РАЗВИТИЕ ИНФОРМАЦИОННЫХ УГРОЗ В ТРЕТЬЕМ КВАРТАЛЕ 2014 ГОДА

ДЭВИД ЭММ
МАРИЯ ГАРНАЕВА
ВИКТОР ЧЕБЫШЕВ
РОМАН УНУЧЕК
ДЕНИС МАКРУШИН
АНТОН ИВАНОВ

KASPERSKY lab

ОГЛАВЛЕНИЕ

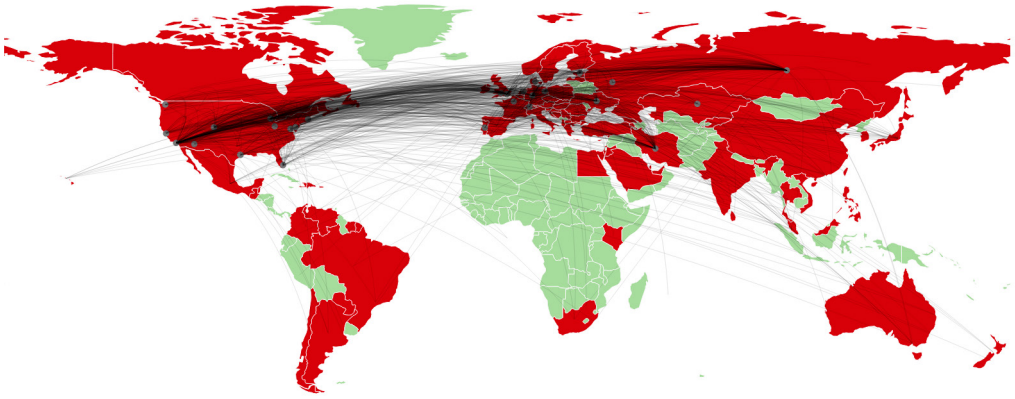
ОБЗОР СИТУАЦИИ

ЦЕЛЕВЫЕ АТАКИ И ВРЕДОНОСНЫЕ КАМПАНИИ

ПО СЛЕДУ ЙЕТИ

В июле мы опубликовали подробный анализ кампании по проведению целевых атак, которой мы дали название Crouching Yeti («крадущийся йети»). Эта кампания известна также под названием Energetic Bear («энергичный медведь»).

Эта кампания, которая активно ведется с конца 2010 года, нацелена на следующие секторы: энергетика/машиностроение, промышленность, фармацевтический сектор, строительство, образование и информационные технологии. Число жертв атак по всему миру превышает 2800; нам удалось выявить 101 атакованную организацию, в основном в США, Испании, Японии, Германии, Франции, Италии, Турции, Ирландии, Польше и Китае.



Если судить по списку жертв, злоумышленники, стоящие за Crouching Yeti, подбирают объекты для атаки, имеющие стратегическое значение. Однако выбор некоторых целей, атакованных группировкой, очевидным не назовешь.

В ходе атак группа Crouching Yeti применяет несколько видов вредоносных программ (все они предназначены для операционных систем семейства Windows), с помощью которых они проникают на компьютеры жертв, расширяют охват сети атакуемой организации, крадут конфиденциальные данные, в том числе интеллектуальную собственность и другую стратегически важную информацию. Зараженные компьютеры соединяются с большой сетью взломанных сайтов, используемой киберпреступниками для размещения вредоносных модулей, хранения информации о жертвах и отправки команд на зараженные системы.

Для заражения компьютеров жертв киберпреступники применяют три метода. Во-первых, они используют легитимные инсталляторы с внедренной в них вредоносной DLL-библиотекой. Такие модифицированные самораспаковывающиеся архивы могут загружаться непосредственно на взломанный сервер или отправляться одному из сотрудников атакуемой организации по электронной почте. Во-вторых, атакующие с помощью методов адресного фишинга доставляют на компьютеры жертв вредоносный файл XDP (XML Data Package), содержащий эксплойт для Flash (CVE-2011-0611). В-третьих, злоумышленники прибегают к атакам типа watering hole. На взломанных сайтах посетители с помощью нескольких эксплойтов (CVE-2013-2465, CVE-2013-1347 и CVE-2012-1723) перенаправляются на другие сайты, на которых киберпреступниками размещены вредоносные JAR или HTML-файлы. Термин watering hole (буквально – водопой) обозначает сайты, которые с высокой степенью вероятности посещают потенциальные жертвы. Злоумышленники заранее взламывают эти сайты, внедряя в них код, устанавливающий вредоносные программы на компьютеры всех посетителей взломанных ресурсов.

В состав троянца Havex – одной из вредоносных программ, применяемых киберпреступниками, – входят специальные модули для сбора данных в определенных промышленных IT-средах. Прежде всего это модуль OPC-сканера. Этот модуль предназначен для сбора чрезвычайно подробных данных об OPC-серверах, работающих в локальной сети. Серверы OPC (Object Linking and Embedding (OLE) for Process Control), как правило, используются там, где работают несколько автоматизированных систем управления. Вместе с данным модулем применяется

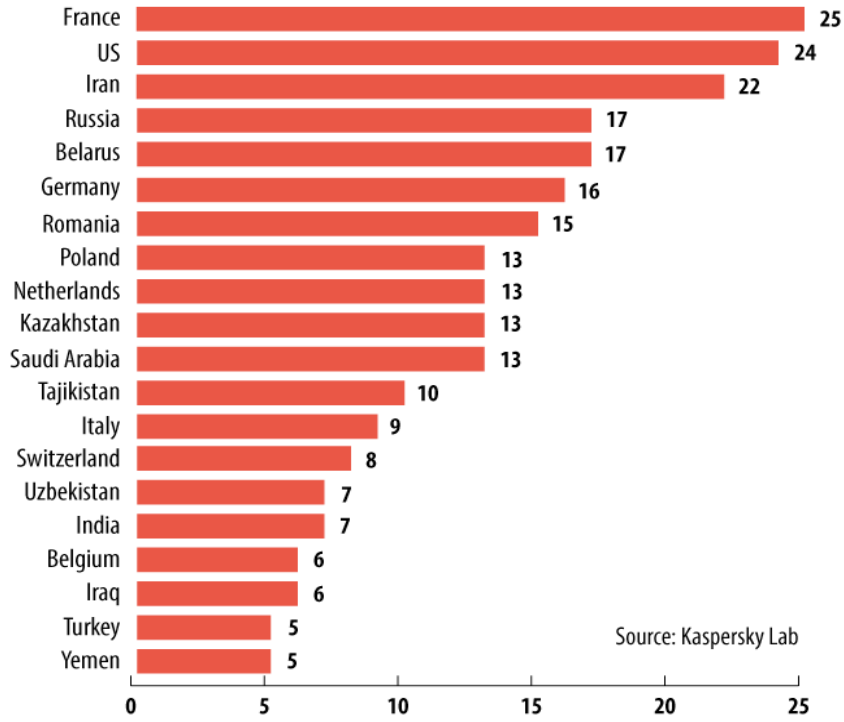
сканер сети, который сканирует локальную сеть в поисках компьютеров с открытыми портами, связанными с работой систем АСУ/SCADA (Supervisory Control and Data Acquisition), и пытается соединиться с этими хостами, чтобы определить систему АСУ/SCADA, которая, возможно, на них работает. Затем он передает все найденные данные на командные серверы, с помощью которых злоумышленники управляют вредоносной кампанией.

В процессе анализа кода мы искали признаки, по которым можно было бы идентифицировать злоумышленников.

Анализ временных меток в 154 файлах показал, что большинство образцов было скомпилировано между 06:00 и 16:00 часами UTC. Это может означать, что злоумышленники находятся в одной из стран Европы. Мы также обращали внимание на используемый киберпреступниками язык. Вредоносная программа содержит строки на английском языке (написанные людьми, для которых этот язык неродной). Некоторые признаки указывают на то, что члены группы, возможно, говорят по-французски или по-шведски. Однако в отличие от некоторых других исследователей, изучавших Crouching Yeti, мы не нашли ничего, что позволило бы нам сделать однозначный вывод о российском происхождении злоумышленников. Контент, написанный кириллицей (или транслитом) не был обнаружен в 200 вредоносных исполняемых файлах и в связанном с атакой дополнительном контенте, – в отличие от того, что мы находили в предыдущих кампаниях по проведению целевых атак, в том числе Red October, MiniDuke, CosmicDuke, Snake и TeamSpy.

EPIC TURLA: САГА О КИБЕРШПИОНАЖЕ

Уже больше года «Лаборатория Касперского» изучает сложную кампанию по кибершпионажу, которой мы присвоили название Epic Turla. Эта кампания, продолжающаяся с 2012 года, нацелена на государственные учреждения, посольства, военных, исследовательские центры, образовательные учреждения и фармацевтические компании. Большинство жертв находятся на Ближнем Востоке и в Европе, однако мы находили жертв атак и в других местах, в том числе США. В целом мы обнаружили несколько сотен принадлежащих жертвам IP-адресов более чем в 45 странах.



Операция Epic Turla: распределение IP жертв по странам (TOP 20)

На момент первой публикации материалов, связанных с нашим исследованием этой кампании, не было ясности относительно того, каким образом заражались компьютеры жертв атак. В нашем последнем исследовании, опубликованном в августе, мы описали механизмы заражения, примененные в Epic Turla, и их связь с общей структурой кампании.

Для заражения жертв киберпреступники используют приемы социальной инженерии – в частности, адресный фишинг и атаки типа watering hole.

