РАЗВИТИЕ ИНФОРМАЦИОННЫХ УГРОЗ ВО ВТОРОМ КВАРТАЛЕ 2014 ГОДА

ДЭВИД ЭММ
ВИКТОР ЧЕБЫШЕВ
РОМАН УНУЧЕК
МАРИЯ ГАРНАЕВА
ДЕНИС МАКРУШИН

KASPERSKY lab

ОГЛАВЛЕНИЕ

ЦИФРЫ КВАРТАЛА

- По данным KSN, во втором квартале 2014 года продукты «Лаборатории Касперского» заблокировали 995 534 410 вредоносных атак на компьютерах и мобильных устройствах пользователей.
- Решения «Лаборатории Касперского» отразили 354 453 992 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.
- Нашим веб-антивирусом задетектировано 57 133 492 уникальных вредоносных объектов (скрипты, веб-страницы, эксплойты, исполняемые файлы и т.д.).
- Зафиксировано 145 386 473 уникальных URL, на которых происходило срабатывание веб-антивируса.
- 44% веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США и Германии.
- Наши антивирусные решения обнаружили 528 799 591 вирусных атак на компьютеры пользователей. Всего в данных инцидентах было зафиксировано 114 984 065 уникальных вредоносных и потенциально нежелательных объектов.
- Во втором квартале 2014 года банковским вредоносным ПО были атакованы 927 568 компьютеров пользователей продуктов «Лаборатории Касперского».
- С атакованных компьютеров было получено 3 455 530 уведомлений о попытках заражения финансовыми зловредами.

ОБЗОР СИТУАЦИИ

ЦЕЛЕВЫЕ АТАКИ И ВРЕДОНОСНЫЕ КАМПАНИИ

«ВОДА НА ВОДОПОЕ ОТРАВЛЕНА»

В апреле мы сообщили о новой уязвимости нулевого дня в Flash Player, которая, как мы считаем, была использована в атаках типа watering-hole, проводившихся со взломанного сирийского сайта. Этот сайт (http://jpic.gov.sy), созданный в 2011 году по заказу Министерства юстиции Сирии, был предназначен для сбора жалоб граждан о нарушениях законности и правопорядка. По нашему мнению, конечной целью атаки были сирийские диссиденты, которые жаловались на государственные органы.

В середине апреля мы проанализировали два новые SWF-эксплойта (оба проактивно детектируются продуктами «Лаборатории Касперского»). Используемая ими уязвимость была на тот момент нам неизвестна. Позднее компания Adobe подтвердила, что это новая уязвимость нулевого дня (CVE-2014-0515). Уязвимым был компонент Pixel Bender (который на данный момент уже не поддерживается Adobe), применяемый при обработке изображений и видео. В то время как первый из двух эксплойтов вполне стандартен и позволяет заражать практически любые незащищенные компьютеры, второй работает только на машинах, на которых установлены расширения Adobe Flash Player 12 ActiveX и Cisco MeetingPlace Express. Авторы эксплойта рассчитывали на то, что разработчики не найдут уязвимость в данном компоненте, что позволило бы продлить период активности эксплойта. Это свидетельствует о том, что при планировании атак злоумышленники не рассчитывали на массового пользователя.

Вероятнее всего, жертвы перенаправлялись на ресурсы с эксплойтами с помощью плавающих фреймов или скриптов на взломанных сайтах. После публикации нашего постинга об этом эксплойте нулевого дня он был более 30 раз обнаружен на компьютерах семи разных людей, причем все они находились в Сирии.

По нашему мнению, эта атака была тщательно спланирована высокопрофессиональными киберпреступниками, о чем говорит, в частности, применение профессионально написанных эксплойтов нулевого дня для взлома одного конкретного ресурса.

Техническую информацию об эксплойтах можно найти здесь.

ИТАЛЬЯНСКОЕ (И ТУРЕЦКОЕ) ДЕЛО

В июне мы писали о своем расследовании атаки на клиентов крупного европейского банка, в ходе которой злоумышленникам удалось всего за неделю украсть более полумиллиона евро.

Мы столкнулись с первыми признаками вредоносной кампании в январе 2014 года, когда обнаружили подозрительный сервер, содержащий журналы мошеннических финансовых операций. Журналы содержали, в частности, подробные сведения о жертвах и украденных суммах. В ходе дальнейшего анализа была получена дополнительная информация. В частности, удалось идентифицировать банк, против клиентов которого была направлена атака, разобраться в особенностях системы дропов (денежных мулов) и подробностях организации атаки, а также обнаружить код на JavaScript, связанный с инфраструктурой командного сервера. Стало понятно, что это серверная часть инфраструктуры, обслуживающей банковские троянские программы. Мы решили дать этому командному серверу имя luuuk по названию папки, в которой была размещена панель управления: /server/adm/luuuk/.

Вредоносная кампания проводилась против клиентов одного конкретного банка. Несмотря на то что нам не удалось получить вредоносный код, с помощью которого заражались компьютеры жертв, мы полагаем, что киберпреступники использовали банковскую троянскую программу, в которой был реализован метод кражи учетных данных пользователей с применением вредоносной веб-инъекции, известный как «Man-in-the-Browser». Информация, найденная в некоторых лог-файлах на сервере, свидетельствует о том, что вредоносная программа в режиме реального времени крала имена и пароли пользователей, а также одноразовые пароли, необходимые для проведения транзакций.

```
193.XX.X.98    15 10:35:35
step=end&transfer=52d656245b9cc9cab8a999XX&status=complete&sender=005XXXX79&log=
Master__1.1 not have error, first transfer
1.2 show fake
2.2 going to balance page 2.3 get balance list on balance 9404,IT47P0XXXXXXX01574T-
EUR2T476
2.4 balance check at minimum is ok
3.1 open transfer page 3.2 page open, click - new transfer 3.2 page open, go next step
4.1 enter transfer info page
4.2 is page with account select
4.3 found a good account, open it
4.3 and balance of account is 9404
4.4 account oppend
4.5 get drop
4.6 server response ready{"drop":{"description":"SALDO FATTURA N
157","iban":"IT0XXXXXXXXXXXX410","company":"XXX XXX","name":"XXX XXX"},
"balance":X.2,"amount":2755, "transfer":"52d656245b9cc9cab8a999XX","type":"boit"} 4.5
drop ready, enter info[object Object] 4.6 send transfer data 4.7 error 5.1 check errors
page 5.2 found otp framere place installed:{"amount":"2.755,00","rawAmount":"2755"}
6.1 OTP page 6.2 enter token 753684 6.3 click button 6.4 frame with result loaded
second timer startI=>convAviI=>confermaAttenzioneI=>success end6.5 transfer
complete&_=138978480XX
```

Подобные веб-инъекции часто применяются в разнообразных вариациях на тему Zeus (Citadel, SpyEye, IceIX и т. д.) В процессе расследования определить вектор заражения не представлялось возможным. Как известно, банковские троянцы используют для заражения жертв самые разные методы, в том числе рассылки спама и загрузку вредоносного ПО при посещении зараженных сайтов (drive-by загрузки). После публикации нашего постинга аналитики проекта Fox-IT InTELL прислали нам информацию, которая, возможно, связана с данной кампанией. Эти данные говорят о том, что сервер Luuuk, возможно, связан с вредоносной программой ZeusP2P (известной также как Murofet), о чем мы с самого начала подозревали. Однако окончательно доказать это не представляется возможным, поскольку в процессе анализа нам не удалось обнаружить на сервере внедряемый код.

Злоумышленники использовали краденые учетные данные для проверки баланса счета жертвы и автоматического проведения вредоносных транзакций. По всей видимости, вредоносное приложение работало в фоновом режиме одновременно с легитимной сессией онлайн-банкинга. Об этом свидетельствует, например, один из обнаруженных нами вредоносных объектов (VNC-сервер), связанных с вредоносным сервером и применявшихся злоумышленниками.

Краденые средства затем автоматически переводились на заранее подготовленные счета дропов (денежных мулов). Значительный интерес представляет разделение счетов, заранее подготовленных для дропов, на группы. Существовало четыре группы дропов: каждая из них определялась размером суммы, которую дропы, в нее входящие, могли получить на свой счет. По всей видимости, это деление отражает уровень доверия к дропам из каждой группы.

Всего мы выявили 190 жертв атаки, большинство которых находятся в Италии и Турции. Суммы, украденные у каждой из жертв, находились в пределах от 1700 до 39 000 евро – всего было украдено 500 000 евро.

Злоумышленники удалили все относящиеся к вредоносной деятельности компоненты 22 января – через два дня после начала нашего расследования. Те данные об осуществленных злоумышленниками транзакциях, которыми мы располагаем, позволяют нам считать, что это скорее обновление инфраструктуры, чем полное свертывание деятельности. Наш анализ вредоносной кампании показывает, что стоящие за ней киберпреступники высокопрофессиональны и очень активны. Кроме того, они, по-видимому, принимают превентивные меры для защиты своей деятельности, а будучи обнаруженными, меняют тактику и заметают следы.

После обнаружения командного сервера мы сообщили об этом подвергшемуся атаке банку и соответствующим правоохранительным органам. Мы продолжаем расследование атаки, работая в контакте с этими органами.

«ЛЕГАЛЬНОЕ» ШПИОНСКОЕ ПО: ТЕПЕРЬ И НА МОБИЛЬНЫХ УСТРОЙСТВАХ

В июне мы опубликовали результаты своего новейшего исследования, в рамках которого была проанализирована «легальная» шпионская программа Remote Control System (RCS), созданная итальянской компанией HackingTeam. С ПО, разработанным этой компанией, мы сталкиваемся уже не первый раз. Однако с момента публикации нашей предыдущей статьи об RCS произошли значительные события.

