Dr.WEB®
с 1992 года

Обзор вирусной активности в мае 2015 года

Обзор вирусной активности в мае 2015 года

29 мая 2015 года

Май 2015 года выдался относительно спокойным с точки зрения информационной безопасности, т.к. не наблюдалось какой-либо существенной активизации бот-сетей или массовых вредоносных рассылок.

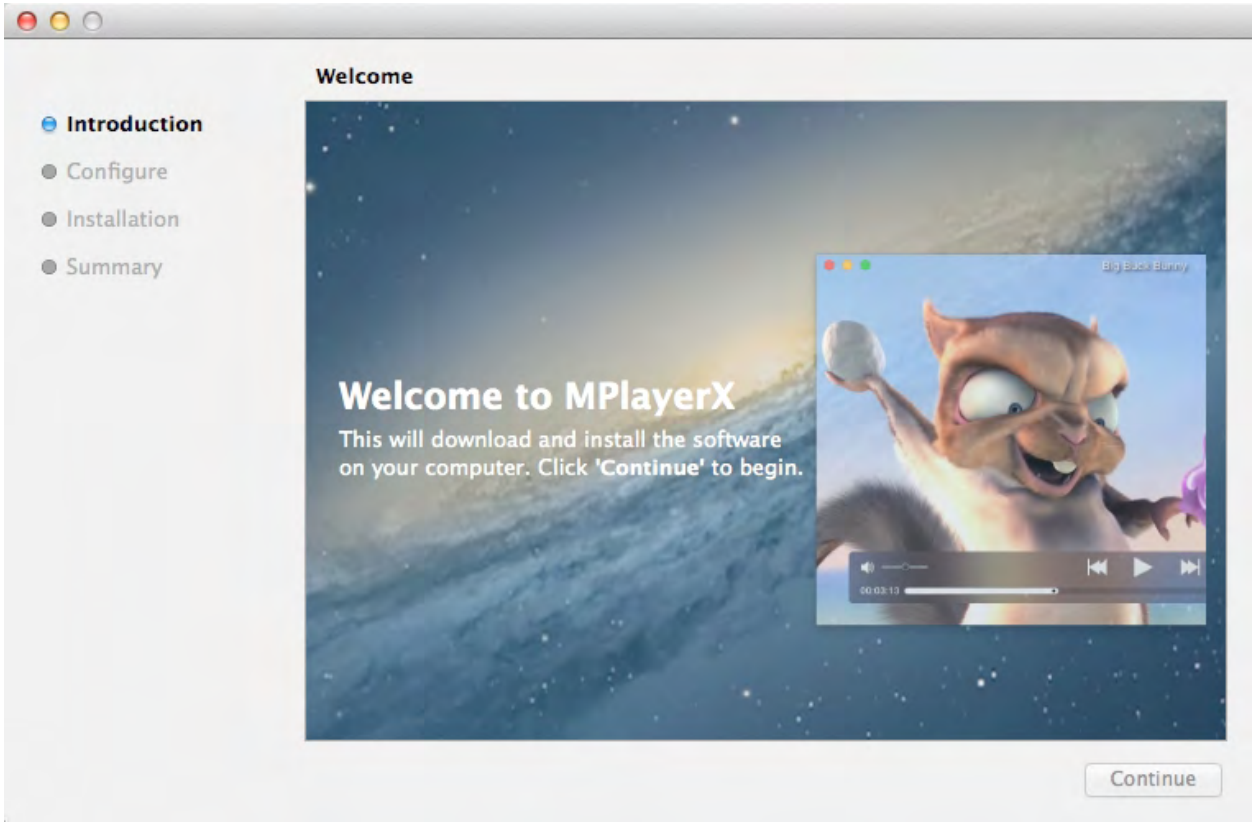
Главные тенденции мая

- Увеличение числа обнаруженных рекламных программ или установщиков нежелательных приложений для платформы Mac OS X.
- Активизация сетевых мошенников, выманивающих деньги у доверчивых интернет-пользователей.
- Появление новых вредоносных программ для мобильной платформы Google Android.