В некоторые из электронных писем, отправляемых в рамках адресного фишинга, вложены эксплойты нулевого дня. Первый из них использует уязвимость в Adobe Acrobat Reader (CVE-2013-3346) и позволяет атакующим выполнять произвольный код на компьютере жертвы. Второй использует уязвимость в Windows XP и Windows Server 2003, связанную с

возможностью повышения привилегий (CVE-2013-5065), и обеспечивает бэкдору Epic Turla получение прав администратора на компьютере жертвы. Кроме того, злоумышленники обманным путем добиваются запуска жертвами инсталляторов вредоносного ПО – файлов с расширением .SCR, которые иногда к тому же упакованы в RAR-архив. Когда ничего не подозревающие жертвы открывают зараженный файл, на их компьютерах устанавливается бэкдор, предоставляя атакующим полный контроль над этими машинами.

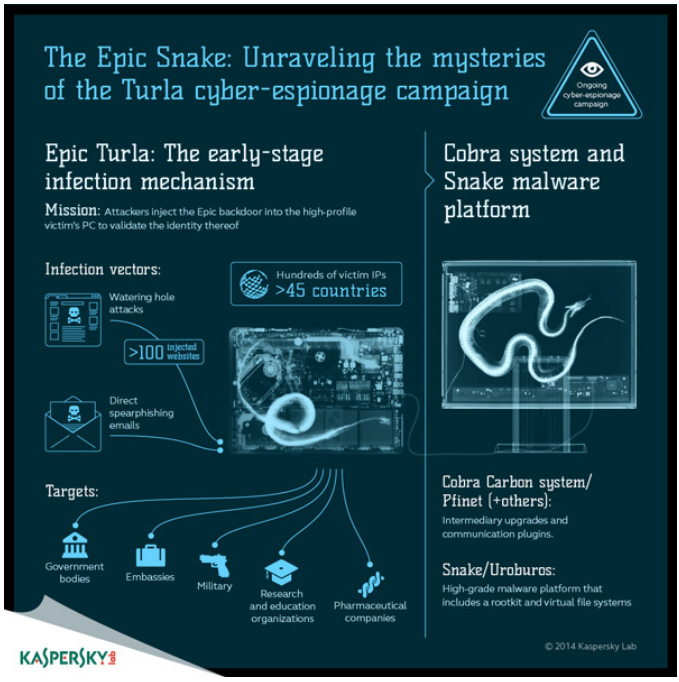
Организаторы кампании Epic Turla также используют атаки типа watering hole с применением Java-эксплойтов (CVE-2012-1723), эксплойтов для Adobe Flash и эксплойтов для Internet Explorer. Кроме того, применяются приемы социальной инженерии, с помощью которых жертв убеждают запустить вредоносные инсталляторы, выдаваемые за Flash Player. В зависимости от IP-адреса жертвы для заражения используются эксплойты для Java или браузера, подписанная фальшивая программа Adobe Flash Player или фальшивый вариант Microsoft Security Essentials. Нам удалось обнаружить более 100 сайтов с вредоносным кодом, внедренным киберпреступниками. Очевидно, что выбор сайтов отражает специфические интересы атакующих (и в той же степени интересы жертв). Например, многие из зараженных испанских сайтов принадлежат муниципальным властям.

Сразу же после заражения компьютера бэкдор Epic Turla (известный также под названиями WorldCupSec, TadjMakhal, Wipbot и Tadvig) устанавливает соединение с командным сервером и отправляет пакет данных о системе жертвы. Исходя из информации о системе, полученной командным сервером, злоумышленники отправляют на зараженную машину заранее подготовленный пакетный файл, содержащий набор команд, которые следует выполнить на данном компьютере. Атакующие также загружают на зараженный компьютер нестандартные инструменты для распространения по сети (в том числе специальный клавиатурный шпион и архиватор RAR), а также стандартные утилиты, такие как созданное Microsoft средство отправки запросов на DNS-серверы.

Наш анализ показал, что применение бэкдора Epic Turla – лишь первый этап многоступенчатого процесса заражения. С его помощью в систему устанавливается бэкдор с более сложным функционалом, известный как Cobra/Carbon system (в некоторых антивирусных продуктах он фигурирует под именем Pfinet). В какой-то момент злоумышленники сделали следующий шаг – использовали установленный в системе бэкдор Epic Turla для обновления конфигурационного

файла Carbon, прописав в нем новый набор командных серверов. То, что для управления работой обоих бэкдоров необходимо обладать одной и той же уникальной информацией, свидетельствует о наличии прямой связи между ними. Первый из них применяется для закрепления в системе и верификации высокого статуса жертвы. Если жертва действительно представляет интерес для атакующих, на взломанный компьютер устанавливается полнофункциональная система Carbon.

Вот обзор кампании по кибершпионажу Epic Turla:



Атрибуция подобных атак всегда связана с большими сложностями. Однако некоторые особенности кода позволяют получить определенную информацию о злоумышленниках. Очевидно, что английский язык для них не родной. Они часто делают ошибки в словах и фразах, например:

> ‘Password it’s wrong!’

> ‘File is not exists’

> ‘File is exists for edit’

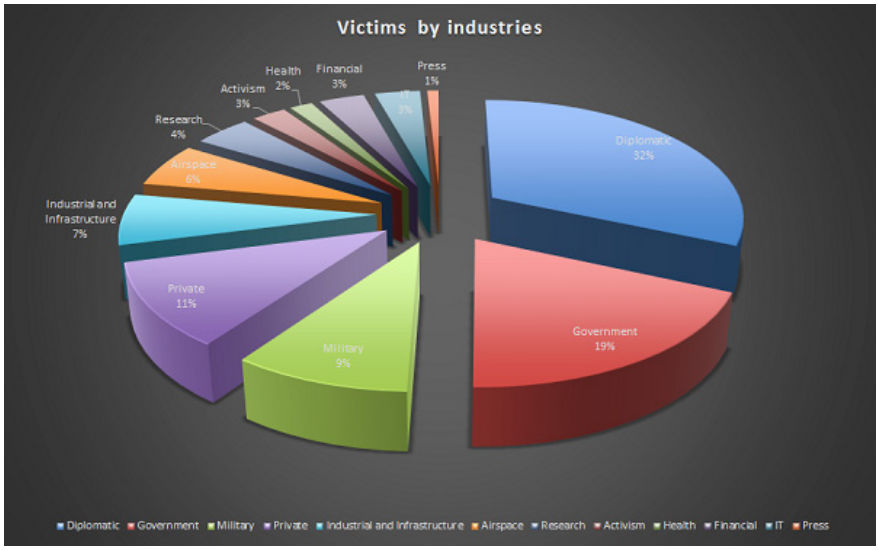
Есть и другие признаки, по которым можно догадаться о происхождении киберпреступников. Например, некоторые из бэкдоров скомпилированы на компьютере, на котором русский язык был установлен в качестве языка системы. Кроме того, во внутреннем имени одного из бэкдоров Epic Turla – «Zagruzchik.dll» – использовано русское слово «загрузчик». И наконец, в панели управления серверов – «баз» Epic Turla установлена кодовая страница 1251, которая предназначена для отображения кириллических символов.

NETTRAVELER: НОВАЯ ВЕРСИЯ КО ДНЮ РОЖДЕНИЯ

Об этой кампании целевых атак, которая идет вот уже 10 лет, мы писали несколько раз.

Ранее в этом году мы наблюдали рост числа атак на уйгурских и тибетских активистов с применением обновленной версии бэкдора NetTraveler. Злоумышленники использовали для привлечения жертв адресные фишинговые рассылки: в электронные письма вложен документ Microsoft Word, содержащий эксплойт для уязвимости CVE-2012-0158. Из документа распаковывается и устанавливается на компьютере главный модуль (net.exe), который, в свою очередь, устанавливает еще несколько файлов, в том числе главный командный модуль. Этот модуль с помощью пакетного файла dot.bat регистрируется в системе как служба (под именем Windowsupdata). Формат конфигурационного файла NetTraveler также обновлен: злоумышленники, очевидно, пытались скрыть конфигурацию вредоносной программы (однако примененный для этого шифр легко взломать).

Интересы киберпреступников постепенно менялись. На протяжении долгого времени в число основных целей NetTraveler входили дипломатические, правительственные и военные организации. Последнее время деятельность группы, связанная с кибершпионажем, нацелена прежде всего на космические исследования, нанотехнологии, производство энергии, ядерную энергетику, лазеры, медицину и связь.



Атаки на уйгурских и тибетских активистов остаются неизменной составляющей деятельности группы.

СИРИЙСКОЕ ВРЕДОНОСНОЕ ПО: «КАРТОЧНЫЙ ДОМИК»

Компьютерные технологии стали неотъемлемой частью нашей жизни, и нет ничего удивительного в том, что у вооруженных конфликтов по всему миру появилось «киберизмерение». Это особенно верно для Ближнего Востока, где геополитические конфликты стали в последние годы еще более напряженными. Глобальный центр исследований «Лаборатории Касперского» проанализировал недавнее усиление вредоносной активности в Сирии.

Организаторы этих атак прибегают к приемам социальной инженерии, чтобы убедить своих жертв открыть зараженные файлы. Распространение вредоносного кода осуществляется через электронные письма, сообщения в Skype, записи в Facebook и ролики на YouTube.

Злоумышленники пытаются «подцепить» пользователей на разнообразные «крючки», эксплуатируя доверие своих жертв к форумам в социальных сетях, их любопытство относительно новостей, связанных с сирийским конфликтом, их страх перед государственной машиной и невысокий уровень их технических знаний.