Во-первых, мы обнаружили характерный признак, по которому можно распознать командные серверы RCS. При отправке на сервер RCS специального запроса выдается следующее сообщение об ошибке:

```
> GET /con/trust/ HTTP/1.1
User-Agent: curl/7.22.0 (x86_64-pc-linux-gnu)
libcurl/7.22.0 OpenSSL/1.0.1 zlib/1.2.3.4 libidn/1.23
librtmp/2.3

Host: ***

Accept: */*

< HTTP/1.1 500 InternalServerError < Connection: close
< Content-Type: text/html < Content-length: 88 < *
Closing connection #0 undefined method
`prepare_response' for
#<RCS::Collector::CollectorController:0x38ac540
```

С помощью этого метода нам удалось просканировать все пространство IPv4, что позволило определить IP-адреса командных серверов RCS по всему миру. Всего было обнаружено 326 командных серверов, причем большинство из них находится в США, Казахстане и Эквадоре. Список командных серверов можно увидеть здесь. На основе информации WHOIS для некоторых IP-адресов было установлено, что они имеют отношение к государственным организациям. Конечно, мы не можем быть уверены в том, что серверы, расположенные в определенной стране, используются спецслужбами той же страны, однако это имеет свой резон: так проще избежать юридических проблем с другими странами и изъятия серверов.

Во-вторых, мы обнаружили несколько мобильных вредоносных модулей для Android, iOS, Windows Mobile и BlackBerry, созданных HackingTeam. Все эти модули управляются конфигурационными файлами, имеющими одинаковый формат, – это с хорошей долей вероятности указывает на то, что они имеют отношение друг к другу и принадлежат к одному семейству. Ввиду популярности iOS и Android мы, естественно, обращали на эти платформы основное внимание при анализе мобильных модулей.

Вредоносные модули устанавливаются с помощью модулей заражения – специальных исполняемых файлов для Windows или Mac OS, работающих на уже зараженных компьютерах. Модуль для iOS может использоваться только на устройствах, подвергшихся джейлбрейкингу. Это ограничивает возможности распространения, однако метод заражения, применяемый RCS, позволяет злоумышленнику запустить утилиту для джейлбрейкинга (например, Evasi0n) через зараженный компьютер, к которому подключено устройство, – при условии, что устройство разблокировано.

Модуль для iOS обеспечивает злоумышленникам доступ к данным, хранящимся на устройстве (в частности, к электронной почте, контактам, истории звонков, и сохраненным в кэше веб-страницам), и дает возможность без ведома пользователя включать микрофон и регулярно делать снимки камерой устройства. Это позволяет полностью контролировать среду как на компьютере жертвы, так и вокруг него.

Модуль для Android защищен оптимизатором/обфускатором DexGuard, и потому его очень сложно анализировать. Однако мы обнаружили, что образец обладает всем функционалом вышеописанного модуля для iOS, а также поддерживает кражу информации из следующих приложений: ‘com.tencent.mm’, ‘com.google.android.gm’, ‘android.calendar’, ‘com.facebook’, ‘jp.naver.line.android’ и ‘com.google.android.talk’.

Полный список функций можно найти здесь.

Эти новые данные дают представление о том, насколько сложны подобные инструменты слежки. У «Лаборатории Касперского» однозначная позиция по отношению к подобным инструментам. Мы стремимся обнаружить и обезвредить любую вредоносную атаку, вне зависимости от ее источника и целей. Для нас не существует «правильного» и «неправильного» вредоносного ПО; в прошлом мы неоднократно публиковали предупреждения о рисках, связанных с так называемым «легальным» шпионским ПО. Критически важно, чтобы эти инструменты слежки не попали в плохие руки, – именно поэтому индустрия IT-безопасности не может делать исключений в том, что касается обнаружения вредоносных программ.

MINIDUKE: ПЕРЕЗАГРУЗКА

Начало 2014 года ознаменовалось повторной активизацией MiniDuke – вредоносной кампании класса APT, которая впервые проводилась в начале 2013 года. Исходная кампания выделялась на фоне других атак по нескольким причинам. Она использовала нестандартный бэкдор, написанный на «старорежимном» языке ассемблера. Управление атакой осуществлялось через уникальную инфраструктуру, в которой использовались резервные каналы, в том числе учетные записи Twitter. Для скрытой передачи обновленных исполняемых файлов разработчики маскировали их под GIF-изображения.

Среди мишеней новой кампании MiniDuke (известной также под названиями TinyBaron и CosmicDuke) государственные органы, дипломатические учреждения, энергетические компании, военные, включая военных подрядчиков, и операторы связи. При этом, как ни странно, в число жертв также входят лица, причастные к торговле и перепродаже запрещенных препаратов, в том числе стероидов и гормонов. Причины этого неясны. Возможно, что нестандартный бэкдор предлагается в качестве так называемого «легального шпионского ПО». Не исключено также, что несколько игроков фармацевтического рынка приобрели программу на подпольном рынке для слежки друг за другом.

Жертвы кампании находятся в разных странах по всему миру, в том числе в Австралии, Бельгии, Венгрии, Германии, Испании, Нидерландах, США, на Украине и во Франции.

На одном из проанализированных нами серверов был найден длинный список жертв, датируемый апрелем 2012 года. На сервере было обнаружено 265 различных идентификаторов жертв, которым соответствуют 139 уникальных IP-адресов, географически относящихся к Грузии, России, США, Великобритании, Казахстану, Индии, Беларуси, Кипру, Украине и Литве.

Наш анализ показал, что атакующие стремились расширить географический охват своих операций и сканировали диапазоны IP-адресов и серверов в Азербайджане, Греции и на Украине.

Вредоносная программа подменяет популярные приложения, работающие в фоновом режиме, копируя у них описания файлов, пиктограммы и даже размеры файлов. Сам бэкдор скомпилирован с помощью «BotGenStudio» – настраиваемого фреймворка, позволяющего

злоумышленникам включать и отключать компоненты при конструировании бота. Компоненты вредоносной программы можно классифицировать в соответствии с их функционалом:

(1) Устойчивость. Вредоносная программа может запускаться автоматически с помощью Планировщика заданий Windows в определенное время или при активации скринсейвера.

(2) Сбор данных. Вредоносная программа способна не только красть файлы с определенными расширениями, но и собирать на компьютерах жертв пароли, историю посещения сайтов, данные о сети, списки контактов, информацию, выводимую на экран (снимки экрана делаются каждые пять минут) и другие конфиденциальные данные.

Каждой жертве присваивается уникальный идентификатор, который позволяет отправлять индивидуально отобранные обновления. Вредоносная программа защищена при помощи специального обфусцированного загрузчика, который очень сильно загружает процессор на 3-5 минут непосредственно перед выполнением основного кода. Это не только затрудняет анализ троянца, но и приводит к потреблению значительных ресурсов эмуляторами, встроенными в защитные программы. Помимо собственного обфускатора, вредоносный код широко использует шифрование и сжатие, основанное на алгоритмах RC4 и LZRW соответственно. Реализация этих алгоритмов имеет незначительные отличия от стандартной версии – по нашему мнению, эти изменения были сделаны специально, чтобы ввести исследователей в заблуждение.

Одним из технически сложных компонентов вредоносной программы является хранилище данных. Внутренняя конфигурация троянца зашифрована, сжата и организована в сложную, подобную реестру структуру с разными типами записей, включая строковые, целочисленные и внутренние ссылки.

(3) Передача данных. Вредоносная программа использует несколько видов сетевых соединений для передачи данных, включая отправку данных на FTP и три различных способа передачи данных через HTTP. В процессе загрузки на командный сервер файл разбивается на маленькие (размером около 3 КБ) фрагменты. Эти фрагменты сжимаются, шифруются и помещаются в контейнер, который загружается на сервер. Большой файл может быть «разложен» на несколько сотен контейнеров, каждый из которых загружается на сервер независимо от других. По всей вероятности, эти фрагменты данных анализируются, расшифровываются, распаковываются и вновь собираются в файлы на стороне атакующих.

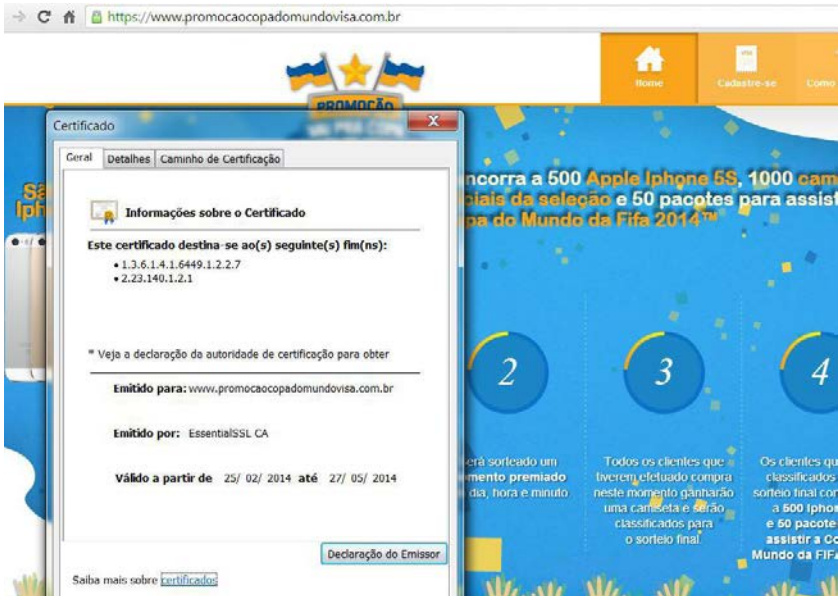
Столь сложная система может выглядеть избыточной, однако все эти уровни дополнительной обработки гарантируют, что очень немногие исследователи смогут добраться до исходных данных. Кроме того, это повышает надежность системы и ее устойчивость к сетевым ошибкам.

Как и с любой другой атакой класса APT, атрибуция в данном случае практически невозможна. Несмотря на то что злоумышленники используют в нескольких местах английский язык, есть основания полагать, что этот язык для них неродной. В участке памяти, добавленном к вредоносному компоненту, отвечающему за устойчивость, мы нашли строки, указывающие на то, что родной язык злоумышленников, возможно, русский. Об этом же говорит и тот факт, что веб-шелл, примененный киберпреступниками для взлома веб-серверов с целью размещения на них командного сервера, использует кодовую страницу 1251. Эта кодовая страница обычно используется для отображения кириллических символов. Точно такой же веб-шелл мы уже встречали в атаках другой группы киберпреступников, известной как Turla, Snake или Uroburos).

