



Количество случаев мошенничества при расчетах в Интернете увеличилось в 3 раза в 2012 г.

Количество случаев мошенничества при расчетах в сети Интернет, по словам эксперта, увеличилось в три раза по сравнению с 2011 годом, тогда как уровень мошенничества при расчетах картой в торгово-сервисных предприятиях существенно уменьшился. Об этом сообщила на пресс-конференции руководитель Форума безопасности расчетов и операций с платежными картами ЕМА Олеся Данильченко, сообщает корреспондент IT Expert.

В 2012 году было выявлено 80 устройств или следов от установки устройств на банкоматах и терминалах для скимминга, которые позволяют мошенникам считывать данные с банковской карты, тогда как годом ранее их было выявлено 45. Полученную информацию мошенники используют для изготовления поддельных карт, с помощью которых они могут снимать средства со счетов клиентов банков.

По словам г-жи Данильченко, в странах Европы в минувшем году одно выявленное скимминговое устройство приносило на 500 банкоматов, в Украине – в среднем 1,5 устройства/на 10 тыс. банкоматов.

Источник: <http://itexpert.org.ua>

Oracle: мы исправим Java и станем более открытыми

Милтон Смит, менеджер Oracle по безопасности Java, пообещал, что в корпорации исправят дефекты языка программирования, часто обнаруживаемые в последнее время. На телефонном совещании с лидерами группы Java User Group он также заявил, что впредь в Oracle будут более широко освещать работу над платформой. По сведениям Смита, большинство недавно найденных дефектов в Java — это бреши уровня браузеров, и в первую очередь будет решаться именно эта проблема.

Oracle часто критикуют за скрытность по поводу всего, что касается работы над Java. Смит заверил, что теперь ситуация изменится. В частности, планируется обеспечить распространение сведений среди всех заинтересованных, от простых пользователей до сисадминов и программистов. По словам Смита, пока не решено, как именно этого добиться, но вероятно, увеличится число докладов на отраслевых мероприятиях и объем общения с прессой.

Возможно также, Oracle станет предоставлять новости о безопасности Java лидерам Java User Group, а те будут делиться с остальными. По утверждению Смита, недавно Oracle внесла «очень важные» улучшения безопасности в Java для блокирования эксплойтов без внешних признаков деятельности, однако «эти особенности людям еще непонятны».

Источник: <http://www.osp.ru>

Самая большая угроза для кибербезопасности – персонал

Хотя DDoS-атаки хакерских группировок типа Anonymous и внедрение вирусов вроде Stuxnet, время от времени и появляются в заголовках, ИТ-эксперты считают, что наиболее серьезные угрозы для организации связаны с неосведомленностью самих сотрудников. Это подтвердило новое исследование сообщества профессионалов в области информационных технологий Wisegate: кибербезопасность организации страдает в первую очередь от неконтролируемого распространения и использования ИТ-ресурсов сотрудниками компании, включая мобильные устройства, приложения и сервисы.

При подготовке своего доклада Wisegate организовало дискуссию среди членов сообщества, работающих в различных отраслях промышленности для того, чтобы получить из первых рук рекомендации для исправления ситуации. Ниже приведены некоторые из угроз, которые, как ожидает сообщество, будут продолжать вносить вклад в эту проблему в 2013 году

1. Хотя ответственные за безопасность в компаниях достаточно продолжительное время предупреждали об опасности использования BYOD (Bring Your Own Device, «принеси на работу свое устройство»), все больше и больше людей используют свои персональные мобильные компьютеры на рабочем месте. В Wisegate признают, что работники могут быть более эффективными, если используют свои собственные устройства, но отмечают при этом, что персонал не предпринимает надлежащих мер обеспечения безопасности и таким образом делает первый шаг к нарушению целостности данных.

2. Социальные медиа. Чем больше сотрудников используют инструменты социальных медиа, таких как Facebook, Twitter и LinkedIn, чтобы пообщаться с клиентами, тем больше внимания должно уделяться развитию и укреплению формальных политик с целью избежать попадания в чужие руки конфиденциальной или частной информации.

3. «Бытовые» приложения. В дополнение к BYOD и социальным средствам массовой информации, персонал все чаще применяет приложения, предназначенные для бытового использования, для бизнеса. Например, работники не используют выделенный FTP-сервер их компании для отправки больших файлов по электронной почте, с большей охотой обращаясь к облачным хранилищами данных вроде Dropbox.

4. Понимание важности ИТ-безопасности. Согласно отчету, принявшие участие в исследовании сказали, что они сталкивались с проблемами, когда дело доходило до осознания сотрудниками важности практик ИТ-безопасности. Появление более удобных для пользователей онлайн-инструментов сделало эту работу еще более сложной для менеджеров ИТ-безопасности.

5. Облачные вычисления. В то время как «облака» позволили многим организациям избавиться от бремени хранения больших объемов данных, они в то же время усложнили ситуацию с точки зрения безопасности и надежности. Многие члены сообщества говорят, что компании принимают решение использовать облачную платформу без надлежащего взвешивания всех рисков.

6. Защита данных. Сутью ИТ-безопасности каждой организации является обеспечение защиты данных, но по мере того, как в компании теряется контроль над многими из вышеупомянутых ресурсов, используемых сотрудниками, эта задача становится все более трудной.

«Последний доклад Wisegate свидетельствует о важности и трудности решения вопросов безопасности, а также о том, что средний пользователь компьютера стал легкой добычей для кибер-преступников», - сказала Сара Гейтс (Sara Gates), основатель и генеральный директор Wisegate.

Источник: <http://www.securityinfowatch.ru>

Eurograbber ограбил европейцев на 36 миллионов евро

Группа мошенников, которая распространяла банковский троян **Eurograbber**, поставила новый рекорд по объему средств, изъятых у жителей Западной Европы. По информации из нового отчета, опубликованного компаниями **Versafe** и **Check Point Software Technologies**, ущерб от этой вредоносной программы оценивается в сумму около 36 миллионов евро, а количество пострадавших — примерно в 30 000 человек.

Eurograbber — один из вариантов известного трояна **Zeus**, а точнее — модифицированная версия трояна **ZITMO (Zeus in the mobile)**, мобильной версии зловред. Она оптимизирована на обход двухфакторной аутентификации, которая используется в ряде банков. Это осуществляется за счет перехвата одноразовым номером, отправляемым банком на мобильный телефон по **SMS**, которые нужно вводить для подтверждения финансовых транзакций на веб-сайте онлайн-банкинга. Как можно понять, троян успешно проделывал это, заразив предварительно и персональный компьютер, и смартфон жертвы. После заражения персонального компьютера он никак себя не проявлял до тех пор, пока не установит программу-«компаньона» на мобильное устройство.

Заражение смартфона осуществлялось через сайт онлайн-банкинга, куда троян внедрял **JavaScript** с сообщением о необходимости программы осуществить «апгрейд для безопасности», запрашивал версию мобильной ОС (**Android**, **BlackBerry**, **iOS**, **Symbian** или другая) и номер телефона. Информация, собранная у всех жертв, сохранялась на предварительно взломанном веб-сайте, в так называемой дроп-зоне. После этого на известный номер телефона высылались SMS с просьбой завершить апгрейд, перейдя по ссылке.

Скачив и установив файл, жертва завершала процедуру установки трояна.

Eurograbber угрожал клиентам 16 банков Италии, 7 банков Испании, 6 банков Германии и 3 банков Нидерландов. Специалисты предупреждают, что иные варианты Eurograbber могли применяться и за пределами Евросоюза. Перевод средств с банковских счетов осуществлялся в автоматическом режиме, когда пользователь заходил на сайт онлайн-банкинга, суммы ущерба варьируются от 500 евро до 223 тысяч евро на одного человека.

Источник: <http://www.truehackers.ru>

Сервис верификации Android пропускает 85% вредоносного ПО

С новой версией **Android 4.2 (Jelly Bean)** 13 ноября 2012 года компания Google представила замечательный сервис верификации устанавливаемых приложений. Смысл в том, что при установке программы хэш SHA1 бинарника отправляется для проверки на сервер верификации Google, вместе с информацией об источнике установки и некоторыми другими данными. Проверяются программы и из каталога Google Play, и со сторонних сайтов.

Это делается автоматически для каждого приложения, настройка активирована по умолчанию в меню Settings > Security > Verify apps. В случае обнаружения опасности Google может предупредить пользователя об угрозе или полностью блокировать установку.

К сожалению, независимое исследование показывает, что эффективность работы сервиса верификации крайне мала. Во время эксперимента сервис проверили на базе из 1260 вредоносных программ от 49 различных семейств. В результате, Google смог предупредить об опасности только в 193 случаях. Получается, что эффективность его работы составляет 15,32%. Если считать по распознаванию семейств зловредов, эффективность равняется 20,41%. Для сравнения, у обычных антивирусов различных компаний процент распознавания варьируется от 51,02% до 100%.

Исследователи обращают внимание, что Google не использует для верификации программ антивирусный сервис VirusTotal, который она купила в сентябре 2012 года.

