Dr.WEB®
с 1992 года

Обзор вирусной активности в декабре 2015 года

Обзор вирусной активности в декабре 2015 года

24 декабря 2015 года

Первый месяц зимы традиционно оказывается довольно-таки спокойным с точки зрения событий в сфере информационной безопасности — в преддверии новогодних и рождественских праздников вирусописатели редко проявляют повышенную активность. Не стал исключением и декабрь 2015 года. В начале месяца было зафиксировано распространение троянца для ОС Linux, способного скачивать и устанавливать на инфицированном устройстве различные программы, а также установщика нежелательных приложений для OS X. Вместе с тем вирусные аналитики компании «Доктор Веб» вновь зафиксировали распространение опасного банковского троянца для мобильной платформы Google Android, который был обнаружен еще в начале года и к настоящему моменту выявлен на мобильных устройствах более чем 31 000 раз.

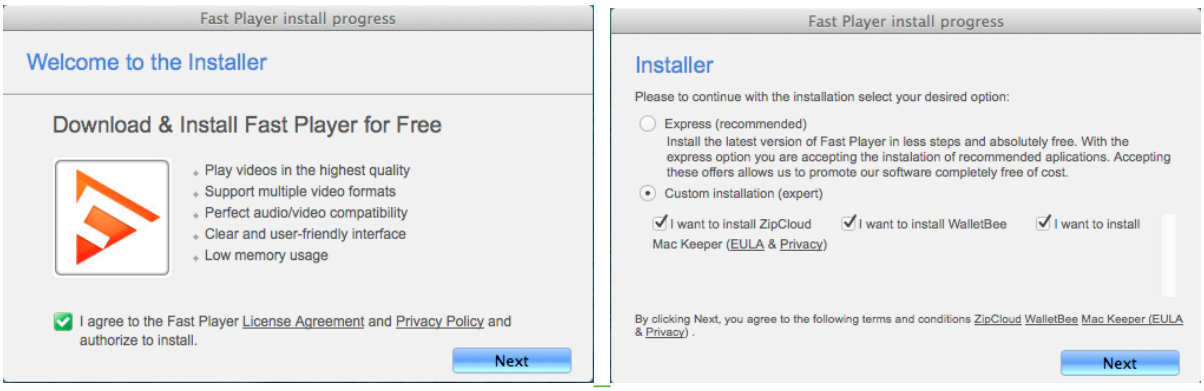
Главные тенденции декабря

- Распространение новой троянской программы для Linux
- Появление установщика нежелательных приложений для OS X
- Распространение опасного банковского троянца для Android

Обзор вирусной активности в декабре 2015 года

Угроза месяца

Интерес злоумышленников к операционной системе OS X постепенно увеличивается — об этом говорит непрерывный рост количества вредоносных программ для этой платформы. Причем подавляющее большинство угроз для компьютеров Apple в настоящее время представляет собой рекламных троянцев и установщиков нежелательных приложений. Именно к последней категории относится Adware.Mac.Tuguu.1, обнаруженный вирусными аналитиками компании «Доктор Веб» в декабре 2015 года. Adware.Mac.Tuguu.1 позволяет скрытно устанавливать на «мак» потенциальной жертвы различные дополнительные приложения, обычно — бесполезные, а иногда и вредоносные.