ОНЛАЙН-МОШЕННИКИ: КУБОК МИРА, ОН ЖЕ ПОЛНАЯ ЧАША

Мошенники всегда пристально следят за крупными спортивными событиями, на которых можно сделать деньги; мировой чемпионат по футболу не стал исключением. Перед чемпионатом мы уже рассказывали о том, как мошенники разными способами пытались нагреть руки на доверчивых футбольных фанатах, приезжающих в Бразилию на главное событие всего футбольного мира.

Один из очевидных способов заработать на мошенничестве – это проведение фишинговых атак. Часто фишеры прибегают к такому методу, как взлом легитимного веб-сайта и размещение на нем своей страницы. Однако бразильские киберпреступники пошли дальше и научились проводить атаки, которые обычным людям распознать очень сложно: они зарегистрировали домены под имена известных локальных брендов – компаний, выпускающих кредитные карты, банков, интернет-магазинов и т.д. Причем киберпреступники и на этом не остановились: веб-сайты были не только очень профессионально оформлены, но для большего эффектаподлинности были куплены SSL-сертификаты у соответствующих центров сертификации: Comodo, EssentialSSL, Starfield, Register.com и др. Понятно, что если на сайте есть «легитимный» SSL-сертификат, то на удочку, скорее всего, попадутся даже самыебдительные пользователи.



Киберпреступники воспользовались доступностью сертификатов, которыми можно подписывать вредоносные программы. Для начала злоумышленники рассылают сообщения, в которых предлагаются бесплатные билеты на Чемпионат мира; сообщения содержат ссылку, ведущую на банковский троянец:

В некоторые из этих писем для достоверности вставляются личные данные из взломанной базы данных.

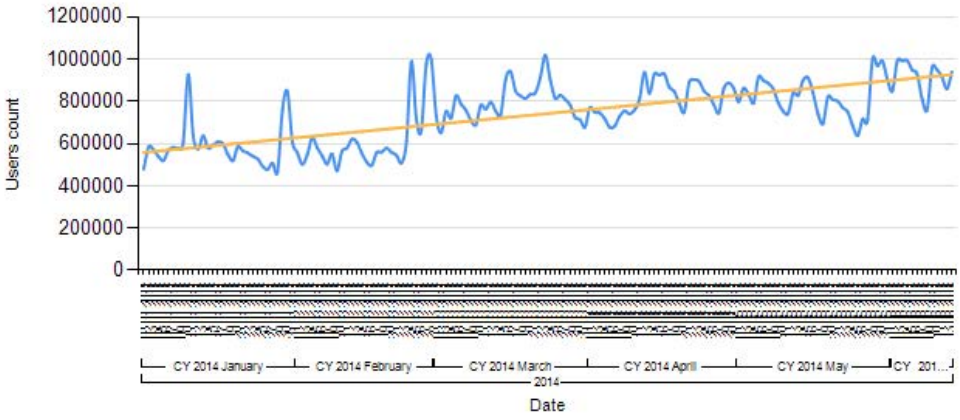
Надо сказать, что бразильские киберпреступники не ограничиваются одним фишингом. Ранее мы рассказывали о том, как они перехватывают данные кредитных карт, используя вредоносные программы, заражающие кассовые терминалы и устройства для ввода PID-кодов. Эти устройства подсоединяются к компьютеру через USB или последовательный порт и в процессе работы обмениваются данными с ПО для осуществления электронных платежей. Троянцы, используемые киберпреступниками, заражают компьютер и перехватывают данные, передаваемые через эти порты. Устройства для ввода PIN-кодов имеют специальные средства защиты, которые удаляют ключи безопасности в случае попыток вмешаться в работу устройства. PIN-код шифруется сразу после ввода, обычно шифром Triple DES. Однако на

устройствах устаревшего образца данные первой дорожки (Track 1): номер кредитной карты, срок действия, код подтверждения и CVV-код, – а также открытые данные, хранящиеся на чипе карты, не шифруются и передаются на компьютер через USB или последовательный порт в открытом виде. В этом случае в руки киберпреступников попадает все, что им нужно, чтобы создать клон карты.

Еще киберпреступники используют в своих интересах стремление пользователей оставаться на связи, где бы они ни находились: пользователи выходят в интернет, чтобы опубликовать фотографии, рассказать в соцсетях о происходящих событиях, узнать новости, найти информацию о ресторанах, магазинах и гостиницах. К сожалению, в роуминге мобильная связь обычно стоит очень дорого, и потому люди стремятся найти ближайшую точку доступа Wi-Fi. Как мы писали в отчете о Wi-Fi в Бразилии, такая практика опасна: данные, отправляемые и получаемые через открытые Wi-Fi сети, могут перехватываться, а пароли, PIN-коды и другие конфиденциальные данные легко могут быть украдены. В довершение всего, киберпреступники устанавливают фальшивые точки доступа, настроенные так, чтобы пропускать весь трафик через хост, который может использоваться для контроля потока данных и даже функционировать в качестве устройства-посредника, способного перехватывать и читать зашифрованный трафик (атака типа «man-in-the-middle»).

Кроме того, в нашем отчете говорилось о рисках, связанных с зарядкой мобильных устройств через USB-порты, установленные в публичных местах. Вредоносные зарядные станции вполне справятся с зарядкой аккумулятора вашего устройства, но при этом они могут незаметно скопировать данные с него или даже установить вредоносное ПО.

Есть еще один способ, с помощью которого мошенники могут вытянуть деньги у обычных пользователей, даже если те не занимаются поиском билетов на чемпионат мира. Футбольных фанатов по всему миру огромное количество, и живут они все в разных часовых поясах. У некоторых не получается посмотреть матч по телевизору, попросту потому, что во время матча они находятся не дома, и зачастую они ищут онлайн-трансляцию матча в Сети. К сожалению, такой поиск прямых трансляций в интернете может стоить слишком дорого или привести к заражению вашего компьютера. Дело в том, что некоторые рекламные ссылки, которые вы найдете при поиске, ведут на мошеннические или вредоносные ресурсы. Попав на мошеннический веб-сайт, вы получите сообщение, что для просмотра онлайн-трансляции нужно установить специальный плагин. На самом деле это рекламная программа, которая ничего не показывает, но расходует значительную часть ресурсов вашего компьютера. Рекламное ПО находится на тонкой грани, разделяющей легитимное и вредоносное ПО. Не приходится удивляться, что обнаружение подобных программ учитывается в нашей статистике. Подробную информацию о программах этого типа можно найти здесь.

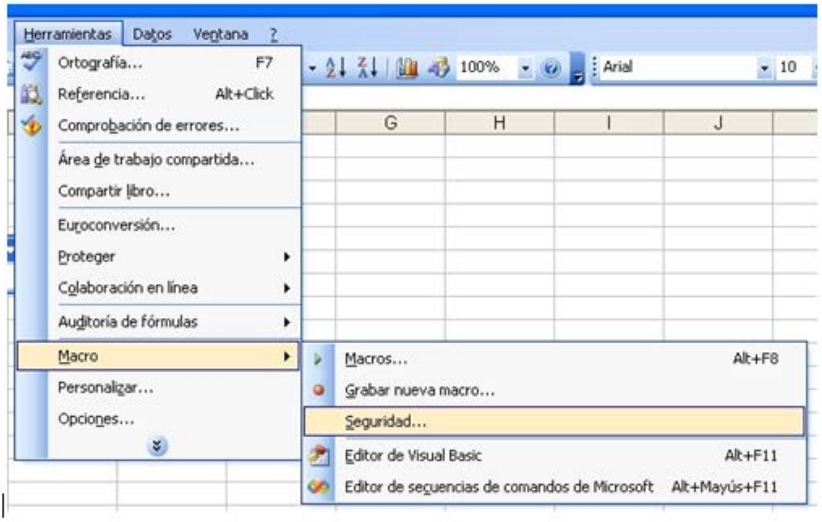


ЗАПЛАТИ НАЛОГИ – НО НЕ ПОПАДИСЬ НА УДОЧКУ ФИШЕРАМ

Фишеры используют в своих целях не только крупные спортивные состязания. Зачастую они проводят свои кампании, ориентируясь на более прозаические стороны жизни. В мае многие жители Колумбии получили электронное письмо с обвинениями в мошенничестве и уклонении от налогов. Чтобы придать сообщению убедительности, злоумышленники утверждали, что это уже третье уведомление на данную тему. Электронное письмо содержало ссылку на зараженный документ Word. Microsoft Office по умолчанию блокирует макрокоманды, внедренные в документы, поэтому киберпреступники приложили к письму инструкцию для получателей по разблокированию макросов.

Dirección de Impuestos y Aduanas Nacionales de Colombia.

DIAN



2. Seleccione nivel Bajo y Acepte
3. Cierre Word o Excel y ábralo de nuevo para que se apliquen los cambios.

Кликнув по документу, жертва запустит загрузку на компьютер еще одного вредоносного файла со взломанного сервера, находящегося в Эквадоре. Это вредоносная программа, предназначенная для кражи паролей к учетным записям в онлайн-играх, PayPal, файлообменных сервисах, социальных сетях (в том числе Facebook и Twitter), системах онлайн-банкинга и т.д.

Попытки запугивания потенциальных жертв и в частности фальшивые письма, якобы отправленные налоговыми органами, – это приемы, широко используемы фишерами по всему миру.

В апреле мы опубликовали подробный отчет о финансовой киберпреступности, подготовленный на основе данных Kaspersky Security Network. Отчет по фишингу можно прочитать здесь.

ВРЕДОНОСНЫЕ ПРОГРАММЫ: РАННЯЯ ЗАГРУЗКА. БУТКИТЫ В АРСЕНАЛЕ КИБЕРПРЕСТУПНИКОВ

При создании вредоносного кода одна из ключевых задач, которые ставят перед собой киберпреступники, – обеспечить как можно более раннюю загрузку вредоносного контента при загрузке операционной системы. Это позволяет получить максимально возможный контроль над системой. Буткиты – наиболее сложная и эффективная технология подобного рода, позволяющая запускать вредоносный код еще до загрузки операционной системы. Эта технология реализована в многочисленных вредоносных программах. Среди наиболее заметных примеров – XPAJ и TDSS, однако существует множество других вредоносных программ, использующих буткиты, в частности такие целевые атаки, как Mask.

