Dr.WEB®
с 1992 года

Обзор вирусной активности в январе 2015 года

Обзор вирусной активности в январе 2015 года

2 февраля 2015 года

По данным специалистов компании «Доктор Веб», в первом месяце 2015 года злоумышленники организовали несколько массовых рассылок вредоносных программ, предназначенных для установки на инфицированные компьютеры других опасных приложений. Многие пользователи ОС Microsoft Windows пострадали в январе от действия шифровальщиков. Также по-прежнему велико количество троянцев и других опасных программ, угрожающих пользователям мобильной платформы Google Android.

Главные тенденции января

- Массовая почтовая рассылка троянцев, предназначенных для установки других вредоносных приложений.
- Распространение троянцев-шифровальщиков, представляющих серьезную опасность для пользователей Microsoft Windows.
- Появление новых вредоносных приложений для мобильной платформы Google Android.

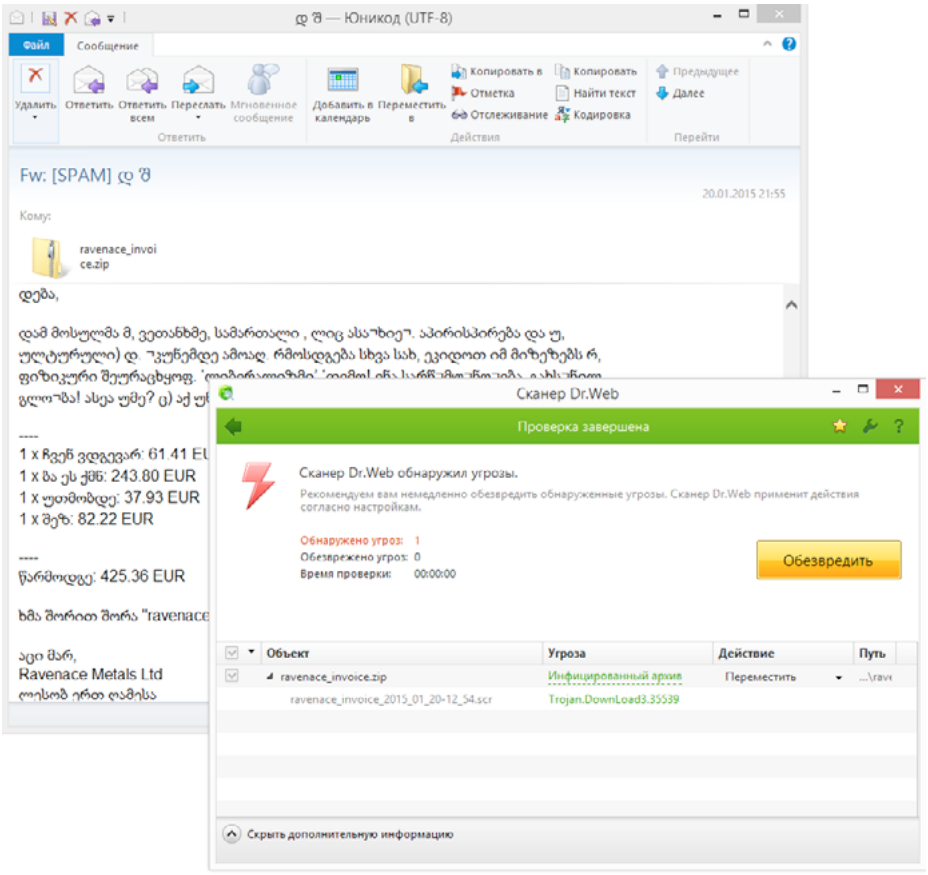
Обзор вирусной активности в январе 2015 года

Угроза месяца

В середине января злоумышленники осуществили массовую почтовую рассылку троянца-загрузчика Trojan.DownLoad3.35539.

- Распространяется в виде вложенного в сообщения электронной почты ZIP-архива.
- Основное назначение данной вредоносной программы — скачивание и запуск на инфицированном компьютере троянца-шифровальщика Trojan.Encoder.686, также известного как CTBLocker.