Обзор вирусной активности в мае 2015 года

Угроза месяца

Пользователей Windows уже давно не удивишь наличием большого числа установщиков совершенно ненужных и бесполезных приложений, однако для операционной системы Mac OS X подобные программы все же редкость. Тем интереснее для исследователей компании «Доктор Веб» оказалось приложение, добавленное в вирусные базы Dr.Web под именем Adware.Mac.InstallCore.1



Обзор вирусной активности в мае 2015 года

Помимо собственно инсталляции ненужных пользователю программ, состоящий из нескольких компонентов установщик Adware.Mac.InstallCore.1 способен изменять стартовую страницу и используемую браузерами по умолчанию поисковую систему. Кроме того, эта программа обладает функциями антиотладки: если при запуске ей удается обнаружить работающие на «маке» виртуальные машины, ряд антивирусов, а также некоторые иные приложения, пользователю не будут навязываться какие-либо дополнительные программы. Среди программ и утилит, устанавливаемых на компьютер Adware.Mac.InstallCore.1, можно перечислить следующие:

- Yahoo Search;
- MacKeeper (Program.Unwanted.MacKeeper);
- ZipCloud;
- WalletBee (Adware.Mac.DealPly.1);
- MacBooster 2 (Program.Unwanted.MacBooster);
- PremierOpinion (Mac.BackDoor.OpinionSpy);
- RealCloud;
- MaxSecure;
- iBoostUp;
- ElmediaPlayer.

Более подробную информацию об этом установщике можно получить, ознакомившись с опубликованным компанией «Доктор Веб» информационным материалом

Для Mac OS X

Из проанализированных в мае 2015 года рекламных программ Adware.Mac.InstallCore.1 — не единственная, ориентированная на пользователей Mac OS X. Так, распространяемое ею приложение WalletBee, добавленное в вирусные базы Dr.Web под именем **Adware.Mac.DealPly**, предназначено для установки различных расширений для браузеров Chrome и Safari.

Другая рекламная программа для компьютеров Apple получила наименование **Adware.Mac.WebHelper** — с этим названием в вирусные базы были добавлены приложения, распространяющиеся под именами WebTools и ShopMall. Сам пакет состоит из набора сценариев командного интерпретатора sh, скриптов на языке Python и нескольких бинарных файлов.

Автозагрузка **Adware.Mac.WebHelper** обеспечивается с использованием файлов .plist. Приложение способно подменять начальную страницу для браузеров Chrome, Firefox и Safari, а также изменять установленную в настройках браузера по умолчанию поисковую систему на my-search-start.com. Входящий в состав **Adware.Mac.WebHelper** бинарный файл выполняет в бесконечном цикле два сценария AppleScript — один для бразуера Chrome, второй — для Safari, которые встраивают в просматриваемые пользователем веб-страницы код на языке JavaScript, а тот, в свою очередь, загружает еще 4 JavaScript-сценария, показывающих в окне браузера рекламу.

Еще одной вредоносной программой со схожим функционалом, угрожающей пользователям Mac OS X, стал **Mac.Trojan.Crossrider**. Троянцы семейства Crossrider хорошо известны пользователям Microsoft Windows, однако новая версия этой вредоносной программы ориентирована на компьютеры производства компании Apple.

Обзор вирусной активности в мае 2015 года

Распространяется **Mac.Trojan.Crossrider** в виде установочного пакета с названием Safari Helper. При запуске установщика на экран не выводится никаких диалоговых окон, однако в этот момент на компьютер устанавливается расширение FlashMall для браузеров Safari, Chrome и Firefox. Кроме того, в автозагрузку устанавливаются два приложения: «WebSocketServerApp» и «Safari Security»: первое из них осуществляет связь с управляющим сервером, второе — устанавливает расширения в браузеры. Также в автозагрузку прописывается несколько сценариев командного интерпретатора, предназначенных для обновления браузерных расширений.

Все рекламные и вредоносные приложения для Mac OS X, обнаруженные специалистами нашей компании, были добавлены в вирусные базы Антивируса Dr.Web для Mac OS X.