В качестве примера можно привести шокирующий ролик на YouTube, в котором показаны люди, раненные в недавних бомбежках. Зрителям ролика предлагается загрузить файл, размещенный на общедоступном файлообменном сайте (на деле этот файл является вредоносным). Кроме того, мы обнаружили набор сжатых файлов на сайте популярной социальной сети, который, как выяснилось после распаковки, содержал список активистов и разыскиваемых лиц в Сирии. Ссылка на загрузку этого приложения была размещена в информационном разделе видеоролика, опубликованного 9 ноября 2013 года. Киберпреступники используют для обмана своих жертв и фальшивые антивирусы – например, поддельную антивирусную программу под названием «Ammazon Internet Security», а также вариант легитимной утилиты для мониторинга сети Total Network Monitor с внедренной в нее троянской программой. Кроме фальшивых антивирусов, распространяются и фальшивые версии интернет-пейджеров Whatsapp и Viber.

При проведении кибератак применяются также несколько широко известных средств удаленного управления (RAT – Remote Administration Tools) – вредоносных программ, позволяющих удаленному «оператору» управлять работой взломанного компьютера так, как если бы у него был физический доступ к этому компьютеру. Эти инструменты широко применяются во всех видах кибератак – даже в некоторых атаках, поддерживаемых на государственном уровне. В число RAT, используемых в рамках этой компании, входят ShadowTech, Xtreme, NjRAT, Bitcoment, Dark Comet и Blackshades. Вредоносные программы ведут мониторинг активности жертв, собирают информацию и в некоторых случаях предпринимают попытки остановить их деятельность.

Жертвы таких атак находятся не только в Сирии. Атаки также зафиксированы в Турции, Саудовской Аравии, Ливане, Палестине, Объединенных Арабских Эмиратах, Израиле, Марокко, Франции и США.

Нам удалось определить адреса командных серверов киберпреступников, находящихся на территории Сирии, России, Ливана, США и Бразилии. В общей сложности мы обнаружили 110 файлов, 20 доменов и 47 IP-адресов, связанных с этими атаками.

За последний год число подобных атак заметно возросло. Очевидно, что осуществляющие их группы хорошо организованы. До сих пор атакующие применяли только существующее вредоносное ПО, а не создавали собственный вредоносный код (но при этом они используют

различные приемы обфускации для обхода сигнатурных методов обнаружения). По нашему мнению, вероятен дальнейший рост как числа, так и сложности вредоносного ПО, применяемого в регионе.

Полный отчет об этом вредоносном ПО можно найти здесь.

ИСТОРИИ О ЗЛОВРЕДАХ

БАНКОВСКИЙ ТРОЯНЕЦ SHYLOCK

В этом году «Лаборатория Касперского» внесла свою лепту в работу объединения правоохранительных и отраслевых организаций, координируемого британским Национальным агентством по правонарушениям (National Crime Agency, NCA), поучаствовав в прекращении работы инфраструктуры троянца Shylock. Вот хороший пример того, как международное сотрудничество в борьбе с киберпреступностью может принести положительные результаты.

Банковский троянец Shylock был стал известен в 2011 г. и получил свое название из-за того, что в нем содержатся отрывки из «Венецианского купца» Шекспира. Как и другие известные банковские троянцы – Zeus, SpyEye и Carberp – Shylock представляет собой атаку типа man-in-the-browser, предназначенную для кражи логинов и паролей к учетным записям клиентов онлайн-банкинга. Троянец использует заранее определенный список банков-жертв, расположенных в разных странах по всему миру.

Троянец вставляет поддельные поля для ввода данных в веб-страницы, загружаемые браузером на зараженном компьютере. Обманом пользователей заставляют запустить зловред, нажав на вредоносные ссылки. Затем Shylock пытается получить доступ к денежным средствам, находящимся на корпоративных или личных банковских счетах, и переводит их на счета, принадлежащие злоумышленникам.

Со временем география жертв киберпреступников менялась. Когда Shylock только появился, он был нацелен в первую очередь на пользователей в Великобритании; в течение 2012 г. троянец перекинулся на пользователей других европейских стран и США. К концу 2013 г.

интерес киберпреступников стал больше направлен на развивающиеся рынки, такие как Бразилия, Россия и Вьетнам. Дополнительная информация о географии жертв Shylock и о распространении троянце доступна здесь.

Все банковские троянцы, включая Shylock, нацелены на клиентов банков и созданы из расчета обмануть пользователя, который зачастую оказывается наименее защищенным звеном любой финансовой транзакции. Вот почему важно, чтобы безопасность начиналась дома: всем нам нужно эффективно защищать свои компьютеры.

КОШЕЛЕК ИЛИ ФАЙЛЫ!

Число программ-вымогателей в последние годы быстро росло; не все они были нацелены на компьютеры, работающие под Windows. Некоторые из них, в том числе направленные на Android-устройства, просто блокируют доступ к устройству и требуют выкуп за разблокирование устройства.

Однако многие программы-вымогатели идут дальше и шифруют данные на компьютере-жертве. Недавний пример – вымогатель ZeroLocker.

В отличие от большинства программ-вымогателей, которые шифруют типы файлов из заранее определенного списка, ZeroLocker шифрует почти все виды файлов на компьютере-жертве и добавляет к зашифрованным файлам расширение .encrypt. ZeroLocker не шифрует файлы, находящиеся в директориях, в названиях которых содержат слова Windows, WINDOWS, Program Files, ZeroLocker и Destroy, а также файлы размером более 20 Мб.

ZeroLocker генерирует 160-битный AES-ключ, которым и шифрует все файлы. Размер ключа несколько ограничен способом его генерации, но все же достаточен, чтобы подбор перебором оказался практически невозможным. После шифрования файлов зловред запускает утилиту cipher.exe, которая удаляет с диска все неиспользуемые данные, что значительно усложняет восстановление файла. Ключ шифрования вместе с CRC32-кодом MAC-адреса компьютера и номером связанного Bitcoin-кошелька отсылается на сервер, используемый злоумышленниками. Есть указания на то, что в конфигурации командного сервера есть

кое-какие ошибки, из-за которых успешная расшифровка может оказаться невозможной – еще один аргумент против того, чтобы платить выкуп, требуемый вымогателем.

Ключ шифрования вместе с прочей информацией отсылается через GET-запрос, а не через POST. Это приводит к ошибке 404 на сервере. Это может означать, что сервер не хранит информацию, т.е. жертвы, вероятно, не получат назад свои файлы, даже если выплатят выкуп.

Несколько других URL-ссылок, к которым пытается обратиться зловред, также приводят к ошибке 404. Это может означать, что данная операция еще недоработана киберпреступниками. Когда (и если) эти ошибки будут исправлены, киберпреступники могут задействовать ZeroLocker более широко.

За расшифровку файла киберпреступники, стоящие за ZeroLocker, первоначально требуют сумму в биткойнах, эквивалентную $300. Если жертва затягивает с платежом, сумма вырастает сначала до $500, а затем и до $1000.

В код зловреда жестко зашит номер кошелька Bitcoin, однако же зловред пытается загрузить с командного сервера новый адрес кошелька – вероятно, для того чтобы было сложнее отследить, насколько успешно проходит операция и куда уходят деньги. Из всех кошельков Bitcoin, адреса которых мы проверили, ни за одним не числилось никаких проведенных транзакций. Поскольку командный сервер предоставляет информацию о кошельке Bitcoin, возможно, злоумышленники используют уникальный кошелек для каждой жертвы.

Еще одна программа-вымогатель, недавно проанализированная нами – это Onion. Эта вредоносная программа использует проверенный на практике метод, используемый в последнее время и другими вымогателями – она шифрует данные пользователя и требует выкуп в биткойнах.

При этом в Onion используются и новые технологии. Во-первых, Onion использует анонимную сеть Tor, чтобы скрыть свои командные серверы. Таким образом оказывается сложнее отследить киберпреступников, стоящих за зловредом. В прошлом были и другие вредоносные программы, использовавшие Tor, но этот троянец стоит особняком, поскольку взаимодействует с Tor без всякого участия пользователя. Другие программы этого типа взаимодействуют с

сетью Tor, запуская легитимный файл tor.exe (иногда путем внедрения кода в другие процессы). У Onion, в отличие от них, весь код, необходимый для реализации общения с анонимной сетью, совмещен с вредоносным кодом.

Onion также использует необычный криптографический алгоритм, из-за которого расшифровка файла оказывается невозможной, даже если удается перехватить трафик между троянцем и командным сервером. Этот троянец не только использует асимметричное шифрование, но еще и использует криптографический протокол, известный как протокол Диффи-Хеллмана (Elliptic Curve Diffie-Hellman). Это делает расшифровку невозможной без личного мастер-ключа, который никогда не выходит за пределы сервера, контролируемого киберпреступниками. Подробности доступны в нашем отчете о троянце Onion.

Все перечисленные характеристики делают троянец Onion продвинутым с технической точки зрения, и очень опасным.

Киберпреступники рассчитывают на то, что жертвы выплатят требуемый выкуп. Не следует этого делать! Лучше регулярно создавайте резервные копии ваших данных. В этом случае, если однажды вы вдруг станете жертвой программы-вымогателя (или проблемы с «железом» лишат вас доступа к вашим данным), вы не потеряете ни байта из ваших данных.