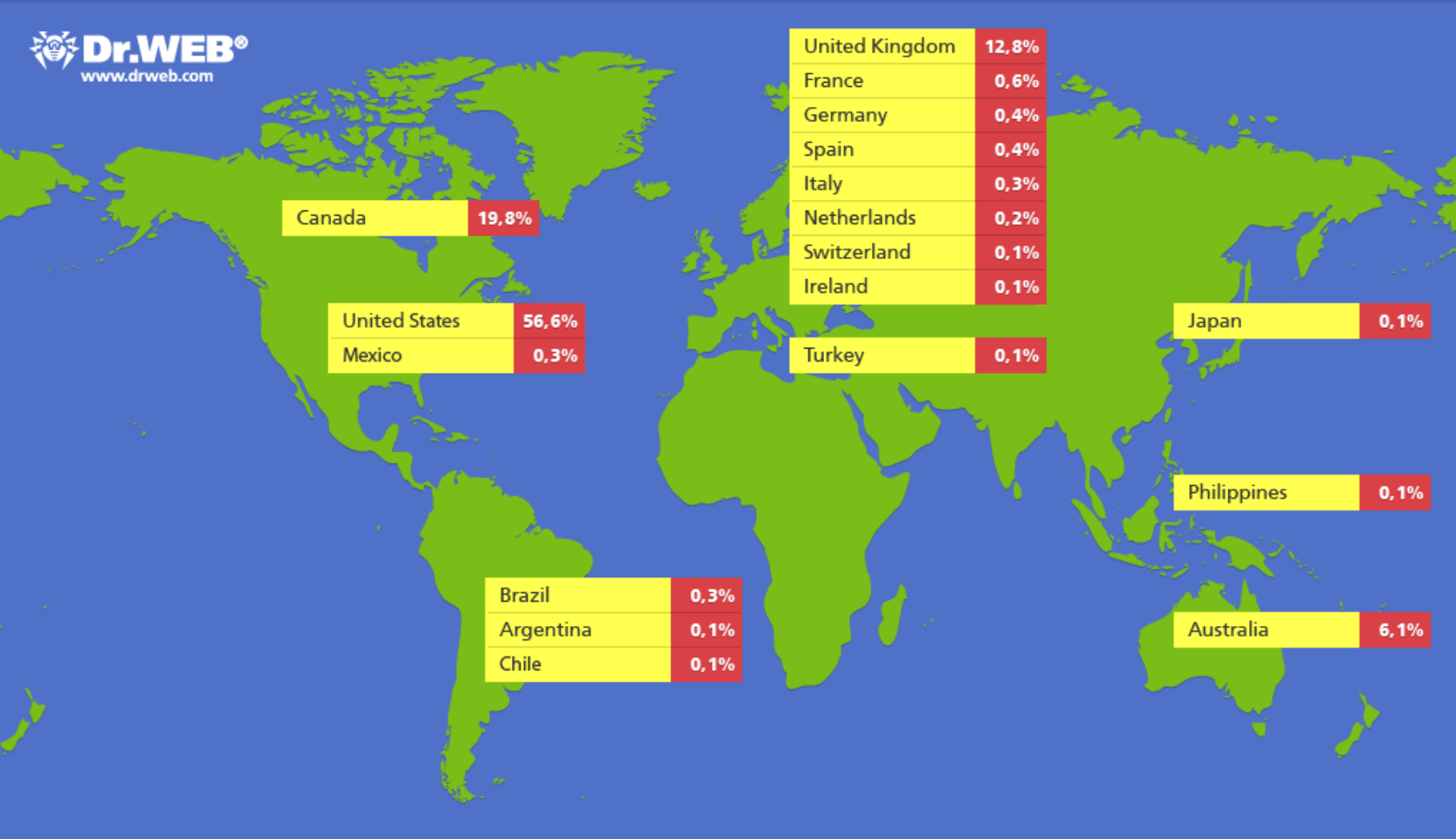
Источник: <http://www.truehackers.ru>

Нас читают многие.

**Мы можем
рассказать и о Вас.**

Компания «Доктор Веб» представляет обзор вирусной активности в 2012 году. Прошедший год запомнится, прежде всего, крупнейшей в истории эпидемией троянской программы [Backdoor.Flashback.39](#) для «маков». Это событие всколыхнуло мировую общественность и во многом подорвало веру пользователей в «непогрешимость» операционной системы от Apple. Кроме того, за прошедшие двенадцать месяцев значительно выросло количество разновидностей троянцев-энкодеров, а также число заражений этими вредоносными программами. Одна из крупнейших на сегодняшний день бот-сетей, состоящая из персональных компьютеров, инфицированных файловым вирусом [Win32.Rmnet.12](#), превысила рекордную шестимиллионную отметку. К сожалению, значительно возросло разнообразие угроз для мобильной платформы Google Android.

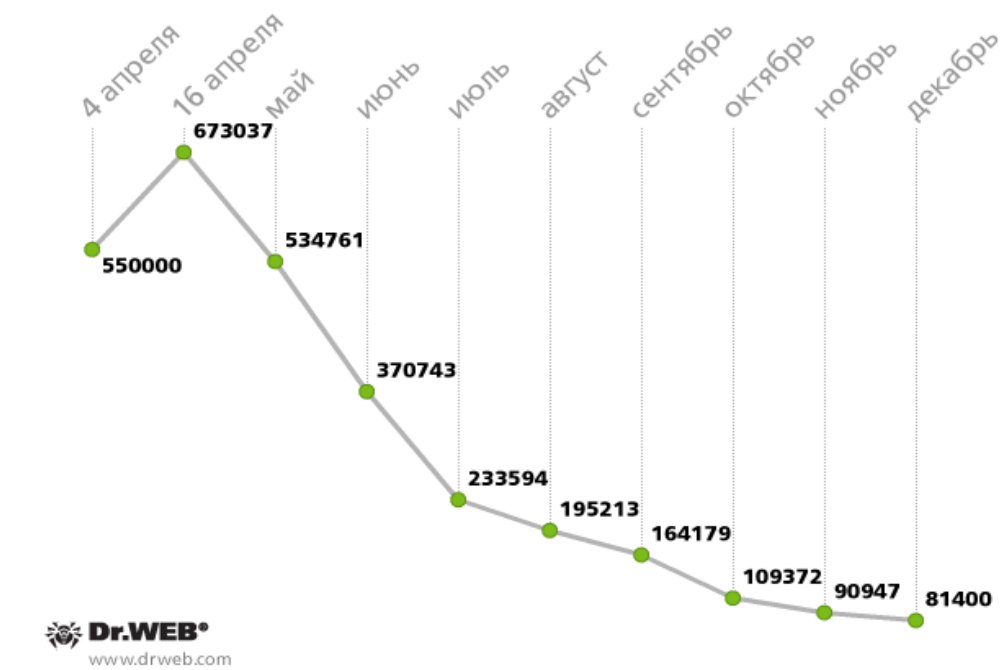
Крупнейший ботнет для Mac OS X
Появление троянской программы [Backdoor.Flashback.39](#), из-за которой разразилась самая настоящая эпидемия среди Apple-совместимых компьютеров, можно назвать, пожалуй, самым ярким событием 2012 года в сфере информационной безопасности. Впервые это вредоносное ПО было обнаружено специалистами компании «Доктор Веб» еще в конце марта 2012 года, а информационное сообщение о выявлении крупнейшего в истории ботнета, работающего под управлением Mac OS X, было опубликовано 4 апреля. Еще в конце марта в вирусную лабораторию стали поступать сообщения о распространении троянцев для Mac OS X с использованием уязвимости Java, именно тогда и возникло предположение о том, что [Backdoor.Flashback.39](#) способен объединять «маки» в бот-сети. Аналитики «Доктор Веб» изучили алгоритм, используемый этим троянцем для генерации имен управляющих серверов, и зарегистрировали несколько таких имен. Результат превзошел все ожидания: уже в первые сутки стало понятно, что количество зараженных «маков» превысило 600 000 и продолжает стремительно расти. География распространения инфекции также была весьма обширной:



География распространения [Backdoor.Flashback.39](#)

За последующие 10 дней размер бот-сети достиг максимальной отметки в 670 000 с лишним одновременно работающих инфицированных компьютеров (более 800 000 уникальных компьютеров с учетом «излечившихся») и постепенно пошел на спад. Опубликованный компанией «Доктор Веб» пресс-релиз с описанием данной угрозы наделал много шума в мировой прессе и вызвал широчайший общественный резонанс.

Динамика изменения численности бот-сети Backdoor.Flashback.39 в 2012 году



Миф о том, что Mac OS X является одной из самых защищенных операционных систем в мире, был в одночасье разрушен.

Основной причиной эпидемии стало то обстоятельство, что корпорация Apple выпустила обновление безопасности для собственной реализации Java спустя два месяца после аналогичного обновления, опубликованного корпорацией Oracle, что позволило злоумышленникам безнаказанно распространять вредоносное ПО в течение длительного времени. Другая причина — это, безусловно, слепая вера пользователей продукции Apple в абсолютную защищенность платформы Mac OS X: в пользу этого суждения говорил, в частности, тот факт, что число инфицированных «маков» продолжало увеличиваться даже после того, как компания «Доктор Веб» сообщила на весь мир об этой угрозе.

Исследования, проведенные аналитиками компании «Доктор Веб», позволили определить версии платформы Mac OS X, которые инфицировала вредоносная программа, версии ядра ОС, а также ряд других характеристик ботнета, исходя из анализа обращений этой вредоносной программы к управляющим серверам. Результаты этих исследований по данным на апрель 2012 года показаны на представленных ниже иллюстрациях (**Приложение 1**).

В декабре 2012 года рост бот-сети [Backdoor.Flashback.39](#) практически полностью остановился, однако окончательно она не побеждена — во всем мире еще насчитывается несколько десятков тысяч инфицированных «маков».

Поскольку популярность системной платформы от Apple постепенно растет, а пользователи этой ОС не привыкли использовать антивирусное программное обеспечение, Mac OS X становится лакомым куском для многочисленных злоумышленников. Вряд ли среднестатистический правонарушитель пройдет мимо богато обставленной квартиры, хозяева которой по идеологическим соображениям не желают запирать входную дверь на замок.