Специалисты «Доктор Веб» зафиксировали случаи распространения сообщений, содержащих опасное вложение, на разных языках, в том числе английском, немецком и даже грузинском.



Расшифровка пострадавших от действия данного энкодера файлов в настоящий момент не представляется возможной.

Тем не менее, данная вредоносная программа успешно детектируется Антивирусом Dr.Web и потому пользователи защищены от действия этого троянца.

Подробнее об этом инциденте можно узнать в опубликованной компанией «Доктор Веб» информационной статье.

Троянцы-шифровальщики

Количество запросов на расшифровку, поступивших в службу технической поддержки

Декабрь 2014	Январь 2015	Динамика
1096	1305	+16,1%

В январе увеличилось число пострадавших от действия троянца **Trojan.Encoder.686** — в вирусной лаборатории зафиксировано 51 обращение. Этот шифровальщик собран с использованием библиотек TOR и OpenSSL, криптографию которых он активно использует. В процессе шифрования пользовательских файлов энкодер активно эксплуатирует возможности CryptoAPI с целью получения случайных данных и эллиптическую криптографию.

Обзор вирусной активности в январе 2015 года

Вирусописатели отводят своим жертвам лишь 96 часов на оплату расшифровки файлов,

угрожая при этом, что в случае отказа от сотрудничества все зашифрованные файлы будут потеряны навсегда, а за подробной информацией об условиях и сумме выкупа предлагают обратиться на сайт, расположенный в анонимной сети TOR.

К сожалению, в настоящий момент расшифровка файлов, пострадавших от действия Trojan.Encoder.686, не представляется возможной. Однако данная вредоносная программа успешно детектируется Dr.Web, и пользователи наших продуктов защищены от ее действий.

Обзор вирусной активности в январе 2015 года

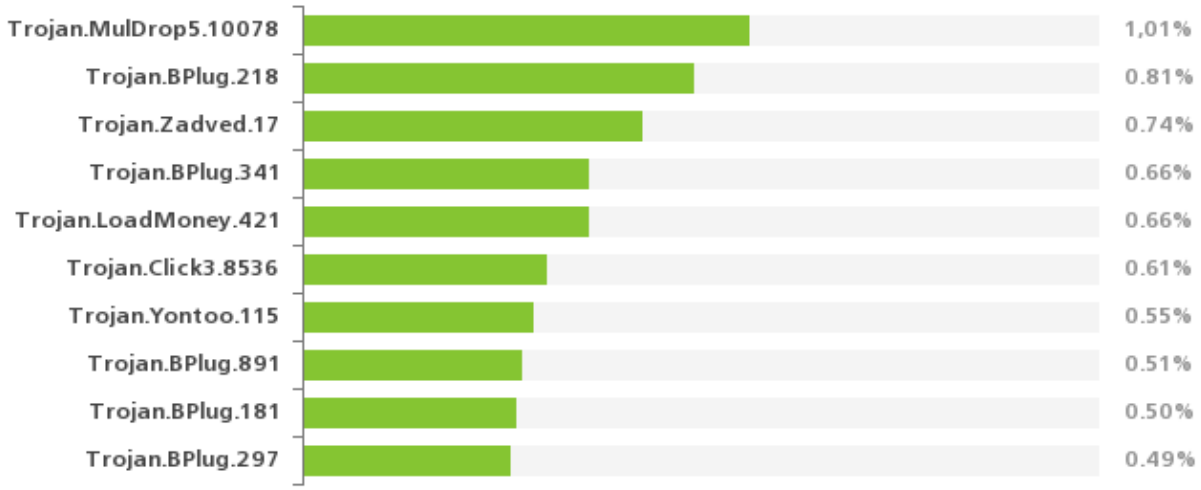
Другие наиболее распространенные шифровальщики:

- Encoder.556,
- Encoder.858
- Encoder.567
- Encoder.398.

Защитить владельцев персональных компьютеров от действия троянцев-шифровальщиков может своевременное резервное копирование данных, разумное разделение прав пользователей операционной системы, и, безусловно, современная антивирусная система защиты. Эффективными инструментами противодействия шифровальщикам обладает ***Dr.Web Security Space версии 10.0****, который включает специальные компоненты превентивной защиты данных от действия троянцев-вымогателей.*

По данным статистики лечащей утилиты Dr.Web CureIt!

