Dr.WEB®
с 1992 года

Обзор вирусной активности в июле 2015 года

Обзор вирусной активности в июле 2015 года

30 июля 2015 года

В июле 2015 года вновь активизировались вирусописатели, создающие вредоносные программы для операционных систем семейства Linux. Также вирусные базы Dr.Web пополнились новыми записями для троянцев, угрожающих пользователям ОС Windows. Не сидят сложа руки и злоумышленники, создающие опасное ПО для мобильной платформы Google Android: в июле вирусные аналитики компании «Доктор Веб» обнаружили множество подобных троянцев, а одного из них пользователи даже скачали с различных интернет-ресурсов более 1,5 млн. раз.

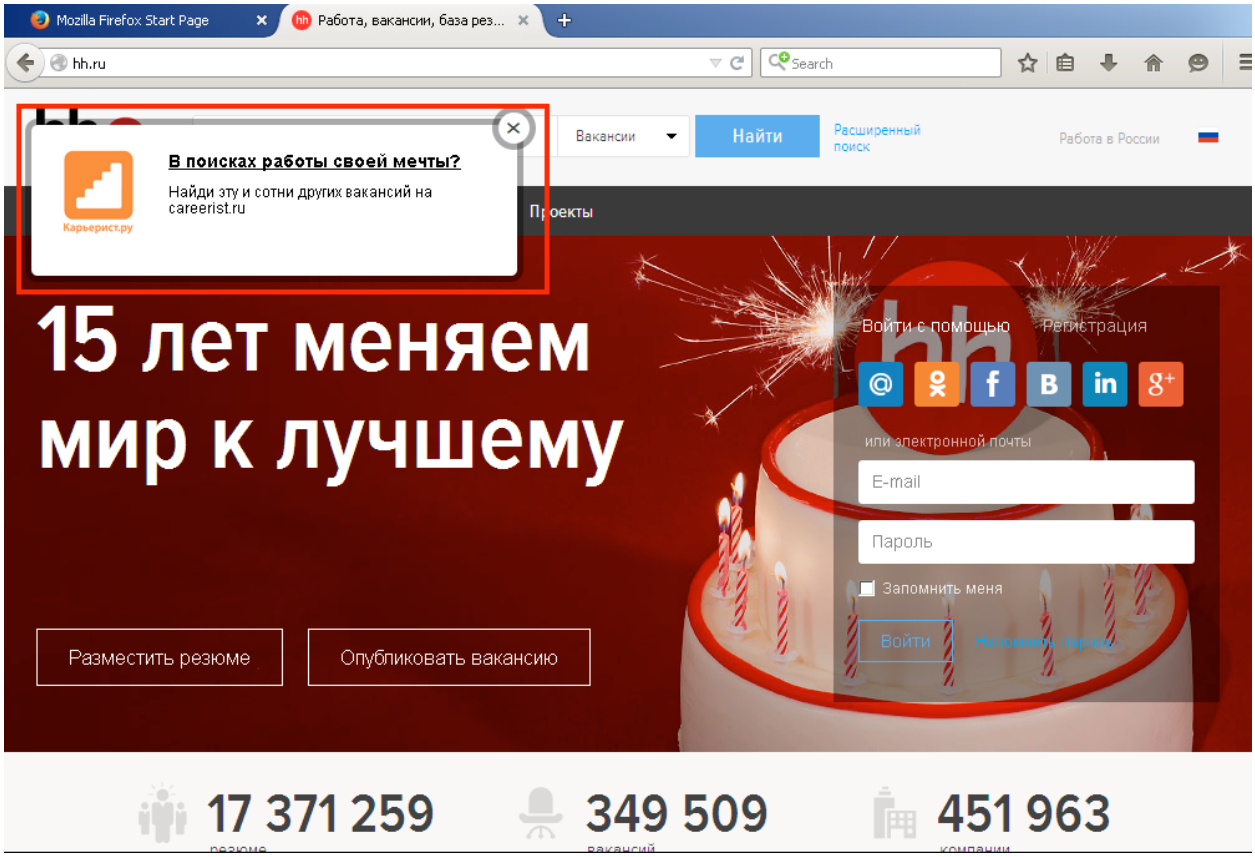
Главные тенденции июля

- Появление новых троянцев для операционных систем семейства Linux
- Рост количества вредоносных программ для Microsoft Windows
- Распространение троянцев для мобильной платформы Google Android

Обзор вирусной активности в июле 2015 года

Угроза месяца

Вредоносные программы, предназначенные для демонстрации жертвам назойливой рекламы при открытии в окне браузера различных веб-страниц, постепенно совершенствуются, используемые ими алгоритмы — усложняются, а ассортимент таких троянцев постепенно растет. Так, в июле 2015 года вирусными аналитиками компании «Доктор Веб» был обнаружен троянец Trojan.Ormes.186, использующий технологию веб-инжектов для внедрения в веб-страницы посторонней рекламы.



