом 2015 года загрузчик Trojan-Downloader.Win32.Upatre [был замечен](#) на скомпрометированных домашних роутерах, что говорит о многоцелевом использовании этого троянца злоумышленниками.

Бессменный резидент данного рейтинга — Trojan-Spy.Win32.Zbot (второе место). Его постоянное присутствие на верхних строчках рейтинга неслучайно. Троянцы семейства Zbot одними из первых стали использовать веб-инжекты для компрометации платежных данных пользователей систем онлайн-банкинга и модификации содержимого банковских веб-страниц. Они используют несколько уровней шифрования своих конфигурационных файлов, и при этом сам расшифрованный файл конфигурации не хранится в памяти целиком, а загружается по частям. Это дает технологическое преимущество троянцам семейства Trojan-Spy.Win32.Zbot перед их вредоносными конкурентами.

В этом квартале на третьем месте оказалось семейство Trojan-Banker.JS.Agent – вредоносный JS-код, который является результатом процедуры инъекта в страницу онлайн-банкинга. Задача данного кода – перехватить платежные данные, которые пользователь вводит в формы на странице онлайн-банкинга.

Отметим, что в этом рейтинге присутствуют три семейства мобильных банковских троянцев: Trojan-Banker.AndroidOS.Faketoken, Trojan-Banker.AndroidOS.Marcher (мы писали о них [в прошлом квартале](#)) и новичок рейтинга — Trojan-Banker.AndroidOS.Agent. Программы этого семейства воруют платежные данные с мобильных устройств под управлением операционной системы Android.

ТОР 10 операционных систем, атакуемых банковскими троянцами

В третьем квартале атакам финансовых зловредов больше всех подвергались пользователи операционных систем семейства Windows (что не удивительно, принимая во внимание распространенность устройств на базе операционных систем данного семейства). При этом пользователи Windows 7 x64 Edition сталкивались с банковскими троянцами чаще остальных - в третьем квартале на них пришлось **42,2%** всех атак банковеров. Кроме того, в ТОП атакуемых операционных систем попала ОС Android.

	Операционная система	процент атак*
1	Windows 7 x64 Edition	42,2
2	Windows 7	11,6
3	Windows 7 Home x64 Edition	5,5
4	Windows XP Professional	7,0
5	Windows 8.1 Home x64 Edition	3,7
6	Windows 8.1 x64 Edition	2,3
7	Windows 7 Home	1,3
8	Windows 10 x64 Edition	1,2
9	Android 4.4.2	0,6
10	Windows NT 6.3 x64 Edition	0,7

* Процент от всех атак финансовыми зловредами, которые были зафиксированы на компьютерах уникальных пользователей, подтвердивших свое согласие на передачу статистических данных.

Отметим, что хотя семейство операционных систем Mac OS X не попало в ТОП, пользователям этой ОС нельзя считать себя в полной безопасности: в третьем квартале компьютеры под управлением операционной системы Mac OS X были атакованы **12 492** раза.

ТОР 20 детектируемых объектов в интернете

В третьем квартале 2015 года нашим веб-антивирусом было обнаружено **38 233 047** уникальных объектов (скрипты, эксплойты, исполняемые файлы и т.д.), и зафиксировано **75 408 543** уникальных URL, на которых происходило срабатывание веб-антивируса.

Из всех вредоносных и потенциально нежелательных объектов мы выделили 20 наиболее активных – на них пришлось 95% всех атак в интернете.

ТОР 20 детектируемых объектов в интернете

	Название*	% от всех атак**
1	Malicious URL	53,63
2	AdWare.JS.Agent.bg	16,71
3	AdWare.Script.Generic	7,14

4	Trojan.Script.Generic	6,30
5	Trojan.Script.Iframer	3,15
6	Trojan.Win32.Generic	1,52
7	AdWare.Win32.SoftPulse.heur	1,31
8	AdWare.JS.Agent.bt	1,09
9	AdWare.Win32.OutBrowse.heur	0,84
10	Trojan-Downloader.Win32.Generic	0,63
11	AdWare.NSIS.Vopak.heur	0,46
12	Exploit.Script.Blocker	0,46
13	Trojan-Downloader.JS.Iframe.diq	0,30
14	AdWare.Win32.Amonetize.aqxd	0,30
15	Trojan-Downloader.Win32.Genome.tqbx	0,24
16	AdWare.Win32.Eorezo.abyb	0,23
17	Hoax.HTML.ExtInstall.a	0,19
18	Trojan-Clicker.HTML.Iframe.ev	0,17
19	AdWare.Win32.Amonetize.bgnd	0,15
20	Trojan.Win32.Invader	0,14