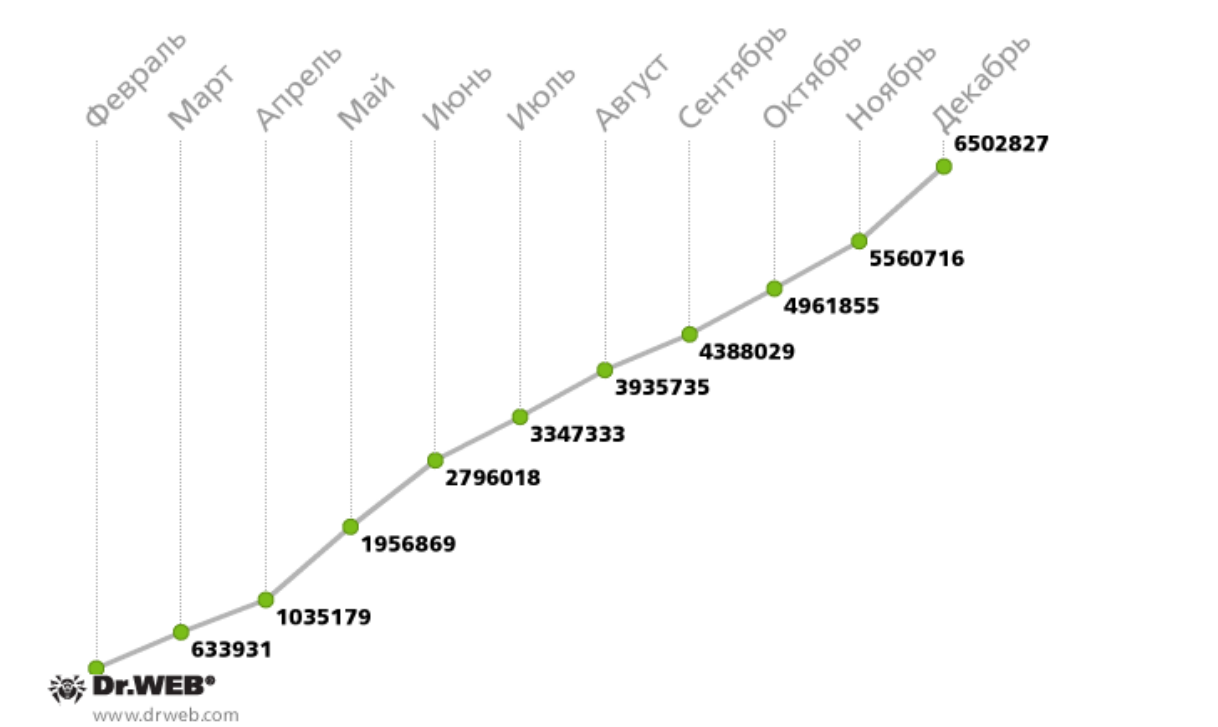
Файловые вирусы и другие ботнеты

Файловый вирус [Win32.Rmnet.12](#), сигнатура которого была добавлена в вирусные базы Dr.Web в сентябре 2011 года, за истекшие 12 месяцев побил все мыслимые рекорды, образовав бот-сеть, состоящую из **шести с половиной миллионов инфицированных узлов**. [Win32.Rmnet.12](#) — сложный многокомпонентный файловый вирус, состоящий из нескольких модулей и обладающий способностью к саморазмножению, то есть, он умеет копировать сам себя и бесконтрольно распространяться без участия пользователя. Этот вирус заражает ПК на базе Microsoft Windows, реализуя функции бэкдора, а также осуществляя кражу паролей от популярных FTP-клиентов, — эти пароли могут быть использованы для организации сетевых атак. Обработывая поступающие от удаленного центра злоумышленников указания, [Win32.Rmnet.12](#) также может дать команду и на уничтожение операционной системы. Его вредоносный функционал позволяет встраивать в просматриваемые веб-страницы посторонний контент (веб-инъекты), перенаправлять пользователя на указанные злоумышленниками сайты, а также передавать на удаленные узлы содержимое заполняемых жертвой форм. Вот почему этот вирус представляет существенную опасность для пользователей.

Наибольшее распространение данный вирус получил в странах юго-восточной Азии, таких как Индонезия, Бангладеш, Вьетнам, Индия и Пакистан. Однако имеется значительное число инфицированных машин и в России.

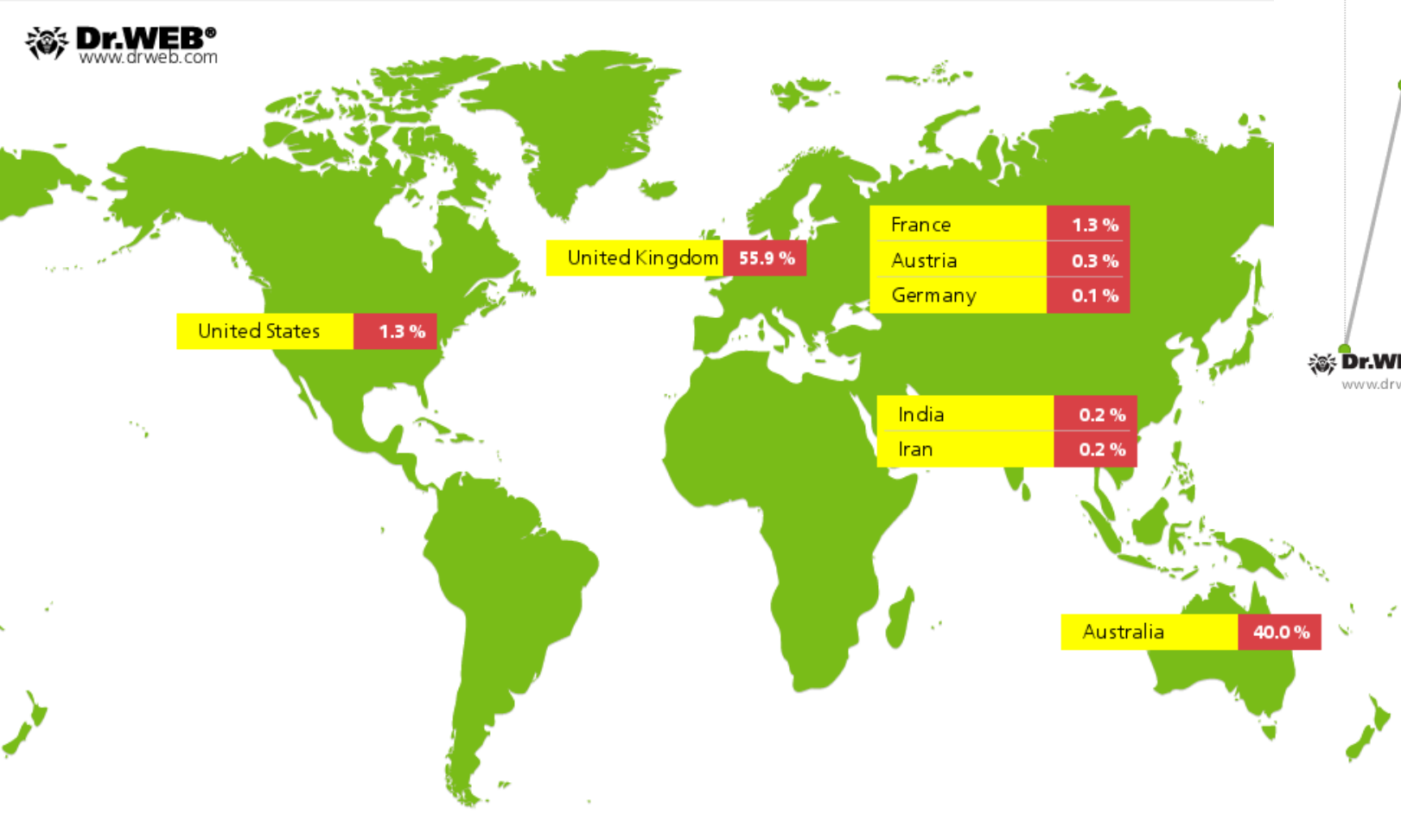
Первоначально число заражений вирусом [Win32.Rmnet.12](#) было относительно невелико, однако с каждым месяцем количество инфицированных ПК увеличивалось, пока к концу года не достигло рекордной отметки в 6,5 миллионов. Динамику этого процесса можно с помощью представленного ниже графика.

Динамика изменения численности ботнета Win32.Rmnet.12 в 2012 году



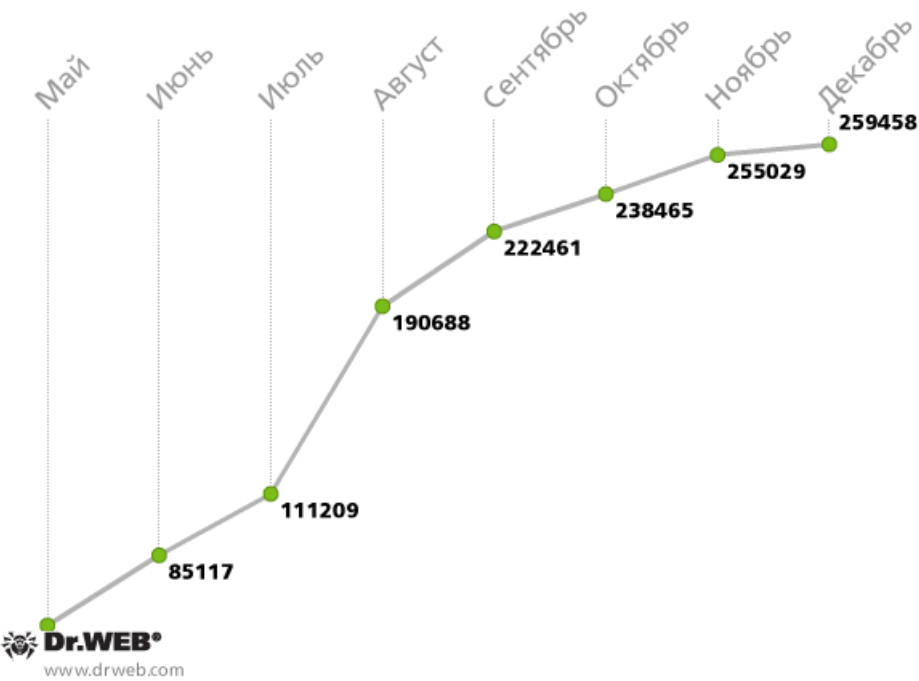
Поскольку тенденций к снижению роста данной угрозы не наблюдается, можно предположить, что вирус[Win32.Rmnet.12](#) продолжит свое распространение. Если расширение ботнета будет продолжаться прежними темпами, то в 2013 году общая численность зарегистрированных в сети инфицированных компьютеров превысит 10 миллионов.

Одной из наиболее распространенных модификаций файлового вируса [Win32.Rmnet.12](#) является его «родной брат» [Win32.Rmnet.16](#). Основное отличие данной вредоносной программы от ее предшественницы заключается том, что она использует цифровую подпись, которой подписывается IP-адрес управляющего сервера. Также вирусописатели обновили основные функциональные модули приложения.