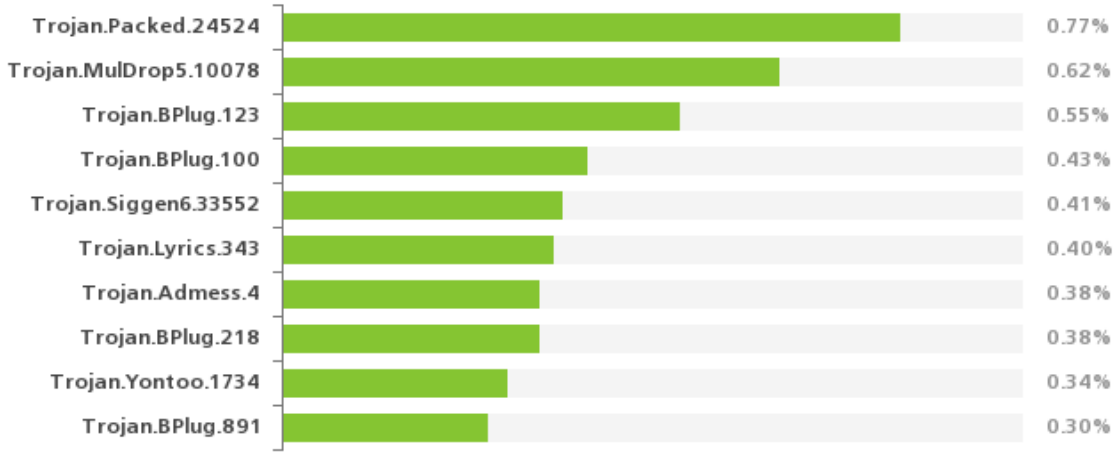
Узнайте подробности о вредоносных программах для Mac OS X!
Посмотрите видео о том, как вредоносные программы проникают на «маки»

По данным статистики лечащей утилиты Dr.Web CureIt!

Всего в течение месяца выявлено 84 063 249 вредоносных и потенциально опасных объектов.

Апрель 2015	Май 2015	Динамика
73 149 430	84 063 249	+ 14.9 %

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



Обзор вирусной активности в мае 2015 года

- **Trojan.Packed.24524**
  Троянец-установщик рекламных и нежелательных приложений.
- **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.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.Lyrics**
  Семейство троянцев, способных демонстрировать на экране назойливую рекламу и открывать в окне браузера веб-сайты сомнительного содержания без ведома пользователя.
- **Trojan.Admess**
  Семейство троянцев, предназначенных для подмены рекламных модулей на просматриваемых пользователем веб-страницах, а также для отображения на таких страницах посторонней рекламы.
- **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 мае2015 года
согласно данным серверов статистики Dr.Web

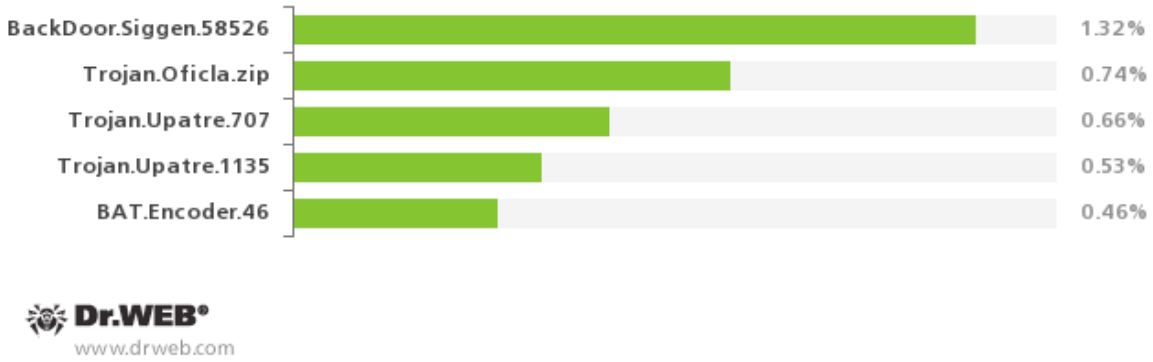
Dr.WEB®
www.drweb.com

Обзор вирусной активности в мае 2015 года

- **Trojan.InstallCube**
  Семейство программ-загрузчиков, инсталлирующих на компьютер пользователя различные ненужные и нежелательные приложения.
- **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 мае 2015 года