ЗАЧЕМ ОДИН ИЗ НАШИХ СПЕЦИАЛИСТОВ ВЗЛОМАЛ СВОЙ СОБСТВЕННЫЙ ДОМ

Мы все теснее и теснее становимся связаны с интернетом– иногда в буквальном смысле: возможность присоединения к Сети внедрена в бытовые устройства. Это тенденция, известная под названием «интернет вещей», в последнее время привлекает все больше внимания по мере того, как хакеры и специалисты по IT-безопасности испытывают и ищут уязвимости в технологиях, встроенных в машины, внедренных в гостиницах, домашних системах тревожной сигнализации, холодильниках и т.п.

Иногда «интернет вещей» может показаться чем-то далеким, не имеющим отношения к реальной жизни. Однако он ближе, чем бы думаем. Очень вероятно, что в современном доме вы найдете несколько устройств, подсоединенных к локальной сети, и это будут не только

традиционные компьютеры, планшеты и сотовые телефоны, но и такие устройства, как Smart TV, принтер, игровая консоль, сетевой накопитель данных, медиа-плеер или спутниковый ресивер.

Один из наших специалистов по IT-безопасности – Дэвид Якоби – исследовал свой собственный дом на предмет его кибербезопасности. Он исследовал несколько устройств: сетевые накопители, Smart TV, маршрутизатор и спутниковый ресивер – и проверил, насколько они уязвимы при атаке. Результаты оказались ошеломляющие. Дэвид нашел 14 уязвимостей в сетевых накопителях, подключенных к сети, одну уязвимость в Smart TV и несколько скрытых функций в маршрутизаторе, которые можно использовать для удаленного контроля над устройством.

Наиболее серьезные уязвимости обнаружились в сетевых накопителях. Эксплуатируя некоторые из них, злоумышленник мог бы удаленно выполнить системные команды с высшими административными правами. Также оказалось, что на протестированных устройствах слабые пароли, установленные по умолчанию; пароли хранились открытым текстом; в конфигурационных файлах на устройствах оказались неправильно выставлены права доступа. Пароль администратора к одному из этих устройств состоял всего из одного знака! А другое устройство охотно делилось своим конфигурационным файлом, в котором содержались пароли в зашифрованном виде, с любым пользователем в сети!

Дэвиду также удалось загрузить файл в в файловой системе за пределами совместно используемых папок, то есть в ту область сетевого накопителя, которая недоступна обычному пользователю. Если злоумышленник загрузит вредоносный файл в эту область, то взломанное устройство станет источником заражения для других устройств, подключенных к накопителю (например для домашнего компьютера) и даже сможет функционировать как бот в составе ботнета, через который проводятся DDoS-атаки. В довершение всего выяснилось, что стереть такой файл можно, только воспользовавшись все той же уязвимостью, - а это непростая задача даже для технического специалиста.

Когда Дэвид исследовал свой Smart TV, он обнаружил, что он обменивается незашифрованными данными с серверами производителя, что потенциально открывает возможность для атаки типа man-in-the-middle (MITM); в результате может получится, что пользователь, сам того не подозревая, отправит деньги злоумышленникам, когда попытается купить контент, используя

Smart TV. Для подтверждения своей идеи Дэвид смог заменить одну из иконок в графическом интерфейсе телевизора на другую картинку. Обычно виджеты и пиктограммы скачиваются с серверов производителя ТВ, но поскольку данные при обмене не шифруются, в них может внести изменения третья сторона. Дэвид также обнаружил, что Smart TV может выполнять Java-код, что (учитывая возможность перехвата сетевого трафика) открывает возможность для проведения вредоносных атак с использованием эксплойтов.

Оказалось, что DSL-маршрутизатор, обеспечивающий беспроводное интернет-соединение для всех прочих домашних устройств, содержит несколько опасных функций, скрытых от владельца. Используя некоторые из этих функций, злоумышленник мог бы получить удаленный доступ к любому устройству, подключенному к частной домашней сети. Более того, разделы веб-интерфейса маршрутизатора под названиями Web Cameras (веб-камеры), Telephony Expert Configure (экспертная конфигурация телефонии), Access Control (управление доступом), WAN-Sensing (сбор данных о территориально-распределенной сети) и Update (обновление) являются невидимыми, и владелец устройства не может внести в них изменения. Попасть в них можно только используя довольно типичную уязвимость, которая позволяет перемещаться между разделами интерфейса (которые в основном являются веб-страницами, каждая со своим текстовыми адресом, состоящим из букв и цифр), с помощью грубого подбора цифр в конце адреса. Изначально эти функции были включены в интерфейс для удобства владельца устройства: функция удаленного доступа позволяет интернет-провайдеру легко и быстро диагностировать и исправлять технические проблемы на устройстве. Однако эта удобная функция может обернуться угрозой безопасности, если контроль над устройством попадет в чужие руки.

«Лаборатория Касперского» придерживается политики ответственного раскрытия информации и потому не раскрывает производителей устройств, которые были протестированы в ходе этого исследования. Мы связались со всеми производителями и сообщили им о существовании уязвимостей, и специалисты «Лаборатории Касперского» тесно сотрудничают с представителями производителей устройств, помогая в устранении обнаруженных уязвимостей.

Всем нам важно понимать потенциальные риски, связанные с использованием сетевых устройств, – они актуальны и для частных пользователей, и для компаний. Нужно также понимать, что сильные пароли и ПО, защищающее от вредоносных программ, еще не гарантируют полной безопасности личной информации. Есть еще много вещей, которые мы

не контролируем; в некотором смысле, мы находимся в руках производителей устройств и ПО. К примеру, не во всех устройствах есть автоматическая проверка на наличие обновлений, и пользователи сами должны скачивать новые версии прошивки и устанавливать их, и это не всегда просто. Еще хуже то, что не всегда возможно обновить устройство: во время исследования оказалось, что поддержка большей части исследованных устройств прекращена более года назад.

Некоторые советы о том, как снизить риски атаки, доступны в обзоре Дэвида Якоби.

ВЕБ-БЕЗОПАСНОСТЬ И ВЗЛОМ ДАННЫХ: SHELLSHOCK

В сентябре в сообществе IT-безопасности был объявлен высший уровень тревоги: была выявлена уязвимость Bash (также известная как ShellShock). Bash – это командная оболочка Unix, написанная в 1989 г.; в Linux и Mac OS X используется как командная оболочка «по умолчанию». Уязвимость (CVE-2014-6271) позволяет злоумышленнику удаленно прикрепить к переменной вредоносный файл, который выполняется при вызове командного интерпретатора Bash. Очень серьезный характер данной уязвимости в сочетании с тем, что ее исключительно легко эксплуатировать, делает ее очень опасной. Некоторые сравнивают ее с уязвимостью Heartbleed. Однако Bash по сравнению с Heartbleed эксплуатируется гораздо легче; еще одно отличие состоит в том, что Heartbleed позволял злоумышленникам только красть данные из памяти уязвимого компьютера, а ShellShock мог обеспечить полный контроль над системой.

Злоумышленники не долго думали, как использовать эту уязвимость – мы уже разбирали первые случаи ее эксплуатации вскоре после обнаружения. В большинстве случаев злоумышленники удаленно атаковали веб-сервисы на которых размещены CGI-скрипты, которые написанные в Bash или передают значения скриптам, написанным в Bash. Однако может оказаться, что уязвимость может влиять и на инфраструктуру на основе Windows.

Ни та, ни другая проблема не ограничиваются веб-серверами. Bash широко используется в прошивках популярных устройств, которые мы используем каждый день: маршрутизаторов, домашних устройств, беспроводных точек доступа и т.д. Как уже было сказано, некоторые из них может быть сложно или даже невозможно перепрошить.

Инструкции о том, как обновить уязвимые системы, доступны здесь.

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.

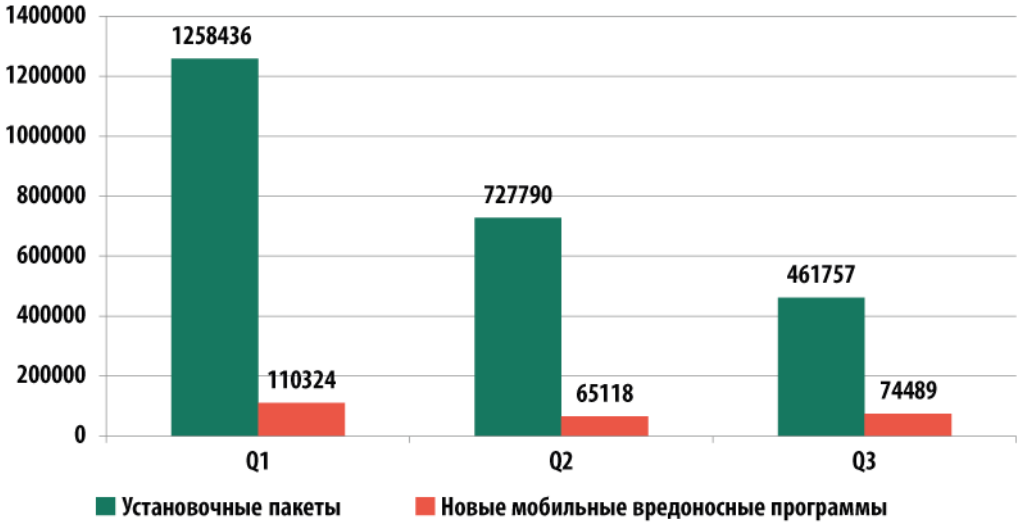
ЦИФРЫ КВАРТАЛА

- По данным KSN, в третьем квартале 2014 года продукты «Лаборатории Касперского» заблокировали 1 325 106 041 вредоносную атаку на компьютерах и мобильных устройствах пользователей.
- Решения «Лаборатории Касперского» отразили 367 431 148 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира.
- Нашим веб-антивирусом задетектировано 26 641 747 уникальных вредоносных объектов (скрипты, веб-страницы, эксплойты, исполняемые файлы и т.д.).
- Зафиксировано 107 215 793 уникальных URL, на которых происходило срабатывание веб-антивируса.
- Треть (33%) всех веб-атак, заблокированных нашими продуктами, проводились с использованием вредоносных веб-ресурсов, расположенных в США.
- Нашим файловым антивирусом зафиксировано 116 710 804 уникальных вредоносных и потенциально нежелательных объектов.
- Продуктами «Лаборатории Касперского» для защиты мобильных устройств было обнаружено:
  - 461 757 установочных пакетов;
  - 74 489 новых мобильных вредоносных программ;
  - 7 010 мобильных банковских троянцев.