Ботнет, состоящий из инфицированных [Win32.Rmnet.16](#) рабочих станций, наиболее распространен на территории Великобритании и Австралии. Однако численность этой бот-сети значительно скромнее по сравнению с [Win32.Rmnet.12](#). Число случаев заражения в течение 2012 года также постепенно росло, однако гораздо менее высокими темпами, о чем свидетельствует представленная ниже диаграмма.

Динамика изменения численности ботнета Win32.Rmnet.16 в 2012 году

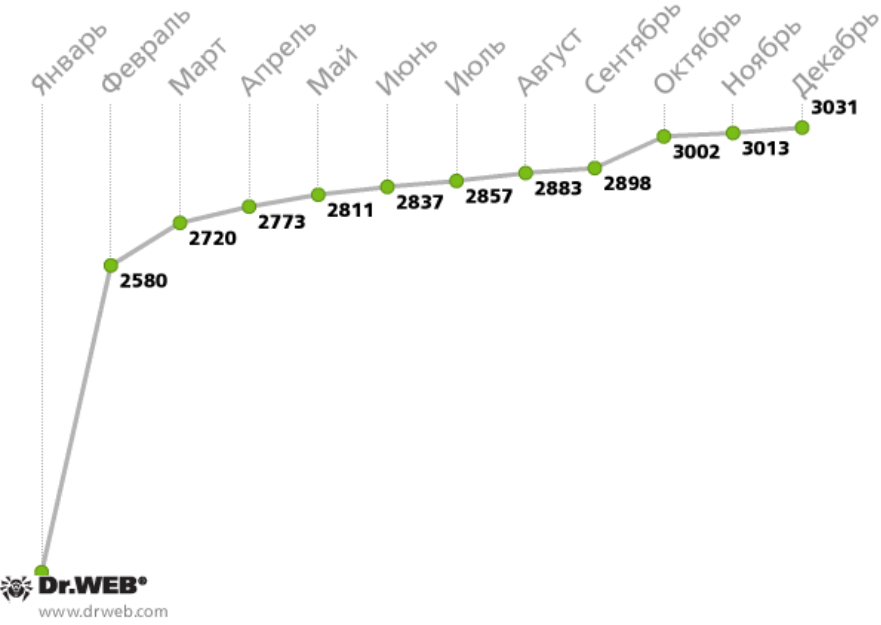


Исходя из имеющейся в распоряжении специалистов «Доктор Веб» статистики можно предположить, что прирост численности ботнета [Win32.Rmnet.16](#) будет понемногу сокращаться, а его общий объем вряд ли превысит миллион инфицированных узлов, если, конечно, лавинообразному росту заражений не поспособствуют какие-либо непредвиденные обстоятельства. Напомним, что специалисты компании «Доктор Веб» полностью контролируют вирусные сети [Win32.Rmnet.12](#) и [Win32.Rmnet.16](#).

Еще в ноябре 2011 года компания «Доктор Веб» сообщила о появлении узкоспециализированной троянской программы [BackDoor.Dande](#), предназначенной для кражи информации у российских фармацевтических компаний и аптек. [BackDoor.Dande](#) — сложный многокомпонентный троянец, шифрующий свои модули ключом, привязанным к конкретной инфицированной машине, и самостоятельно загружающий их в память. Благодаря этому детектировать его вредоносные модули можно только в оперативной памяти зараженного компьютера, а расшифровать их отдельно от инфицированного ПК крайне сложно. Кроме того, загрузчик модулей встраивается в первую секцию одной из системных библиотек Windows, в результате чего по формальным признакам ее становится невозможно отличить от незараженной библиотеки. Троянец крадет данные из так называемых «систем электронного заказа», к которым относятся специализированная конфигурация «Аналит: Фармация 7.7» для платформы 1С, «Система электронного заказа» СЭЗ-2 производства компании «Аптека-Холдинг», программа формирования заявок компании «Российская Фармация», система электронного заказа фармацевтической группы «Роста», программа «Катрен WinPrice» и некоторые другие.

Несмотря на то, что троянец впервые был добавлен в вирусные базы Dr.Web более года назад, к концу декабря 2012 года бот-сеть [BackDoor.Dande](#) продолжала действовать. С учетом того, что троянец продолжает работу только на компьютерах, где установлена одна из систем электронного заказа медикаментов (а при ее отсутствии самоуничтожается), можно с уверенностью говорить, что в бот-сети [BackDoor.Dande](#) состоят преимущественно рабочие станции, принадлежащие аптекам и фармацевтическим компаниям. На 19 декабря 2012 года в ботнете [BackDoor.Dande](#) числился 3 031 инфицированный компьютер. Изменение численности данной бот-сети показано на представленном ниже графике.

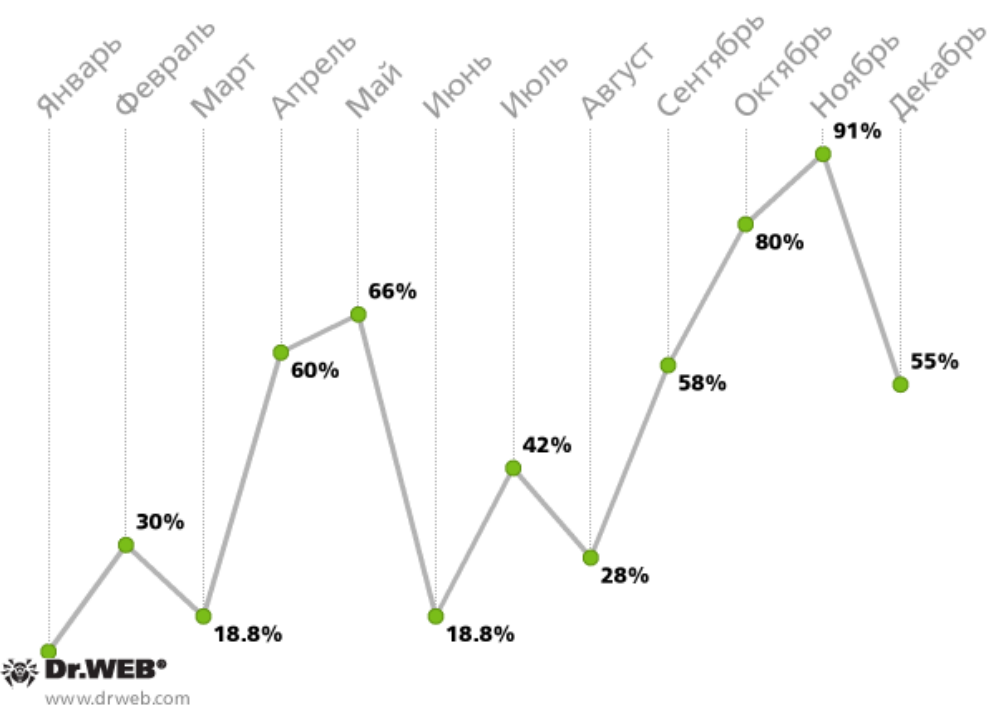
Динамика изменения численности ботнета BackDoor.Dande в 2012 году



Троянцы-кодировщики

2012 год можно, пожалуй, назвать периодом наибольшего распространения троянцев-энкодеров: по приблизительным подсчетам в прошлом году от действия этих вредоносных программ пострадали тысячи человек по всему земному шару. В течение года в вирусные базы Dr.Web было добавлено множество новых модификаций троянцев данного типа. Динамика поступления запросов в службу технической поддержки компании «Доктор Веб» от пользователей, пострадавших в результате действия троянцев-кодировщиков, показана на представленном ниже графике:

Динамика запросов о помощи в лечении последствий заражения Trojan.Encoder в 2012 г.



Появление первых версий троянцев-кодировщиков было зафиксировано еще в 2009 году. Энкодеры отыскивают на дисках инфицированного компьютера пользовательские файлы, в частности, документы Microsoft Office, музыку, фотографии, изображения и архивы, после чего шифруют их. За расшифровку файлов злоумышленники требуют заплатить определенную денежную сумму.

В течение длительного времени от действий троянцев-кодировщиков страдали в основном пользователи на территории России и стран бывшего СССР, однако весной 2012 года вредоносные программы семейства [Trojan.Encoder](#) вышли на зарубежные просторы. Одним из первых троянцев-вымогателей, ориентированных на западную аудиторию, стал [Trojan.Encoder.94](#). Троянец имел англоязычный интерфейс, однако случаи заражения были зафиксированы в Германии, Италии, Испании, Англии, Польше, Австрии, Норвегии, Болгарии и некоторых других странах. Первые обращения пострадавших от [Trojan.Encoder.94](#) зарубежных пользователей были зафиксированы 9–10 апреля 2012 года. Вскоре в службу технической поддержки компании «Доктор Веб» стали обращаться пользователи из Латинской Америки (Бразилии и Аргентины), а также таких европейских стран как Франция, Бельгия, Швейцария, Нидерланды, Хорватия, Словения, Венгрия и Румыния.

К концу года ситуация с троянцами-шифровальщиками кардинально изменилась: если в 2011 году подобные вредоносные программы все еще были ориентированы в основном на русскоязычную аудиторию, то уже к декабрю 2012, по мнению аналитиков «Доктор Веб», соотношение «российских» и «зарубежных» энкодеров составляло примерно 50/50. Основной всплеск распространения шифровальщиков, ориентированных на западный рынок, пришелся на апрель-май 2012 года, однако к осени их число несколько уменьшилось. Основываясь на имеющейся статистике можно предположить, что в наступающем году число энкодеров, направленных на зарубежных пользователей ПК, будет стремительно расти. В целом 2013 год можно будет, по всей видимости, назвать «годом энкодеров» — распространенность этой категории угроз вполне может принять масштабы эпидемии.

Винлоки

Троянцы-вымогатели, парализующие нормальную работу операционной системы и требующие у пользователя заплатить определенную сумму за ее разблокировку, известны уже давно. В течение 2012 года появлялись новые модификации винлоков, но динамику их распространения нельзя было назвать чрезмерно высокой. Всего в течение года в службу технической поддержки «Доктор Веб» обратилось более 10 000 пользователей, пострадавших от действия троянцев-блокировщиков, всем им была оказана квалифицированная помощь. Динамику таких запросов можно отследить с

помощью представленного ниже графика.



