KASPERSKY lab

30 июля 2015 года

РАЗВИТИЕ ИНФОРМАЦИОННЫХ УГРОЗ ВО ВТОРОМ КВАРТАЛЕ 2015 ГОДА

Дэвид Эмм,
Мария Гарнаева,
Роман Унучек,
Денис Макрушин,
Антон Иванов

СОДЕРЖАНИЕ

ЦИФРЫ КВАРТАЛА

- По данным KSN, решения «Лаборатории Касперского» отразили 379 972 834 атаки, которые проводились с интернет-ресурсов, размещенных в разных странах мира.
- Нашим веб-антивирусом было обнаружено 26 084 253 уникальных вредоносных объекта (скрипты, эксплойты, исполняемые файлы и т.д.).
- Зафиксировано 65 034 577 уникальных URL, на которых происходило срабатывание веб-антивируса.
- 51% веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в России.
- Было зарегистрировано 5 903 377 уведомлений о попытках заражения вредоносным ПО для кражи денежных средств через онлайн-доступ к банковским счетам.
- Нашим файловым антивирусом зафиксировано 110 731 713 уникальных вредоносных и потенциально нежелательных объектов.
- Продуктами «Лаборатории Касперского» для защиты мобильных устройств было обнаружено:
  - 1 048 129 установочных пакетов;
  - 291 887 новых мобильных вредоносных программ;
  - 630 мобильных банковских троянцев.

ОБЗОР СИТУАЦИИ

Целевые атаки и кампании по распространению вредоносного ПО

Мартышкин труд

Недавно мы опубликовали свой анализ CozyDuke, еще одной APT-атаки семейства Duke, в которое также входят MiniDuke, CosmicDuke и OnionDuke. CozyDuke (также известный как CozyBear, CozyCar и Office Monkeys) атакует правительственные организации и коммерческие компании в США, Германии, Южной Корее и Узбекистане.

Атака проводится с использованием сложных технологий, таких как шифрование, защита от обнаружения антивирусными программами и тщательно разработанный набор компонентов, которые сходны по своей структуре с более ранними угрозами семейства Duke.

При этом одной из отличительных особенностей CozyDuke является использование методов социальной инженерии для того, чтобы получить плацдарм для атаки организации, которая является целью. Некоторые электронные письма, в которых используются приемы целевого фишинга, содержат ссылку на взломанные сайты (в том числе на популярные легитимные сайты), на которых помещен ZIP-архив. Этот архив содержит самораспаковывающийся RAR-архив, который устанавливает вредоносное ПО, показывая пустой PDF-файл в качестве приманки. Другой вариант – отправка в качестве вложений к письмам мошеннических флеш-видео, содержащих исполняемый вредоносный код. Интересным примером такого видео (по имени которого названо и вредоносное ПО) является OfficeMonkeys LOL Video.zip. Пока воспроизводится приманка-видеоролик с забавным сюжетом об обезьянах, работающих в офисе, зловред загружает на компьютер исполняемый файл CozyDuke. Смешное видео провоцирует сотрудников разослать его коллегам в офисе, увеличивая число зараженных компьютеров.

Успешное использование методов социальной инженерии, для того чтобы ввести сотрудников в заблуждение и заставить делать то, что поставит под угрозу безопасность компании, – с помощью CozyDuke и других целевых вредоносных программ, – подтверждает необходимость обучения персонала основам всякой стратегии корпоративной безопасности.

Геополитические интересы Naikon: сбор разведданных

В мае мы опубликовали отчет о деятельности APT-группировки Naikon, чьи атаки были в основном направлены на важные цели в Юго-Восточной Азии и регионе Южно-Китайского моря. Группировка действует уже как минимум 5 лет. Родным языком злоумышленников, по-видимому, являлся китайский, а их атаки были нацелены в основном на высокого уровня государственные учреждения и гражданские и военные организации таких стран, как Филиппины, Малайзия, Камбоджа, Индонезия, Вьетнам, Мьянма, Сингапур, Непал, Таиланд, Лаос и Китай.

Как и во многих кампаниях такого рода, злоумышленники используют целевой фишинг, чтобы ничего не подозревающие сотрудники загрузили вредоносное ПО на свои компьютеры. Пользователь получает электронное сообщение с вложением, которое может его заинтересовать. Вложение-приманка выглядит как стандартный документ Word. На самом деле это исполняемый файл с двойным расширением или с именем, созданным с помощью приема RTLO (Right-to-Left Override), для маскировки настоящего расширения файла. Если пользователь откроет файл, тот устанавливает на компьютер шпионское ПО и одновременно выводит на экран текст документа – подсадной утки, так чтобы у пользователя не возникло никаких подозрений.

Главный модуль Naikon представляет собой утилиту удаленного администрирования. в его арсенале 48 команд, с помощью которых злоумышленники могут управлять компьютером жертвы. Среди них – возможность получить полную информацию об аппаратном и программном обеспечении компьютера, загрузить и отправить данные, установить модули расширения. Кроме того, иногда Naikon использует программы-кейлоггеры для получения регистрационных данных сотрудников.

Каждой стране, на которую нацелены атаки, назначается свой оператор, который использует ее культурные особенности, например привычку использовать свой личный аккаунт в электронной почте для работы. Используется также специальный прокси-сервер внутри страны, который управляет соединениями с зараженными компьютерами и перенаправляет данные на командный сервер злоумышленников.

Наш основной отчет и следующий за ним можно прочитать на нашем сайте.

Слежка за шпионами

Исследуя операции Naikon, мы раскрыли деятельность APT-группировки Hellsing. Эта группа нацелена в основном на правительственные и дипломатические организации в Азии. Большинство жертв располагалось в Малайзии и на

Филиппинах, хотя мы также фиксировали пострадавших в Индии, Индонезии и США.

Сама по себе Hellsing – небольшая и технически непримечательная кибершпионская группировка, атаковавшая на данный момент около 20 организаций. Интересно то, что эта группировка стала объектом целевого фишинга со стороны APT-группировки Naikon – и решила нанести ответный удар! Получив электронное сообщение, адресаты просили отправителя подтвердить авторство адресной рассылки. Они получили ответ атакующего, но вложение открывать не стали. Вместо этого через некоторое время они отправляли письмо обратно атакующим, и оно содержало уже другую вредоносную программу. Очевидно, что группировка Hellsing, поняв, что подверглась целевой атаке, решила установить, кто ее организовал и собрать информацию о его деятельности.

Мы и раньше сталкивались с тем, что APT-группировки могли случайно наступить на ногу конкуренту, например украсть у жертв списки адресов электронной почты и рассылать письма по каждому адресу из каждого списка.

Grabit

Многие целевые атаки направлены на крупные предприятия, правительственные структуры и другие известные учреждения. Поэтому читая заголовки, легко представить себе, что для злоумышленников интерес представляют именно такие организации. Однако одна из кампаний, о которой мы рассказывали в прошлом квартале, ясно показала, что злоумышленников интересует не только крупная рыба. Любая компания является потенциальной целью – либо благодаря ее активам, либо как путь для проникновения в другую организацию.

Кибершпионская кампания Grabit разработана для кражи данных компаний малого и среднего бизнеса, расположенных в основном в Таиланде, Вьетнаме и Индии, хотя нам встречались ее жертвы и в США, ОАЕ, Турции, России, Китае, Германии и других странах. Целями злоумышленников являлись такие секторы экономики, как химическая промышленность, нанотехнологии, образование, сельское хозяйство, средства массовой информации и строительство. По нашей оценке, группой, стоящей за проведением этих атак, на данный момент украдено около 10 000 файлов.

Вредоносное ПО доставляется в виде вложенного в сообщение электронной почты документа Word, который содержит вредоносный макрос под названием AutoOpen. Этот макрос перед загрузкой вредоносного ПО открывает сокет через TCP и отправляет HTTP-запрос удалённому серверу, который ранее был взломан этой группой и используется в качестве хаба вредоносного ПО. Затем с этого сервера загружается программа, которая используется для выполнения слежки. в некоторых случаях вредоносный макрос защищён паролем (похоже, злоумышленники забыли,

что DOC-файл по сути представляет собой архив и если открыть его в текстовом редакторе, строки макроса будут показаны открытым текстом). Злоумышленники контролируют зараженные компьютеры с помощью коммерческого инструмента для слежки под названием HawkEye (от HawkEyeProducts). Они также используют некоторые инструменты удаленного администрирования.

Злоумышленники использовали технологии, специально разработанные для того, чтобы затруднить анализ Grabit. Это и разный размер кода, и обфускация кода, и шифрование. Однако им так и не удалось скрыть следы своего пребывания в системе. в результате мы видим «слабого рыцаря в тяжелых доспехах», что рождает предположение, что организаторы атаки не писали весь код самостоятельно.