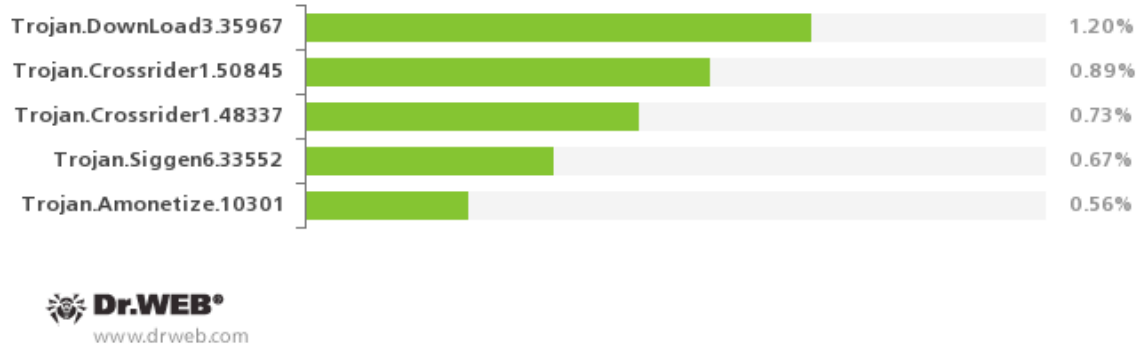


Данный установщик распространяется под видом различных бесплатных программ для OS X. При запуске Adware.Mac.Tuguu.1 считывает содержимое конфигурационного файла «.payload», расположенного в той же папке, откуда была запущена программа, определяет адрес управляющего сервера, специальным образом модифицирует его и обращается к нему за списком дополнительного ПО, установка которого будет предложена пользователю. Все данные, которыми данная программа обменивается с командным центром, шифруются. Судя по используемой установщиком внутренней нумерации, всего существует 736 различных приложений, которые Adware.Mac.Tuguu.1 может установить на пользовательский «мак». При этом перед началом установки Adware.Mac.Tuguu.1 проверяет, совместимы ли предлагаемые им программы друг с другом — так, например, он не станет инсталлировать вместе приложения MacKeeper и MacKeeper Grouped. Также Adware.Mac.Tuguu.1 пытается удостовериться, что такое ПО не было ранее установлено в системе, а перед завершением своей работы проверяет успешность установки. Более подробную информацию об этом опасном приложении можно получить, ознакомившись с опубликованной на сайте компании «Доктор Веб» информационной статьей.

Обзор вирусной активности в декабре 2015 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

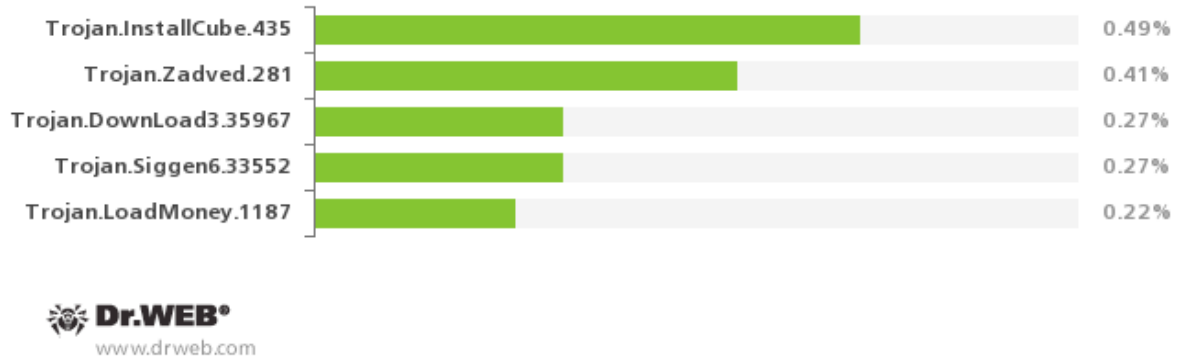


- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.Crossrider1.50845, Trojan.Crossrider1.48337**
  Представители семейства троянцев, предназначенных для демонстрации различной сомнительной рекламы.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.Amonetize.10301**
  Вредоносная программа, предназначенная для установки других нежелательных приложений.

Обзор вирусной активности в декабре 2015 года

По данным серверов статистики «Доктор Веб»

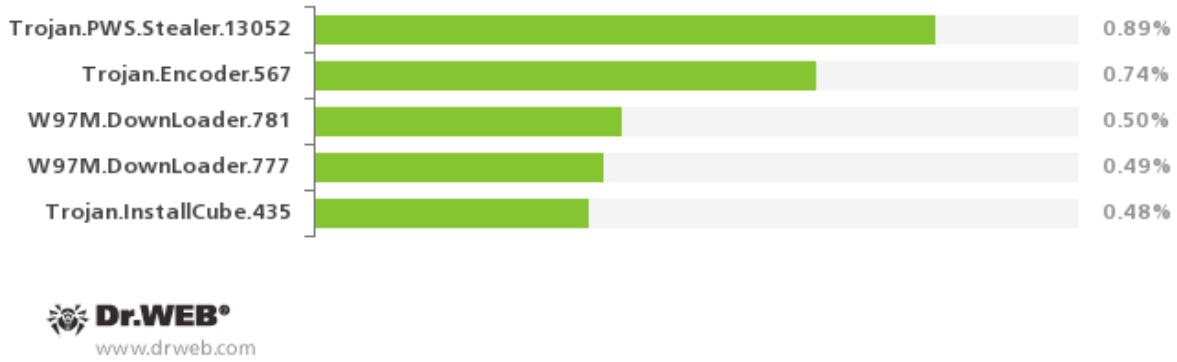
Наиболее распространенные вредоносные программы в декабре 2015 года согласно данным серверов статистики Dr.Web



- **Trojan.InstallCube**
  Семейство программ-загрузчиков, инсталлирующих на компьютер пользователя различные ненужные и нежелательные приложения.
- **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.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.