Осенью 2012 года было зафиксировано распространение троянцев-блокировщиков, получивших общее наименование «мультилокеры», — исходя из заголовка, демонстрировавшегося на входной странице используемых ими управляющих серверов. Такие троянцы не содержат каких-либо изображений, текстовых ресурсов или иных компонентов, которые обычно демонстрируются подобными вредоносными приложениями на экране компьютера при блокировке Windows. Все необходимые элементы мультилокеры загружают с удаленного сервера. Соответственно, это позволяет злоумышленникам оперативно настраивать демонстрируемые на экране инфицированного компьютера текст, изображения, а также менять код разблокировки.

Запустившись на зараженном ПК, троянцы-мультилокеры блокируют возможность загрузки ряда приложений и системных утилит. Кроме того, некоторые модификации этих вредоносных программ способны перехватывать изображение с подключенной к зараженному компьютеру веб-камеры и демонстрировать его в блокирующей систему окне с целью запугивания пользователя. В тексте сообщения, написанного якобы от имени государственных правоохранительных структур, как правило, упоминается о том, что все действия жертвы на данном компьютере записываются, а ее портрет, полученный с помощью веб-камеры, сохраняется для последующей идентификации и получения дополнительной персональной информации.

IHR COMPUTER WURDE BLOCKIERT!

IP: [REDACTED] | Stadt: Saint Petersburg | ISP: Doctor Web

Die ganze Aktivitat von Ihrem Computer ist gespeichert. Wenn Sie die Webkamera benutzen, werden die Vidiodarstellungen fur Ihre Identifizierung benutzt.

Die Information uber Sie wird Ihrem Internetdienstleister zum Empfang der detaillierten Angaben uber Sie und die Statistik des Besuches der Homepages gegeben.

Eine der Grunden

- Sie benutzen raubkopierter Software.
- Sie sehen durch, hören zu Video-Audioaufnahme ohne Lizenz.
- Sie sehen die Information durch oder wechseln die Information auf den verbotenen Web-Sites, und auch auf den Web-Sites mit den Elementen der Kinderpornographie/Zooerastie.

Gemäß der internationalen Gesetzen über Bekämpfung gegen Raubkopierer und über Informationsschutz und Urheberrechtsschutz, sollen Sie eine Strafe im Ausmaß €100 bezahlen. Für die sichere Zahlung ist Ukash zu benutzen.

Um Zahlung zu leisten muss man die Code des von Ihnen erworbenen Vouchers angeben, Pin-Pad benutzen und den Knopf 'Strafe bezahlen' drucken.

€100

PIN-Code einführen

1	2	3
4	5	6
7	8	9
x	0	<
Strafe bezahlen		

** Nach der erfolgreichen Zahlung wird Ihr Computer automatisch freigegeben sein.*

FAQ

Wo kann man sich Ukash erwerben?

In mehreren Plätzen in der Welt, per Internet, elektronische Geldtaschen, Terminale und Bankomate.

IHR COMPUTER WURDE BLOCKIERT!

распространения троянцев для мобильных платформ. Данная тенденция продолжала проследиваться до конца года: уже в декабре были зафиксированы случаи взлома популярных порталов, в частности, официального сайта далай-ламы. Злоумышленники ставили своей целью заразить компьютеры посетителей этих сайтов вредоносными программами для ОС Windows и Mac OS X.

В минувшем году киберпреступники весьма активно использовали в своих целях различные уязвимости Java. Так, весной 2012 года злоумышленники распространяли с использованием уязвимости CVE-2012-0507 вредоносные программы семейства [Trojan.Carberg](#) и бэкдор для Mac OS X [Backdoor.Flashback.39](#). В июле средства массовой информации сообщили об использовании уязвимости CVE-2012-1723 в популярном среди злоумышленников наборе эксплойтов BlackHole. А уже 26 августа была обнаружена очередная критическая уязвимость Java, которая стала использоваться злоумышленниками в направленных атаках на компьютеры, работающие под управлением Mac OS X, Linux и Windows. Аналитики компании «Доктор Веб» полагают, что ситуация на тот момент складывалась критическая: на день публикации первой новости об обнаружении эксплоита злоумышленникам было широко известно о критической уязвимости Java 7, а обновление Java-машины планировалось только на середину октября. Следовательно, примерно 2 месяца вредоносное ПО имело бы возможность потоком идти через эту «незалатанную дыру» в Java, а также перенаправлять пользователей на вредоносные ресурсы посредством взломанных сайтов, которые на первый взгляд совершенно безобидны. Действия компании Oracle в данной ситуации не были оперативными, из-за чего вредоносное ПО проникло на компьютеры незащищенных пользователей. Тем не менее, с выходом очередного обновления Java в сентябре 2012 специалисты в области компьютерной безопасности обнаружили еще несколько критических уязвимостей этой платформы. Кроме того, в начале ноября появились сообщения об обнаружении zero-day уязвимости в программе Adobe Reader (версиях 10 и 11). С помощью этой уязвимости злоумышленникам удавалось запускать на компьютере жертвы вредоносное приложение. Сам содержащий уязвимость файл киберпреступники распространяли в Интернете, а также рассылали по электронной почте.

Весьма резонансным событием в сфере информационной безопасности стало обнаружение специалистами одной из антивирусных компаний вредоносной программы [Win32.HLLW.Flame](#) — сложного многокомпонентного вредоносного приложения, прозванного специалистами «Доктор Веб» за рекордный размер (более 6 МБ) «троянским слоном». Эта программа обладает весьма обширными функциональными возможностями, однако «в дикой природе» практически не встречается. По мнению аналитиков «Доктор Веб», опасность этого троянца, растиражированная многочисленными публикациями в интернете и в СМИ, несколько преувеличена.

Еще одним немаловажным событием в мире информационных технологий стала ликвидация в июле 2012 ботнета [BackDoor.BlackEnergy](#). Это была крупная бот-сеть, ориентированная на массовую рассылку спама, а также проведение DDoS-атак, и прекращение ее деятельности достаточно быстро привело к снижению объемов спам-трафика начиная с июля 2012 года. Вместе с тем, несмотря на уничтожение главных управляющих центров [BackDoor.BlackEnergy](#), специалисты «Доктор Веб» зафиксировали несколько более мелких командных серверов этой сети, которые продолжали свою деятельность и после опубликованных в прессе заявлений об уничтожении данной бот-сети. Тем не менее, уже спустя несколько месяцев прекратили свое существование и эти серверы, поэтому в настоящий момент мы действительно можем говорить о полной и безоговорочной ликвидации ботнета [BackDoor.BlackEnergy](#).

Мошенничество в Интернете



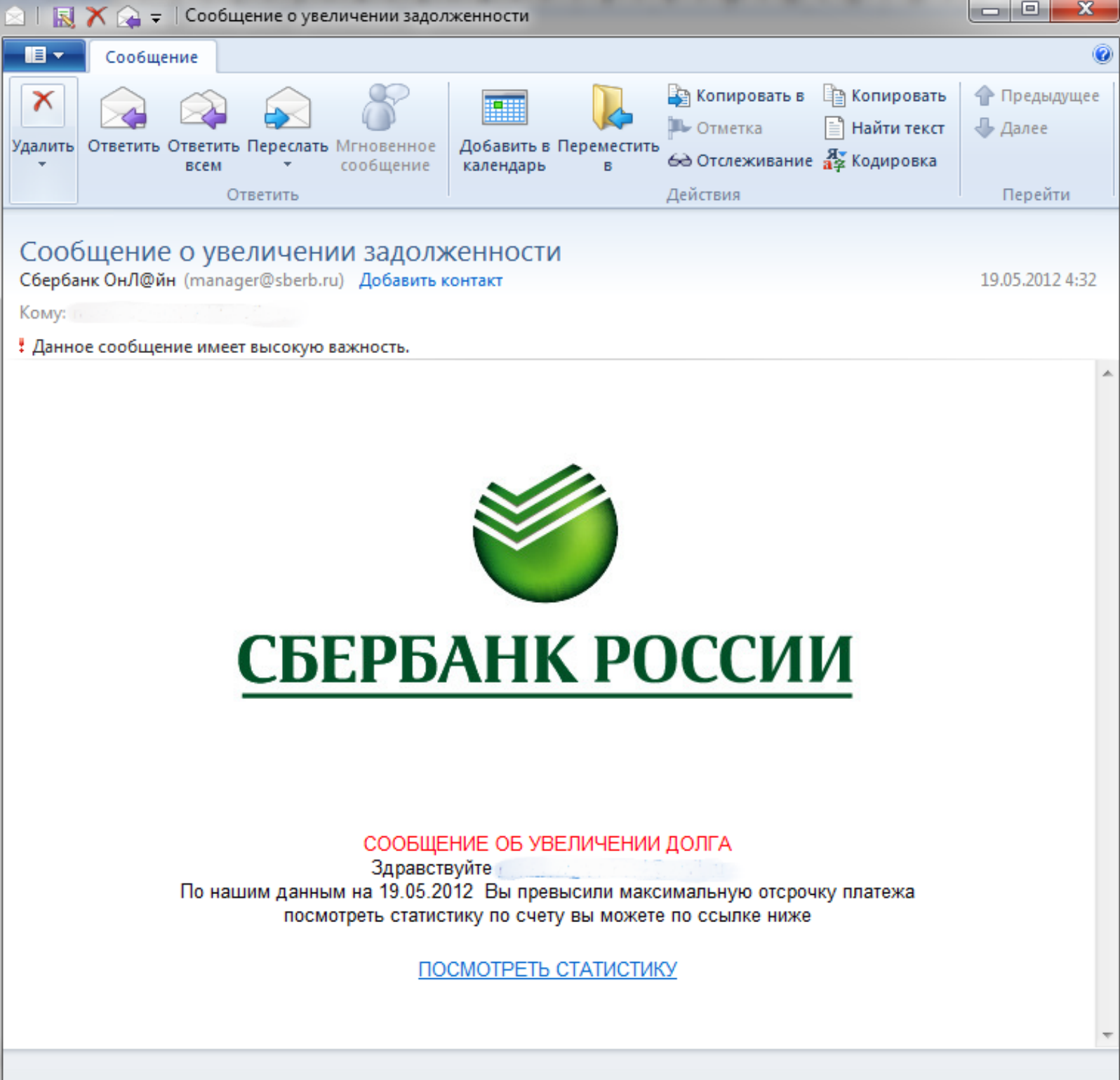
Не дремлют и сетевые мошенники, всеми силами стремящиеся нажиться на доверчивости простых пользователей. Так, в начале мая злоумышленники устроили атаку на пользователей Facebook. Заглянув на свою страницу в этой социальной сети, пользователь обнаруживал в новостной ленте ссылку на программу Profile Visitor, якобы способную фиксировать и демонстрировать на специальной странице посетителей его профиля. Ссылка, как правило, публиковалась от имени одного из друзей пользователя и вела на страницу встроенного приложения Facebook, для активации которого требовалось разрешить программе публиковать контент от имени пользовательской учетной записи. Как только ничего не подозревающая жертва нажимала на кнопку «Разрешить», на стене ее профиля и в новостной ленте всех ее друзей появлялась ссылка на данное приложение, размещенная от ее имени. Однако даже если пользователь не разрешал программе Profile Visitor какие-либо публикации, все, кто зарегистрирован в списке его друзей, получали «отметку» на «фотографии», представляющей собой рекламный баннер-ссылку приложения Profile Visitor. С помощью этого баннера пользователь перенаправлялся на различные мошеннические сайты.