Наиболее распространенные вредоносные программы согласно статистике лечащей утилиты Dr.Web CureIt!



Dr.WEB®
www.drweb.com

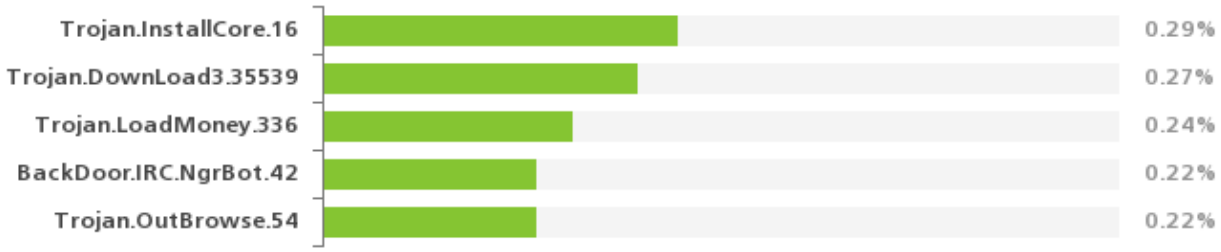
Обзор вирусной активности в январе 2015 года

- **Trojan.MulDrop5.10078**
  Устанавливает на инфицированный компьютер различные нежелательные и рекламные приложения.
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.
- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Click**
  Семейство вредоносных программ, предназначенных для накрутки посещаемости различных интернет-ресурсов путем перенаправления запросов жертвы на определенные сайты с помощью управления поведением браузера.
- **Trojan.Yontoo**
  Семейство надстроек для популярных браузеров, назначение которых заключается в демонстрации пользователю рекламы при просмотре веб-страниц.

Обзор вирусной активности в январе 2015 года

По данным серверов статистики «Доктор Веб»

Наиболее распространенные вредоносные программы в январе 2015 года
согласно данным серверов статистики Dr.Web

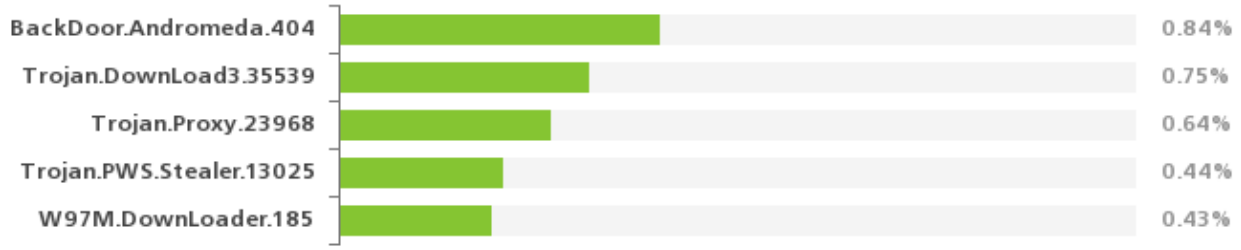


Dr.WEB®
www.drweb.com

- **Trojan.InstallCore.16**
  Троянец-установщик рекламных и сомнительных приложений, также известный под именем Trojan.Packed.24524.
- **Trojan.DownLoad3.35539**
  Троянец-загрузчик, преимущественно распространяющийся по электронной почте в виде ZIP-архива, содержащего .SCR-файл. При попытке открытия файла троянец сохраняет на диске инфицированного компьютера и демонстрирует на экране RTF-документ. Одновременно с этим вредоносная программа загружает с принадлежащих злоумышленникам удаленных серверов и запускает на атакуемом ПК полезную нагрузку, в роли которой был выявлен, в частности, троянец-шифровальщик Trojan.Encoder.686, также известный под названием CTB-Locker.
- **Trojan.LoadMoney.336**
  Один из представителей семейства программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **BackDoor.IRC.NgrBot.42**
  Довольно распространенный троянец, известный специалистам по информационной безопасности еще с 2011 года. Вредоносные программы этого семейства способны выполнять на инфицированном компьютере поступающие от злоумышленников команды, а управление ими киберпреступники осуществляют с использованием протокола обмена текстовыми сообщениями IRC (Internet Relay Chat).
- **Trojan.OutBrowse.54**
  Один из представителей семейства рекламных троянцев, распространяющихся с использованием партнерских программ и предназначенных для монетизации файлового трафика.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в январе 2015 года