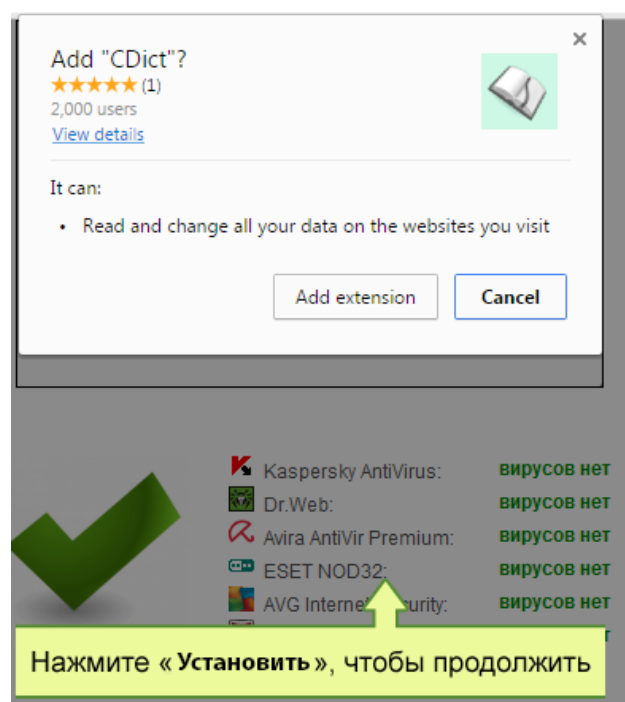
* Детектирующие вердикты модуля веб-антивируса. Информация предоставлена пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

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

В TOP 20 представлены по большей части вердикты, которые присваиваются объектам, использующимся в drive-by атаках, а также рекламным программам, вердикты для которых в этом квартале занимают девять из двадцати позиций.

Интересно отметить вердикт Hoax.HTML.ExtInstall.a, под которым детектируется веб-страница, блокирующая браузер пользователя и навязывающая установку расширения для Chrome. При попытке закрыть страницу часто воспроизводится файл voice.mp3 – **«чтобы закрыть страницу, нажмите кнопку добавить»**.

Предлагаемые расширения не несут вреда пользователям, однако это весьма навязчивое предложение, от которого пользователю практически



Веб-страница, навязывающая установку расширения для Chrome

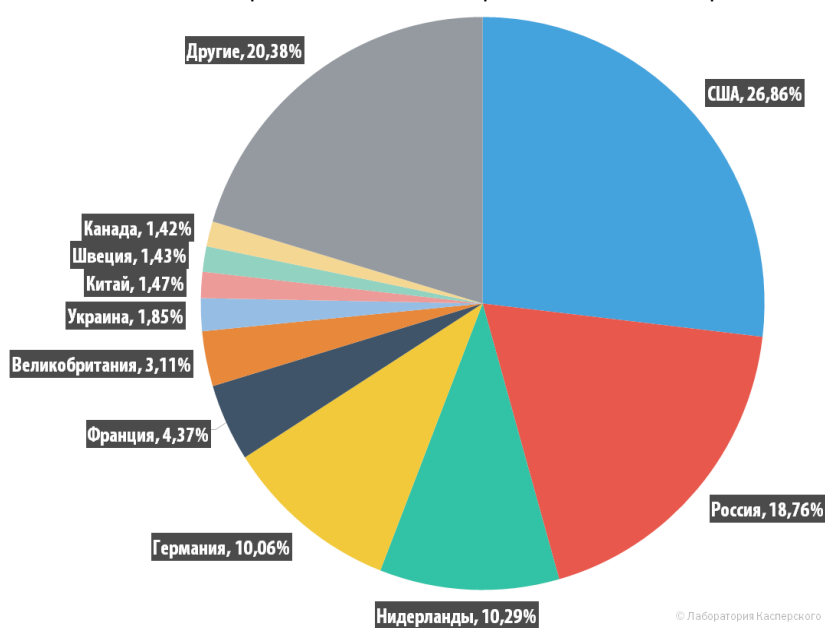
невозможно отказаться. Именно поэтому продукты «Лаборатории Касперского» детектируют соответствующую веб-страницу со всплывающим окном. Этот способ распространения расширения использует одна из партнерских программ.