За последние годы буткиты проделали путь от концептуальных разработок до массового распространения, как мы писали здесь. После публикации исходного кода банковской троянской программы Carberp буткиты, по сути, превратились в ПО с открытым исходным кодом: для защиты Carberp использовался буткит Cidox, и его исходный код был опубликован вместе с исходным кодом Carberp.

Очевидно, что историю развития буткитов следует рассматривать в общем контексте игры в кошки-мышки между создателями вредоносных программ и антивирусными экспертами. Они постоянно ищут новые способы избежать обнаружения - мы постоянно ищем способы повысить эффективность защиты наших пользователей. В упомянутом выше отчете также рассматриваются преимущества интерфейса UEFI (Unified Extensible Firmware Interface), а также возможные способы, с помощью которых авторы вредоносных программ могут пытаться обойти обеспечиваемые UEFI меры безопасности.

БЕЗОПАСНОСТЬ В ИНТЕРНЕТЕ И КРАЖА ДАННЫХ: WINDOWS XP – БЕЗ ПОДДЕРЖКИ, НО С ПОЛЬЗОВАТЕЛЯМИ

Поддержка Windows XP прекращена 8 апреля. Для этой операционной системы больше не будут выпускаться обновления безопасности и не связанные с безопасностью исправления, не будут предлагаться услуги бесплатной или платной технической поддержки и обновления технического контента на сайтах компании. К сожалению, число пользователей Windows XP по-прежнему велико – по нашим данным за период после 8 апреля 2014 года, около 18 процентов всех случаев заражения приходится на компьютеры под управлением этой операционной системы. Это означает, что теперь, когда обновления безопасности больше не выпускаются, появилось большое число пользователей, уязвимых для атаки: по сути, каждая уязвимость, обнаруженная после этого дня, становится уязвимостью нулевого дня – такой, для которой даже теоретически не может быть выпущен патч.

Проблема осложняется еще и тем, что разработчики приложений также прекращают выпуск обновлений для Windows XP. Каждое не обновляемое приложение станет потенциальной точкой проникновения вредоносного кода в систему, расширяя возможности киберпреступников по проведению атак. Этот процесс уже начался: последняя версия Java не поддерживает Windows XP.

Переход на более новую операционную систему кажется на первый взгляд простым решением. Однако несмотря на то что Microsoft задолго предупредила о предстоящем прекращении поддержки, легко понять, почему для некоторых компаний переход на новую операционную систему сопряжен со значительными сложностями. В дополнение к расходам, непосредственно связанным со сменой операционной системы, зачастую необходимо потратиться на новое аппаратное обеспечение, а иногда и решить проблему замены специально разработанных для данной компании приложений, не совместимых с более поздними операционными системами. Поэтому нет ничего удивительного в том, что некоторые организации платят за продолжение поддержки Windows XP.

Если вы не готовы переходить на новую операционную систему прямо сейчас, сможете ли вы обеспечить свою безопасность? Защитит ли вас антивирусное решение?

Антивирусное решение, несомненно, способно обеспечить защиту. Однако это относится лишь к тем антивирусам, которые представляют собой полнофункциональные решения класса Internet Security, использующие технологии проактивной защиты от новых, еще неизвестных угроз – в частности, функционал, предотвращающий применение на компьютере эксплойтов. Базового антивирусного продукта, основанного прежде всего на сигнатурном обнаружении угроз, недостаточно. Но при этом следует понимать, что со временем защитные технологии, вновь создаваемые производителями антивирусных решений, могут оказаться несовместимыми с Windows XP.

В крайнем случае такой вариант можно рассматривать как временное решение, которое позволит вам не торопясь определиться со стратегией перехода на новую операционную систему. Вирусописатели, несомненно, будут ориентироваться на Windows XP, пока у этой системы будет оставаться значительное число пользователей, поскольку необновляемая операционная система будет давать им гораздо большее пространство для маневра. Подключенный к корпоративной сети компьютер под управлением Windows XP – это слабое звено, которым можно воспользоваться в ходе целевой атаки на компанию. В случае успешного взлома такой компьютер может затем быть использован злоумышленниками для заражения других машин сети.

Нет никаких сомнений в том, что переход на новую операционную систему – в равной степени неудобное и затратное дело и для домашних пользователей, и для компаний. Однако потенциальный риск, связанный с использованием все хуже защищенной операционной системы, вероятно, должен перевесить неудобство и расходы.

МОБИЛЬНЫЕ УГРОЗЫ

ЦИФРЫ КВАРТАЛА

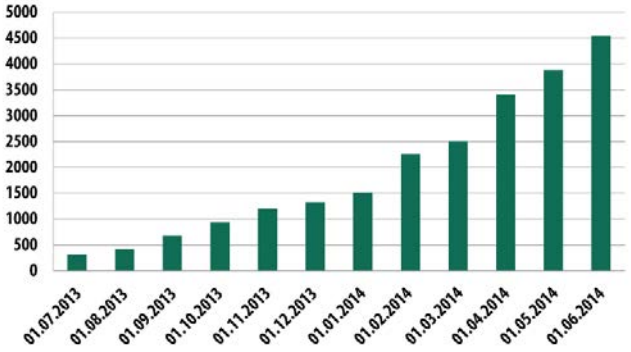
Во втором квартале 2014 года было обнаружено:

- 727 790 установочных пакетов;
- 65 118 новых мобильных вредоносных программ;
- 2 033 мобильных банковских троянцев.

Суммарное количество обнаруженных мобильных вредоносных объектов в 1,7 раз меньше, чем в первом квартале. Мы связываем это с началом сезона отпусков. Так в июне было зафиксировано уменьшение попыток заражений мобильных устройств троянцами.

МОБИЛЬНЫЕ БАНКОВСКИЕ ТРОЯНЦЫ

Хотя общее количество угроз во втором квартале уменьшилось, в отчетный период мы обнаружили 2 033 мобильных банковских троянцев – в 1,7 раз больше, чем в предыдущем квартале. С начала 2014 года численность банковских троянцев увеличилась почти в четыре раза, а за год (с июля 2013) – в 14,5 раз.

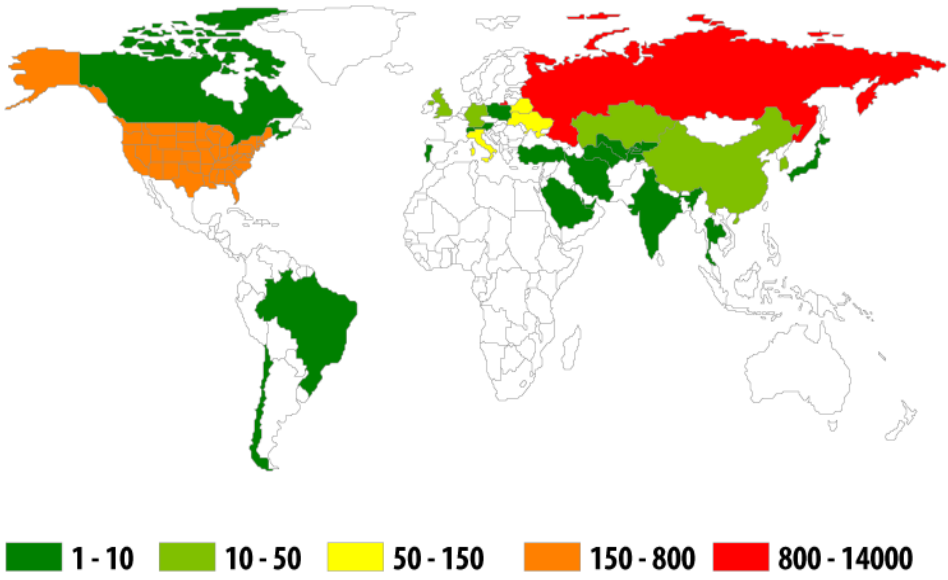


Количество обнаруженных мобильных банковских троянцев

Такой рост обусловлен двумя факторами:

- интересом киберпреступников к «большим» деньгам;
- активным противодействием со стороны антивирусных компаний.

Отметим, что поменялась география заражений мобильными банковскими троянцами:



География мобильных банковских угроз во втором квартале 2014

ТОП 10 СТРАН, АТАКУЕМЫХ БАНКОВСКИМИ ТРОЯНЦАМИ

	СТРАНА	КОЛИЧЕСТВО АТАК	% ОТ ВСЕХ АТАК
1	Россия	13800	91,7%
2	США	792	5,3%
3	Украина	136	0,9%
4	Италия	83	0,6%
5	Белоруссия	68	0,5%

6	Республика Корея	30	0,2%
7	Казахстан	25	0,2%
8	Китай	19	0,1%
9	Великобритания	17	0,1%
10	Германия	12	0,1%

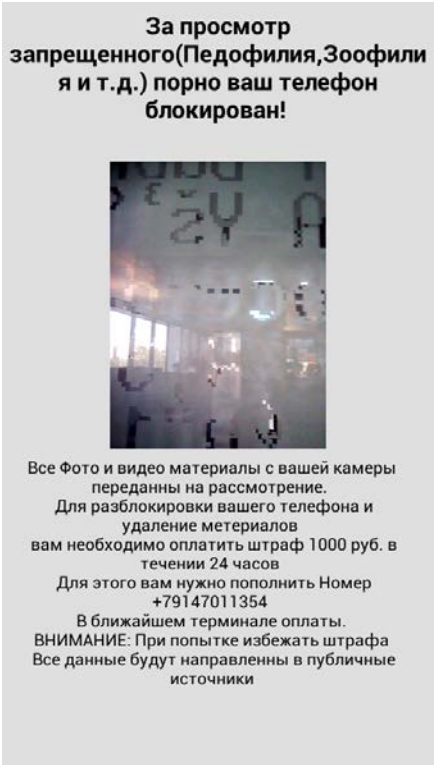
На первом месте в этом рейтинге, как и ранее, Россия, а вот на второе место со значительным отрывом от остальных стран вышли США. Казахстан, который в первом квартале занимал в этом рейтинге второе место, во втором квартале оказался на седьмом.