В конце того же месяца многие российские пользователи стали жертвами массовой рассылки электронных писем, отправленных от имени Сбербанка. Письма с темой «Сообщение об увеличении задолженности» получило множество пользователей. В самом сообщении говорится о том, что получатель «превысил максимальную отсрочку платежа», и предлагается ссылка, якобы позволяющая просмотреть статистику. По ссылке на компьютер жертвы загружался файл .SCR — в RAR- или ZIP-архиве либо в незапакованном виде. При попытке открыть этот файл хранящиеся на жестком диске компьютера документы и изображения оказывались зашифрованными, а за их расшифровку злоумышленники требовали заплатить определенную сумму.

В июне письма с вредоносным содержимым чаще всего отправлялись якобы от имени почтовых служб UPS и EMS. В сообщениях говорилось о том, что служба не смогла доставить пользователю почтовое сообщение, а за подробностями злоумышленники советовали обратиться к вложенному в сообщение файлу, в котором, как правило, скрывалась троянская программа.

В то же самое время сетевые мошенники освоили новый способ обмана пользователей, озадаченных поиском работы. Преследуя свои корыстные цели, злоумышленники создавали на специализированных ресурсах учетную запись несуществующей компании с громким и запоминающимся названием. Затем по электронной почте мошенники отправляли соискателям сообщение, в котором предлагалось занять некую вымышленную вакансию, например, «инженера по подбору оборудования». Для этого потенциальной жертве следовало пройти «онлайн-собеседование» на определенном сайте, созданном специально для этой цели. «Онлайн-собеседование», как правило, состояло из нескольких десятков примитивных вопросов, а после прохождения «теста» жертве предлагалось отправить СМС-сообщение «с личным кодом результата» на короткий номер и ввести в соответствующее поле код подтверждения, полученный в ответном сообщении. На

самом деле, таким образом пользователь соглашался с условиями «псевдоподписки» — услуги по предоставлению доступа к информации, за оказание которой со счета его мобильного телефона регулярно списывалась определенная сумма.



Наиболее интересные угрозы года
Одной из наиболее ярких тенденций четвертого квартала стало резкое снижение числа заражений пользовательских компьютеров троянской программой [Trojan.Mayachok.1](#), уверенно возглавлявшей список наиболее опасных угроз с начала 2012 года. Связано это, прежде всего, с тем, что вирусописатели начали активно модифицировать эту троянскую программу: если на начало года было известно лишь несколько ее версий, то к концу декабря в базах Dr.Web насчитывалось уже более 1 000 соответствующих записей. Изменениям подвергся и код вредоносной программы, и — отчасти — ее функционал, при этом если в начале года новые версии Trojan.Mayachok появлялись не чаще раза в месяц, то в октябре-ноябре модификации данного троянца детектировались практически каждый день, однако их различия в целом были незначительными. Напомним, что вредоносные программы Trojan.Mayachok обладают возможностью встраивать в просматриваемые пользователем веб-страницы постороннее содержимое. Например, блокировать таким образом доступ к Интернету и требовать плату за его разблокировку. Можно предположить, что новые версии троянцев этого семейства будут появляться и в дальнейшем.

В конце июня специалистами компании «Доктор Веб» был проведен анализ вредоносной программы [Trojan.Hottrend](#), которую можно назвать самым маленьким из известных на сегодняшний день банковских троянцев. Размер её составляет всего 20 КБ. Основное функциональное предназначение этой вредоносной программы — отслеживание сетевого трафика с целью перехвата конфиденциальной (в том числе банковской) информации, которая впоследствии передается злоумышленникам.

Одним из самых интересных троянцев, исследованных вирусными аналитиками компании «Доктор Веб» в 2012 году, является вредоносная программа под названием [BackDoor.DaVinci.1](#). Главной отличительной особенностью этого троянского приложения является то, что оно способно работать как в операционной системе Microsoft Windows, так и в Mac OS X. Помимо этого, известно о реализации данной угрозы, представляющей опасность для мобильных платформ. Эта вредоносная программа представляет собой многокомпонентный бэкдор, включающий большое количество функциональных модулей, в том числе драйверы, использующие руткит-технологии для сокрытия работы приложения в операционной системе.

[BackDoor.DaVinci.1](#) позволяет устанавливать полный контроль над инфицированным компьютером. Помимо этого, троянец сохраняет и передает злоумышленникам информацию о зараженной машине, фиксирует нажатие клавиш, способен делать снимки экрана, перехватывать сообщения электронной почты, ICQ, Skype, передавать данные с микрофона или подключенной к компьютеру видеокамеры. Кроме того, бэкдор обладает обширным функционалом по обходу антивирусных программ и персональных брандмауэров, благодаря чему может в течение длительного времени работать на инфицированной машине незаметно для пользователя. Интересной особенностью реализации [BackDoor.DaVinci.1](#) для Mac OS X является то, что впервые в данной платформе используются руткит-технологии для сокрытия файлов и процессов.

Ну а наиболее оригинальным подходом к заражению компьютеров отличился троянец [Trojan.KillFiles.9055](#), распространявшийся по электронной почте в сообщениях с призывами присоединиться к протестным акциям 5 марта 2012 года. Примечателен тот факт, что тело троянца располагалось непосредственно в макросе, встроенном в приложенный к письму документ Word. Вредоносная программа сохранялась на диск и

выполнялась в момент открытия документа. Запустившись на компьютере жертвы, [Trojan.KillFiles.9055](#) вызывал зависание ОС Windows. Одновременно троянец менял содержимое всех обнаруженных на диске C файлов (с расширением .msc .exe .doc .xls .rar .zip .7z) на «цифровой мусор» и помечал их на удаление после перезагрузки системы, вследствие чего Windows приходила в нерабочее состояние. Затем троянец отправлял на удаленный сервер злоумышленников сообщение о том, что операционная система успешно уничтожена.

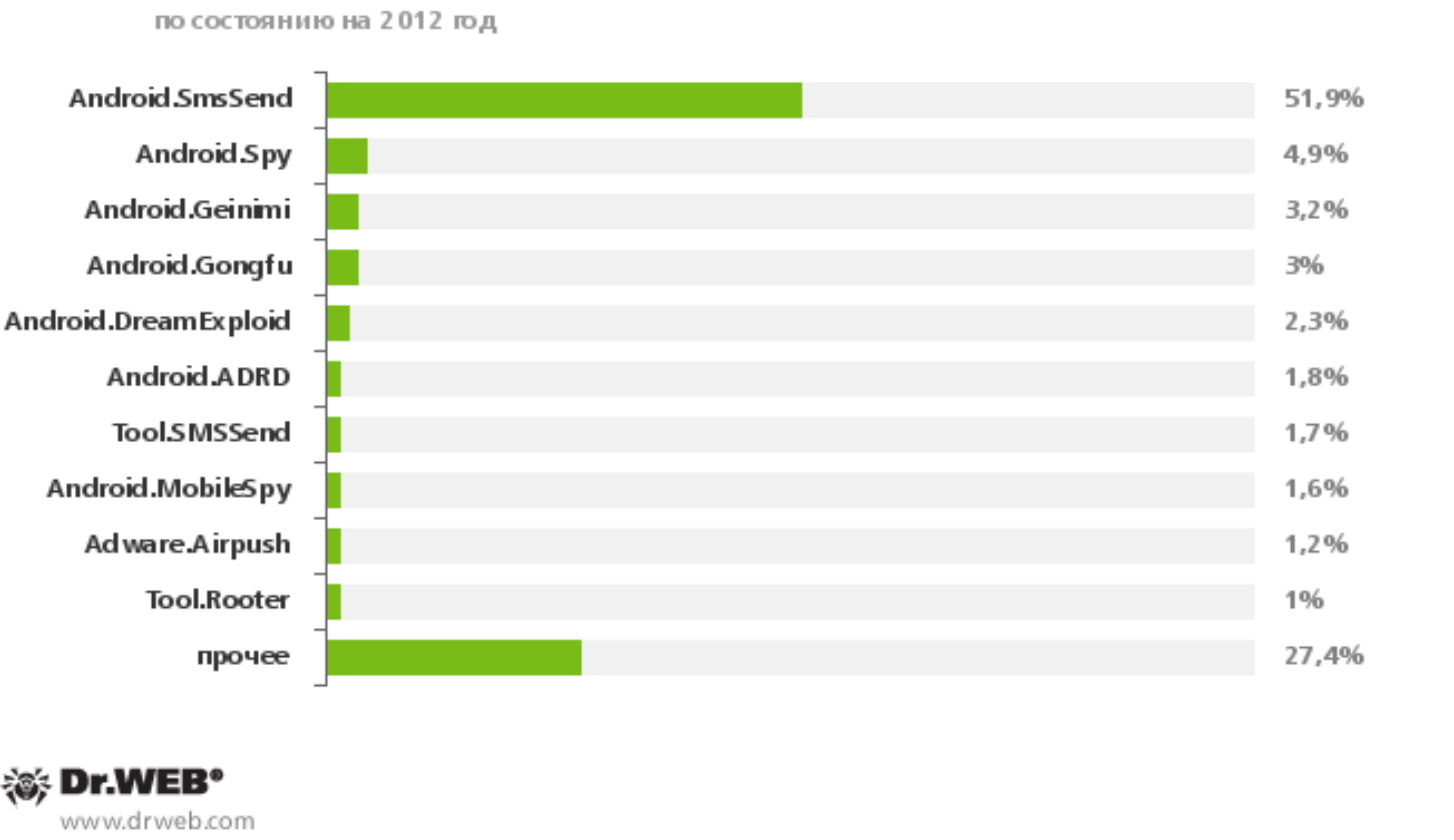
Android под атакой: «легкие» деньги, доступ к конфиденциальной информации и усложнение угроз