Страны – источники веб-атак: TOP 10

Данная статистика показывает распределение по странам источников заблокированных антивирусом 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 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 третьем квартале 2015 года решения «Лаборатории Касперского» отразили **235 415 870** атак, которые проводились с интернет-ресурсов, размещенных в разных странах мира. 80% уведомлений о заблокированных веб-атаках были получены при блокировании атак с веб-ресурсов, расположенных в десяти странах мира.



Распределение по странам источников веб-атак, третий квартал 2015 года

По сравнению с прошлым кварталом США стал лидером рейтинга с 26,9%, поменявшись с Россией (18,8%) местами. Из TOP 10 стран выбыли Виргинские острова и Сингапур, новички рейтинга – Швеция (1,43%) и Канада (1,42%).

Страны, в которых пользователи подвергались наибольшему риску заражения через интернет

Чтобы оценить степень риска заражения 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.

ТОР 20 стран по риску заражения компьютеров через интернет

	Страна*	% атакованных уникальных пользователей**
1	Россия	38,20
2	Непал	36,16
3	Казахстан	33,79
4	Украина	33,55
5	Сирия	32,10
6	Азербайджан	32,01
7	Белоруссия	30,68
8	Вьетнам	30,26
9	Китай	27,82
10	Таиланд	27,68
11	Армения	27,65
12	Бразилия	26,47
13	Алжир	26,16
14	Турция	25,13
15	Монголия	25,10
16	Киргизия	23,96
17	Македония	23,84
18	Литва	23,59
19	Бангладеш	23,56
20	Молдавия	23,36

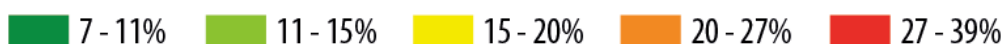
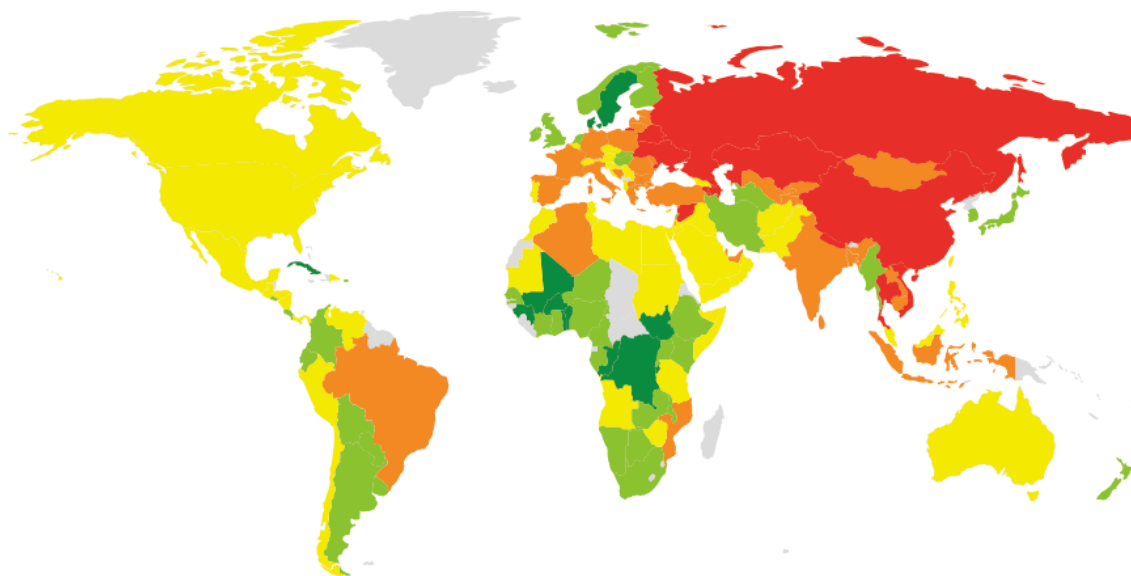
Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

* При расчетах мы исключили страны, в которых число пользователей «Лаборатории Касперского», относительно мало (меньше 10 000).

** Процент уникальных пользователей, подвергшихся веб-атакам, от всех уникальных пользователей продуктов ЛК в стране.

Лидер рейтинга не изменился, им по-прежнему является Россия (38,2%). По сравнению со вторым кварталом из ТОР 20 выбыли Грузия, Хорватия, Катар, Босния и Герцеговина, Греция. Новички рейтинга – Непал, поднявшаяся сразу на второе место (36,16%), Бразилия на 12-м месте (26,47%), Турция на 14-м (25,13%), Литва (23,59%) на 18-м и Бангладеш (23,56%) на 19-м местах.