Статистика вредоносных программ в почтовом трафике

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

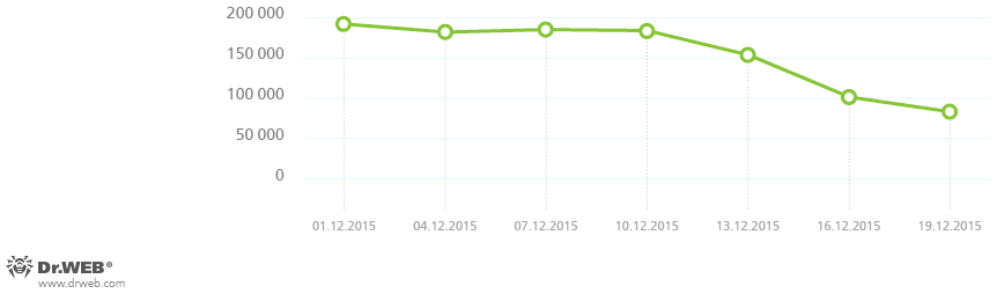


- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **Trojan.Encoder.567**
  Один из представителей семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку. Способен зашифровывать важные файлы, в том числе следующих типов: .jpg, .jpeg, .doc, .docx, .xls, xlsx, .dbf, .1cd, .psd, .dwg, .xml, .zip, .rar, .db3, .pdf, .rtf, .7z, .kwm, .arj, .xlsm, .key, .cer, .accdb, .odt, .ppt, .mdb, .dt, .gsf, .ppsx, .pptx.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в своей работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.
- **Trojan.InstallCube**
  Семейство программ-загрузчиков, инсталлирующих на компьютер пользователя различные ненужные и нежелательные приложения.

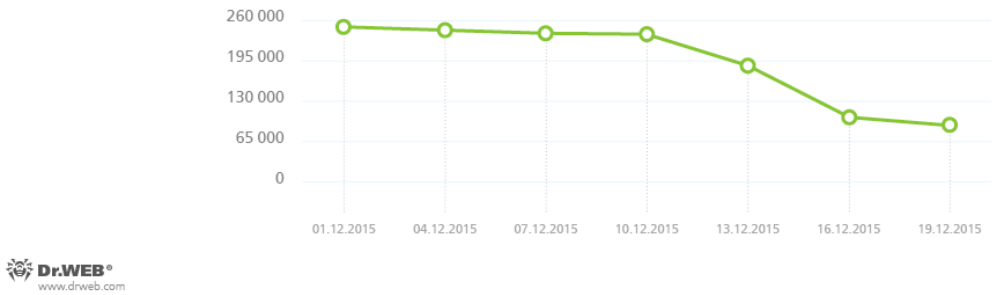
Ботнеты

Специалисты компании «Доктор Веб» продолжают следить за деятельностью бот-сети, созданной злоумышленниками с использованием опасного файлового вирус Win32.Rmnet.12. К концу месяца наметилась тенденция к снижению активности обеих подсетей этого ботнета, о чем свидетельствуют представленные ниже графики:

Активность ботнета Win32.Rmnet.12 в декабре 2015 года (1 подсеть)



Активность ботнета Win32.Rmnet.12 декабре 2015 года (2 подсеть)



Rmnet — это семейство файловых вирусов, распространяющихся без участия пользователя, способных встраивать в просматриваемые пользователям веб-страницы постороннее содержимое (это теоретически позволяет киберпреступникам получать доступ к банковской информации жертвы), а также красть файлы cookies и пароли от наиболее популярных FTP-клиентов и выполнять различные команды, поступающие от злоумышленников.

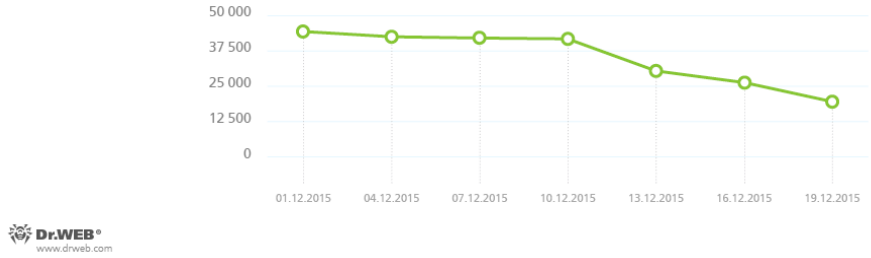
Обзор вирусной активности в декабре 2015 года

Продолжает функционировать и бот-сеть, состоящая из компьютеров, инфицированных файловым вирусом Win32.Sector. Данная вредоносная программа обладает следующими деструктивными функциями:

- 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.

График среднесуточной активности этого ботнета показан на следующей иллюстрации:

Активность ботнета Win32.Sector в декабре 2015 года



Обзор вирусной активности в декабре 2015 года

Трояны-шифровальщики

Количество запросов на расшифровку, поступивших в службу технической поддержки «Доктор Веб»

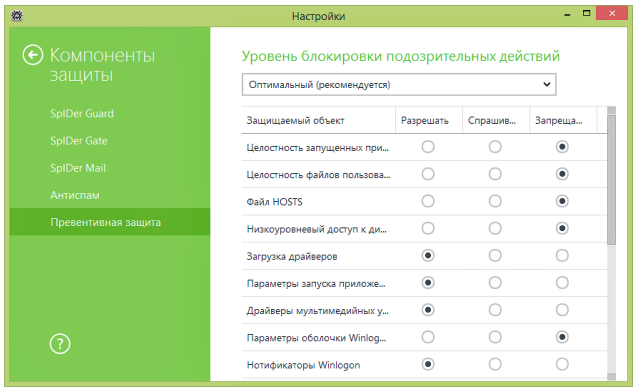
Наиболее распространенные шифровальщики в декабре 2015 года:

- Trojan.Encoder.567
- Trojan.Encoder.2843
- Trojan.Encoder.858

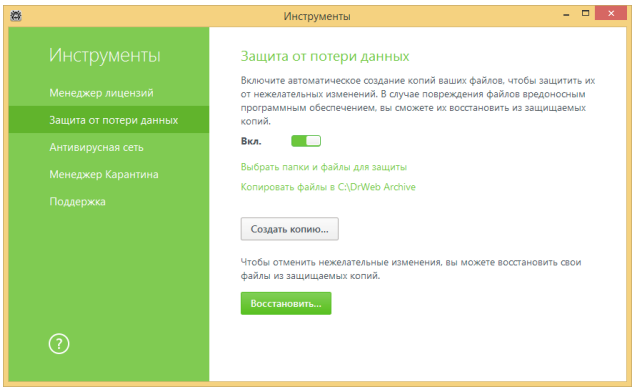
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Узнайте больше

Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека

Вредоносные программы для Linux

Число вредоносных программ для операционных систем семейства Linux постепенно растет: так, в декабре 2015 года вирусные аналитики компании «Доктор Веб» обнаружили троянца Linux.Rekoobe.1, способного по команде злоумышленников скачивать с управляющего сервера и загружать на него различные файлы, а также взаимодействовать с командным интерпретатором Linux на инфицированном устройстве. Первые версии Linux.Rekoobe.1 были ориентированы на заражение работающих под управлением Linux устройств с архитектурой SPARC, однако позже вирусописатели по всей видимости решили модифицировать троянца с целью добиться его совместимости с платформой Intel. При этом специалистам компании «Доктор Веб» известны образцы Linux.Rekoobe.1 как для 32-, так и для 64-разрядных Intel-совместимых версий ОС Linux.

При определенных условиях связь с командным центром этот троянец осуществляет через прокси-сервер, кроме того, Linux.Rekoobe.1 обладает весьма хитроумной системой проверки подлинности получаемых от управляющего сервера «посылок» с зашифрованной информацией. Однако несмотря на столь сложный механизм своей работы Linux.Rekoobe.1 способен выполнять всего лишь три команды злоумышленников, а именно: скачивать с управляющего сервера или загружать на него файлы, передавать принимаемые директивы командному интерпретатору Linux и транслировать полученный вывод на удаленный сервер, благодаря чему киберпреступники получают возможность удаленно взаимодействовать с инфицированным устройством.

Более подробную информацию об этом троянце можно получить из опубликованной на сайте компании «Доктор Веб» статьи.

Опасные сайты

В течение декабря 2015 года в базу нерекомендуемых и вредоносных сайтов было добавлено 210 987 интернет-адресов.

Ноябрь 2015	Декабрь 2015	Динамика
+ 670 545	+ 210 987	- 68.53%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В декабре злоумышленники вновь проявляли интерес к мобильным устройствам, поэтому для их владельцев последний месяц уходящего года стал весьма напряженным. Так, вирусописатели активно распространяли различных банковских троянцев, крадущих деньги со счетов своих жертв. Кроме этого, вирусные аналитики выявили большое число новых СМС-сендеров. Также в декабре была обнаружена очередная вредоносная программа, заражающая мобильные устройства под управлением iOS.

Наиболее заметные события, связанные с «мобильной» безопасностью в декабре:

- Распространение опасных банковских троянцев;
- Появление новых СМС-сендеров;
- Обнаружение нового троянца для iOS.

Более подробно о вирусной обстановке для мобильных устройств в декабре читайте в нашем тематическом обзоре.

Обзор вирусной активности в декабре 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