МОБИЛЬНЫЕ УГРОЗЫ

В третьем квартале 2014 года продуктами «Лаборатории Касперского» для защиты мобильных устройств было обнаружено 74 489 новых мобильных вредоносных программ на 14,4% больше, чем во втором.

При этом уменьшилось количество обнаруженных вредоносных установочных пакетов.

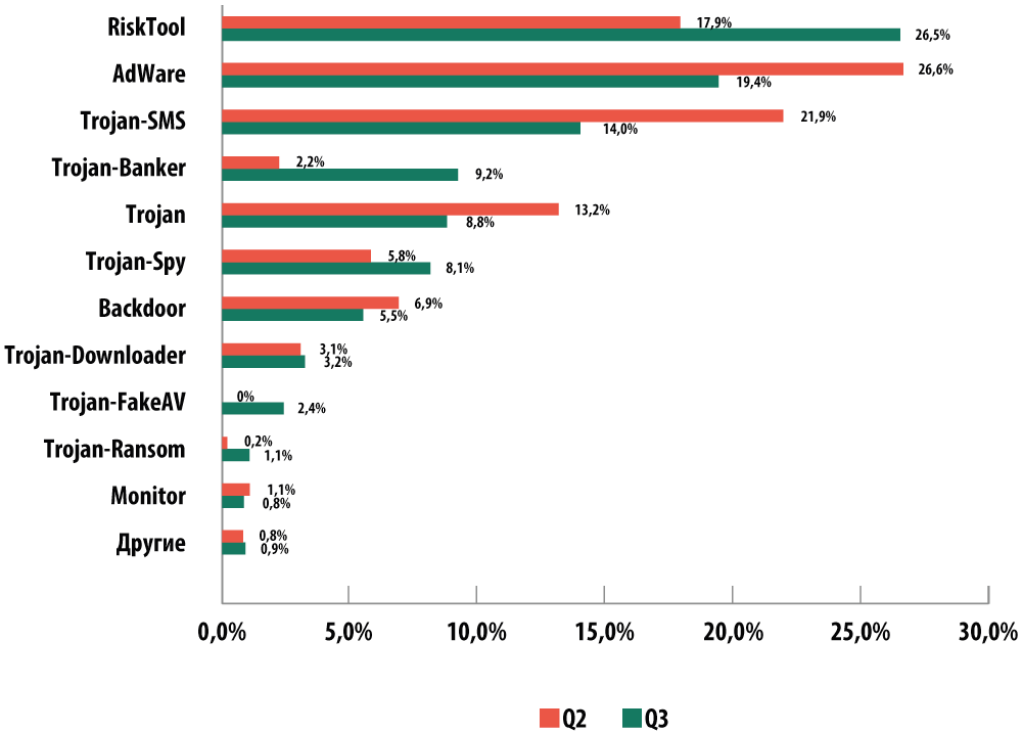


Количество обнаруженных вредоносных установочных пакетов и новых мобильных вредоносных программ (Q1 – Q3 2014 года)

Если в первом полугодии 2014 года на каждую вредоносную программу в среднем приходилось чуть более 11-ти вредоносных установочных пакетов, то в третьем квартале – всего 6,2.

Использование множества установочных пакетов для одной мобильной вредоносной программы характерно для распространителей SMS-троянцев. Например, для одной версии Stealer.a злоумышленники могут использовать до 70 000 пакетов. Вероятно, уменьшение количества вредоносных установочных пакетов связано с тем, что доля таких зловредов в потоке новых мобильных вредоносных программ уменьшилась (см. ниже).

РАСПРЕДЕЛЕНИЕ ПО ТИПАМ МОБИЛЬНЫХ ЗЛОВРЕДОВ



Распределение по типам мобильных зловредов, второй и третий квартал 2014 года

В рейтинге обнаруженных в третьем квартале вредоносных объектов для мобильных устройств по итогам квартала лидируют Risktool, их показатель увеличился на 8,6 процентных пунктов (п.п.) и достиг 26,5%. Это легальные приложения, которые потенциально опасны для пользователей – их неаккуратное использование владельцем смартфона или злоумышленником может привести к финансовым потерям.

На втором месте – Adware, потенциально нежелательные рекламные приложения (19,4%). Доля таких программ уменьшилась на 7,9 п.п.

SMS-троянцы оказались на третьем месте, их доля среди всех мобильных угроз по сравнению с предыдущим кварталом также уменьшилась на 7,2 п.п.

Отметим, что в третьем квартале в потоке нового мобильного вредоносного ПО на фоне уменьшения процента рекламных программ и SMS-троянцев выросла доля мобильных банковских троянцев с 2,2% до 9,2%. Эта категория зловредов оказалась на четвертом месте в рейтинге.

ТОР 20 МОБИЛЬНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

	НАЗВАНИЕ	% АТАК*
1	Trojan-SMS.AndroidOS.Stealer.a	15,63%
2	RiskTool.AndroidOS.SMSreg.gc	14,17%
3	AdWare.AndroidOS.Viser.a	10,76%
4	Trojan-SMS.AndroidOS.FakeInst.fb	7,35%
5	RiskTool.AndroidOS.CallPay.a	4,95%
6	Exploit.AndroidOS.Lotoor.be	3,97%
7	DangerousObject.Multi.Generic	3,94%
8	RiskTool.AndroidOS.MimobSMS.a	3,94%
9	Trojan-SMS.AndroidOS.Agent.ao	2,78%
10	AdWare.AndroidOS.Ganlet.a	2,51%
11	Trojan-SMS.AndroidOS.OpFake.a	2,50%
12	RiskTool.AndroidOS.SMSreg.de	2,36%
13	Trojan-SMS.AndroidOS.FakeInst.ff	2,14%
14	Trojan-SMS.AndroidOS.Podec.a	2,05%
15	Trojan-SMS.AndroidOS.Erop.a	1,53%
16	RiskTool.AndroidOS.NeoSMS.a	1,50%
17	Trojan.AndroidOS.Agent.p	1,47%
18	Trojan-SMS.AndroidOS.OpFake.bo	1,29%
19	RiskTool.AndroidOS.SMSreg.hg	1,19%
20	Trojan-Ransom.AndroidOS.Small.e	1,17%

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

В ТОР 20 детектируемых угроз SMS-троянцы теряют позиции: если во втором квартале они занимали пятнадцать строчек рейтинга, то в третьем – всего восемь. В прошлом квартале

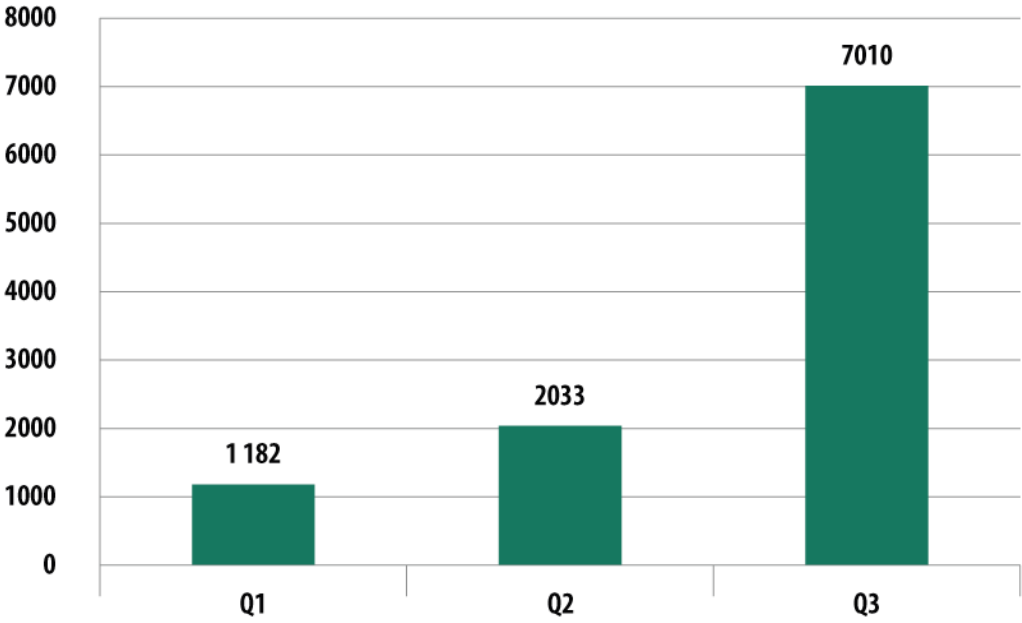
показатель лидера рейтинга Trojan-SMS.AndroidOS.Stealer.a составил 25,42% всех атак, в этом на него пришлось всего 15,63%.

Представили RiskTool заняли в TOP 20 шесть позиций. В том числе вторую, где расположился RiskTool.AndroidOS.SMSreg.gc, на долю которого пришлось 14,17% всех атак.