НОВИНКИ ОТ ВИРУСОПИСАТЕЛЕЙ

ПЕРВЫЙ МОБИЛЬНЫЙ ШИФРОВАЛЬЩИК

В середине мая на одном из форумов вирусописателей появилось объявление о продаже за $5000 уникального троянца-шифровальщика, работающего в ОС Android. 18 мая мы обнаружили первого мобильного шифровальщика в дикой природе (in the wild). Этот зловред детектируется «Лабораторией Касперского» как Trojan-Ransom.AndroidOS.Pletor.a.

После запуска троянец, используя алгоритм шифрования AES, шифрует содержимое карты памяти смартфона медиафайлы и документы. Сразу после начала шифрования Pletor выводит на экран требование о выкупе. Для получения денег от пользователей используются системы QIWI VISA WALLET, MoneXy или обычный перевод денег на номер телефона.



На конец второго квартала нам удалось обнаружить более 47 версий троянца. Все они содержат ключ, зная который можно расшифровать все файлы.

Для коммуникации со злоумышленниками одни версии троянца используют сеть TOR, другие – HTTP и SMS. Троянцы из второй группы в окне с требованием денег показывают пользователю его видеоизображение, которое в режиме реального времени транслируется с помощью фронтальной камеры смартфона.

Отметим, что вирусописатели используют те же приемы социальной инженерии, что и создатели ранних версии шифровальщиков под Windows: телефон пользователя якобы блокирован за просмотр запрещенного порно-контента, а все фото и видеоматериалы со смартфона «переданы на рассмотрение». Кроме того, за неуплату «штрафа» вымогатели грозятся направить все данные «в публичные источники».

Pletor нацелен на граждан России и Украины сообщения написаны на русском языке, а выкуп со своих жертв вымогатели требуют в рублях или гривнах (сумма соответствует приблизительно 300 евро). Однако мы обнаружили заражения этим зловредом в 13 странах – в основном, на территории бывшего СССР.

ЭВОЛЮЦИЯ БЛОКИРОВЩИКОВ

С точки зрения техники атак наметилась явная тенденция развития вымогателей-блокировщиков. Киберпреступники и здесь перенимают методы запугивания своих жертв, которые использовались создателями Windows-зловредов.

Первая модификация мобильного зловреда Svpeng, обладающая возможностями троянца-вымогателя, была обнаружена в начале 2014 года. Троянец блокировал работу телефона якобы за просмотр его владельцем детской порнографии. За разблокировку мобильного устройства злоумышленники требовали уплатить «штраф» в размере 500 долларов.

В начале июня мы обнаружили новую модификацию Svpeng, нацеленную преимущественно на пользователей в США. Кроме того, зловред атаковал пользователей из Великобритании, Швейцарии, Германии, Индии и России.

Эта модификация Svpeng полностью блокирует мобильное устройство, так что у пользователя даже нет возможности вызвать меню отключения/перезагрузки устройства. Смартфон можно отключить только с помощью долгого нажатия кнопки выключения, но троянец стартует сразу же после повторного запуска системы.

При этом злоумышленники использовали проверенные временем приемы социальной инженерии. После запуска троянец имитирует сканирование телефона и якобы находит запрещенный контент. Для устрашения пользователя окно с сообщением о «находке» снабжено логотипом ФБР:

Троянец блокирует телефон и требует заплатить 200 долларов за разблокировку. Для получения денег создатели троянца используют ваучеры MoneyPak.

Отметим, что в этом окне Svpeng показывает фотографию пользователя, сделанную фронтальной камерой – это напоминает Trojan-Ransom.AndroidOS.Pletor.a, о котором речь шла выше, только Pletor транслировал видеоизображение.

На конец второго квартала нам удалось найти 64 версии нового Svpeng. В каждой версии есть упоминание класса Cryptor, хотя использование этого класса мы не зафиксировали. Возможно, злоумышленники намерены в дальнейшем с помощью зловреда шифровать данные пользователя и требовать выкуп за их расшифровку.

НЕ ТОЛЬКО ANDROID

Как и ранее, основной целью киберпреступников является платформа Android. На нее приходится 99% нового мобильного вредоносного ПО.

Однако не стоит списывать со счетов другие мобильные платформы. Так, во втором квартале 2014 года появились новые вредоносные объекты для платформы Apple iOS (но только для Jailbroken устройств). Наряду с вредоносным ПО киберпреступники воспользовались защитными функциями iOS в злонамеренных целях. Атака на Apple ID позволяла злоумышленникам полностью блокировать устройство и вымогать у жертвы деньги за восстановление его работоспособности.

Неприятной новостью стало разоблачение Hacking Team, по результатам которого выяснилось, что можно провести успешную атаку и на не Jailbroken iOS устройства.

Не осталась без внимания платформа Windows Phone. Здесь вирусописатели не изобрели ничего технически уникального, а отделались выкладкой в официальный магазин платных приложений фальшивок без какого-либо функционала. Досталось и нашему бренду: мошенники использовали торговую марку и логотип «Лаборатории Касперского».

Таким образом вскрылись сразу две уязвимости в магазине Windows Phone Store:

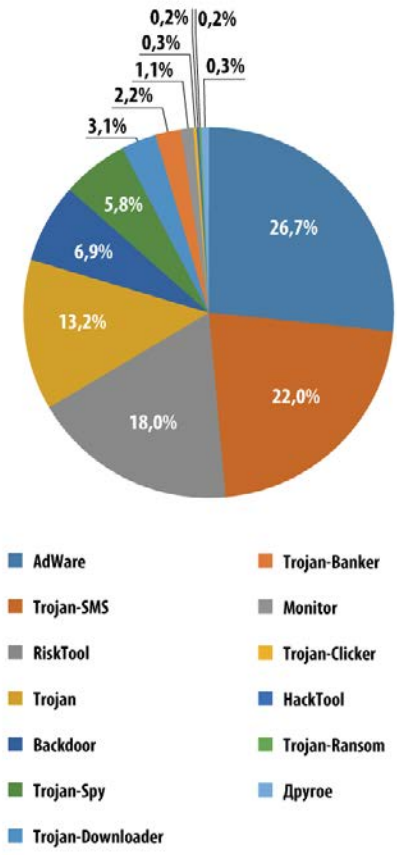
- отсутствие проверки на чистоту бренда;
- отсутствие проверки на функционал.

Фальшивые приложения этого же издателя попали и в Google Play.

МОБИЛЬНЫЕ УГРОЗЫ: СТАТИСТИКА

Во втором квартале 2014 года объектов было обнаружено в 1,7 раз меньше мобильных вредоносных, чем в первом квартале: 727 790 установочных пакетов, 65 118 новых мобильных вредоносных программ, 2 033 мобильных банковских троянцев. Вероятно, уменьшение активности злоумышленников обусловлено началом сезона отпусков.

РАСПРЕДЕЛЕНИЕ ПО ТИПАМ МОБИЛЬНЫХ ЗЛОВРЕДОВ



Распределение по типам мобильных зловредов,
второй квартал 2014 года

В рейтинге обнаруженных во втором квартале вредоносных объектов для мобильных устройств лидируют потенциально нежелательные рекламные приложения (27%). Не сдают свои позиции и SMS-троянцы (22%). Если показатели этих двух типов мобильных угроз практически не изменились, то Risktool за квартал поднялись с пятого на третье место: их доля в потоке обнаруженного мобильного вредоносного ПО увеличилась с 8,6% до 18%. Это легальные приложения, которые потенциально опасны для пользователей – их неаккуратное использование владельцем смартфона или злоумышленником может привести к финансовым потерям.

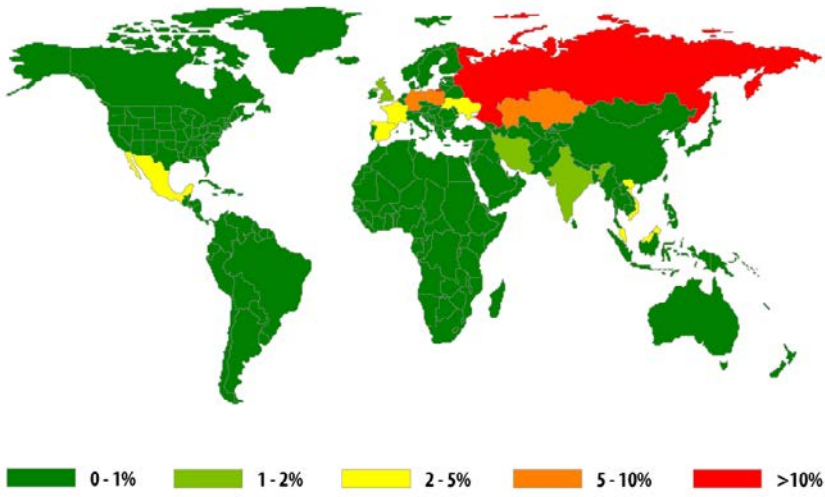
ТОР 20 МОБИЛЬНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

	НАЗВАНИЕ	% АТАК*
1	Trojan-SMS.AndroidOS.Stealer.a	25,42%
2	RiskTool.AndroidOS.SMSreg.gc	6,37%
3	RiskTool.AndroidOS.SMSreg.hg	4,82%
4	Trojan-SMS.AndroidOS.FakeInst.a	4,57%
5	Trojan-SMS.AndroidOS.Agent.ao	3,39%
6	AdWare.AndroidOS.Viser.a	3,27%
7	Trojan-SMS.AndroidOS.Opfake.a	2,89%
8	Trojan-SMS.AndroidOS.Erop.a	2,76%
9	Trojan-SMS.AndroidOS.FakeInst.ff	2,76%
10	Trojan-SMS.AndroidOS.Agent.en	2,51%
11	Trojan-SMS.AndroidOS.Agent.ev	2,43%
12	RiskTool.AndroidOS.SMSreg.eh	2,41%
13	Trojan-SMS.AndroidOS.Opfake.bw	1,96%
14	Trojan-SMS.AndroidOS.Opfake.bo	1,53%
15	RiskTool.AndroidOS.MimobSMS.a	1,48%
16	Trojan-SMS.AndroidOS.Skanik.a	1,35%
17	Trojan-SMS.AndroidOS.Agent.mw	1,33%
18	RiskTool.AndroidOS.SMSreg.ey	1,31%
19	Trojan-SMS.AndroidOS.Agent.ks	1,24%
20	Trojan-SMS.AndroidOS.Agent.ay	1,21%

В TOP 20 детектируемых угроз по-прежнему преобладают SMS-троянцы – эти вредоносные программы заняли пятнадцать позиций в рейтинге.