В числе самых безопасных при серфинге в интернете стран – Швейцария (17%), Чехия (16%), США (16,3%), Сингапур (15%), Венгрия (13,8%), Норвегия (13%), Ирландия (12,2%), Швеция (10,8%).



© Лаборатория Касперского

В среднем в течение квартала 23,4% компьютеров пользователей интернета в мире хотя бы раз подвергались веб-атаке. По сравнению с предыдущим кварталом этот показатель уменьшился на 0,5 п.п.

Локальные угрозы

Важным показателем является статистика локальных заражений пользовательских компьютеров. 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.).

В этом разделе мы анализируем статистические данные, полученные на основе работы антивируса, сканирующего файлы на жестком диске в момент их создания или обращения к ним, и данные по сканированию различных съемных носителей информации.

В третьем квартале 2015 года нашим файловым антивирусом было зафиксировано **145 137 553** уникальных вредоносных и потенциально нежелательных объектов.

Детектируемые объекты, обнаруженные на компьютерах пользователей: TOP 20

	Название*	% атакованных уникальных пользователей**
1	DangerousObject.Multi.Generic	19,76
2	Trojan.Win32.Generic	14,51
3	Trojan.WinLNK.StartPage.gena	5,56
4	WebToolbar.JS.Conduit.a	4,98
5	AdWare.Script.Generic	4,97

6	WebToolbar.Win32.Agent.azm	4,48
7	RiskTool.Win32.GlobalUpdate.dx	3,63
8	WebToolbar.JS.AgentBar.e	3,63
9	WebToolbar.JS.CroRi.b	3,32
10	Downloader.Win32.Agent.bxib	3,20
11	AdWare.Win32.OutBrowse.heur	3,13
12	Adware.NSIS.ConvertAd.heur	3,08
13	AdWare.Win32.Generic	3,06
14	Downloader.Win32.MediaGet.elo	2,98
15	Trojan.Win32.AutoRun.gen	2,92
16	AdWare.Win32.BrowseFox.e	2,91
17	WebToolbar.Win32.MyWebSearch.si	2,82
18	AdWare.Win32.MultiPlug.heur	2,66
19	Virus.Win32.Sality.gen	2,61
20	RiskTool.Win32.BackupMyPC.a	2,57

* Детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

** Процент уникальных пользователей, на компьютерах которых антивирус детектировал данный объект, от всех уникальных пользователей продуктов ЛК, у которых происходило срабатывание файлового антивируса.

Традиционно в данном рейтинге представлены вердикты, которые присваиваются рекламным программам и их компонентам, и червям, распространяющимся на съемных носителях.

Единственный представитель вирусов – Virus.Win32.Sality.gen – продолжает сдавать позиции. Доля зараженных этим вирусом компьютеров пользователей снижается на протяжении длительного времени. В этом квартале Sality занимает 19-е место с показателем 2,61%, что на 0,25 п.п. меньше, чем в прошлом квартале.

Страны, в которых компьютеры пользователей подвергались наибольшему риску локального заражения

Для каждой из стран мы подсчитали, какой процент пользователей продуктов «Лаборатории Касперского» столкнулся со срабатыванием файлового антивируса в отчетный период. Эта статистика отражает уровень зараженности персональных компьютеров в различных странах мира.

ТОР 20 стран по уровню зараженности компьютеров

	Страна*	% уникальных пользователей**
1	Бангладеш	64,44
2	Вьетнам	60,20
3	Непал	60,19

4	Грузия	59,48
5	Сомали	59,33
6	Лаос	58,33
7	Россия	57,79
8	Армения	57,56
9	Афганистан	56,42
10	Эфиопия	56,34
11	Руанда	56,21
12	Сирия	55,82
13	Мозамбик	55,79
14	Йемен	55,17
15	Камбоджа	55,12
16	Алжир	55,03
17	Ирак	55,01
18	Казахстан	54,83
19	Монголия	54,65
20	Украина	54,19