На 7-м месте в рейтинге DangerousObject.Multi.Generic (3,94%). Так новые вредоносные приложения детектируются облачными технологиями Kaspersky Security Network, которые позволяет нашему продукту быстро реагировать на новые и неизвестные угрозы.

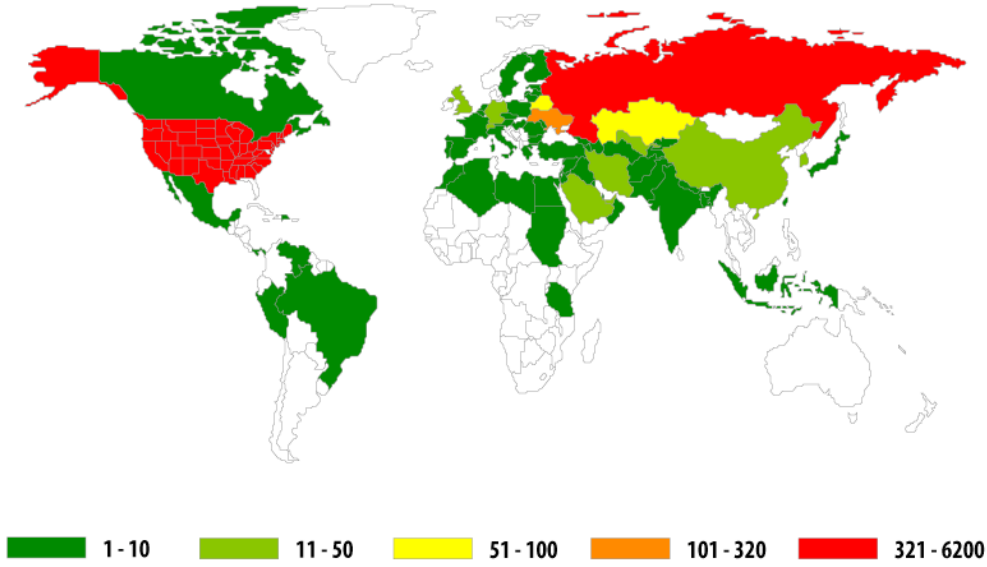
МОБИЛЬНЫЕ БАНКОВСКИЕ ТРОЯНЦЫ

За отчетный период мы обнаружили 7 010 мобильных банковских троянцев – в 3,4 раза больше, чем в предыдущем квартале.



Количество обнаруженных мобильных банковских троянцев (Q1 – Q3 2014)

Растет и количество атакованных стран: если во втором квартале атаки мобильных банковских троянцев хотя бы раз были зафиксированы в 31-й стране, то в третьем квартале – в 70-ти странах мира.



География мобильных банковских угроз в третьем квартале 2014 года

(количество атакованных пользователей)

ТОП 10 СТРАН, АТАКУЕМЫХ БАНКОВСКИМИ ТРОЯНЦАМИ:

	СТРАНА	% ОТ ВСЕХ АТАК*
1	Россия	83,85%
2	США	7,09%
3	Украина	1,79%
4	Белоруссия	1,18%
5	Казахстан	0,92%
6	Республика Корея	0,68%
7	Германия	0,62%
8	Китай	0,50%

9	Великобритания	0,50%
10	Саудовская Аравия	0,35%

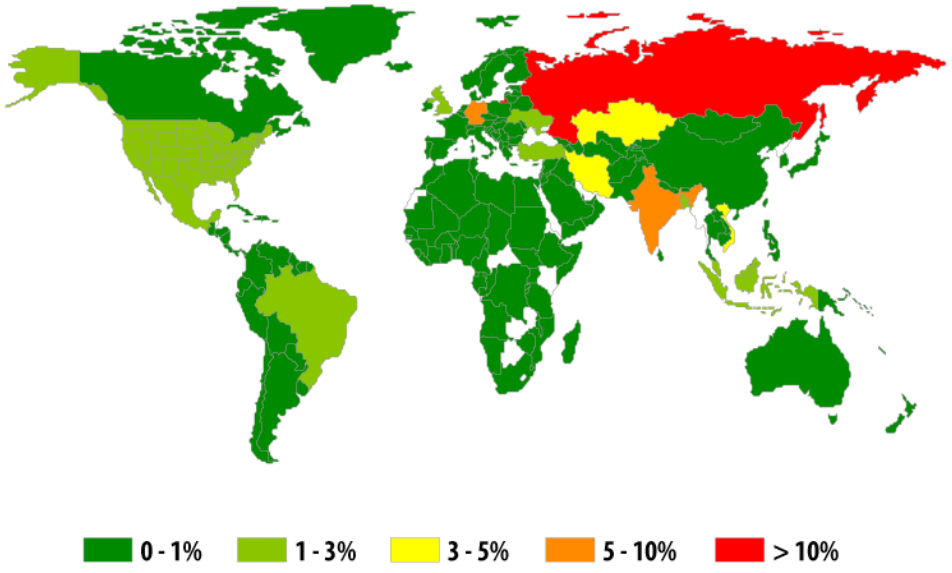
** Процент пользователей, атакованных в стране, по отношению ко всем атакованным пользователям*

Из TOP 10 выбыла Италия, на 10-м месте оказалась Саудовская Аравия.

Традиционным лидером этого рейтинга остается Россия, однако ее показатель уменьшился на 7,85 п.п. В то же время показатели других стран из TOP 10 немного увеличились: мобильный киберкриминал постепенно расширяет ареал своей активности.

ГЕОГРАФИЯ МОБИЛЬНЫХ УГРОЗ

В течение третьего квартала атаки мобильных вредоносных программ хотя бы раз были зафиксированы в 205 странах мира.



Карта попыток заражений мобильными зловредами в третьем квартале 2014 года

(процент от всех атакованных пользователей)

ТОР 10 АТАКУЕМЫХ СТРАН:

	СТРАНА	% АТАК*
1	Россия	44,0%
2	Индия	7,6%
3	Германия	5,6%
4	Иран	3,4%
5	Вьетнам	3,1%
6	Казахстан	3,1%
7	Украина	2,7%
8	Малайзия	1,9%
9	Бразилия	1,7%
10	США	1,7%

** Процент пользователей, атакованных в стране, по отношению ко всем атакованным пользователям*

Лидером этого рейтинга с большим отрывом от остальных стран остается Россия (44%). На второе место вернулась Индия (7,6%). Впервые в 2014 году в рейтинг попали Иран (3,4%) и США (1,7%). Выбыли из первой десятки Польша, Франция, Испания и Мексика.

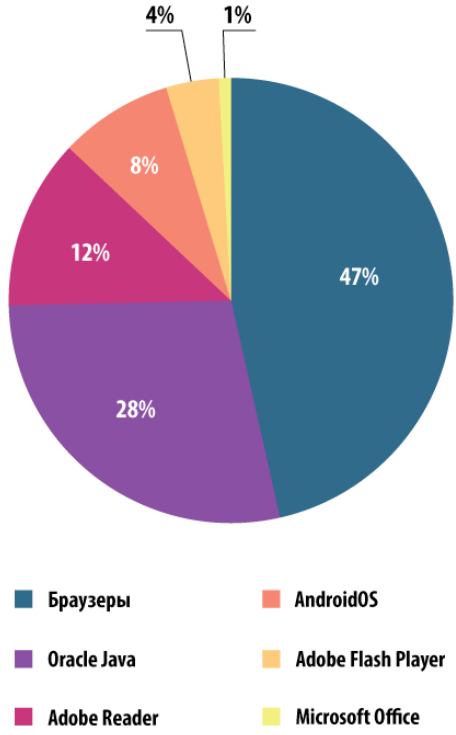
УЯЗВИМЫЕ ПРИЛОЖЕНИЯ, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКАМИ

Приведенный ниже рейтинг уязвимых приложений 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.

Из всех зафиксированных нами попыток эксплуатации уязвимостей 47% пришлось на эксплойты к уязвимостям в браузерах, в первую очередь в Internet Explorer – эксплойт для него присутствует почти в каждом эксплойт-паке.

На втором месте находятся Java-эксплойты, уязвимости для которых эксплуатируются в ходе drive-by атак через интернет. Java-эксплойты входят в состав множества эксплойт-паков, хотя вот уже год не было информации о новых уязвимостях в Java. В третьем квартале доля Java-эксплойтов составила 28%, что немного меньше показателя второго квартала (29%).

На третьем месте расположились эксплойты для уязвимостей в Adobe Reader (12%). Такие уязвимости также эксплуатируются в ходе drive-by атак через интернет, и PDF-эксплойты входят в состав множества эксплойт-паков.