В течение всего второго квартала на фоне уменьшения количества атак мы наблюдали устойчивый рост попыток атаковать пользователей троянцем Trojan-SMS.AndroidOS.Stealer.a. Этот зловред занял первое место в рейтинге с показателем, превышающим 25% всех атак. Особенно активны злоумышленники были в апреле, когда попыток заражений Stealer было почти в два раза больше, чем в мае или марте. А в июне количество попыток заражений этим троянцем в 7 раз превосходило аналогичный показатель ближайшего конкурента.

ГЕОГРАФИЯ УГРОЗ



Карта попыток заражений мобильными зловредами
(процент от всех атакованных уникальных пользователей)

Небольшие изменения произошли в территориальном распределении атак. Так на второе место вышла Германия, а Индия, которая занимала второе место во первом квартале, вообще выпала из ТОП 10. Казахстан сохранил третье место, а Украина сместилась с четвертой на пятую позицию, уступив место Польше, которая поднялась с десятого на четвертое место.

ТОР 10 АТАКУЕМЫХ СТРАН:

	СТРАНА	% АТАК
1	Россия	46,96%
2	Германия	6,08%
3	Казахстан	5,41%
4	Польша	5,02%
5	Украина	3,72%
6	Малайзия	2,89%
7	Вьетнам	2,74%
8	Франция	2,32%
9	Испания	2,28%
10	Мексика	2,02%

Пользователи устанавливают довольно много приложений на свои мобильные устройства. Стоит отметить, что в разных странах процент вредоносных приложений среди всех приложений, которые устанавливают пользователи, отличается.

ТОР 10 СТРАН ПО РИСКУ ЗАРАЖЕНИЯ

	СТРАНА*	% ВРЕДОНОСНЫХ ПРИЛОЖЕНИЙ
1	Вьетнам	2,31%
2	Греция	1,89%
3	Польша	1,89%
4	Казахстан	1,73%
5	Узбекистан	1,51%
6	Армения	1,24%
7	Сербия	1,15%
8	Марокко	1,09%
9	Чехия	1,03%
10	Румыния	1,02%

**При расчетах мы исключили страны, в которых число скачиваний приложений менее 100 000*

Хотя Россия занимает первое место по числу зафиксированных атак, в этой стране не самая большая вероятность заразиться мобильным зловредом. По этому показателю лидирует Вьетнам, где вредоносные приложения составляют 2,31% от всех приложений, которые пытались установить пользователи.

Ниже для сравнения приведены показатели риска заражения еще по 15 странам разных регионов мира:

СТРАНА	% ВРЕДОНОСНЫХ ПРИЛОЖЕНИЙ
Китай	0,94%
Франция	0,85%
Россия	0,74%
Мексика	0,58%
Испания	0,55%
Индия	0,41%
Германия	0,19%
Великобритания	0,18%
Аргентина	0,13%
Бразилия	0,12%
Италия	0,11%
США	0,09%
Перу	0,07%
Гонконг	0,06%
Япония	0,02%

Во Франции вредоносными являются 0,85% приложений, заинтересовавших пользователей, в России - 0,74%, в Германии 0,19%, в Великобритании – 0,18%, в США – 0,09%, а в Японии - всего 0,02%.

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.

ОНЛАЙН-УГРОЗЫ В БАНКОВСКОМ СЕКТОРЕ

ОСНОВНЫЕ СОБЫТИЯ КВАРТАЛА

Одним из основных событий второго квартала этого года стало появление в апреле информации об уязвимости в OpenSSL, приводящей к возможности несанкционированного доступа к секретным ключам, именам и паролям пользователей и всему контенту, который должен передаваться в зашифрованном виде.

Уязвимость, которая получила название Heartbleed, эксплуатируется в криптографической библиотеке OpenSSL, использующейся в различном программном обеспечении, в том числе в ПО банковских инфраструктур. Отсутствие официального патча в течение нескольких часов и продолжительная процедура его инсталляции спровоцировали утечку платежных данных клиентов банков и ценных данных в различных сферах бизнеса. Поэтому после публикации данной информации и произошедших утечек можно ожидать увеличения числа мошеннических транзакций. Все это стало одним тревожным «звоночком», который в очередной раз подтверждает необходимость пристально следить за безопасностью платежных данных как финансовым организациям, так и их клиентам.

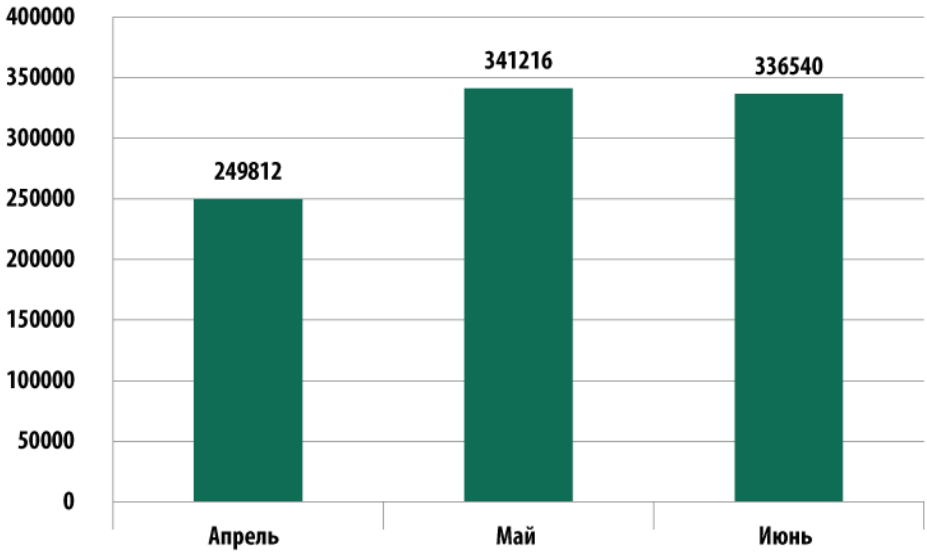
Во втором квартале 2014 года появился новый банковский троянец Pandemiya, который использует типичные для данного вида вредоносного ПО техники кражи платежной информации - например, веб-инжект.

Кроме того, во втором квартале началась спецоперация по уничтожению ботнета ZeuS Game-over. Разработчик банковского троянца ZeuS объявлен ФБР в международный розыск.

Финансовые угрозы не обошли стороной и такие громкие события, как Чемпионат Мира по футболу 2014, который прошел в Бразилии – стране, которая по итогам квартала лидирует по числу атакованных банковскими зловредами пользователей. Так, например, обнаружен вредоносный контент, который распространяется под видом рекламы, использующей ажиотаж вокруг главного спортивного события этого лета.

КОЛИЧЕСТВО КОМПЬЮТЕРОВ, АТАКОВАННЫХ ФИНАНСОВЫМ ВРЕДОНОСНЫМ ПО

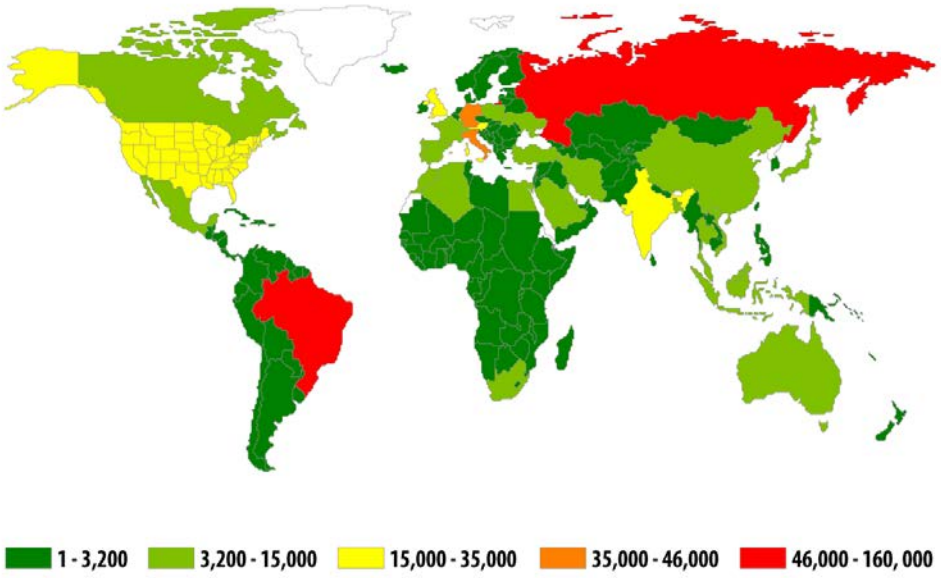
Во втором квартале 2014 года решения «Лаборатории Касперского» отразили попытки заражения банковскими вредоносными программами на компьютерах 927 568 пользователей. Отметим, что в мае по сравнению с апрелем этот показатель увеличился на 36,6%.



Количество компьютеров, атакованных финансовым вредоносным ПО, Q2 2014

Всего за квартал защитными продуктами «Лаборатории Касперского» было зарегистрировано 3 455 530 уведомлений о вредоносной активности ПО для кражи денежных средств через онлайн-доступ к банковским счетам.