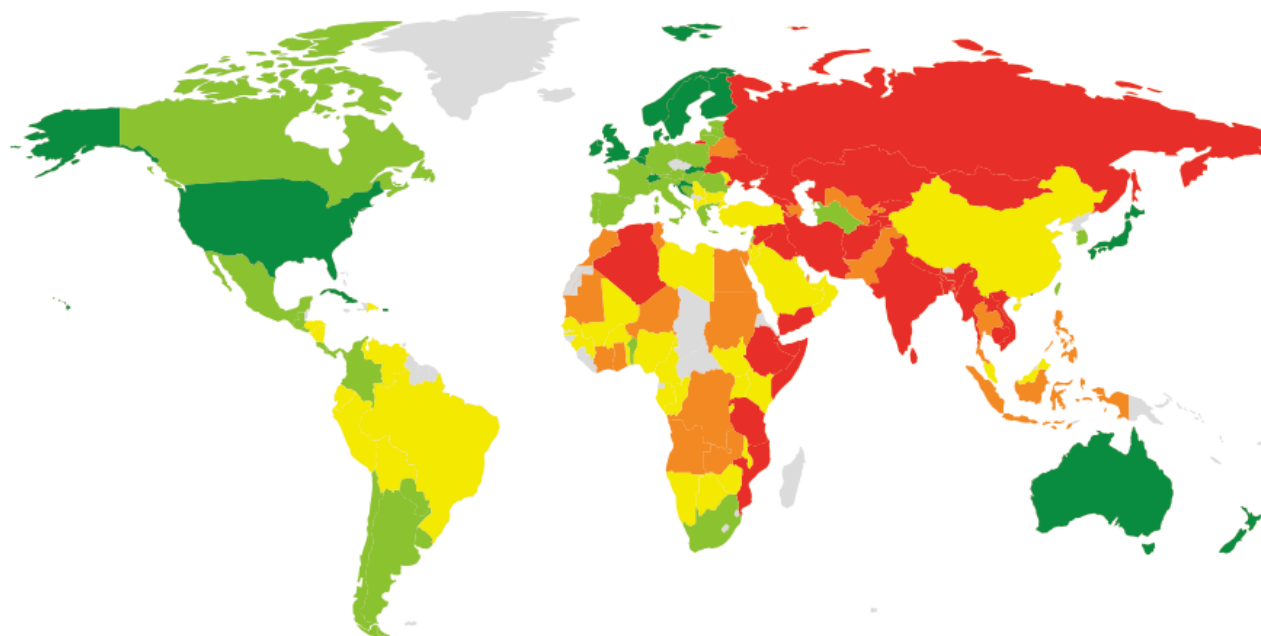
Настоящая статистика основана на детектирующих вердиктах модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных. Учитывались вредоносные программы, найденные непосредственно на компьютерах пользователей или же на съемных носителях, подключенных к компьютерам — флешках, картах памяти фотоаппаратов, телефонов, внешних жестких дисках.

* При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (менее 10 000).

** Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов ЛК в стране.

Новички рейтинга – Мозамбик на 13-й строчке рейтинга (55,8%) и Йемен на 14-й строчке (55,2%).

Страны с наименьшим уровнем заражения – Швеция (21,4%), Дания (19,8%) и Япония (18,0%).



© Лаборатория Касперского

В среднем в мире хотя бы один раз в течение третьего квартала локальные угрозы были зафиксированы на 42,2% компьютеров пользователей – это на 2,2 п.п. больше, чем во втором квартале 2015 года.

О «Лаборатории Касперского»

«Лаборатория Касперского» – крупнейшая в мире частная компания, работающая в сфере информационной безопасности, и один из наиболее быстро развивающихся вендоров защитных решений. Компания входит в четверку ведущих мировых производителей решений для обеспечения IT-безопасности пользователей конечных устройств (IDC, 2014). С 1997 года «Лаборатория Касперского» создает инновационные и эффективные защитные решения и сервисы для крупных корпораций, предприятий среднего и малого бизнеса и домашних пользователей. «Лаборатория Касперского» – международная компания, работающая почти в 200 странах и территориях мира; ее технологии защищают более 400 миллионов пользователей по всему миру. Более подробная информация доступна на сайте www.kaspersky.ru.



[Securelist](#), ресурс экспертов «Лаборатории Касперского»
с актуальной информацией о киберугрозах



[Сайт «Лаборатории Касперского»](#)



[B2B блог «Лаборатории Касперского»](#)



[Блог Евгения Касперского](#)



[B2C блог «Лаборатории Касперского»](#)



[Новостная служба
«Лаборатории Касперского»](#)



[Блог Kaspersky Academy](#)

Москва, 125212
Ленинградское шоссе, д.39А, стр.3
БЦ «Олимпия Парк»

Телефон: +7-495-797-8700
+7-495-737-3412
Факс: +7-495-797-8709