Как и ожидалось, число угроз, ориентированных на ОС Android, в 2012 году продолжило неуклонно расти, что неудивительно: мобильные устройства под управлением этой операционной системы продолжают занимать все более прочное положение на рынке. Так, согласно последнему исследованию компании IDC, в третьем квартале 2012 года три четверти поставляемых смартфонов работали именно на этой платформе. На представленной ниже диаграмме отображено процентное распределение вредоносных программ для Android.

Наиболее распространенной и массовой угрозой по-прежнему остаются троянцы семейства Android.SmsSend, появившиеся еще в 2010 году. Основная функция этих вредоносных программ — отправка дорогостоящих СМС-сообщений и подписка пользователей на различные контент-услуги. Подавляющее большинство троянцев [Android.SmsSend](#) с технологической точки зрения является примитивными разработками, однако простота создания и высокая окупаемость побуждают киберпреступников выпускать бесчисленные модификации этих вредоносных программ.

Одной из наиболее заметных тенденций 2012 года стало существенное увеличение числа троянских программ-шпионов для ОС Android. Так, весьма показательным стало появление целого ряда троянцев, которые начиная с середины 2012 года атаковали японских пользователей. Все эти вредоносные программы, среди которых были Android.EmailSpy.origin, Android.MailSteal.1.origin и Android.Maxbet.1.origin, распространялись при помощи спам-писем, содержавших ссылку, которая вела на загрузку якобы полезного приложения. Программы-шпионы предназначались для кражи персональной информации, такой как адреса электронной почты. Были обнаружены и новые представители банковских троянцев, в частности, [Android.SpyEye.2.origin](#), Android.Panda.2.origin и Android.FakeSber.1.origin. Последний особенно интересен тем, что предназначался для атаки на клиентов одного из крупнейших российских банков, в то время как другие вредоносные программы данного типа раньше представляли угрозу лишь для зарубежных пользователей. Это свидетельствует о том, что география применения таких вредоносных программ постепенно расширяется. Несмотря на то, что банковские троянцы для ОС Android все еще встречаются нечасто, они представляют серьезную опасность из-за точечного и хорошо спланированного характера атак. Появление первой подобной вредоносной программы в России может стать отправной точкой к увеличению инцидентов с их участием.

Распределение различных типов угроз для ОС Android



В прошедшем году продолжил расширяться рынок коммерческого шпионского ПО: на протяжении всего года в вирусные базы Dr.Web вносились не только новые модификации известных приложений для кибершпионажа и мониторинга, но также целый ряд новых семейств.

В 2013 году стоит ожидать увеличения количества подобных потенциально опасных программ, а также различных троянцев-шпионов. Весьма вероятной представляется угроза со стороны АРТ-кампаний (атак с перебором различных видов угроз и уязвимостей до получения результата), в которых будут использоваться Android-троянцы. В целом же можно говорить о том, что все большее число Android-угроз, так или иначе участвующих в краже конфиденциальной информации, применяется в узконаправленных атаках. Эта тенденция в ближайшем будущем сохранится.

Одной из наиболее опасных вредоносных программ для мобильных Android-устройств в 2012 году стал троянец [Android.SmsSend.186.origin](#). От большинства других представителей этого семейства он отличался весьма продвинутыми методами сокрытия вредоносного функционала. Во-первых, при его распространении был использован дроппер, не требующий для работы никаких специальных разрешений.