Trojan.Ormes.186 реализован в виде расширения для браузеров Mozilla Firefox, Chrome и Opera, распространяется он с использованием программ-дропперов. В теле вредоносной программы содержится список, состоящий из порядка 200 адресов интернет-ресурсов, при обращении к которым Trojan.Ormes.186 выполняет веб-инжекты. Среди них — различные сайты для поиска и размещения вакансий, а также адреса популярных поисковых систем и социальных сетей.

Обзор вирусной активности в июле 2015 года

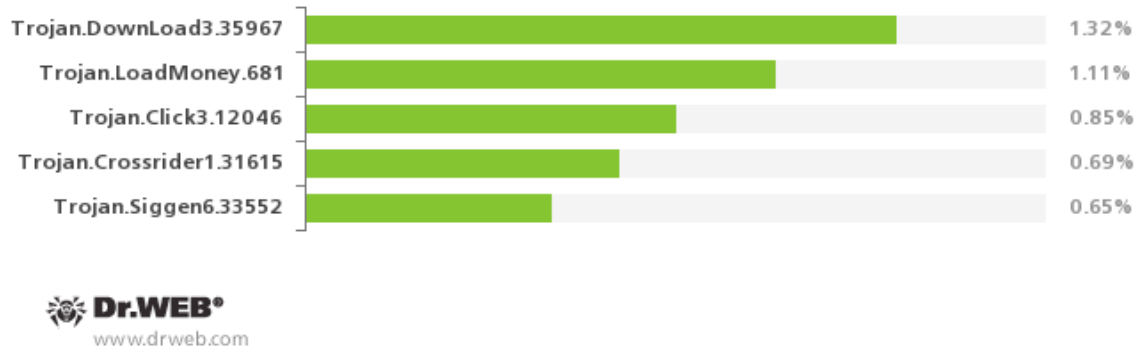
Помимо встраивания в веб-страницы рекламных баннеров, троянец обладает возможностью эмулировать щелчки мышью по различным элементам веб-страниц с целью подтверждения подписок для абонентов мобильных операторов «Мегафон» и «Билайн». Можно смело сказать, что эта вредоносная программа обладает значительным количеством функциональных возможностей:

- встраивание в веб-страницы рекламы с использованием веб-инжектов;
- при открытии в окне браузера сайтов «Яндекс», Youtube, а также социальных сетей «ВКонтакте», «Одноклассники» и Facebook перенаправление пользователя через цепочку редиректов на сайты различных файлообменных систем, использующих для монетизации платные подписки;
- подмена выдачи в популярных поисковых системах;
- установка отметок «Like» («мне нравится») различным сайтам в социальной сети Facebook;
- автоматический вход на сайты некоторых онлайн-казино и автоматическая установка приложения казино для социальных сетей.

Более подробная информация о данной угрозе приведена в опубликованной на сайте компании «Доктор Веб» обзорной статье.

По данным статистики лечащей утилиты Dr.Web CureIt!

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



Обзор вирусной активности в июле 2015 года

- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **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.Crossrider1.31615**
  Троянская программа, предназначенная для демонстрации пользователям Интернета различной сомнительной рекламы.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.

По данным серверов статистики «Доктор Веб»

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

Dr.WEB®
www.drweb.com

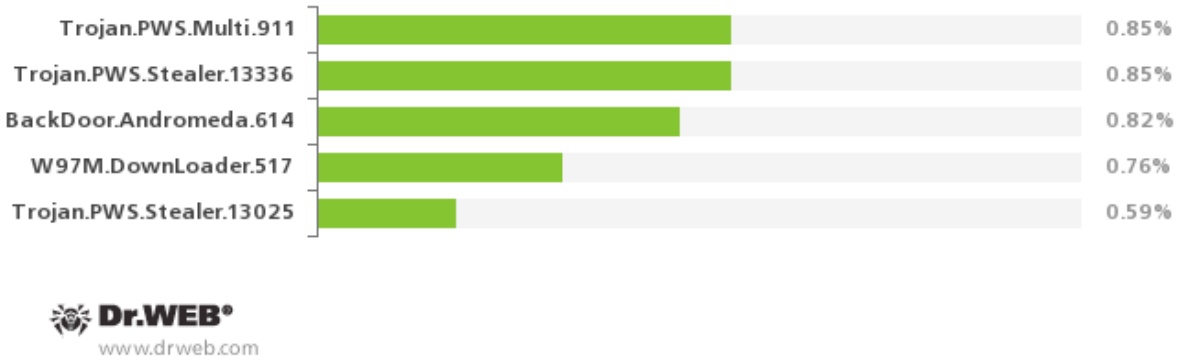
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.Installmonster**
  Семейство вредоносных программ, созданных с использованием партнерской программы installmonster. Данные приложения устанавливают на компьютер жертвы различное нежелательное ПО.