Возвращение Duqu

Весной 2015 года в ходе плановой проверки безопасности «Лаборатория Касперского» обнаружила попытку вторжения, затрагивающую несколько внутренних систем компании. По этому факту было проведено широкомасштабное расследование, в результате которого мы обнаружили новую вредоносную платформу, разработанную одной из наиболее профессиональных, загадочных и мощных APT-группировок – Duqu, которую еще иногда называют «сводным братом» Stuxnet. Мы дали этой новой вредоносной платформе имя «Duqu 2.0".

В атаке на «Лабораторию Касперского» использовалась уязвимость нулевого дня в ядре Windows (закрыта Microsoft 9 июня 2015 года), а также, вероятно, еще одна-две уязвимости нулевого дня (которые в данный момент уже закрыты). Основной задачей злоумышленников был шпионаж: их интересовали технологии, исследования и внутренние процессы «Лаборатории Касперского».

Однако «Лаборатория Касперского» была не единственной целью. Некоторые из новых случаев заражения Duqu 2.0 связаны с работой «иранской шестерки» и проведением переговоров с Ираном по ядерной программе. По всей видимости, атаки начались в тех местах, где проходили некоторые из встреч на высоком уровне. Кроме того, аналогичную атаку группировка предприняла в связи с 70-й годовщиной освобождения Освенцима.

Одной из наиболее примечательных особенностей Duqu 2.0 явилось то, что зловред практически не оставляет следов своего присутствия в системе. Эта вредоносная программа не меняет настроек диска или системы, поскольку ее платформа разработана таким образом, что она сохраняется исключительно в памяти зараженных систем. Это наводит на мысль о том, что злоумышленники были абсолютно уверены, что они могут сохранить свое присутствие в системе, даже если компьютер конкретной жертвы был перезагружен и вредоносные программы были удалены из памяти.

Техническое описание Duqu 2.0 и анализ модуля Duqu 2.0, сохраняющего присутствие в сети можно найти на нашем веб-сайте.

Вредоносные истории

Simda: игра в прятки и бизнес по распространению вредоносного ПО

В апреле «Лаборатория Касперского» приняла участие в операции по уничтожению ботнета Simda, координируемой Глобальным комплексом инноваций Интерпола. Это расследование было начато компанией Microsoft, затем круг участников расширился, и к расследованию подключились компания TrendMicro, японский Cyber Defense Institute, сотрудники голландского Национального центра по борьбе с преступлениями в сфере высоких технологий (NHTCU), ФБР, полиция Люксембурга, а также сотрудники Управления «К» МВД России при поддержке Национального центрального бюро Интерпола в Москве.

В результате совместных действий была остановлена работа 14 командных серверов в Нидерландах, США, Люксембурге, Польше и России. Предварительный анализ некоторых журналов событий sinkhole-серверов, подменивших командные серверы, показал, что ботнет Simda нанес ущерб 190 странам.

Боты распространяются через несколько зараженных веб-сайтов, которые перенаправляют пользователей на набор эксплойтов. Боты загружают и запускают дополнительные компоненты с собственных серверов обновления и могут изменять файл hosts на зараженном компьютере. Таким образом компьютеры, однажды зараженные Simda, могут продолжать посылать HTTP-запросы вредоносным серверам, сообщая, что они по-прежнему уязвимы и могут быть вновь заражены с помощью всё тех же наборов эксплойтов.

Хотя ботнет Simda довольно велик – по оценкам, им заражены около 770 000 компьютеров, его авторы приложили немалые усилия, чтобы он оставался незамеченным защитными системами. Зловред способен распознавать эмуляцию, средства безопасности и виртуальные машины; использует целый ряд методов для распознавания изолированных сред (sandbox) – в этом случае он намеренно запутывает исследователей, занимая все ресурсы ЦП, или сообщает владельцу ботнета внешний IP-адрес исследовательской сети; наконец, он применяет полиморфизм на стороне сервера.

Кроме того, Simda деактивирует себя через короткое время. Это тесно связано с задачей этого конкретного ботнета: он является инструментом доставки, и разработан для распространения потенциально нежелательного и вредоносного ПО. Распространители хотят гарантировать своему клиенту, что на зараженные машины будет устанавливаться только его вредоносное ПО.

На сегодняшний день продукты «Лаборатории Касперского» детектируют сотни тысяч модификаций Simda, а также многочисленные вредоносные программы сторонних разработчиков, распространяемые при помощи ботнета Simda. При помощи нашего бесплатного IP-сканера вы можете проверить, не было ли в прошлом с вашего IP-адреса соединений с командным сервером Simda.

Фишинг, но не такой, к которому мы привыкли

В начале 2014 года Ван Джинг (Wang Jing), студент-докторант Наньянского технологического университета в Сингапуре, выявил серьезную уязвимость в протоколах OAuth и OpenID. Выявленная им уязвимость, которую он назвал 'Covert Redirect' («скрытая переадресация»), позволяет атакующей стороне украсть данные пользователя при аутентификации (краткое изложение проблемы доступно на Threatpost, там же есть ссылка на блог Ван Джинга).

А недавно мы обнаружили фишинговую кампанию, эксплуатирующую данную уязвимость в протоколе OAuth. Протокол OAuth позволяет пользователям онлайн-сервисов предоставлять третьей стороне ограниченный доступ к своим защищенным ресурсам без предоставления ей своих логина и пароля. Это часто используется в веб-приложениях для социальных сетей – например, чтобы получить доступ к списку контактов пользователя или другим данным. Пользователь продукта «Лаборатории Касперского», сообщивший об атаке, получил письмо, в котором его информировали, что кто-то воспользовался его учетными данными Windows Live, и просили перейти на сайт Windows Live и пройти там определенную процедуру безопасности.

Все это выглядит как типичный фишинг – по идее, жертву должны переадресовать на поддельную страницу сайта. Но в данном случае ссылка из мошеннического письма вела на легитимный сайт Windows Live; учетные данные не крадутся, и пользователь действительно авторизуется на легитимном сайте. Однако после авторизации пользователь получает запрос на предоставление целого ряда прав неизвестному приложению, в том числе на автоматический вход, доступ к данным профиля, списку контактов и адресам электронной почты. Если пользователь соглашается, он предоставляет киберпреступникам доступ к своей личной информации; эту информацию злоумышленники могут использовать для рассылки спама и фишинговых ссылок или для других мошеннических целей.

Наши рекомендации для защиты ваших личных данных:

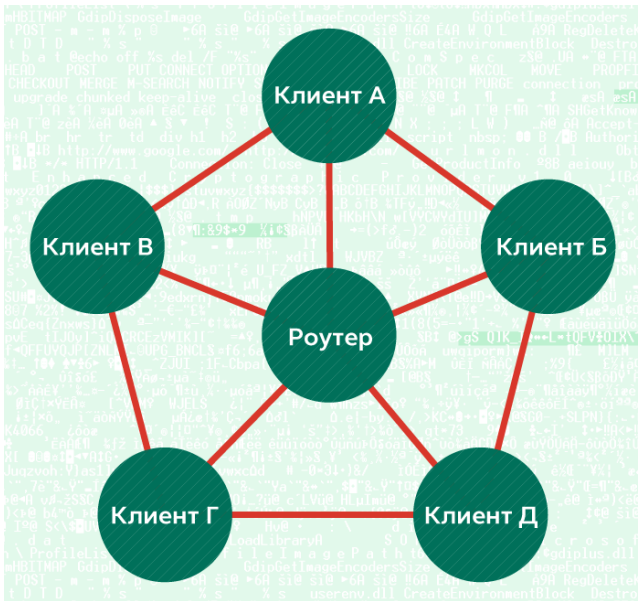
- Не переходите по ссылкам, полученным по почте или в личных сообщениях в социальных сетях.
- Не давайте права на доступ к вашим личным данным неизвестным приложениям.
- Прежде чем дать согласие на такой запрос, внимательно прочтите описание прав на доступ к аккаунту, которые запрашивает приложение.
- Почитайте в интернете обзоры приложения и отзывы пользователей.
- Проверьте права приложений, установленных на данный момент, в случае необходимости измените настройки.