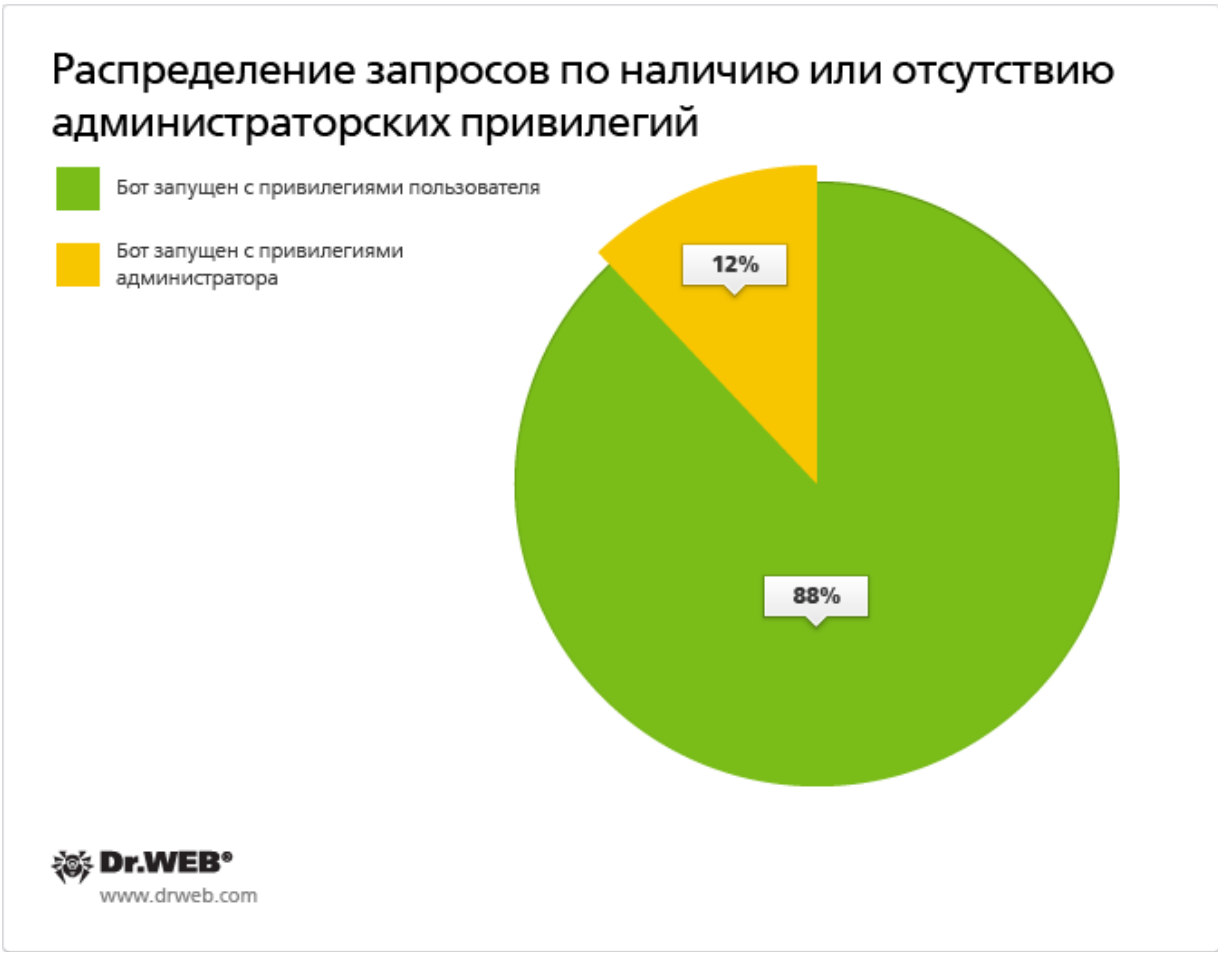
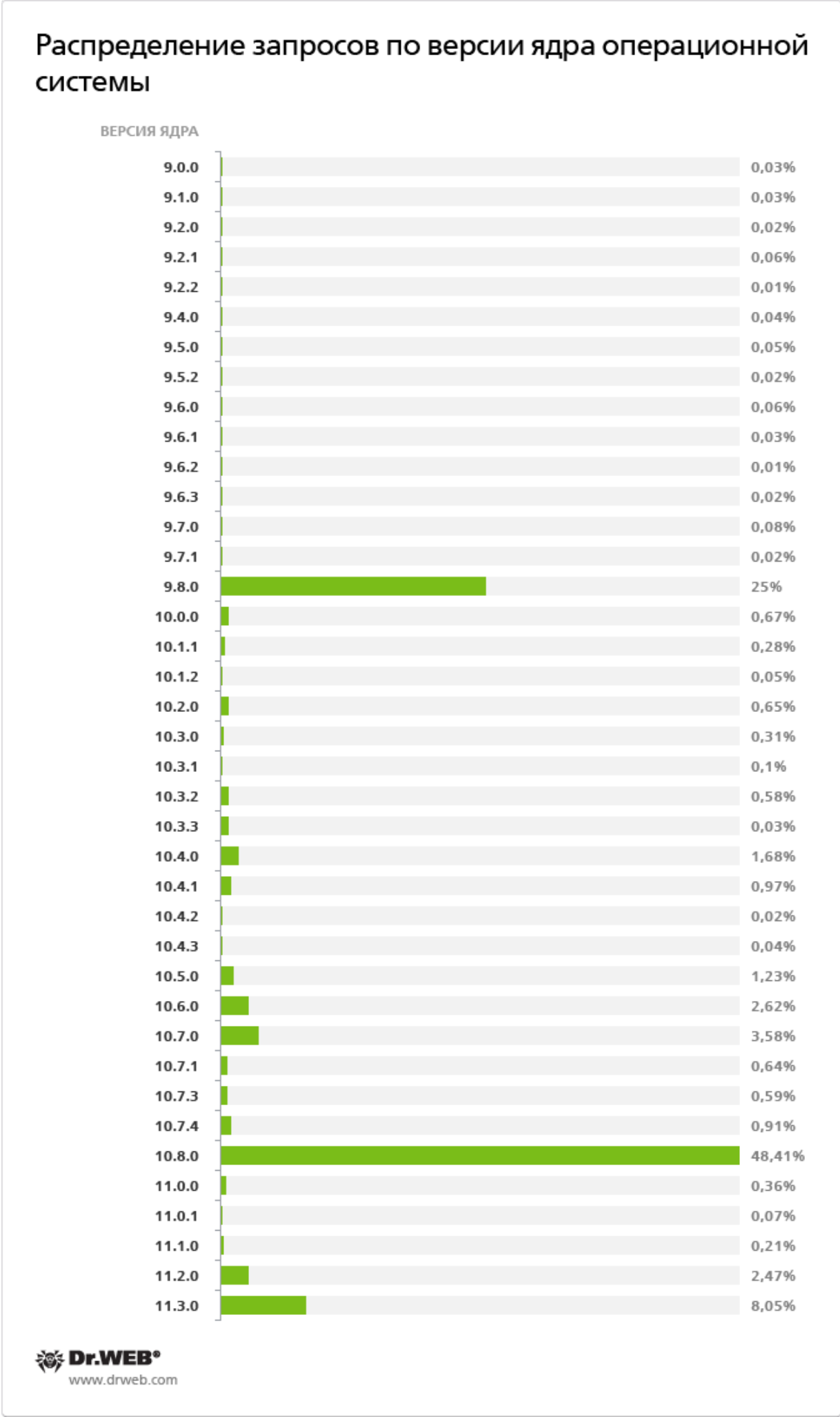
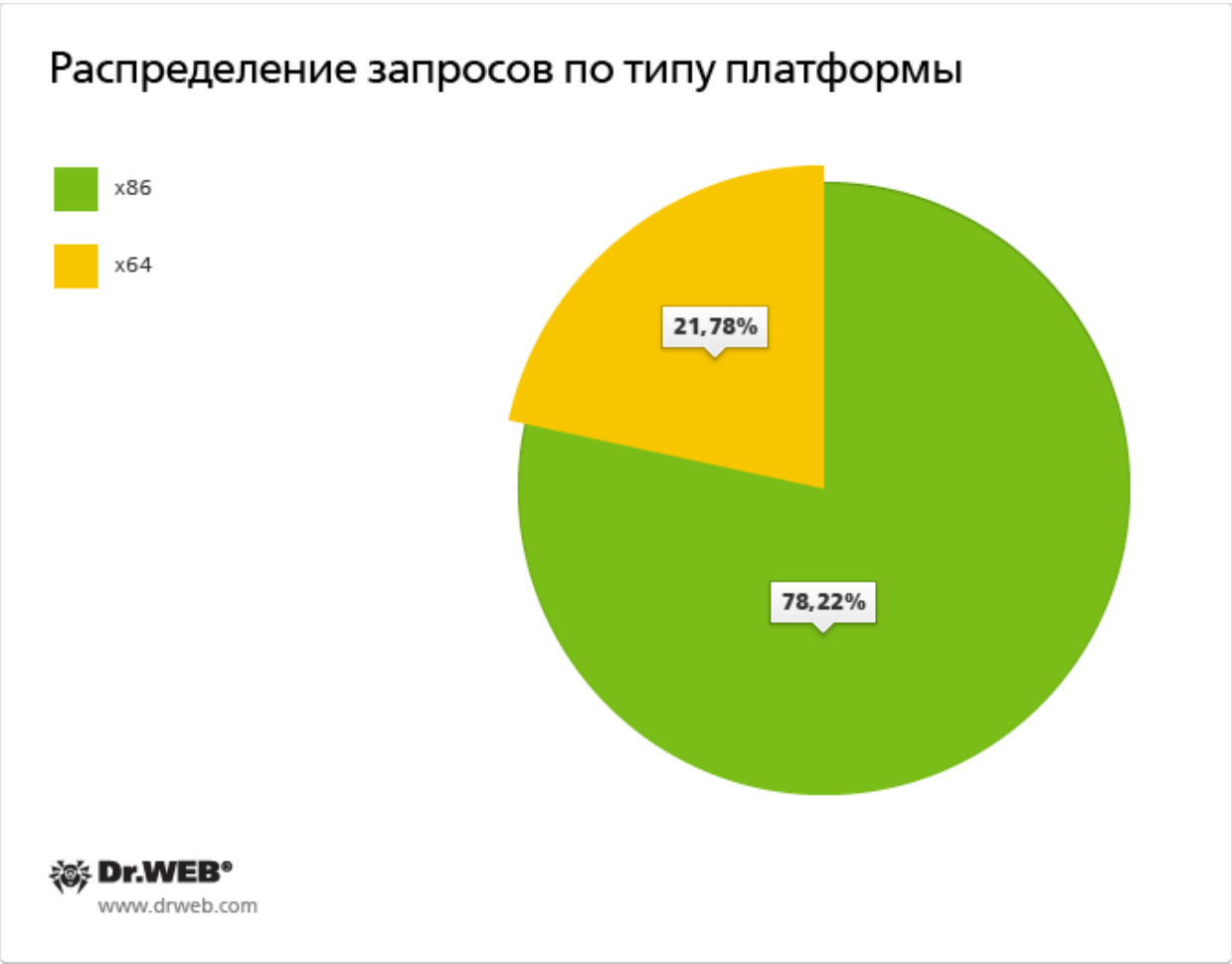
Во-вторых, после установки Android.SmsSend.186.origin заставлял пользователя предоставить ему права администратора мобильного устройства, а после их получения на некоторых версиях ОС Android его было очень сложно удалить. Вполне вероятно, что в 2013 году появятся новые вредоносные программы, в той или иной степени противостоящие попыткам своего удаления, а также использующие различные техники для сокрытия своего присутствия в системе от пользователей.

Вредоносные программы, использующие уязвимости ОС Android для повышения системных привилегий, в прошедшем году не проявляли сколь-нибудь заметной активности. Причиной этого мог стать постепенный переход пользователей на более новые версии Android, в которых соответствующие уязвимости были исправлены, а также усиление безопасности платформы в целом. Однако нельзя исключить, что в 2013 году могут появиться новые вредоносные приложения, которые будут использовать неизвестные ранее уязвимости.

Последняя версия ОС Android 4.2, вышедшая относительно недавно, содержит ряд улучшений, направленных на борьбу с вредоносным ПО. В частности, добавлена функция проверки приложений, основанная на рейтинге их безопасности, а также введена ограничивающая мера для приложений, имеющих возможность отправлять СМС-сообщения на премиум-номера — теперь пользователи имеют возможность выбора: разрешить или запретить отправку таких СМС. Однако эффективность этих нововведений можно будет полноценно оценить лишь тогда, когда обновленная версия операционной системы станет использоваться на существенном количестве мобильных устройств. Учитывая огромный рынок совместимого с ОС Android оборудования, можно предположить, что злоумышленники найдут способы обхода новых защитных функций.

- Прогнозы и перспективы**
- Исходя из анализа угроз, поступивших в вирусную лабораторию компании «Доктор Веб» в течение 2012 года, можно спрогнозировать основные тенденции, которые с определенной долей вероятности получат развитие в следующие двенадцать месяцев.
- Будет расти число угроз для операционной системы Mac OS X. Возможно как распространение троянских программ, использующих для проникновения в систему различные уязвимости (в том числе уязвимости Java), так и бот-сетей, ориентированных исключительно на Apple-совместимые компьютеры.
 - Значительно увеличится и «ассортимент» вредоносных приложений для мобильной платформы Android. Предполагаемые темпы роста могут составить порядка 50–100% от нынешнего числа известных угроз.
 - Продолжится рост ботнетов, ориентированных на операционную систему Microsoft Windows. Так, уже в первом квартале 2013 года численность зарегистрированных в бот-сети компьютеров, инфицированных файловым вирусом [Win32.Rmnet.12](#), превысит 10 миллионов (если не будут предприняты масштабные меры, направленные на ликвидацию ботнета).
 - Возможно появление вирусов или троянских программ, эксплуатирующих уязвимости или характерные технологии, применяемые в ОС Microsoft Windows 8. Например, возможно возникновение вредоносных приложений, перехватывающих координаты GPS-модуля планшетных компьютеров, использующих эту платформу.
 - Будет расти число и усложняться функционал банковских троянцев, ориентированных на перехват конфиденциальных данных и хищение информации, необходимой для работы в системах дистанционного банковского обслуживания. Возможно увеличение количества заранее спланированных таргетированных атак на различные коммерческие структуры.
 - В целях слежения за пользователями вредоносные программы будут все чаще использовать данные, полученные с помощью веб-камер, микрофонов, GPS-приемников. Вырастет ассортимент троянцев-шпионов.
 - Возможно появление угроз, использующих для осуществления атак облачные сервисы и другие распределенные системы. Увеличится количество вредоносных программ, применяющих в своих целях P2P-сети, а также сеть TOR.

Приложение 1





{ Secure Shell }

Нам можно доверять!

И про Вас узнают Все...

{

Адрес журнала в интернете:
<http://ualinux.com/index.php/journal>

Обсуждение журнала на форуме:
<http://ualinux.com/index.php/forum>

}

{

Адрес редакции:

Украина, 03040, г.Киев, а/я 56
email: journal@ualinux.com

}

Тип издания: электронный/печатный
Тираж: *более 15 000 копий.

*указано суммарное количество прошлого
выпуска журнала с первичных источников, а также
загрузок с других известных ftp, http и torrent серверов.

Все права на материалы принадлежат их авторам
и опубликованы в открытых источниках.
Адреса на оригинальные источники публикуются.

{

Для размещения рекламы обращаться
по тел.:

+38 (048) 770-0425

+38 (094) 995-4425

Или на email: journal@ualinux.com

}