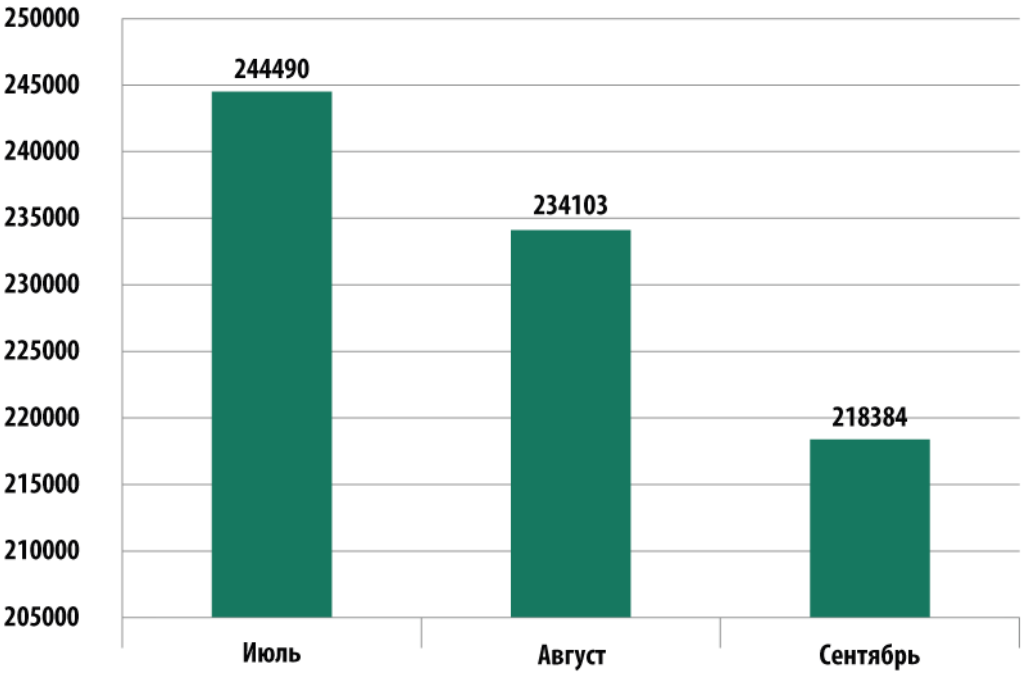
Распределение эксплойтов, использованных в атаках злоумышленников, по типам атакуемых приложений, третий квартал 2014 года

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

В третьем квартале 2014 года решения «Лаборатории Касперского» отразили попытки запуска вредоносного ПО для кражи денежных средств через онлайн-доступ к банковским счетам на компьютерах 696 977 пользователей. По сравнению с предыдущим отчетным периодом (927 568) данный показатель уменьшился на 24,9%.

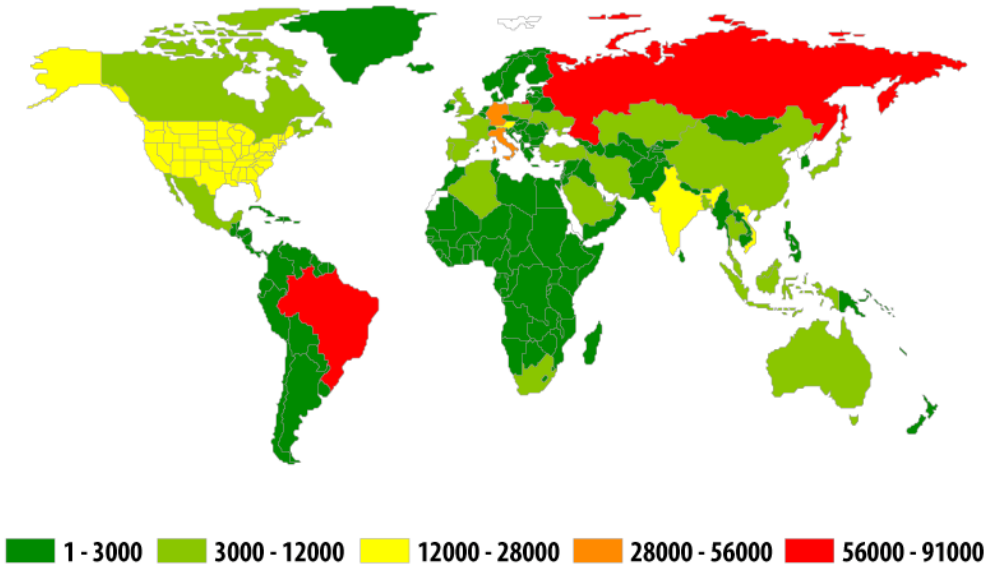


Число компьютеров, атакованных финансовым вредоносным ПО, третий квартал 2014 года

Отметим, что количество атак постепенно уменьшалось в течение квартала – если в июле было зафиксировано 244 490 атак, то в сентябре – уже 218 384 атак, на 11% меньше.

Всего защитными продуктами «Лаборатории Касперского» было зарегистрировано 2 466 952 уведомлений о попытках заражения вредоносными программами, предназначенными для кражи денежных средств через онлайн-доступ к банковским счетам.

ГЕОГРАФИЯ АТАК



География атак банковского вредоносного ПО, третий квартал 2014 года

ТОП-10 СТРАН ПО ЧИСЛУ АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ

СТРАНЫ	КОЛИЧЕСТВО АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ
Бразилия	90176
Россия	57729
Германия	55225
Италия	32529
Индия	24975
США	22340
Австрия	22013
Вьетнам	13495
Великобритания	11095
Китай	9060

Бразилия по-прежнему лидирует среди самых атакуемых стран, хотя по сравнению с предыдущим кварталом ее показатель снизился более чем в 1,5 раза. Второе место по-прежнему занимает Россия. Италия опустилась на 4-ую позицию в нашем списке. Третье место заняла Германия количество атакованных пользователей в этой стране выросло в 1,5 раза.

ТОП-10 СЕМЕЙСТВ БАНКОВСКОГО ВРЕДОНОСНОГО ПО

TOP 10 семейств вредоносных программ, использованных для атак на пользователей онлайн-банкинга в третьем квартале 2014 года (по количеству уведомлений о попытках заражения и по количеству атакованных пользователей):

НАЗВАНИЕ	КОЛИЧЕСТВО НОТИФИКАЦИЙ	КОЛИЧЕСТВО АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ
Trojan-Spy.Win32.Zbot	1381762	285559
Trojan-Banker.Win32.ChePro	322928	92415
Trojan-Banker.Win32.Shiotob	123150	24839
Trojan-Banker.Win32.Agent	49563	23943
Trojan-Banker.HTML.PayPal	117692	21138
Trojan-Spy.Win32.SpyEyes	73496	19113
Trojan-Banker.Win32.Lohmys	47188	16619
Trojan-Banker.Win32.Banker	39892	12673
Trojan-Banker.Win32.Banbra	20563	9646
Backdoor.Win32.Sinowal	18921	8189

Самым распространенным банковским троянцем по-прежнему остается ZeuS (Trojan-Spy. Win32.Zbot), хотя количество атак с использованием этого зловреда, равно как и количество атакованных пользователей, уменьшилось почти в два раза по сравнению с предыдущим кварталом.

В третьем квартале на третьем месте в этом рейтинге оказался банковский троянец Trojan-Banker.Win32.Shiotob, который распространяется преимущественно посредством спам-сообщений и осуществляет мониторинг трафика с целью перехвата платежных данных.

Подавляющее большинство зловредов (9 из 10) из TOP-10 используют технику внедрения произвольного HTML-кода в отображаемую браузером веб-страницу и перехвата платежных данных, вводимых пользовтелем в оригинальные и вставленные веб-формы.

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

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

третий квартал 2014 года

Второй по популярности угрозой является похищение Bitcoin-кошельков – популярность этого способа заработка у злоумышленников выросла с 8% во втором квартале до 15% в третьем. Еще одна угроза, связанная с криптовалютой, - Bitcoin-майнинг (11%), т.е. использование компьютера жертвы для генерации биткойнов.

ТОР 20 ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ В ИНТЕРНЕТЕ

Во третьем квартале 2014 года нашим веб-антивирусом было задетектировано 26 641 747 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 20 наиболее активных. На них пришлось 96,2% всех атак в интернете.

ТОР 20 ДЕТЕКТИРУЕМЫХ ОБЪЕКТОВ В ИНТЕРНЕТЕ

	НАЗВАНИЕ*	% ОТ ВСЕХ АТАК**
1	Malicious URL	59,83%
2	AdWare.Script.Generic	14,46%
3	Trojan.Script.Generic	13,13%
4	Trojan.Script.Iframer	1,77%
5	AdWare.Win32.Agent.fflm	1,23%
6	Trojan-Downloader.Script.Generic	1,02%
7	AdWare.Win32.Agent.allm	1,02%
8	AdWare.JS.Agent.ao	0,78%
9	AdWare.JS.Agent.an	0,55%
10	AdWare.Win32.Agent.aiyc	0,32%
11	AdWare.Win32.OutBrowse.g	0,32%
12	Trojan.Win32.Generic	0,30%
13	AdWare.Win32.Amonetize.bcw	0,23%
14	AdWare.Win32.Amonetize.cmg	0,18%
15	AdWare.Win32.Yotoon.heur	0,18%
16	Trojan-Downloader.Win32.Generic	0,15%
17	AdWare.Win32.Amonetize.cmd	0,14%
18	Trojan-Dropper.Win32.Agent.lefs	0,12%
19	AdWare.Win32.Linkun.j	0,11%
20	AdWare.Win32.Amonetize.aik	0,09%

** 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.*

Как и прежде, в TOP 20 по большей части представлены вердикты, которые присваиваются объектам, использующимся в drive-by атаках, а также рекламным программам. 59,8% всех срабатываний веб-антивируса пришлись на ссылки из черного списка.

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).

Распределение по странам источников веб-атак, третий квартал 2014 года

В третьем квартале 2014 года решения «Лаборатории Касперского» отразили 367 431 148 атак, проводившихся с интернет-ресурсов, размещенных в разных странах мира. 87% нотификаций о заблокированных веб-атаках были получены при блокировании атак с веб-ресурсов, расположенных в десяти странах мира. Это на 1,3 п.п. меньше, чем в предыдущем квартале.

В третьем квартале изменился состав десятки стран-лидеров: TOP 10 покинули Канада (-7 п.п.) и Ирландия (-0,7 п.п.). Китай, который не попадал в TOP со второго квартала 2013 года, вновь оказался в десятке с показателем 1,87% на 7-м месте. Впервые в TOP 10 фигурирует Швейцария (1,03%).