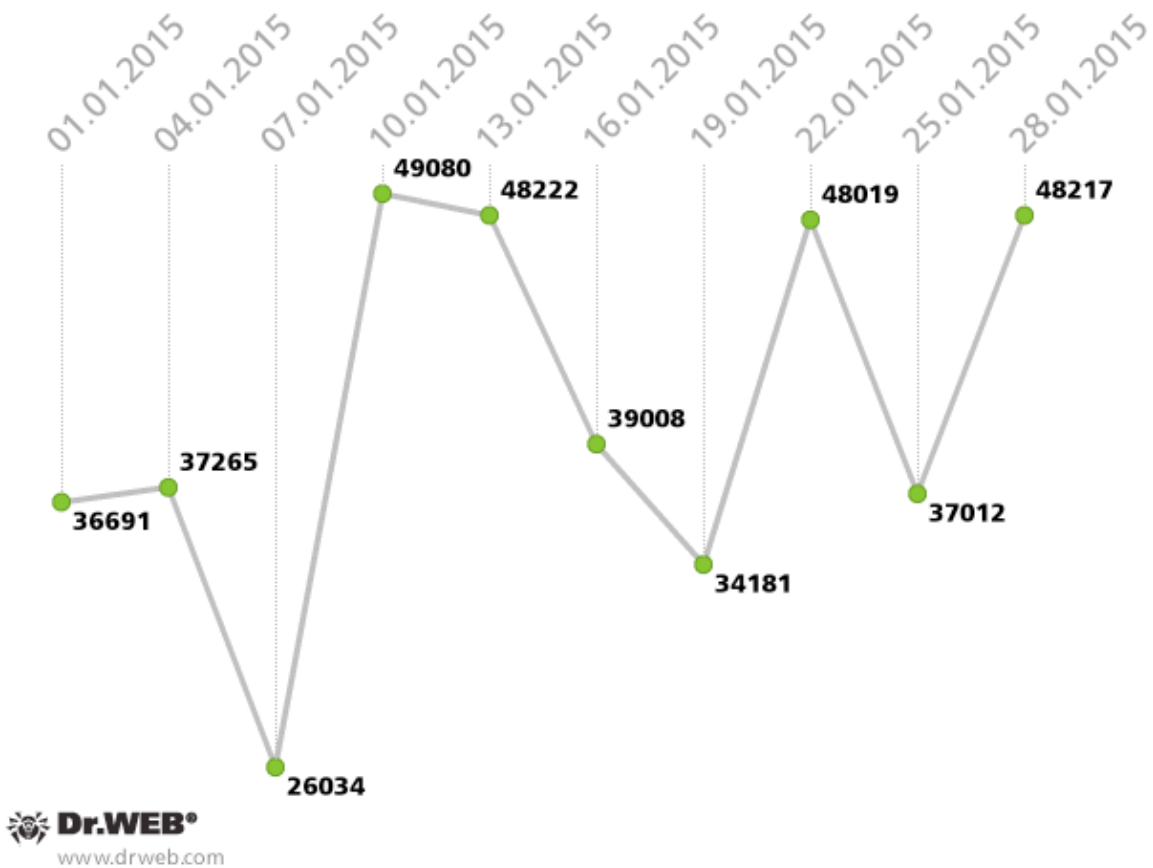
- **BackDoor.Andromeda.404**
  Троянец-загрузчик, предназначенный для скачивания с удаленных серверов злоумышленников и запуска на инфицированном компьютере других вредоносных программ.
- **Trojan.DownLoad3.35539**
  Троянец-загрузчик, преимущественно распространяющийся по электронной почте в виде ZIP-архива, содержащего .SCR-файл. При попытке открытия файла троянец сохраняет на диске инфицированного компьютера и демонстрирует на экране RTF-документ. Одновременно с этим вредоносная программа загружает с принадлежащих злоумышленникам удаленных серверов и запускает на атакуемом ПК полезную нагрузку, в роли которой был выявлен, в частности, троянец-шифровальщик Trojan.Encoder.686, также известный под названием CTB-Locker.
- **Trojan.Proxy.23968**
  Троянец, предназначенный для установки в инфицированной системе прокси-сервера с целью перехвата конфиденциальной информации при работе с системами дистанционного банковского обслуживания нескольких российских банков. Запустившись на компьютере жертвы, изменяет параметры сетевого соединения, прописывая в них ссылку на сценарий автоматической настройки. Трафик пользователя перенаправляется через прокси-сервер злоумышленников, который способен подменять веб-страницу системы «банк-клиент». Для организации HTTPS-соединения устанавливает в систему поддельный цифровой сертификат.