Обзор вирусной активности в июле 2015 года

- **Trojan.Kbdmai.8**
  Представитель семейства вредоносных программ, предназначенных для загрузки из Интернета и запуска на инфицированном компьютере других опасных приложений.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.

Статистика вредоносных программ в почтовом трафике

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



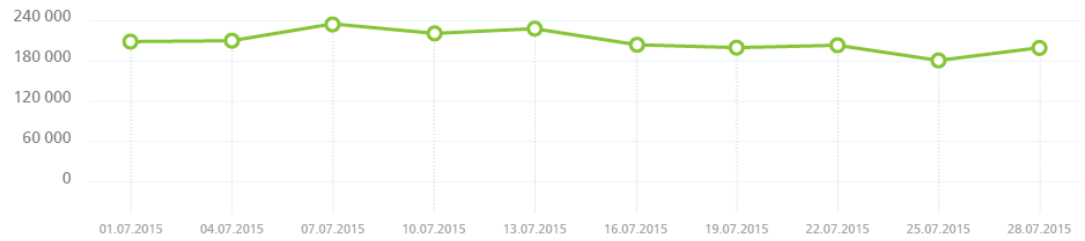
- **Trojan.PWS.Multi.911**
  Представитель семейства банковских троянцев, предназначенных для кражи на инфицированном компьютере различной конфиденциальной информации, в том числе данных, необходимых для доступа к системам дистанционного банковского обслуживания.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой ценной конфиденциальной информации.

- **BackDoor.Andromeda**
  Семейство троянцев-загрузчиков, предназначенных для скачивания с удаленных серверов злоумышленников и запуска на инфицированном компьютере других вредоносных программ.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Ботнеты

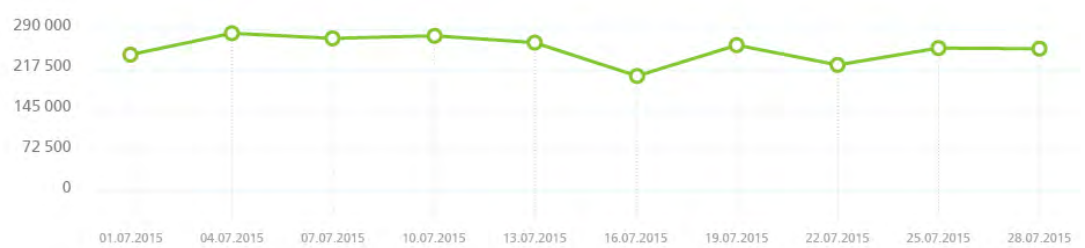
В июле, как и прежде, продолжают функционировать бот-сети, за деятельностью которых внимательно следят вирусные аналитики компании «Доктор Веб». Среди них — ботнет, состоящий из зараженных файловым вирусом Win32.Rmnet.12 компьютеров, активность двух подсетей которого показана на следующих диаграммах:

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



Dr.WEB®
www.drweb.com

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



Dr.WEB®
www.drweb.com

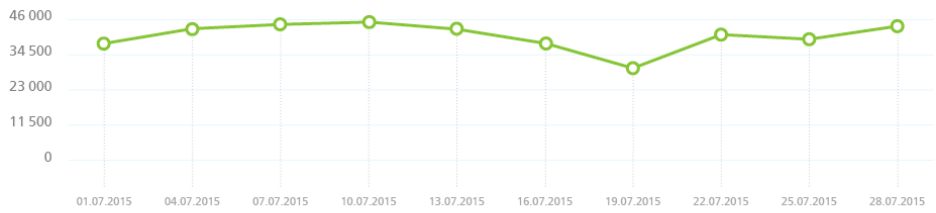
Обзор вирусной активности в июле 2015 года

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.

Также продолжает свое существование бот-сеть, состоящая из зараженных вирусом Win32.Sector. компьютеров — ее среднесуточная активность показана на следующей иллюстрации. 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.

Активность ботнета Win32.Sector в июле 2015 года



По сравнению с предыдущим месяцем еще заметнее снизилось число DDoS-атак на веб-сайты, предпринятых злоумышленниками с использованием вредоносной программы Linux.BackDoor.Gates.5. Число целей этих атак в июле составило 954, что на 25,7% меньше июньских показателей. Сократились и географические масштабы использования ботнета: 74.8% атак приходится на веб-сайты, расположенные на территории Китая, еще 20.4% атакованных сайтов находится в США.