ГЕОГРАФИЯ АТАК



География атак банковских вредоносных программ, Q2 2014
(количество атакованных пользователей в стране)

ТОР 10 СТРАН ПО КОЛИЧЕСТВУ АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ:

	СТРАНА	КОЛИЧЕСТВО АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ
1	Бразилия	159 597
2	Россия	50 003
3	Италия	43 938
4	Германия	36 102
5	США	34 539
6	Индия	27 447
7	Великобритания	25 039
8	Австрия	16 307
9	Вьетнам	14 589
10	Алжир	9 337

Бразилия традиционно лидирует по числу атакованных пользователей. В этой стране злоумышленники, промышляющие финансовыми зловредами, всегда были весьма активны. Во втором квартале они получили дополнительные возможности для атак: на прошедший в Бразилии Чемпионат мира по футболу 2014приехало множество болельщиков, которые пользуются онлайн-банкингом. Эксперты «Лаборатории Касперского» провели исследование безопасности Wi-Fi сетей и составили рекомендации для тех, кто не хочет рисковать своими платежными данными в Бразилии.

ТОР 10 СЕМЕЙСТВ БАНКОВСКИХ ВРЕДОНОСНЫХ ПРОГРАММ

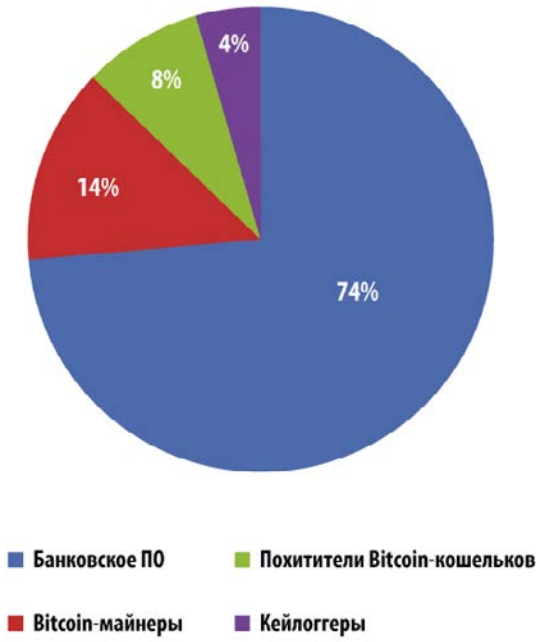
ТОР 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга во втором квартале 2014 года (по количеству уведомлений о попытках заражения):

	НАЗВАНИЕ*	КОЛИЧЕСТВО АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ	КОЛИЧЕСТВО НОТИФИКАЦИЙ
1	Trojan-Spy.Win32.Zbot	559 988	2 353 816
2	Trojan-Banker.Win32.Lohmys	121 675	378 687
3	Trojan-Banker.Win32.ChePro	97 399	247 467
4	Trojan-Spy.Win32.Spyeyes	35 758	99 303
5	Trojan-Banker.Win32.Agent	31 234	64 496
6	Trojan-Banker.Win32.Banbra	21 604	60 380
7	Trojan-Banker.Win32.Banker	22 497	53 829
8	Trojan-Banker.Win32.Shiotob	13 786	49 274
9	Backdoor.Win32.Clampi	11 763	27 389
10	Backdoor.Win32.Shiz	6 485	17 268

Самым распространенным банковским троянцем по-прежнему остается ZeuS (Trojan-Spy.Win32.Zbot). Согласно исследованиям «Лаборатории Касперского» данный троянец используется в 53% атак на клиентов онлайн-банкинга с использованием вредоносного ПО.

Девять из десяти семейств вредоносных программ, представленных в таблице, используют техники веб-инжектирования произвольного HTML-кода в отображаемую браузером веб-страницу и перехвата платежных данных, вводимых пользователем в оригинальные и вставленные веб-формы. Кроме того, четыре из десяти банковских угроз наряду с данными техниками используют технологию перехвата клавиатурного ввода. Этот факт говорит о том, что подобная техника кражи платежных данных по-прежнему эффективна при атаке на клиентов онлайн-банкинга.

Финансовые угрозы не ограничиваются банковским вредоносным ПО, которое атакует клиентов систем онлайн-банкинга.

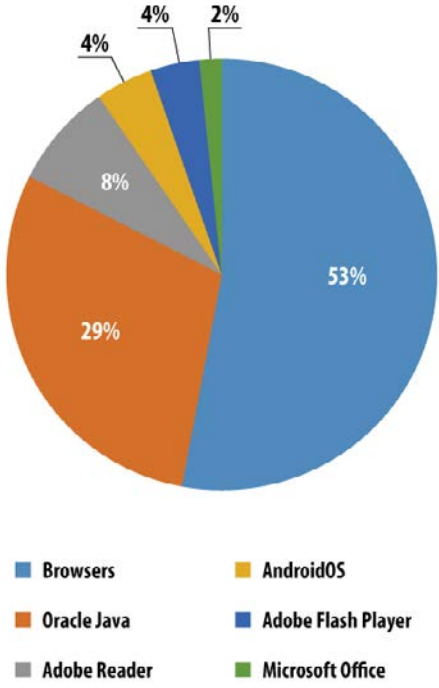


Распределение атак, нацеленных на деньги пользователей, по типам вредоносного ПО

Помимо банковских троянцев, которые используют техники модификации HTML-страниц в браузере, существуют альтернативные методы кражи электронных денег, одним из которых является кража Bitcoin-кошельков. При этом злодеи не брезгуют использовать вычислительные ресурсы жертвы для генерации криптовалюты – использование Bitcoin-майнеров составляет 14% от всех финансовых атак. Еще одна возможность добраться до денег пользователей – заполучить данные, дающие доступ к аккаунту пользователя в различных платежных системах и системах онлайн-банкинга, с помощью кейлоггеров.

УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ

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



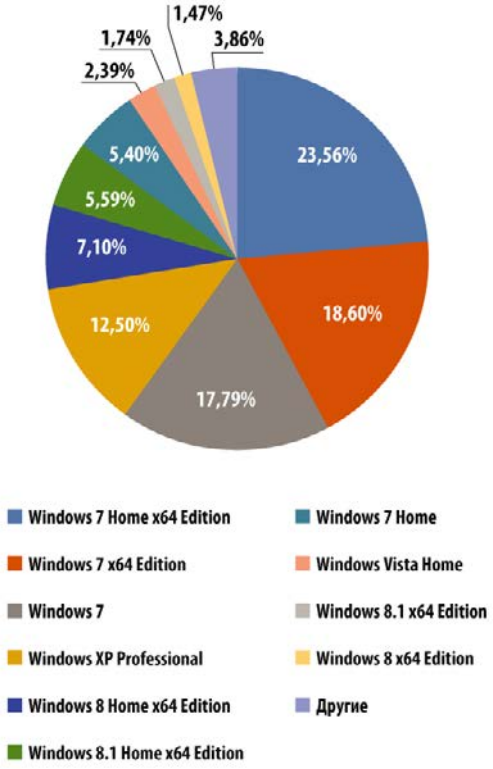
Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, Q2 2014

Из всех зафиксированных нами попыток эксплуатации уязвимостей 53% пришлось на уязвимости в браузерах. Почти в каждом эксплойт-паке используется эксплойт под Internet Explorer.

На втором месте находятся Java-эксплойты, уязвимости для которых эксплуатируются в ходе drive-by атак через интернет, и новые Java-эксплойты входят в состав множества эксплойт-

паков. В 2013 году из всех зафиксированных нами попыток эксплуатации уязвимостей 90,5% пришлось на уязвимости в Oracle Java. Но в 2014 году их популярность стала падать. В первом квартале этого года на уязвимости в Java пришлось 54% всех попыток эксплуатации уязвимостей, во втором – только 29%. Снижение популярности эксплойтов данного типа связано с тем, что уже почти год не было информации о новых уязвимостях в Java.

На третьем месте находятся эксплойты для уязвимостей в Adobe Reader. Такие уязвимости также эксплуатируются в ходе drive-by атак через интернет, и PDF эксплойты входят в состав множества эксплойт-паков.



Распределение установленных у пользователей OS Windows по версиям, Q2 2014

Среди пользователей наших продуктов, подтвердивших свое участие в KSN, 65,35% используют различные версии операционной системы Windows 7; 12,50% – Windows XP.

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.

ТОР 20 ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ В ИНТЕРНЕТЕ

Во втором квартале 2014 года нашим веб-антивирусом было задетектировано 57 133 492 уникальных вредоносных объектов (скрипты, веб-страницы, эксплойты, исполняемые файлы и т.д.).

Из всех вредоносных объектов, участвовавших в интернет-атаках на компьютеры пользователей, мы выделили двадцать наиболее активных. На них пришлось 97% всех атак.

	НАЗВАНИЕ*	% ОТ ВСЕХ АТАК**
1	Malicious URL	72,94%
2	Trojan.Script.Generic	11,86%
3	Trojan-Downloader.Script.Generic	5,71%
4	Trojan.Script.Iframer	2,08%
5	Adware.Win32.Amonetize.heur	1,00%
6	AdWare.Script.Generic	0,88%
7	AdWare.Win32.Agent.aiyc	0,76%
8	AdWare.Win32.Yotoon.heur	0,25%
9	Trojan.Win32.AntiFW.b	0,23%
10	AdWare.Win32.Agent.allm	0,19%
11	AdWare.Win32.AirAdInstaller.aldw	0,17%
12	Trojan.Win32.Generic	0,15%
13	Trojan-Downloader.Win32.Generic	0,14%
14	Trojan.Win32.Vague.cg	0,11%

15	Trojan.Win32.Invader	0,11%
16	AdWare.Win32.BetterSurf.b	0,10%
17	AdWare.Win32.Lollipop.qp	0,08%
18	Exploit.Script.Blocker	0,08%
19	AdWare.Win32.Lollipop.agzn	0,08%
20	Trojan.JS.Small.aq	0,07%

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

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

Традиционно в TOP 20 по большей части представлены вердикты, которые присваиваются объектам, использующимся в drive-by атаках, а также рекламным программам. По сравнению с прошлым кварталом количество рекламных программ в TOP 20 увеличилось с девяти до одиннадцати.

На 20-м месте расположился вердикт Trojan.JS.Small.aq, присваиваемый скрипту, который вставляет в веб-страницы определенных сайтов вредоносное расширение для браузеров с целью навязчивого показа рекламы.