Обзор вирусной активности в январе 2015 года

- **Trojan.PWS.Stealer.13025**
  Один из представителей семейства вредоносных программ, предназначенных для хищения на инфицированном компьютере конфиденциальной информации, в том числе паролей из почтовых программ, ftp-клиентов, браузеров, мессенджеров.
- **W97M.DownLoader.185**
  Представитель семейства вредоносных программ, распространяющихся преимущественно по электронной почте в документах Microsoft Word. Предназначен для загрузки на атакуемый компьютер других вредоносных приложений.

Ботнеты

Активность борнета Win32.Sector в январе 2015 года



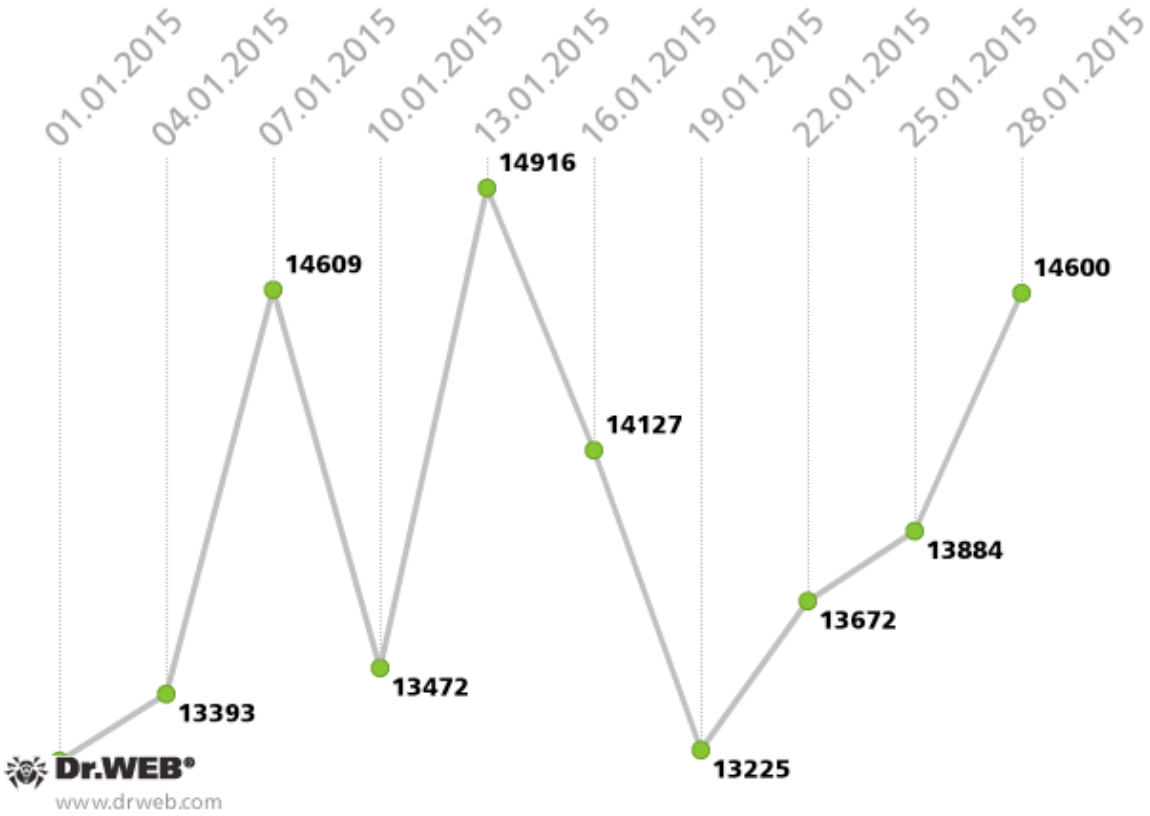
Вредоносная программа Win32.Sector известна с 2008 года и представляет собой сложный полиморфный вирус, способный распространяться самостоятельно (без участия пользователей) и заражать файловые объекты.