Обзор вирусной активности в июле 2015 года

Троянцы-шифровальщики

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

Июль 2015	Июль 2015	Динамика
1417	1414	- 0,2 %

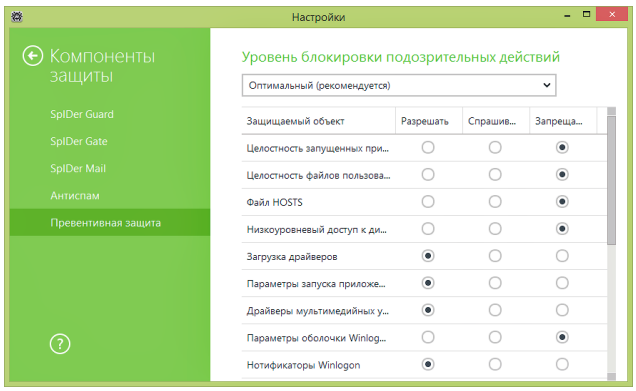
Наиболее распространенные шифровальщики в июле 2015 года:

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

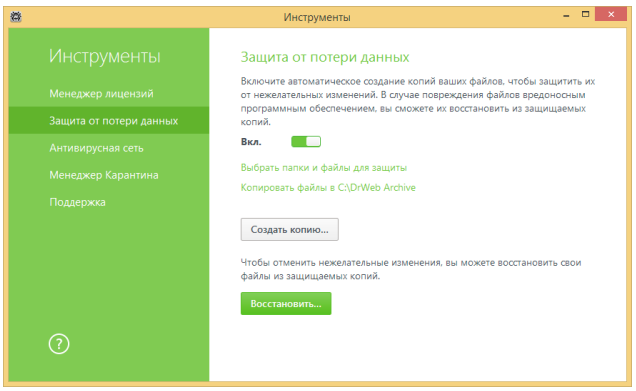
Dr.Web Security Space 10.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Вредоносные программы для Linux

Злоумышленники продолжают создавать все новые и новые вредоносные программы для операционных систем семейства Linux. В июле 2015 года вирусные аналитики компании «Доктор Веб» обнаружили еще одного троянца для этой платформы, получившего наименование Linux.BackDoor.Dklkt.1.

Этот бэкдор по задумке авторов должен реализовывать довольно обширный набор функций, однако на текущий момент большая часть предусмотренных в его архитектуре команд игнорируется. Фактически троянец в состоянии выполнять следующие команды злоумышленников: директиву начала DDoS-атаки, запуска SOCKS proxy-сервера, запуска указанного в пришедшей команде приложения, перезагрузки или выключения компьютера. Исходные компоненты бэкдора были созданы таким образом, чтобы исполняемый файл можно было собрать как для архитектуры Linux, так и для Windows. Более подробно функциональные возможности и особенности этой вредоносной программы описаны в опубликованной нами статье.

Опасные сайты

В течение июля 2015 года в базу нерекомендуемых и вредоносных сайтов было добавлено 821 409 интернет-адреса.

Июнь 2015	Июль 2015	Динамика
+ 978 982	+ 821 409	- 16 %

Вредоносное и нежелательное ПО для Android

Прошедший июль оказался весьма насыщенным на события вирусной тематики в мобильном сегменте: на протяжении всего месяца специалисты компании «Доктор Веб» фиксировали появление очередных вредоносных Android-приложений, а также отмечали различные атаки на пользователей Android-смартфонов и планшетов. В частности, в конце месяца вирусными аналитиками был обнаружен троянец Android.DownLoader.171.origin, распространявшийся в официальном каталоге приложений Google Play. Общее количество его загрузок с учетом альтернативных площадок составило порядка 1,5 млн. Этот троянец умеет не только устанавливать программы по команде злоумышленников, но также незаметно для пользователя удалять их. Кроме того, он способен демонстрировать пользователю уведомление в панели нотификаций Android, при нажатии на которое открывается окно браузера и выполняется переход на указанный злоумышленниками веб-сайт. Дополнительную информацию об этой вредоносной программе можно получить, ознакомившись с соответствующей статьей.

Наиболее заметные тенденции в сфере безопасности ОС Android в июле:

- использование злоумышленниками для собственного обогащения различных рекламных платформ в составе Android-троянцев;
- появление в каталоге Google play новых вредоносных приложений;
- распространение новых Android-вымогателей;
- появление очередных опасных троянцев-бэкдоров, выполняющих вредоносные действия по команде вирусописателей;
- увеличение числа СМС-троянцев.

Обзор вирусной активности в июле 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