Наиболее значительно среди стран-лидеров изменились показатели США (+11,2 п.п.), занявших первую строчку рейтинга, и Германии (-9 п.п.), которая сместилась с первого на третье место.

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	46,68%
2	Казахстан	45,92%
3	Азербайджан	43,50%
4	Армения	41,64%
5	Украина	40,70%
6	Иран	39,91%
7	Вьетнам	38,55%
8	Белоруссия	38,08%
9	Молдавия	36,64%
10	Алжир	36,05%
11	Таджикистан	36,05%
12	Киргизия	33,59%
13	Монголия	33,59%
14	Катар	30,84%

15	Узбекистан	29,22%
16	Грузия	29,17%
17	Турция	28,91%
18	ОАЭ	28,76%
19	Индонезия	28,59%
20	Германия	28,36%

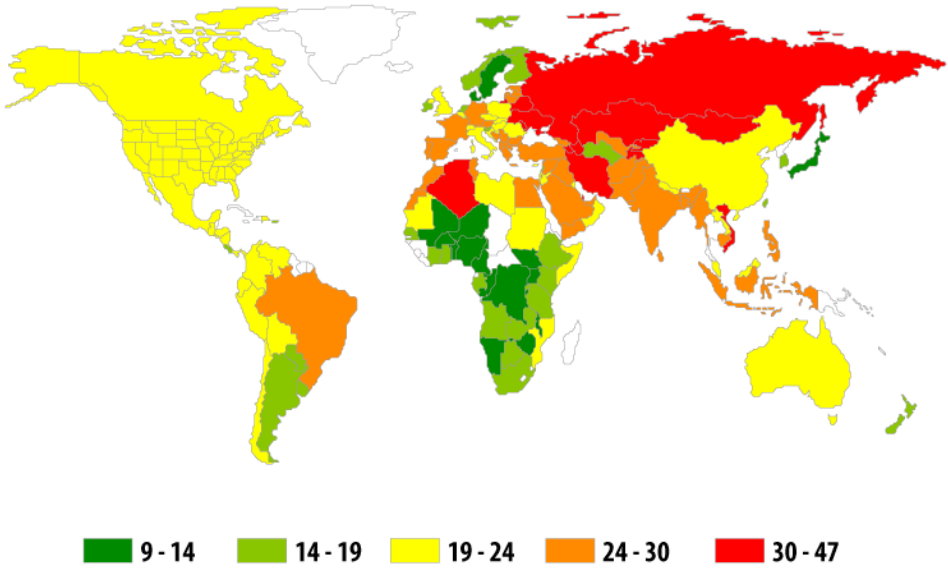
Настоящая статистика основана на детектирующих вердиктах модуля веб-антивируса, которые были предоставлены пользователями продуктов ЛК, подтвердившими свое согласие на передачу статистических данных.

**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.*

В третьем квартале 2014 года из TOP 20 выбыли Хорватия, Тунис и Испания. Новички рейтинга – ОАЭ (28,76%), Индонезия (28,59%) и Германия (28,36%), которые заняли три последние позиции в топе.

В числе самых безопасных при серфинге в интернете стран – Швеция (12,4%), Дания (13,2%), Япония (13,3%), ЮАР (16,0%), Финляндия (16,1%), Нидерланды (16,6%).



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

ЛОКАЛЬНЫЕ УГРОЗЫ

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.

В третьем квартале 2014 года нашим файловым антивирусом было зафиксировано 116 710 804 уникальных вредоносных и потенциально нежелательных объектов.

ДЕТЕКТИРУЕМЫЕ ОБЪЕКТЫ, ОБНАРУЖЕННЫЕ НА КОМПЬЮТЕРАХ ПОЛЬЗОВАТЕЛЕЙ: TOP 20

	НАЗВАНИЕ*	% УНИКАЛЬНЫХ АТАКОВАННЫХ ПОЛЬЗОВАТЕЛЕЙ**
1	Trojan.Win32.Generic	18,95%
2	DangerousObject.Multi.Generic	18,39%
3	AdWare.MSIL.Kranet.heur	11,61%
4	AdWare.Win32.Agent.ahbx	5,77%
5	Trojan.Win32.AutoRun.gen	4,81%
6	AdWare.Win32.Kranet.heur	4,68%
7	AdWare.NSIS.Zaitu.heur	4,51%
8	Worm.VBS.Dinihou.r	4,51%
9	Virus.Win32.Sality.gen	4,08%
10	AdWare.Win32.Yotoon.abs	4,03%
11	AdWare.Win32.IBryte.dolh	3,14%

12	AdWare.Win32.Agent.aljt	3,12%
13	AdWare.Win32.Agent.allm	3,11%
14	AdWare.Win32.Yotoon.heur	3,10%
15	Adware.Win32.Amonetize.heur	2,86%
16	AdWare.Win32.Agent.heur	2,80%
17	WebToolbar.JS.Condonit.a	2,59%
18	Worm.Win32.Debris.a	2,56%
19	AdWare.Win32.Kranet.c	2,55%
20	Trojan.Script.Generic	2,51%

**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 большинство мест занимают рекламные программы – на этот раз они заняли 13 мест в TOP 20.

Черви, распространяющиеся на съемных носителях, заняли два места в рейтинге – 8-е и 18-е.

Единственный оставшийся в топе вирус - Virus.Win32.Sality.gen – занял в третьем квартале 9-е место.

Отметим, что в третьем квартале значительно возросло число детектирования файловым антивирусом рекламных программ и их компонентов, которые участвуют в активном распространении этих программ и в противодействии детектированию антивирусами.

СТРАНЫ, В КОТОРЫХ КОМПЬЮТЕРЫ ПОЛЬЗОВАТЕЛЕЙ ПОДВЕРГАЛИСЬ НАИБОЛЬШЕМУ РИСКУ ЛОКАЛЬНОГО ЗАРАЖЕНИЯ

	СТРАНА*	% УНИКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ**
1	Вьетнам	61,89%
2	Бангладеш	55,01%
3	Монголия	54,13%
4	Непал	53,08%
5	Алжир	51,71%
6	Камбоджа	51,26%
7	Афганистан	50,59%
8	Лаос	50,55%
9	Йемен	50,38%
10	Пакистан	50,35%
11	Египет	49,65%
12	Индия	49,44%
13	Ирак	49,33%
14	Иран	48,85%
15	Эфиопия	47,87%
16	Мьянма	46,71%
17	Шри-Ланка	46,67%
18	Сирия	46,24%
19	Катар	46,03%
20	Тунис	45,36%

Настоящая статистика основана на детектирующих вердиктах модулей OAS и ODS 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).*

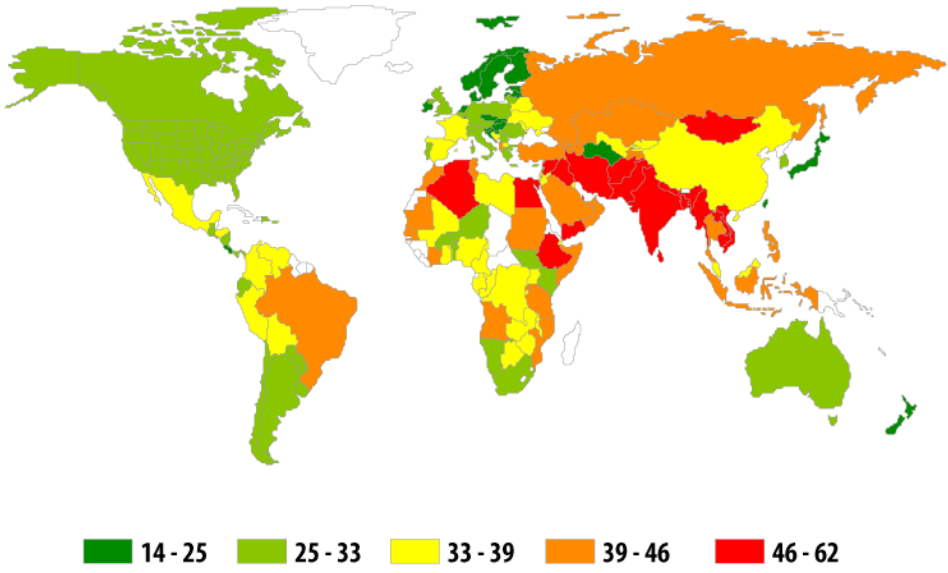
*** Процент уникальных пользователей, на компьютерах которых были заблокированы локальные угрозы, от всех уникальных пользователей продуктов ЛК в стране.*

Страны Африки, Ближнего Востока и Юго-Восточной Азии стабильно занимают все позиции в этом рейтинге. Как и в предыдущем квартале, лидирует в нем Вьетнам (61,89%).

Монголия (54,13%) опустилась на третье место, уступив вторую строчку рейтинга Бангладеш (55,01%).

Впервые в TOP 20 попал Катар (46,03%). Вновь вернулись в рейтинг Мьянма (46,71%) и Шри-Ланка (46,67%). Выбыли из TOP 20 Саудовская Аравия, Турция и Джибути.

В России в третьем квартале локальные угрозы были обнаружены на компьютерах 44,4% пользователей.



В числе самых безопасных по уровню локального заражения стран: Япония (15%), Швеция (16,4%), Дания (16,5%), Финляндия (18%), Сингапур (19,7%).

В среднем в мире хотя бы раз в течение третьего квартала локальные угрозы были зафиксированы на 37,2% компьютеров пользователей – это на 4,4 п.п. больше, чем во втором квартале.