Обзор вирусной активности в январе 2015 года

Его основные функции:

- загрузка из P2P-сети и запуск на зараженной машине различных исполняемых файлов;
- встраивание в запущенные на инфицированном компьютере процессы;
- возможность останавливать работу некоторых антивирусных программ и блокировать доступ к сайтам их разработчиков;
- инфицирование файловых объектов на локальных дисках и сменных носителях (где в процессе заражения создает файл автозапуска autorun.inf), а также файлов, хранящиеся в общедоступных сетевых папках.

Активность борнета BackDoor.Flashback.39
в январе 2015 года



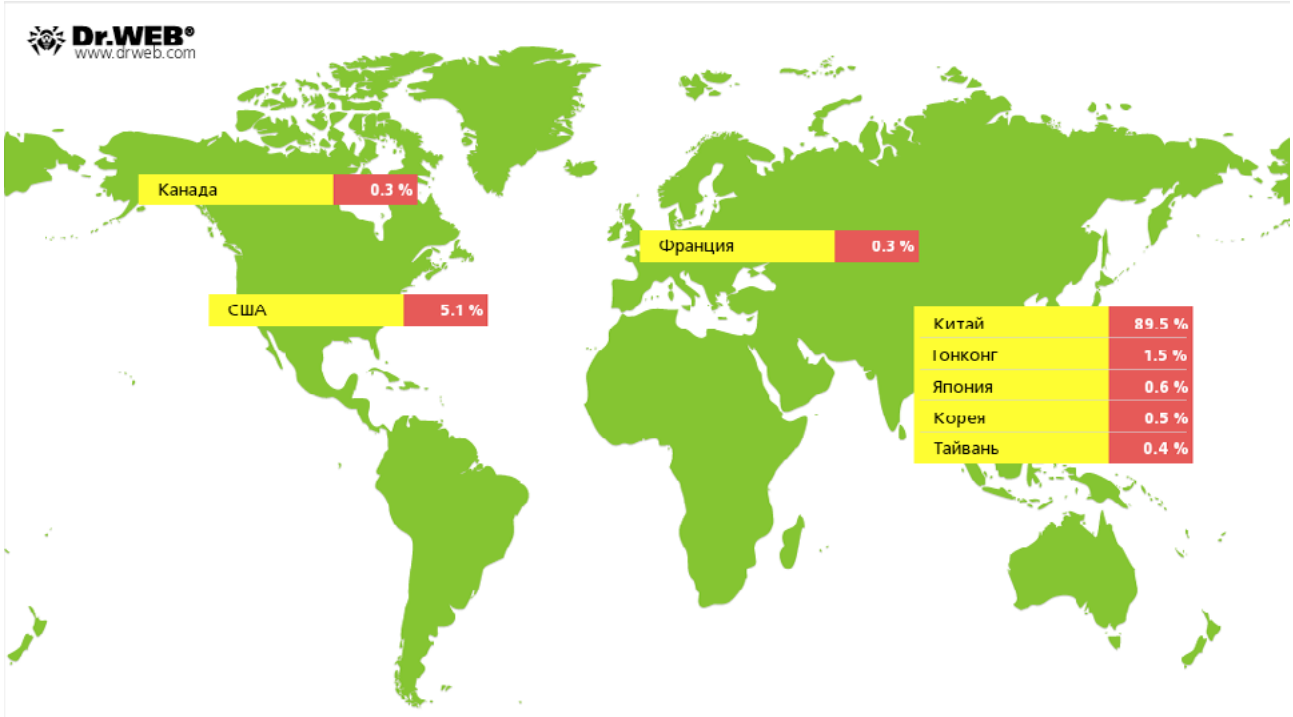
- **BackDoor.Flashback.39**
  Троянская программа для Mac OS X, получившая распространение в апреле 2012 года. Заражение осуществлялось с использованием уязвимостей Java. Предназначение троянца – загрузка и запуск на инфицированной машине полезной нагрузки, в качестве которой может выступать любой исполняемый файл, указанный в полученной троянцем от злоумышленников директиве.