«Умные» города, но не слишком умная безопасность

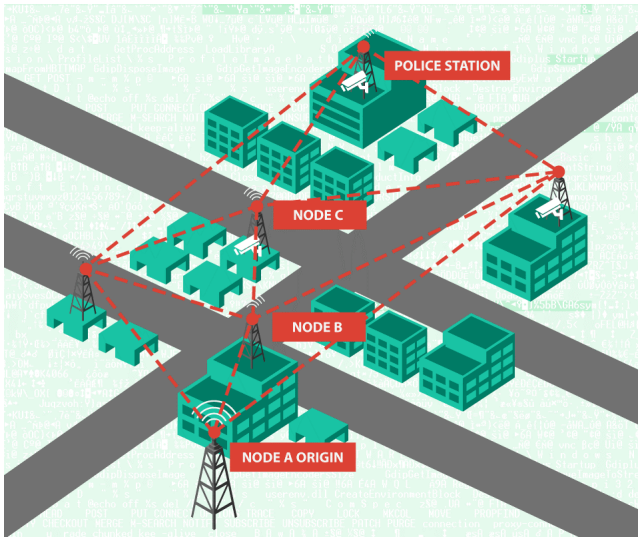
В последние годы государства и правоохранительные органы значительно расширили использование систем видеонаблюдения для наблюдения в общественных местах. Большинство из нас воспринимает это как разумный компромисс между неприкосновенностью частной жизни и безопасностью. Однако при этом мы предполагаем, что с данными, полученными при видеонаблюдении, будут обращаться ответственно и безопасным образом, чтобы наблюдение не принесло больше вреда, чем пользы.

Многие камеры видеонаблюдения подключаются к интернету по беспроводным каналам, благодаря чему полиция может следить за ними удалённо. Однако такая практика не обязательно является безопасной: киберпреступники могут незаметно отслеживать потоки данных с камер, внедрять код в сети, заменяя данные с камеры поддельными, а также отключать системы. Два эксперта по системам безопасности (Василиос Хиуреас (Vasilios Hioureas) из «Лаборатории Касперского» и Томас Кинзи (Tomas Kinsey) из компании Exigent Systems) недавно провели исследование потенциальных слабых мест в системах видеонаблюдения в одном городе. Отчёт Василиоса доступен на нашем сайте.

Исследователи начали с того, что ездили по городу и смотрели, как установлено оборудование видеослежения. Обнаружилось, что обозначения производителей на камерах никак не скрыты от посторонних глаз, так что легко можно было различить название и модель оборудования, изучить технические параметры и создать в лаборатории собственную масштабную модель. Используемое оборудование было оснащено эффективными средствами безопасности, но они не использовались. Передаваемые по ячеистой сети пакеты данных не шифровались, так что атакующая сторона могла создать свою собственную версию используемого ПО и получить возможность использовать пересылаемые данные.



Важно отметить, что исследователи не предпринимали попыток проникнуть в существующую сеть, а изучили оборудование и протоколы передачи данных и создали масштабную модель. Сети, по которым передаются данные с камер видеонаблюдения, имеют иную топологию, чем стандартная домашняя беспроводная сеть. в домашней сети все устройства сообщаются с интернетом и друг с другом через маршрутизатор. Любое устройство, подключенное к маршрутизатору, может выдавать себя за маршрутизатор перед другими устройствами, и отслеживать или менять данные, проведя атаку типа man-in-the-middle.



Сеть камер наблюдения более сложная; это связано с тем, что данные пересылаются на большие расстояния.

Данные с каждой конкретной камеры должны пройти через серию узлов и в конечном итоге вернуться на хаб (в данном случае это может быть полицейский участок). Трафик идет по линии наименьшего сопротивления: у каждого узла есть связь с несколькими другими узлами, так что выбирается самый простой путь к хабу.

Хиуреас и Кинзи создали серию фальшивых узлов, которые транслировали в сеть, что у них есть прямая связь с полицейским участком. Поскольку исследователи знали все используемые в сети протоколы, они сумели создать узел, который выполнял функцию man-in-the-middle: он предлагал кратчайший путь к хабу, так что реальные узлы действительно начали передавать свой трафик через него.

Как могут воспользоваться данной информацией злоумышленники? Можно, например, подменять видеопотоки, передаваемые на полицейские участки. Таким образом можно заставить полицию поверить, что в каком-либо месте произошёл инцидент, и таким образом отвлечь ее силы от реального происшествия в другом месте.

Исследователи сообщили о выявленных проблемах соответствующим органам, отвечающим за системы видеобезопасности; проблемы в данный момент устраняются. в целом же важно, чтобы в этих сетях было внедрено WPA-шифрование, защищенное надежными паролями; с оборудования следует удалять всю маркировку моделей и производителей, чтобы потенциальным злоумышленникам было не так просто выяснить, как работает оборудование; наконец, следует применять шифрование видеоданных, пересылаемых по сети.

Если же посмотреть шире, то проблема заключается в том, что всё больше аспектов нашей каждодневной жизни приобретают «цифровое измерение». Если меры безопасности не планируются на этапе разработки, то это может привести к серьезным последствиям, и исправлять задним числом проблемы безопасности может оказаться не таким простым делом. Инициатива Securing Smart Cities, поддерживаемая «Лабораторией Касперского», направлена на то, чтобы помочь ответственным за разработку «умных» городов делать свою работу, не забывая о кибербезопасности.

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

Одной из главных мобильных угроз продолжают оставаться мобильные банкеры. в отчете за первый квартал 2015 года мы упоминали троянец Trojan-SMS. AndroidOS.OpFake.cc, который был способен атаковать как минимум 29 банковских и финансовых приложений. Самая последняя версия этого троянца способна атаковать уже 114 банковских и финансовых приложений. Его основная цель – украсть логин и пароль от аккаунта. с той же целью он атакует и несколько популярных почтовых приложений.

Отметим также Trojan-Spy.AndroidOS.SmsThief.fc. Злоумышленники добавили свой код в оригинальное банковское приложение, не нарушив его работоспособность, благодаря чему этого троянца было сложнее обнаружить.

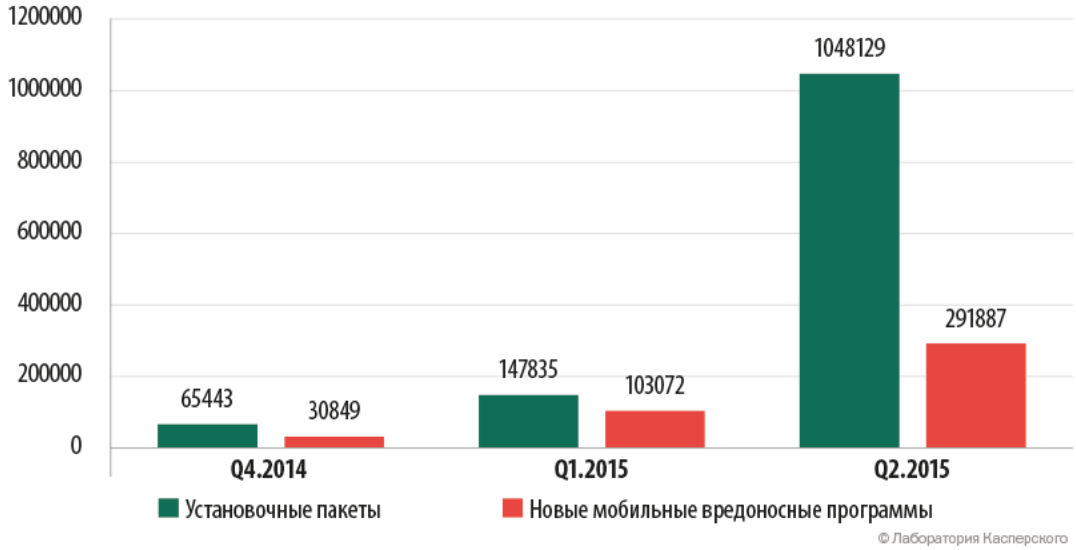
Во втором квартале появился новый троянец под iOS – Trojan.IphoneOS.FakeTimer.a. Он интересен тем, что существует его Android версия, которая появилась несколько лет назад. FakeTimer.a. атакует даже устройства, не подвергшиеся процедуре джейлбрейкинга. Его функционал достаточно примитивен: это обычное фишинговое приложение, созданное для того, чтобы красть деньги у пользователей из Японии.

В этом квартале были особенно заметны троянцы, которые могу использовать права root для показа рекламы пользователям или установки рекламных приложений. По итогам квартала в TOP 20 вредоносных мобильных программ попали шесть таких зловредов.

Количество новых мобильных угроз

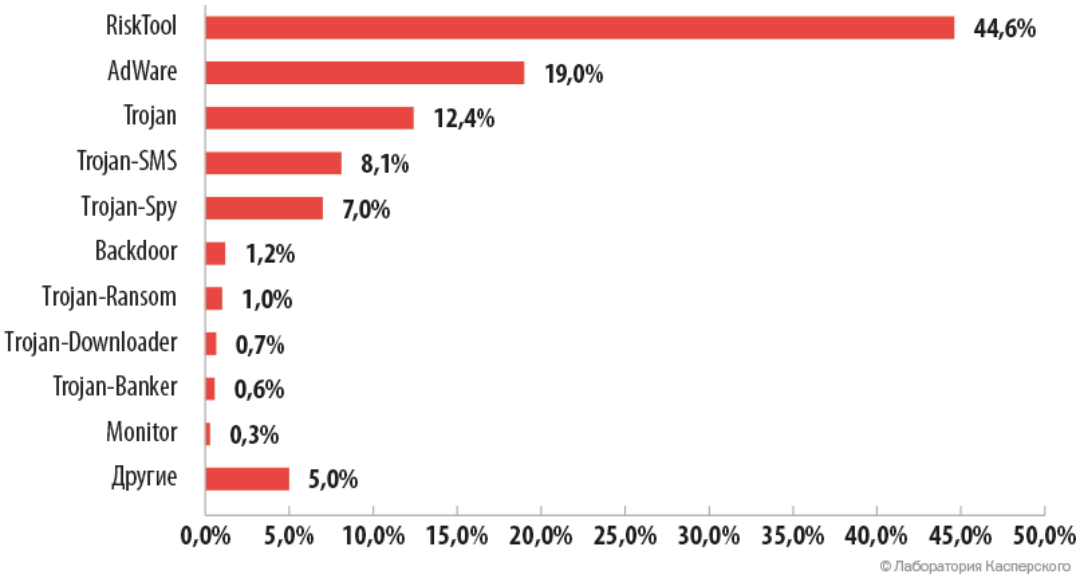
Во втором квартале 2015 года «Лабораторией Касперского» было обнаружено **291 887** новых мобильных вредоносных программ – в 2,8 раза больше, чем в первом квартале 2015 года.

При этом количество обнаруженных вредоносных установочных пакетов составило 1 048 129 – это в 7 раз больше, чем в предыдущем квартале.



Количество обнаруженных вредоносных установочных пакетов и новых мобильных угроз (Q4 2014 – Q2 2015)

Распределение детектируемых мобильных программ по типам



Распределение новых детектируемых мобильных программ по типам, второй квартал 2015 года

В рейтинге обнаруженных во втором квартале 2015 года объектов для мобильных устройств лидируют RiskTool (44,6%). Это легальные приложения, которые потенциально опасны для пользователей – их использование злоумышленником или неаккуратное использование владельцем смартфона может привести к финансовым потерям.

На втором месте – потенциально нежелательные рекламные приложения (19%). SMS-троянцы, которые долгое время лидировали в этом рейтинге, во втором квартале оказались только на четвертом месте с показателем 8,1%. Это на 12,9% меньше, чем в первом квартале. Уменьшение доли таких зловредов отчасти обусловлено тем, что те, кто ранее активно распространял SMS-троянцев, либо стали использовать более чистые схемы монетизации (о чем свидетельствует

увеличение доли RiskTool), либо предпочли использовать зловреды других типов. Так, доля Trojan выросла с 9,8% в первом квартале до 12,4% во втором.

TOP 20 мобильных вредоносных программ

Отметим, что, начиная с этого квартала, мы публикуем рейтинг ***вредоносных*** программ, в него не входят потенциально опасные или нежелательные программы, такие как RiskTool и рекламные программы.

	Название	Процент атак*
1	DangerousObject.Multi.Generic	17,5%
2	Trojan-SMS.AndroidOS.Podec.a	9,7%
3	Trojan-SMS.AndroidOS.Opfake.a	8,0%
4	Backdoor.AndroidOS.Obad.f	7,3%
5	Trojan-Downloader.AndroidOS.Leech.a	7,2%
6	Exploit.AndroidOS.Lotoor.be	5,7%
7	Trojan-Spy.AndroidOS.Agent.el	5,5%
8	Trojan.AndroidOS.Ztorg.a	3,1%
9	Trojan.AndroidOS.Rootnik.a	3,0%
10	Trojan-Dropper.AndroidOS.Gorpo.a	2,9%
11	Trojan.AndroidOS.Fadeb.a	2,7%
12	Trojan-SMS.AndroidOS.Gudex.e	2,5%
13	Trojan-SMS.AndroidOS.Stealer.a	2,5%
14	Exploit.AndroidOS.Lotoor.a	2,1%
15	Trojan-SMS.AndroidOS.Opfake.bo	1,6%
16	Trojan.AndroidOS.Ztorg.b	1,6%
17	Trojan.AndroidOS.Mobtes.b	1,6%
18	Trojan-SMS.AndroidOS.FakeInst.fz	1,6%
19	Trojan.AndroidOS.Ztorg.pac	1,5%
20	Trojan-SMS.AndroidOS.FakeInst.hb	1,4%

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

На 1-м месте в рейтинге – DangerousObject.Multi.Generic (17,5%). Так новые вредоносные приложения детектируются облачными технологиями Kaspersky Security Network, которые позволяют нашим продуктам быстро реагировать на новые и неизвестные угрозы.

Trojan-SMS.AndroidOS.Podec.a (9,7%) входит в TOP 3 вредоносных мобильных угроз уже три квартала подряд, что обусловлено его активным распространением. Trojan-SMS.AndroidOS.Opfake.a (8,0%) быстро поднимается на верхние строчки рейтинга. Если в третьем квартале 2014 года он находился на 11-м месте, то сейчас

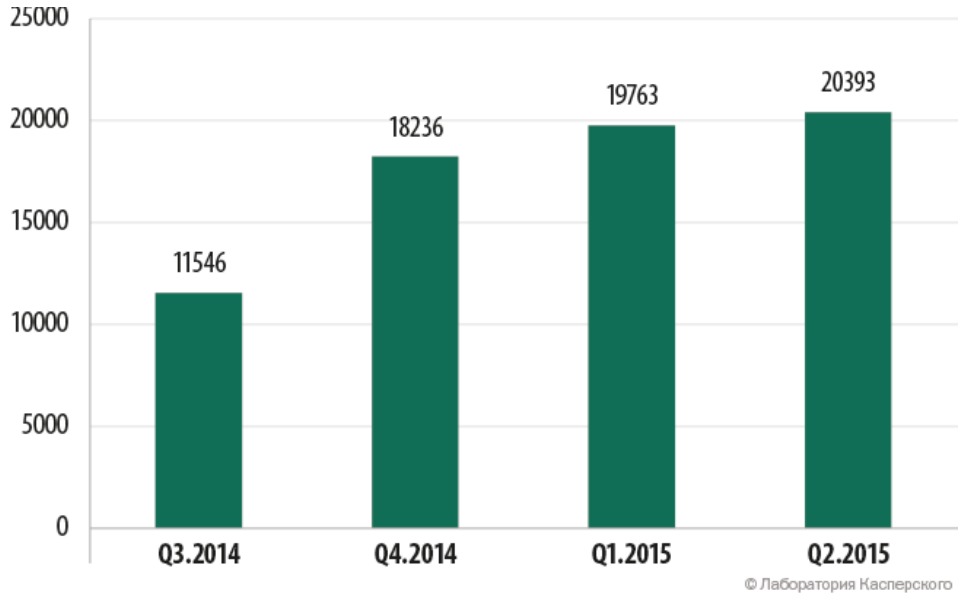
он входит в TOP 3 мобильных угроз за второй квартал 2015 года. На 15-м месте еще один представитель этого семейства – Obfake.bo.

Также отметим появление.Backdoor.AndroidOS.Obad в TOP 20, причем сразу на 4-м месте. Это многофункциональный троянец, который может отправлять SMS на премиум-номера, загружать и устанавливать на зараженное устройство другие вредоносные программы и/или рассылать их по Bluetooth; выполнять удаленные команды в консоли. Мы писали о нем еще два года назад, и с тех пор его функционал практически не менялся.

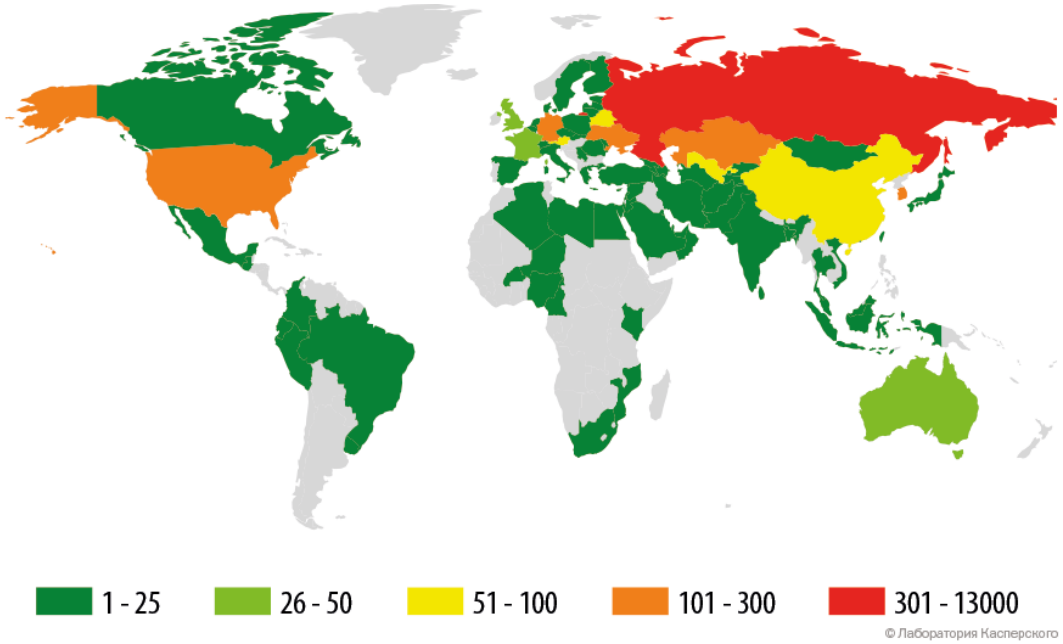
Еще один интересный момент – хотя в этот рейтинг не входят рекламные программы, 6 из 20 программ в топе используют рекламу в качестве основного средства монетизации. Trojan.AndroidOS.Rootnik.a, три программы семейства Trojan.AndroidOS.Ztorg, Trojan-Downloader.AndroidOS.Leech.a и Trojan.AndroidOS.Fadeb.a в отличие от обычных рекламных модулей не несут никакого полезного функционала. Их цель – доставить до пользователя как можно больше рекламы различными способами, в том числе за счет установки новых рекламных программ. Эти троянцы могут воспользоваться правами root для того, чтобы скрыться в системной папке, откуда в таком случае удалить их будет очень сложно.

Мобильные банковские троянцы

За отчетный период мы обнаружили 630 мобильных банковских троянцев. Отметим, что рост количества новых программ этой категории значительно замедлился.



Количество мобильных банковских троянцев в коллекции «Лаборатории Касперского» (Q3 2014 – Q2 2015)



География мобильных банковских угроз во втором 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	Республика Корея	2,37%
2	Россия	0,87%
3	Узбекистан	0,36%
4	Белоруссия	0,30%
5	Украина	0,29%
6	Китай	0,25%
7	Казахстан	0,17%
8	Австралия	0,14%
9	Швеция	0,13%
10	Австрия	0,12%

* 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.

Наиболее активно мобильные банкеры распространяются в Корее. Злоумышленники традиционно активны также в России и других странах постсоветского пространства. Именно эти страны заняли четыре из пяти первых строчек рейтинга.

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:

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

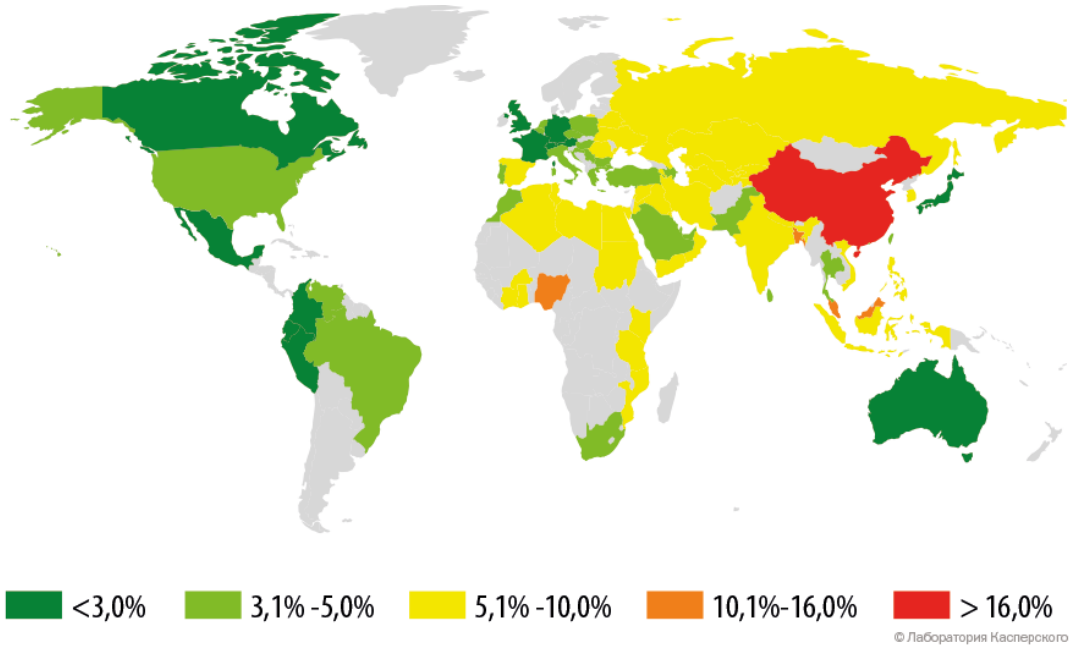
	Страна	% пользователей, атакованных банкерами, от всех атакованных пользователей
1	Республика Корея	31,72%
2	Россия	10,35%
3	Австралия	6,62%
4	Австрия	6,03%
5	Япония	4,73%
6	Узбекистан	4,17%
7	Белоруссия	3,72%
8	Эквадор	3,50%
9	Украина	3,46%
10	Швейцария	3,09%

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

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

В Корее почти треть всех пользователей, атакованных мобильными зловредами, были атакованы в том числе мобильными банкерами. в России атакам мобильных банкеров подвергся каждый десятый из атакованных пользователей. в остальных странах этот показатель меньше. Интересно, что из 5 самых безопасных стран по вероятности заражения мобильными зловредами (см. ниже), 4 попали в этот TOP. Это Австралия, Австрия, Япония и Швейцария.

География мобильных угроз



Карта попыток заражений мобильными зловредами во втором квартале 2015 года (процент атакованных пользователей в стране)

TOP 10 стран, по проценту пользователей, атакованных мобильными зловредами:

	Страна*	% атакованных пользователей**
1	Китай	16,34
2	Малайзия	12,65
3	Нигерия	11,48
4	Бангладеш	10,89
5	Танзания	9,66
6	Алжир	9,33
7	Узбекистан	8,56
8	Россия	8,51
9	Украина	8,39
10	Белоруссия	8,05

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

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

Лидером этого рейтинга стал Китай, где атакам хотя бы раз в течение квартала подверглись 16,34% пользователей нашего продукта. На втором месте Малайзия с показателем 12,65%. Россия (8,51%), Украина (8,39%) и Белоруссия (8,05%) замыкают TOP 10, пропустив вперед страны Азии и Африки.

Корея в этом рейтинге заняла 11-е место с показателем 7,46%. Напомним, что Корее у злоумышленников очень популярны мобильные банковские троянцы: ими были атакованы 31,72% всех атакованных мобильными зловредами пользователей.

Самые безопасные страны по этому показателю:

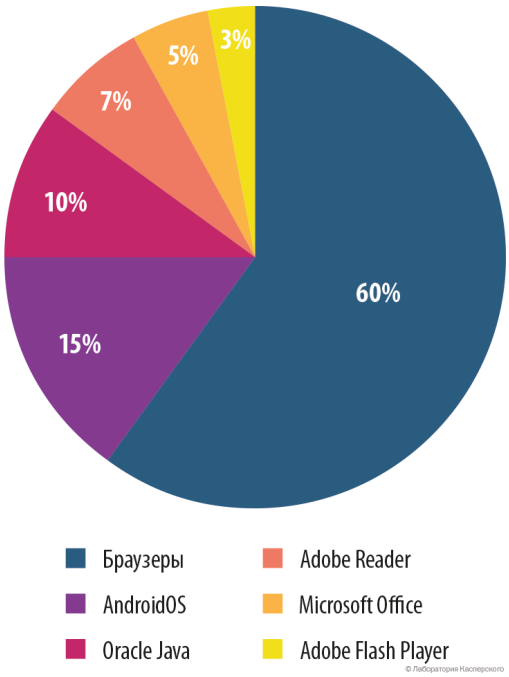
	Страна	% атакованных пользователей
1	Япония	1,06
2	Канада	1,82
3	Австрия	1,96
4	Австралия	2,16
5	Швейцария	2,19

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.

Расстановка сил эксплойтов практически не изменилась по сравнению с первым кварталом. По-прежнему лидерами рейтинга являются эксплойты для браузеров (60%). На данный момент большинство эксплойт-паков содержат связку эксплойтов для Adobe Flash Player и Internet Explorer. Отметим значительный рост числа эксплойтов для Adobe Reader (+6 п.п.). Это связано с большим количеством спам-рассылок, содержащих вредоносные PDF-документы.

Традиционно отметим уменьшение доли Java-эксплойтов (-4 п.п.). Во втором квартале мы практически не встречали новых Java-эксплойтов.



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

Во втором квартале было отмечено использование новых уязвимостей в Adobe Flash Player:

- CVE-2015-3113
- CVE-2015-3104
- CVE-2015-3105
- CVE-2015-3090

Хотя доля эксплойтов к Adobe Flash Player в нашем рейтинге составляет всего 3%, «в дикой природе» их больше. При рассмотрении данной статистики необходимо учитывать, что технологии «Лаборатории Касперского» детектируют эксплойты на различных этапах. в категорию «браузеры» попадают также детектирования лэндинг-страниц, которые «раздают» эксплойты. По нашим наблюдениям, чаще всего это эксплойты к Adobe Flash Player.

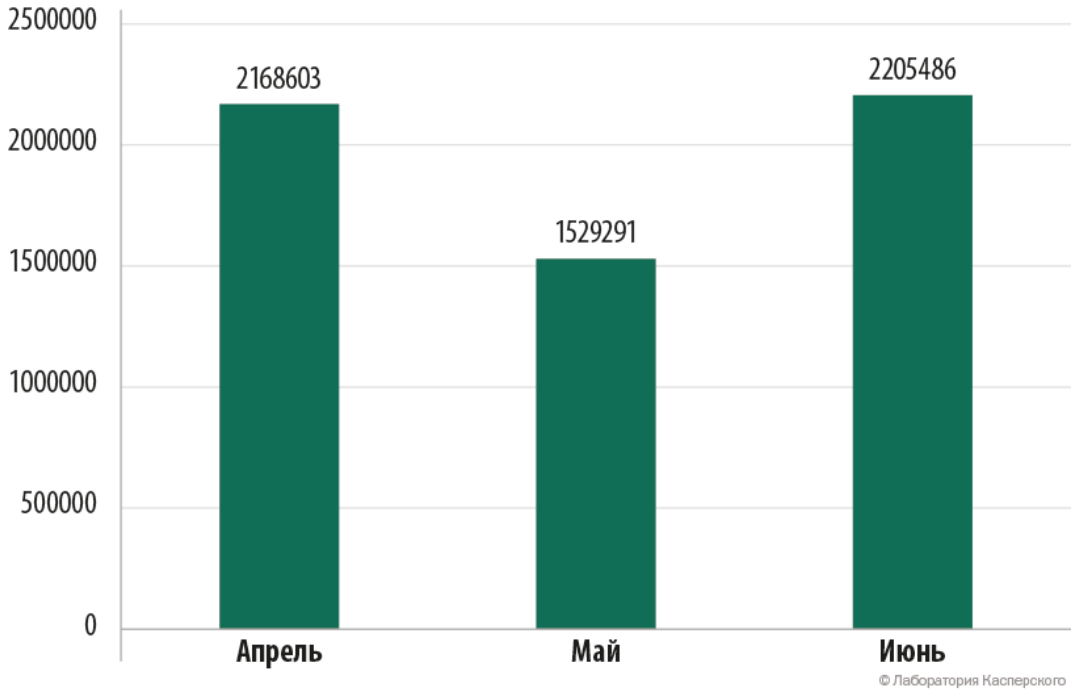
Вредоносные программы в интернете (атаки через Web)

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 банковском секторе

Во втором квартале 2015 года решения «Лаборатории Касперского» отразили попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на **755 642** компьютерах пользователей. По сравнению с предыдущим кварталом (929 082) данный показатель снизился на 18,7%. Во втором квартале 2014 года он составлял 735 428 компьютеров пользователей.

Всего защитными продуктами «Лаборатории Касперского» было зарегистрировано **5 903 377** уведомлений о попытках заражения вредоносными программами, предназначенными для кражи денежных средств через онлайн-доступ к банковским счетам.

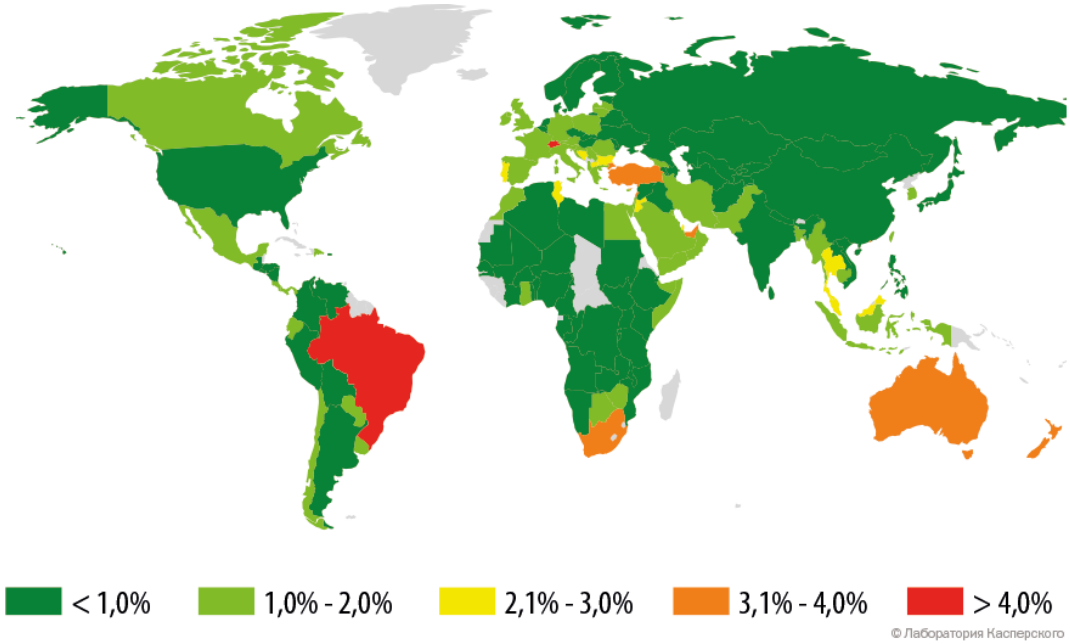


Число атак на пользователей со стороны финансового вредоносного ПО, второй квартал 2015 года

География атак

Во втором квартале 2015 года мы поменяли методику составления рейтинга стран по вредоносной активности банковских троянцев. в предыдущих отчетах мы составляли рейтинг по количеству атакованных пользователей. Это важный показатель, однако он зависит от количества пользователей продуктов «Лаборатории Касперского» в странах.

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.



География атак банковского вредоносного ПО во втором квартале 2015 года (процент атакованных пользователей)

TOP-10 стран по проценту атакованных пользователей

	Страна*	% атакованных пользователей**
1	Сингапур	5,28
2	Швейцария	4,16
3	Бразилия	4,07
4	Австралия	3,95
5	Гонконг	3,66
6	Турция	3,64
7	Новая Зеландия	3,28
8	Южная Африка	3,13
9	Ливан	3,10
10	ОАЭ	3,04

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

** Процент уникальных пользователей ЛК, подвергшихся атакам банковских троянцев, от всех уникальных пользователей продуктов «Лаборатории Касперского» в стране.

Во втором квартале 2015 года лидером по проценту пользователей «Лаборатории Касперского», атакованных банковскими троянцами, стал Сингапур. Отметим, что большинство стран из TOP 10 имеют высокий уровень технологического развития и/или развитую банковскую систему, что и привлекает к ним внимание киберпреступников.

В России с банковскими троянцами хотя бы раз в течение квартала столкнулись 0,75% пользователей, в США – 0,89%, в Испании – 2,02%, в Великобритании – 1,58%, в Италии – 1,57%, в Германии – 1,16%.

TOP 10 семейств банковского вредоносного ПО

TOP 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга во втором квартале 2015 года (по количеству атакованных пользователей):

	Название	Количество нотификаций	Количество атакованных пользователей
1	Trojan-Downloader.Win32.Upatre	3888061	419940
2	Trojan-Spy.Win32.Zbot	889737	177665
3	Trojan-Banker.Win32.ChePro	264534	68467
4	Backdoor.Win32.Caphaw	72128	25923
5	Trojan-Banker.Win32.Banbra	56755	24964
6	Trojan.Win32.Tinba	175729	22942
7	Trojan-Banker.AndroidOS.Marcher	60819	19782
8	Trojan-Banker.AndroidOS.Faketoken	43848	13446
9	Trojan-Banker.Win32.Banker	23225	9209
10	Trojan-Banker.Win32.Agent	28658	8713

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

Состав первой тройки банковских зловредов не изменился по сравнению с предыдущим кварталом. Trojan-Downloader.Win32.Upatre по-прежнему лидирует в рейтинге. Зловреды этого семейства довольно просты, не больше 3,5 Кб, и обычно скачивают троянцев-банкеров семейства, известного как Dyre/Dyzap/Dyreza. Список атакуемых этим банкером финансовых учреждений зависит от файла конфигурации, который подкачивается с сервера командного центра.