СТРАНЫ - ИСТОЧНИКИ ВЕБ-АТАК: TOP 10

Данная статистика показывает распределение по странам источников заблокированных антивирусом веб-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 2014 года решения «Лаборатории Касперского» отразили 354 453 992 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира. 88,3% уведомлений были получены при блокировании атак с веб-ресурсов, расположенных в десяти странах мира. Это на 4,9% больше, чем в предыдущем квартале.

Распределение по странам источников веб-атак, второй квартал 2014

Состав десятки стран-лидеров не изменился. По сравнению с прошлым кварталом Германия поднялась с 4-го на 1-е место, ее доля увеличилась почти на 12%. Россия опустилась со 2-го места на 4-е, ее показатель уменьшился на 2,5%. С 10-го на 5-е место поднялась Канада (+6,29%).

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, сколько уникальных пользователей продуктов «Лаборатории Касперского» в каждой стране сталкивались со срабатыванием веб-антивируса. Полученные данные являются показателем агрессивности среды, в которой работают компьютеры в разных странах.

	СТРАНА*	% УНИКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ **
1	Россия	46,53%
2	Казахстан	45,35%
3	Армения	42,26%
4	Украина	41,11%
5	Азербайджан	40,94%
6	Вьетнам	39,59%
7	Белоруссия	37,71%
8	Молдова	36,65%
9	Монголия	33,86%
10	Киргизия	33,71%
11	Алжир	32,62%
12	Таджикистан	32,44%
13	Грузия	31,38%
14	Хорватия	29,46%
15	Турция	29,31%
16	Узбекистан	29,20%
17	Катар	28,76%
18	Тунис	28,67%
19	Иран	28,35%
20	Испания	28,05%

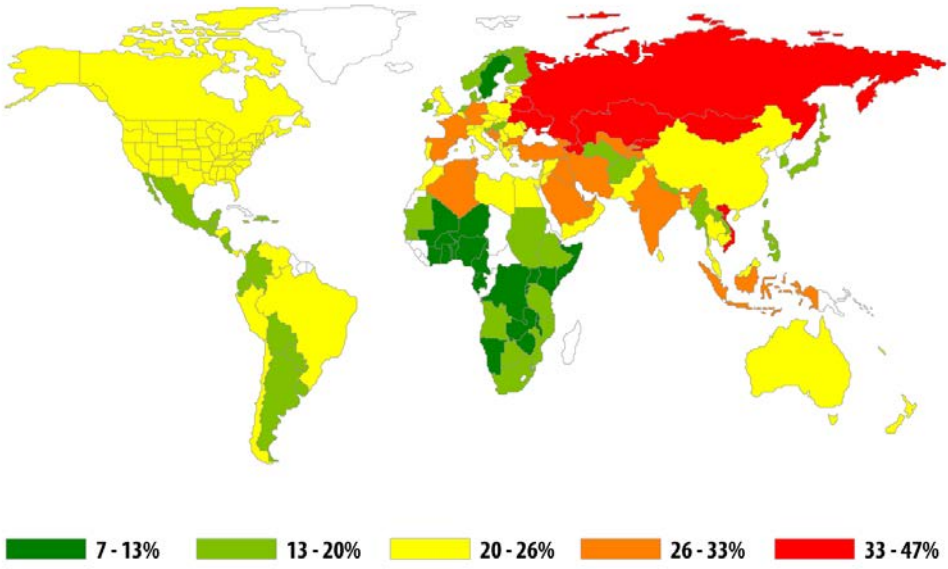
Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

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

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

Во втором квартале 2014 года Вьетнам потерял лидерство, уступив его России. Из новичков в рейтинге Тунис на 18-м месте и Иран на 19-м. Выбыли Литва и Греция.

В числе самых безопасных при серфинге в интернете стран – Сингапур (10,4%), Швеция (12,8%), Япония (13,3%), Финляндия (16,3%), ЮАР (16,9%), Эквадор (17,1%), Норвегия (17,5%), Нидерланды (17,5%), Гонконг (17,7%) и Аргентина (17,9%).



В среднем в течение квартала 29,5% компьютеров пользователей интернета по всему миру хотя бы раз подвергались веб-атаке.

ЛОКАЛЬНЫЕ УГРОЗЫ

Исключительно важным показателем является статистика локальных заражений пользовательских компьютеров. В эти данные попадают объекты, которые проникли на компьютеры не через интернет, почту или сетевые порты.

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 2014 года наши антивирусные решения заблокировали 528 799 591 вирусных атак на компьютерах пользователей. Всего в данных инцидентах было зафиксировано 114 984 065 уникальных вредоносных и потенциально нежелательных объектов.

ДЕТЕКТИРУЕМЫЕ ОБЪЕКТЫ, ОБНАРУЖЕННЫЕ НА КОМПЬЮТЕРАХ ПОЛЬЗОВАТЕЛЕЙ: TOP 20

	НАЗВАНИЕ*	% УНИКАЛЬНЫХ АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ**
1	DangerousObject.Multi.Generic	17,69%
2	Trojan.Win32.Generic	15,59%
3	AdWare.Win32.Agent.ahbx	14,81%
4	Adware.Win32.Amonetize.heur	13,31%
5	Trojan.Win32.AutoRun.gen	6,13%
6	Worm.VBS.Dinihou.r	5,95%
7	Virus.Win32.Sality.gen	4,94%
8	AdWare.Win32.BetterSurf.b	4,29%
9	AdWare.Win32.Yotoon.heur	4,01%
10	AdWare.Win32.Agent.aknu	3,64%
11	AdWare.Win32.Agent.aljb	3,57%
12	Worm.Win32.Debris.a	3,29%
13	AdWare.Win32.Skyli.a	2,90%
14	Trojan.Win32.Starter.lgb	2,74%
15	AdWare.Win32.Agent.heur	2,64%
16	AdWare.Win32.Agent.aljt	2,30%

17	Trojan.Win32.AntiFW.b	2,27%
18	AdWare.JS.MultiPlug.c	2,21%
19	Worm.Script.Generic	1,99%
20	Virus.Win32.Nimnul.a	1,89%

**Детектирующие вердикты модулей OAS и ODS антивируса, которые были предоставлены пользователями продуктов ЛК, 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, червям, распространяющимся на съемных носителях, и вирусам.

Доля вирусов в TOP 20 продолжает стабильно падать. Во втором квартале вирусы представлены вердиктами Virus.Win32.Sality.gen и Virus.Win32.Nimnul.a с общим показателем 6,83%, для сравнения в первом квартале этот показатель был 8%.

СТРАНЫ, В КОТОРЫХ КОМПЬЮТЕРЫ ПОЛЬЗОВАТЕЛЕЙ ПОДВЕРГАЛИСЬ НАИБОЛЬШЕМУ РИСКУ ЛОКАЛЬНОГО ЗАРАЖЕНИЯ

	СТРАНА	% УНИКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ*
1	Вьетнам	58,42%
2	Монголия	55,02%
3	Алжир	52,05%
4	Йемен	51,65%
5	Бангладеш	51,12%
6	Пакистан	50,69%
7	Непал	50,36%
8	Афганистан	50,06%
9	Ирак	49,92%
10	Египет	49,59%

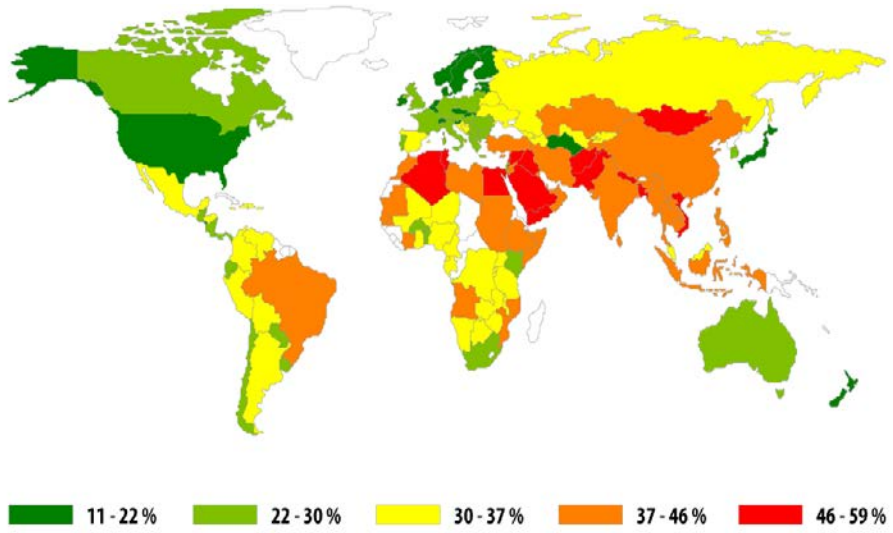
11	Тунис	46,75%
12	Сирия	46,29%
13	Саудовская Аравия	46,01%
14	Эфиопия	45,94%
15	Иран	45,40%
16	Лаос	45,20%
17	Турция	44,98%
18	Индия	44,73%
19	Камбоджа	44,53%
20	Джибути	44,52%

Настоящая статистика основана на детектирующих вердиктах модуля антивируса, которые были предоставлены пользователями продуктов ЛК, 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 (меньше 10 тысяч).*

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

Страны Африки, Ближнего Востока и Юго-Восточной Азии стабильно занимают все позиции в этом рейтинге. Как и в предыдущем квартале, лидирует в нем Вьетнам, Монголия осталась на втором месте. Непал опустился с третьего места на седьмое. Новички рейтинга Саудовская Аравия, Эфиопия, Турция. Выбыли Марокко, Мьянма, Судан.



В числе самых безопасных по уровню локального заражения стран Япония (11%), Швеция (13,8%), Дания (15,3%), Финляндия (16,4%), Сингапур (16,8%), Нидерланды (17,1%), Чехия (18,3%), Норвегия (19,1%), Гонконг (19,2%).

В среднем в мире хотя бы раз в течение года локальные угрозы были зафиксированы на 32,8% компьютеров пользователей.