Угрозы для Linux

В январе 2015 года было выявлено несколько новых образцов вредоносных программ для операционных систем семейства Linux, наиболее интересным из которых является файловый вирус **Linux.EbolaChan**.

- Основное назначение нового файлового вируса **Linux.EbolaChan** — запуск по расписанию специального скрипта, который загружает с сайта злоумышленников и выполняет на инфицированном компьютере другие sh-сценарии.

По-прежнему активен Linux-троянец **Linux.BackDoor.Gates.5**, продолжающий осуществлять DDoS-атаки на различные интернет-ресурсы. В январе 2015 года специалистами «Доктор Веб» было зафиксировано 5009 уникальных IP-адресов, на которые осуществлялись атаки, большинство из них, как и прежде, расположено на территории Китая:



Обзор вирусной активности в январе 2015 года

Мошеннические и нерекомендуемые сайты

Для защиты пользователей от различных способов мошенничества в Интернете служит компонент Родительский контроль, входящий в комплект поставки Dr.Web Security Space 10.0. Родительский контроль позволяет ограничивать доступ к интернет-сайтам определенной тематики, осуществляет фильтрацию подозрительного контента, а также, используя базы нерекомендуемых ссылок, защищает пользователя от мошеннических, потенциально опасных сайтов, шокирующего контента и ресурсов, замеченных в распространении вредоносного ПО.

В течение января 2015 года в базу нерекомендуемых сайтов Dr.Web был добавлен 10 431 интернет-адрес.

Декабрь 2014	Январь 2015	Динамика
10 462	10 431	+0,3%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для Android

В январе 2015 года было выявлено большое число новых вредоносных, а также других опасных Android-программ. Среди них наиболее актуальны следующие:

- Троянцы, распространяющиеся внутри модифицированных злоумышленниками Android-прошивок;
- Банковские Android-троянцы

Обзор вирусной активности в январе 2015 года

Немалую активность подобные вредоносные приложения вновь проявили в Южной Корее, где для распространения Android-троянцев злоумышленники активно используют содержащие ссылку на их загрузку СМС-сообщения.

Выявлено более 40 подобных спам-кампаний, в которых было задействовано несколько вредоносных программ.

- **Коммерческое шпионское ПО**
  В январе вирусная база компании «Доктор Веб» пополнилась большим числом записей для разнообразных коммерческих шпионских приложений, предназначенных для установки на мобильные Android-устройства и осуществления слежки за их владельцами.
- **Угрозы в каталоге Google Play**
  Агрессивные и потенциально опасные рекламные платформы для мобильных устройств остаются актуальной проблемой. Одна из таких систем была внедрена в ряде бесплатных программ, размещенных в каталоге Google Play.

УЗНАЙТЕ БОЛЕЕ ПОДРОБНУЮ ИНФОРМАЦИЮ О ВРЕДОНОСНЫХ ПРОГРАММАХ ДЛЯ МОБИЛЬНОЙ ПЛАТФОРМЫ Google Android, ОЗНАКОМИВШИСЬ С НАШИМ СПЕЦИАЛЬНЫМ ОБЗОРОМ.

Обзор вирусной активности в январе 2015 года

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.

«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.

Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах