Dr.WEB®
с 1992 года

Обзор вирусной активности за март 2015 года

Обзор вирусной активности за март 2015 года

2 апреля 2015 года

Первый месяц весны 2015 года ознаменовался появлением новых вредоносных программ для различных системных платформ. Так, некоторые пользователи Windows стали жертвами многофункционального троянца-бэкдора, добавленного в вирусную базу Dr.Web под именем BackDoor.Yebot. По-прежнему продолжают распространяться троянцы-энкодеры, требующие у пользователей выкуп за расшифровку файлов — так, в марте была зафиксирована массовая почтовая рассылка, с помощью которой злоумышленники распространяли шифровальщика Trojan.Encoder.514. Не угасает интерес вирусописателей и к мобильной платформе Google Android, для которой в течение минувшего месяца появлялись новые вредоносные программы.

Главные тенденции марта

- Массовые почтовые рассылки, с помощью которых распространяются троянцы-шифровальщики.
- Появление новых вредоносных программ для мобильной платформы Google Android.

Угроза месяца

В марте 2015 года специалисты компании «Доктор Веб» завершили исследование многофункционального троянца-шпиона **BackDoor.Yebot.** Он распространяется с использованием другой вредоносной программы, добавленной в вирусную базу Dr.Web под именем **Trojan.Siggen6.31836.** Бэкдор **BackDoor.Yebot** обладает следующими функциональными возможностями:

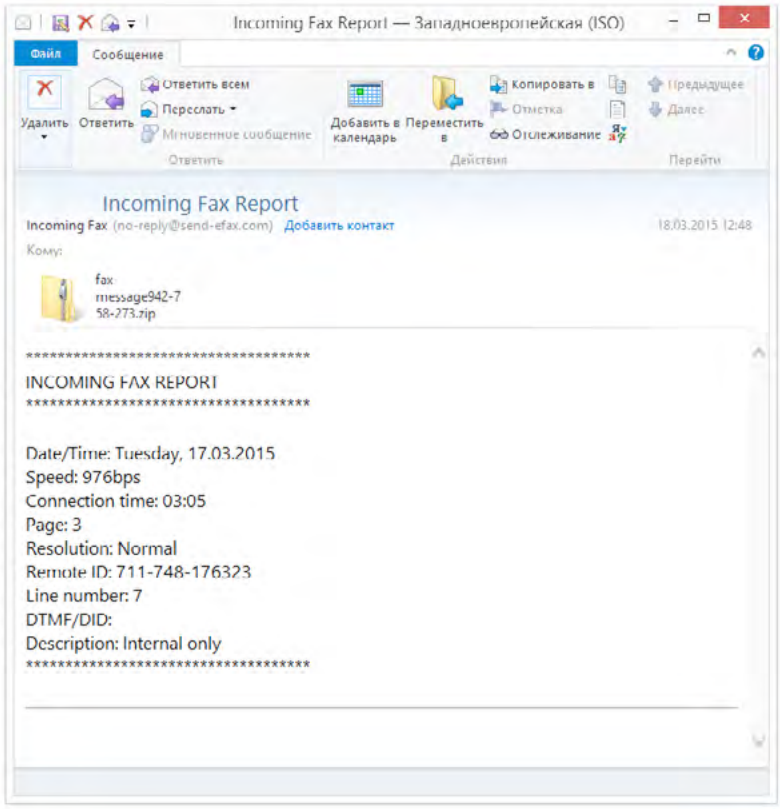
- запуск на инфицированном компьютере FTP-сервера;
- запуск на инфицированном компьютере Socks5 прокси-сервера;
- модификация протокола RDP для обеспечения удаленного доступа к инфицированному компьютеру;
- фиксация нажатий пользователем клавиш (кейлоггинг);
- возможность установки обратной связи с инфицированным ПК для FTP, RDP и Socks5, если в сети используется NAT (бэкконнект);
- перехват данных по шаблонам PCRE (Perl Compatible Regular Expressions) — библиотеки, реализующей работу регулярных выражений в среде Perl, для чего троянец перехватывает все возможные функции, связанные с работой в Интернете;
- перехват токенов SCard;
- встраивание в просматриваемые пользователем веб-страницы постороннего содержимого (веб-инжекты);
- расстановка перехватов различных системных функций в зависимости от принятого конфигурационного файла;
- модификация кода запущенного процесса в зависимости от принятого конфигурационного файла;
- взаимодействие с различными функциональными модулями (плагинами);
- создание снимков экрана;
- поиск в инфицированной системе приватных ключей.

Обзор вирусной активности за март 2015 года

Более подробную информацию об этой вредоносной программе, способах ее распространения и методах работы можно получить, ознакомившись с опубликованной на сайте компании «Доктор Веб» информационной статьей.

Троянцы-шифровальщики

В марте активизировались злоумышленники, распространяющие троянцев-шифровальщиков с использованием массовых почтовых рассылок. Так, в минувшем месяце вирусописатели активно рассылали письма с заголовком «Incoming Fax Report» якобы от имени службы по передаче факсов через Интернет. В приложении к письму под видом факсимильного сообщения содержался ZIP-архив, внутри которого располагался вредоносный SCR-файл, детектируемый антивирусным ПО Dr.Web как **Trojan.DownLoader11.32458**.



Обзор вирусной активности за март 2015 года

При попытке открытия вложения вредоносная программа **Trojan.DownLoader11.32458** распаковывает и запускает на атакуемом компьютере троянца-энкодера **Trojan.Encoder.514**, шифрующего хранящиеся на диске пользовательские файлы и требующего выкуп за их расшифровку. Подробности об этом инциденте рассказаны в опубликованной нами статье.

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

Февраль 2015	Март 2015	Динамика
1840	2361	+ 28.31%

Наиболее распространенные шифровальщики в марте 2015 года:

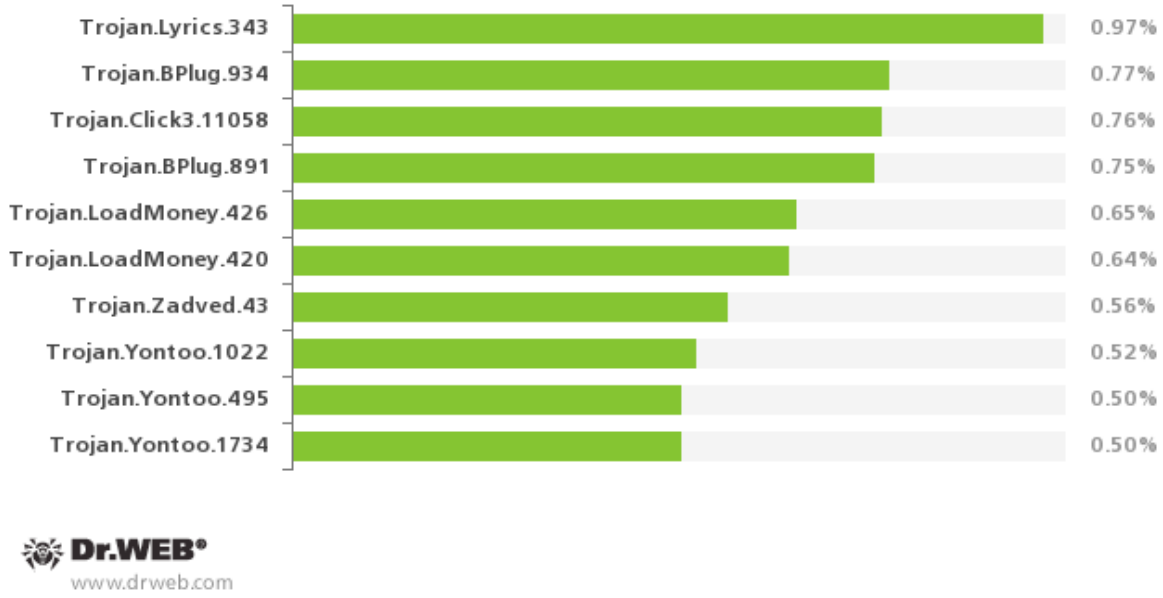
- Trojan.Encoder.761;
- Trojan.Encoder.858;
- BAT.Encoder;
- Trojan.Encoder.741;
- Trojan.Encoder.567.

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.*

Обзор вирусной активности за март 2015 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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



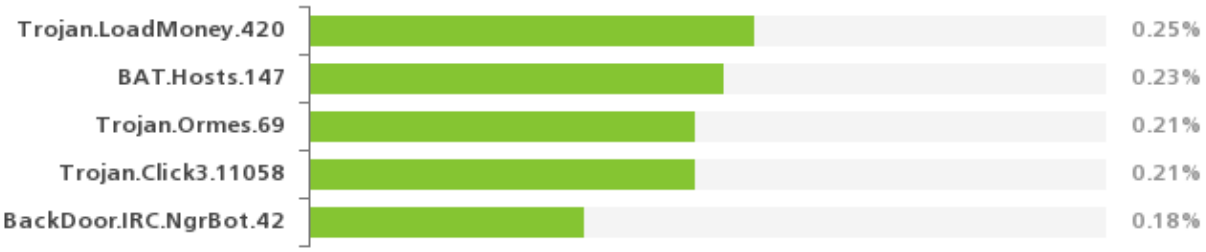
- **Trojan.Lyrics**
  Семейство троянцев, способных демонстрировать на экране назойливую рекламу и открывать в окне браузера веб-сайты сомнительного содержания без ведома пользователя.
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.
- **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.LoadMoney**
  Семейство троянцев, способных демонстрировать на экране назойливую рекламу и открывать в окне браузера веб-сайты сомнительного содержания без ведома пользователя.

Обзор вирусной активности за март 2015 года

- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **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.Yontoo**
  Семейство надстроек для популярных браузеров, назначение которых заключается в демонстрации пользователю рекламы при просмотре веб-страниц.

По данным серверов статистики «Доктор Веб»

Наиболее распространенные вредоносные программы в марте2015 года согласно данным серверов статистики Dr.Web



Dr.WEB®
www.drweb.com

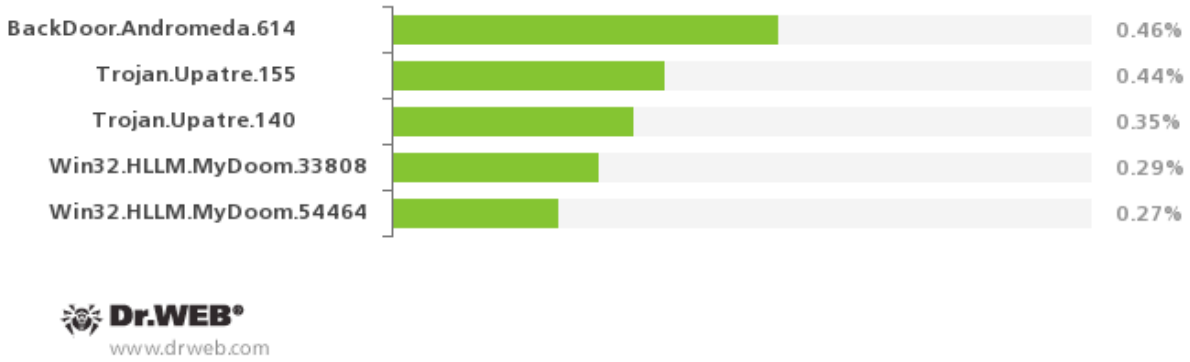
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **BAT.Hosts.147**
  Вредоносный сценарий, позволяющий изменить содержимое файла hosts, расположенного в системной папке Windows и отвечающего за трансляцию DNS-имен сайтов в их сетевые адреса. В результате при попытке перейти на один из указанных в данном файле сайтов браузер автоматически перенаправляется на специально созданную злоумышленниками веб-страницу.

Обзор вирусной активности за март 2015 года

- **Trojan.Ormes.69**
  Рекламный троянец, демонстрирующий пользователю назойливую рекламу при просмотре веб-страниц.
- **Trojan.Click**
  Семейство вредоносных программ, предназначенных для накрутки посещаемости различных интернет-ресурсов путем перенаправления запросов жертвы на определенные сайты с помощью управления поведением браузера.
- **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).

Статистика вредоносных программ в почтовом трафике

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



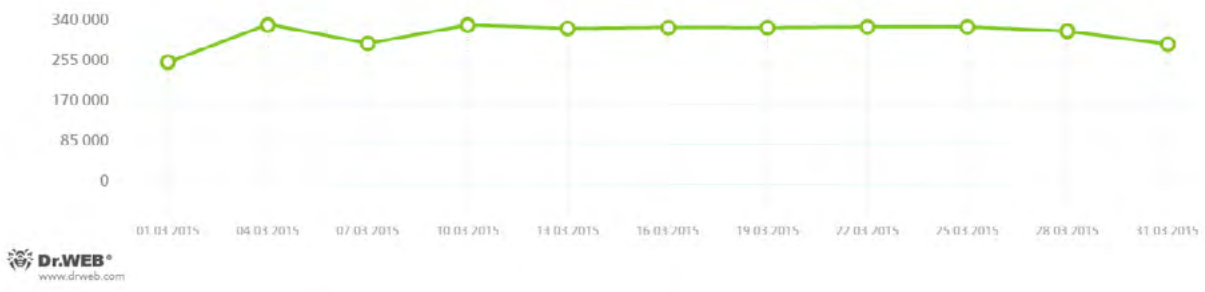
- **BackDoor.Andromeda**
  Семейство троянцев-загрузчиков, предназначенных для скачивания с удаленных серверов злоумышленников и запуска на инфицированном компьютере других вредоносных программ.
- **Trojan.Upatre**
  Семейство троянцев-загрузчиков, предназначенных для скачивания на инфицированный компьютер и скрытной установки других вредоносных приложений.
- **Win32.HLLM.MyDoom**
  Давно известное и широко распространенное семейство почтовых червей, способных рассылать себя по каналам электронной почты без участия пользователя, для чего они собирают информацию о почтовых адресах потенциальных жертв непосредственно на инфицированном компьютере.

Ботнеты

Специалисты компании «Доктор Веб» продолжают следить за деятельностью бот-сети, созданной злоумышленниками с использованием файлового вируса **Win32.Rmnet.12**. Среднесуточная активность двух подсетей этого ботнета показана на следующих диаграммах:

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

Активность ботнета Win32.Rmnet.12 в марте 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 за март 2015 года

Также продолжает свою деятельность бот-сеть, созданная злоумышленниками с использованием файлового вируса **Win32.Sector**, реализующего следующие функциональные возможности:

- 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.

Среднесуточная активность этого ботнета в марте 2015 года показана на следующей диаграмме:

Активность ботнета Win32.Sector в марте 2015 года

Также специалисты компании «Доктор Веб» продолжают наблюдать за активностью ботнета Back.Door.Flashback.39:

Активность ботнета BackDoor.Flashback. в марте 2015 года

Обзор вирусной активности за март 2015 года

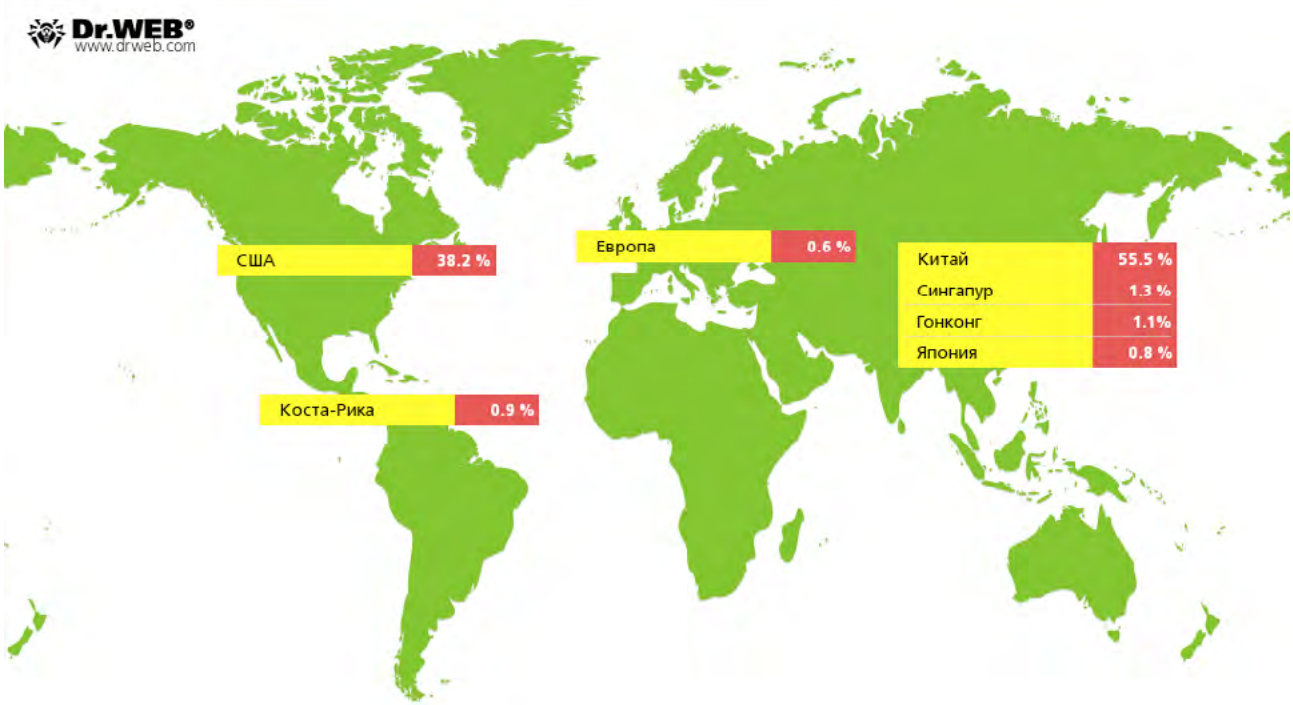
BackDoor.Flashback.39

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

По-прежнему проявляет активность Linux-троянец **Linux.BackDoor.Gates.5**, продолжающий осуществлять DDoS-атаки на различные интернет-ресурсы.

В марте 2015 года специалистами «Доктор Веб» было зафиксировано 2236 уникальных IP-адресов, на которые осуществлялись атаки, что почти в два раза больше по сравнению с прошлым месяцем.

Большинство из атакованных ресурсов, как и ранее, расположено на территории Китая, на втором месте располагаются США:



Мошеннические и нерекомендуемые сайты

Для защиты пользователей от различных способов мошенничества в Интернете служат компоненты SpiDerGate и Родительский контроль, входящие 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 марта 2015 года в базу нерекомендуемых и вредоносных сайтов Dr.Web было добавлено 74 108 интернет-адресов.

Февраль 2015	Март 2015	Динамика
22 033	74 108	+ 236.35%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для Android

Прошедший март оказался весьма неспокойным месяцем для владельцев мобильных Android-устройств: злоумышленники не переставали совершать атаки на пользователей и применяли для этого как известные, так и новые вредоносные программы. Самыми актуальными Android-троянцами в марте стали:

- СМС-троянцы
- Троянцы-вымогатели
- Банкеры

БОЛЕЕ ПОДРОБНУЮ ИНФОРМАЦИЮ О ВРЕДОНОСНЫХ ПРОГРАММАХ ДЛЯ МОБИЛЬНОЙ ПЛАТФОРМЫ Android ЧИТАЙТЕ В НАШЕМ СПЕЦИАЛЬНОМ ОБЗОРЕ.

Обзор вирусной активности за март 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