Во втором квартале 2015 года в рейтинг попали новые банковские троянцы: Backdoor.Win32.Caphaw, Trojan-Banker.AndroidOS.Marcher и Trojan-Banker.AndroidOS.Faketoken.

Backdoor.Win32.Caphaw был впервые обнаружен в 2011 году и использует технику Man-in-the-Browser для кражи платежных данных клиента онлайн-банкинга.

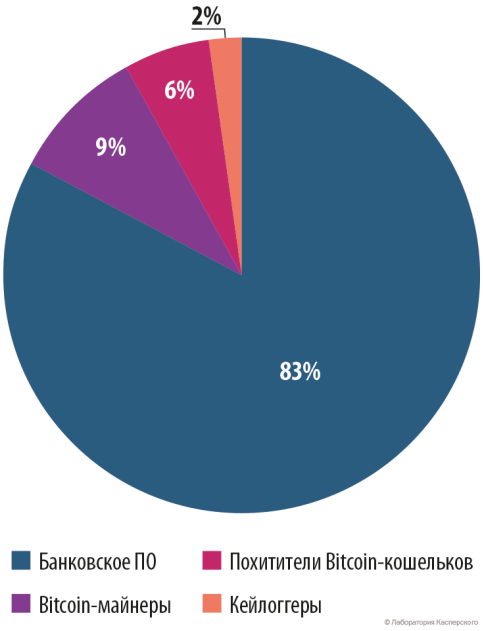
Trojan-Banker.AndroidOS.Faketoken и Trojan-Banker.AndroidOS.Marcher атакуют мобильные устройства на базе операционной системы Android.

Faketoken работает в паре с компьютерными банковскими троянцами. Для его распространения киберпреступники используют технологии социальной инженерии. Когда клиент банка с зараженного компьютера посещает страницу онлайн-банкинга, троянец модифицирует эту страницу, предлагая загрузить Android-приложение, которое якобы будет защищать транзакции. На самом деле ссылка ведет на приложение Faketoken. После того как Faketoken оказывается на смартфоне жертвы, преступники через зараженный банковским троянцем компьютер пользователя получают доступ к банковскому счету, а зараженное мобильное устройство позволяет им перехватывать одноразовый пароль двухфакторной аутентификации (mTAN). Второй мобильный банковский троянец – Trojan-Banker.AndroidOS.Marcher. Заразив мобильное устройство, он отслеживает запуск всего двух приложений: клиента мобильного банкинга одного из европейских банков и Google Play. в случае, если пользователь входит в магазин Google Play, Marcher демонстрирует пользователю фальшивое окно Google Play для ввода данных о платежной карте, которые попадают к злоумышленникам. Аналогичным образом троянец действует и в случае открытия пользователем банковского приложения.

Финансовые угрозы

Финансовые угрозы – это не только банковское вредоносное ПО, которое атакует клиентов систем онлайн-банкинга.

По сравнению с предыдущим кварталом увеличилась доля банковскго вредоносного ПО – с 71% до 83%. Второй по популярности финансовой угрозой во втором квартале стали Bitcoin-майнеры – вредоносное программное обеспечение, которое использует вычислительные ресурсы компьютера жертвы для генерации биткойнов. В предыдущем квартале эта категория зловредов была на третьем месте. Отметим, что некоторые разработчики легитимного программного обеспечения скрытым образом устанавливают Bitcoin-майнеры в свои приложения.



Количество атак со стороны финансового вредоносного ПО, второй квартал 2015 года

TOP 20 детектируемых объектов в интернете

Во втором квартале 2015 года нашим веб-антивирусом было обнаружено 26 084 253 уникальных объекта (скрипты, эксплойты, исполняемые файлы и т.д.).

Из всех вредоносных и потенциально нежелательных объектов мы выделили 20 наиболее активных – на них пришлось 96,5% всех атак в интернете.

TOP 20 детектируемых объектов в интернете

	Название*	% от всех атак**
1	AdWare.JS.Agent.bg	47,66%
2	Malicious URL	32,11%
3	Trojan.Script.Generic	4,34%
4	AdWare.Script.Generic	4,12%
5	Trojan.Script.Iframer	3,99%
6	AdWare.JS.Agent.bt	0,74%
7	Exploit.Script.Blocker	0,56%
8	Trojan.Win32.Generic	0,49%
9	AdWare.AndroidOS.Xynyin.a	0,49%
10	Trojan-Downloader.Win32.Generic	0,37%
11	Trojan-Ransom.JS.Blocker.a	0,34%
12	Trojan-Clicker.JS.Agent.pq	0,23%
13	AdWare.JS.Agent.an	0,20%
14	AdWare.JS.Agent.by	0,19%
15	Trojan.Win32.Invader	0,12%
16	Trojan-Downloader.Win32.Genome.qhcr	0,11%
17	AdWare.Win32.Amonetize.ague	0,11%
18	AdWare.Win32.MultiPlug.nnnn	0,10%
19	AdWare.NSIS.Agent.cv	0,09%
20	Trojan-Downloader.Script.Generic	0,09%

* 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. Агрессивное распространение рекламных программ в очередной раз получило отражение в этом рейтинге: десять из двадцати позиций занимают объекты, относящиеся к рекламным программам, а первое место занял скрипт AdWare.JS.Agent.bg, который внедряется рекламными программами в произвольные

веб-страницы. Последний вытеснил даже Malicious URL – вердикт для ссылок из черного списка, который занял второе место по итогам квартала.

Также интересно отметить появление вердикта AdWare.AndroidOS.Xynyin.a с нетипичной для данного рейтинга платформой. Соответствующая этому вердикту программа представляет собой рекламный модуль для Android, встраиваемый в различные приложения (например, в программы, «ускоряющие» работу телефона). Одно из таких приложений было популярно в марте-апреле этого года, когда его активно загружали пользователи. Поскольку в Google Play подобные приложения не встречаются, желающие находили их в интернете и в основном загружали через компьютеры.

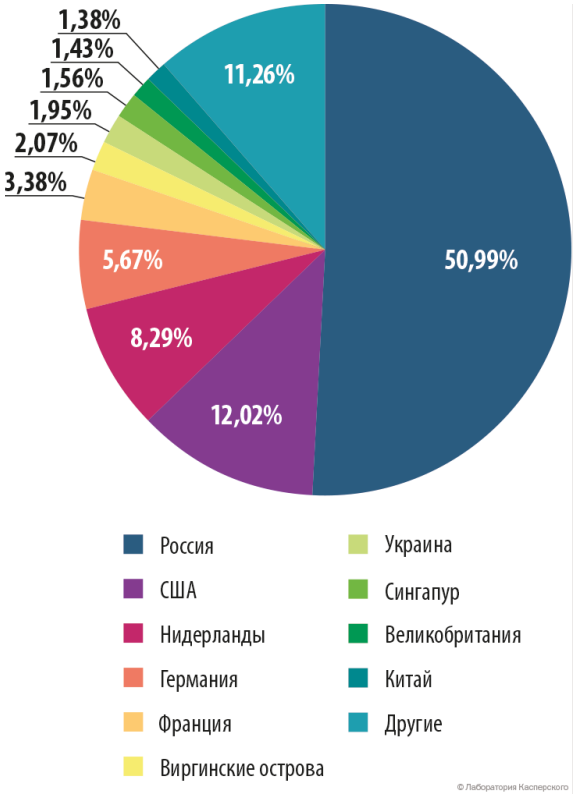
Вердикт Trojan-Ransom.JS.Blocker.a представляет собой скрипт, который с помощью циклического обновления страницы пытается блокировать браузер и выводит сообщение о необходимости оплаты «штрафа» на заданный электронный кошелек за просмотр неподобающих материалов. Встречается данный скрипт в основном на порносайтах.

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).

Во втором квартале 2015 года решения «Лаборатории Касперского» отразили 379 972 834 атаки, которые проводились с интернет-ресурсов, размещенных в разных странах мира. 89% уведомлений о заблокированных веб-атаках были получены при блокировании атак с веб-ресурсов, расположенных в десяти странах мира.



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

Лидер нашего рейтинга не изменился, им по-прежнему является Россия (51%), ее доля увеличилась на 11,27%. Из TOP 10 по сравнению с прошлым кварталом выбыла Швейцария. На восьмом месте с показателем 1,56% оказался Сингапур.

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.

	Страна*	% уникальных пользователей**
1	Россия	38,98%
2	Казахстан	37,70%
3	Украина	35,75%
4	Сирия	34,36%
5	Белоруссия	33,02%
6	Азербайджан	32,16%
7	Таиланд	31,56%
8	Грузия	31,44%
9	Молдавия	31,09%
10	Вьетнам	30,83%
11	Армения	30,19%
12	Киргизия	29,32%
13	Хорватия	29,16%
14	Алжир	28,85%
15	Катар	28,47%
16	Китай	27,70%
17	Монголия	27,27%
18	Македония	26,67%
19	Босния и Герцеговина	25,86%
20	Греция	25,78%

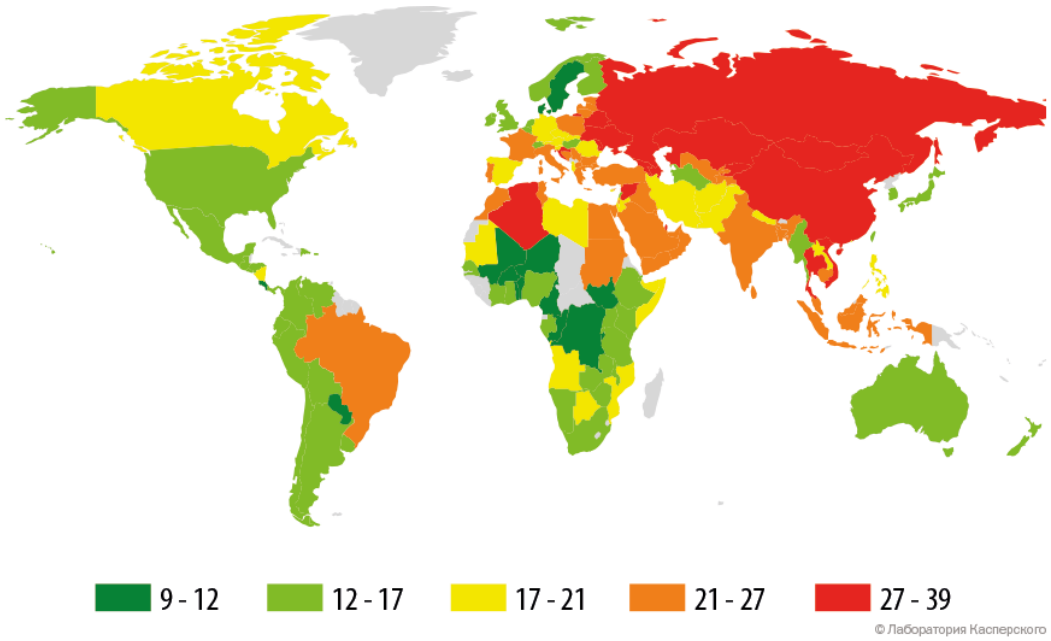
Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов «Лаборатории Касперского», подтвердившими свое согласие на передачу статистических данных.

* 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.

Во втором квартале 2015 года на первую строчку рейтинга вернулась Россия, которая в прошлом квартале оказалась на втором месте. По сравнению с первым кварталом из TOP 20 выбыли ОАЭ, Латвия, Таджикистан, Тунис и Болгария. Новички рейтинга – Сирия, поднявшаяся сразу на четвертое место (34,36%), Таиланд на седьмом месте (31,56%), Вьетнам на десятом месте (30,83%), Китай (27,70%) и Македония (26,67%) – на 16-м и 18-м местах соответственно.

В числе самых безопасных при серфинге в интернете стран – Аргентина (13,2%), Нидерланды (12,5%), Корея (12,4%), Швеция (11,8%), Парагвай (10,2%), Дания (10,1%).



В среднем в течение квартала 23,9% компьютеров пользователей интернета в мире хотя бы раз подвергались веб-атаке.

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.

Во втором квартале 2015 года нашим файловым антивирусом было зафиксировано 110 731 713 уникальных вредоносных и потенциально нежелательных объектов.

Детектируемые объекты, обнаруженные на компьютерах пользователей: TOP 20

	Название*	% атакованных уникальных пользователей**
1	DangerousObject.Multi.Generic	22,64%
2	Trojan.Win32.Generic	15,05%
3	Trojan.WinLNK.StartPage.gena	8,28%
4	AdWare.Script.Generic	7,41%
5	Adware.NSIS.ConvertAd.heur	5,57%
6	WebToolbar.Win32.Agent.azm	4,48%
7	WebToolbar.JS.Condonit.a	4,42%
8	Trojan-Downloader.Win32.Generic	3,65%
9	Downloader.Win32.MediaGet.elo	3,39%
10	Trojan.Win32.AutoRun.gen	3,29%
11	Downloader.Win32.Agent.bxib	3,26%
12	WebToolbar.JS.CroRi.b	3,09%
13	RiskTool.Win32.BackupMyPC.a	3,07%
14	Virus.Win32.Sality.gen	2,86%
15	Worm.VBS.Dinihou.r	2,84%
16	WebToolbar.Win32.MyWebSearch.si	2,83%
17	DangerousPattern.Multi.Generic	2,75%
18	AdWare.NSIS.Zaitu.heur	2,70%
19	AdWare.BAT.Clicker.af	2,67%
20	AdWare.Win32.MultiPlug.heur	2,54%

* 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 (таким как AdWare.BAT.Clicker.af) 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 14-е место с показателем 2,86%, что на 0,32% 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.

TOP 20 стран по уровню зараженности компьютеров

	Страна*	% уникальных пользователей**
1	Бангладеш	60,53%
2	Вьетнам	59,77%
3	Пакистан	58,79%
4	Монголия	58,59%
5	Грузия	57,86%
6	Сомали	57,22%
7	Непал	55,90%
8	Афганистан	55,62%
9	Алжир	55,44%
10	Армения	55,39%
11	Россия	54,94%
12	Лаос	54,77%
13	Ирак	54,64%
14	Казахстан	54,23%
15	Сирия	53,00%
16	Тунис	53,75%
17	Эфиопия	53,44%
18	Руанда	53,17%
19	Украина	53,01%
20	Камбоджа	52,88%

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.

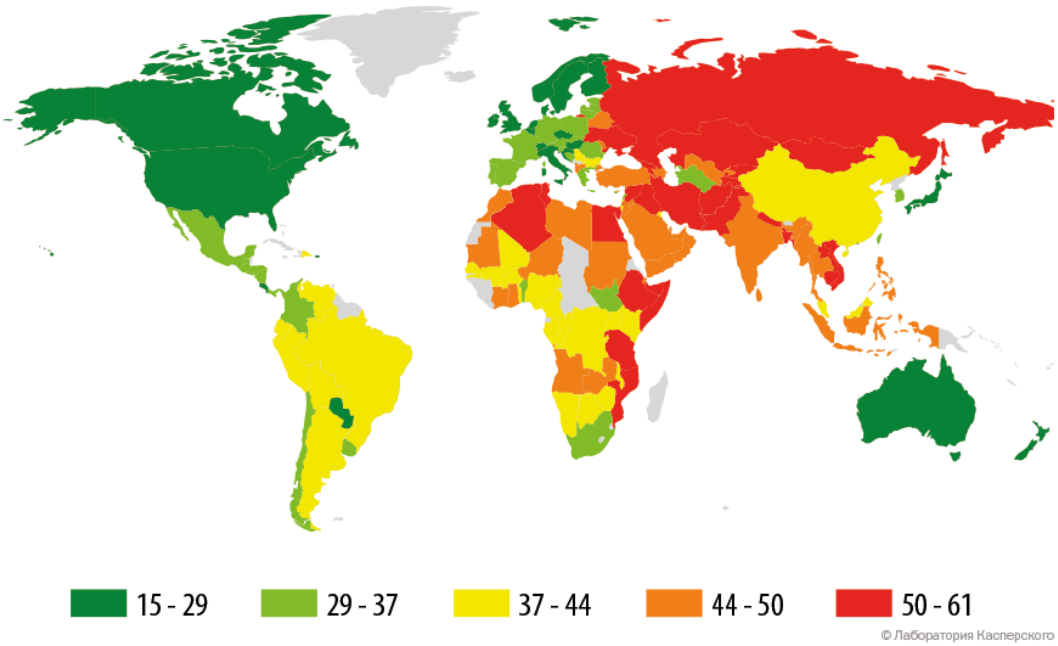
* При расчетах мы исключили страны, в которых число пользователей ЛК относительно мало (менее 10 000).

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

В этом квартале Бангладеш занимает первое место с показателем 60,53%, сместив на второе место Вьетнам, который лидировал на протяжении двух лет. Пакистан (58,79%) поднялся с тринадцатого места, которое он занимал в прошлом квартале, на третье.

Новички рейтинга – Грузия, оказавшаяся сразу на пятом месте (57,8%), Россия, которая по итогам второго квартала заняла одиннадцатое место (55%), Тунис на шестнадцатой строчке рейтинга (53,7%) и Украина на девятнадцатой (53%).

Страны, с наименьшим уровнем заражения – Швеция (19,7%), Дания (18,4%) и Япония (15,5%)



В среднем в мире хотя бы один раз в течение второго квартала локальные угрозы были зафиксированы на 40% компьютеров пользователей – это на 0,2% больше, чем в первом 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

KASPERSKY lab