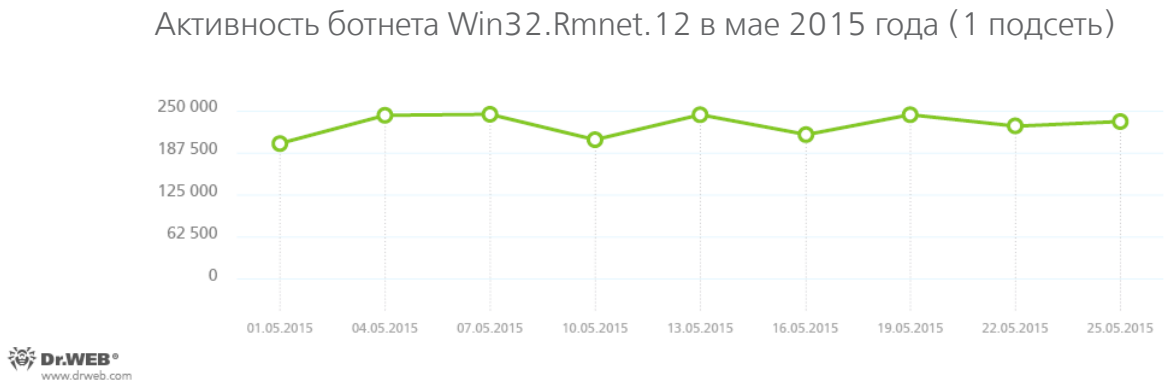


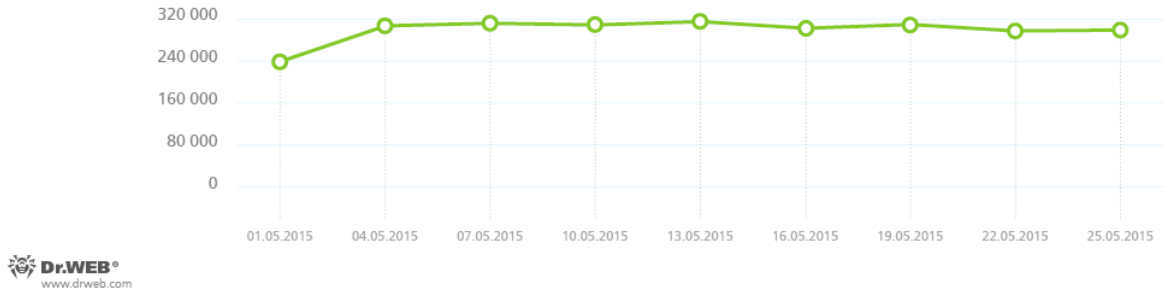
- **BackDoor.Siggen.58526**
  Троянец, без ведома пользователей загружающий и запускающий на инфицированном компьютере другие вредоносные программы, а также способный выполнять поступающие от злоумышленников команды.
- **Trojan.Oficla**
  Семейство троянцев, распространяющихся преимущественно по каналам электронной почты. При заражении компьютера они скрывают свою вредоносную активность. В дальнейшем Trojan.Oficla включает компьютер в бот-сеть и позволяет злоумышленникам загружать на него другое вредоносное ПО. После заражения системы владельцы бот-сети, формируемой Trojan.Oficla, получают возможность контролировать компьютер жертвы. В частности, они могут загружать, устанавливать и использовать на нем практически любое вредоносное ПО.

- **Trojan.Upatre**
  Семейство троянцев-загрузчиков, предназначенных для скачивания на инфицированный компьютер и скрытной установки других вредоносных приложений.
- **BAT.Encoder.46**
  Один из представителей семейства троянцев-шифровальщиков, шифрующих файлы при помощи легитимной криптографической утилиты GPG с использованием BAT-скриптов.

Ботнеты

Специалисты компании «Доктор Веб» продолжают следить за целым рядом функционирующих в настоящее время бот-сетей, среди которых — ботнет, созданный злоумышленниками с использованием файлового вируса **Win32.Rmnet.12.** Среднесуточная активность двух его подсетей представлена на следующих диаграммах:





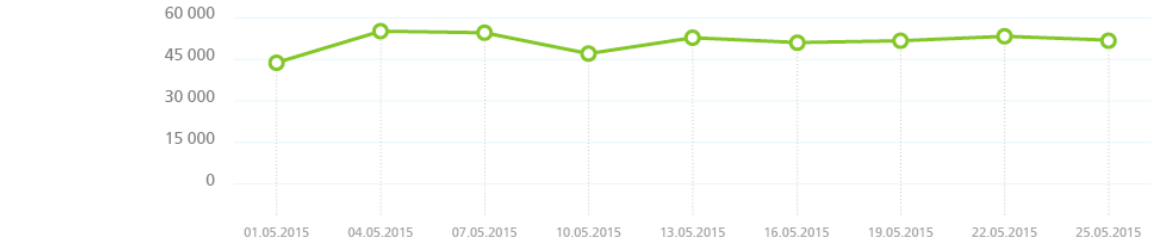
Обзор вирусной активности в мае 2015 года

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.

Как и прежде, продолжает проявлять активность бот-сеть, состоящая из компьютеров, инфицированных файловым вирусом **Win32.Sector**. Данная вредоносная программа имеет следующие функциональные возможности:

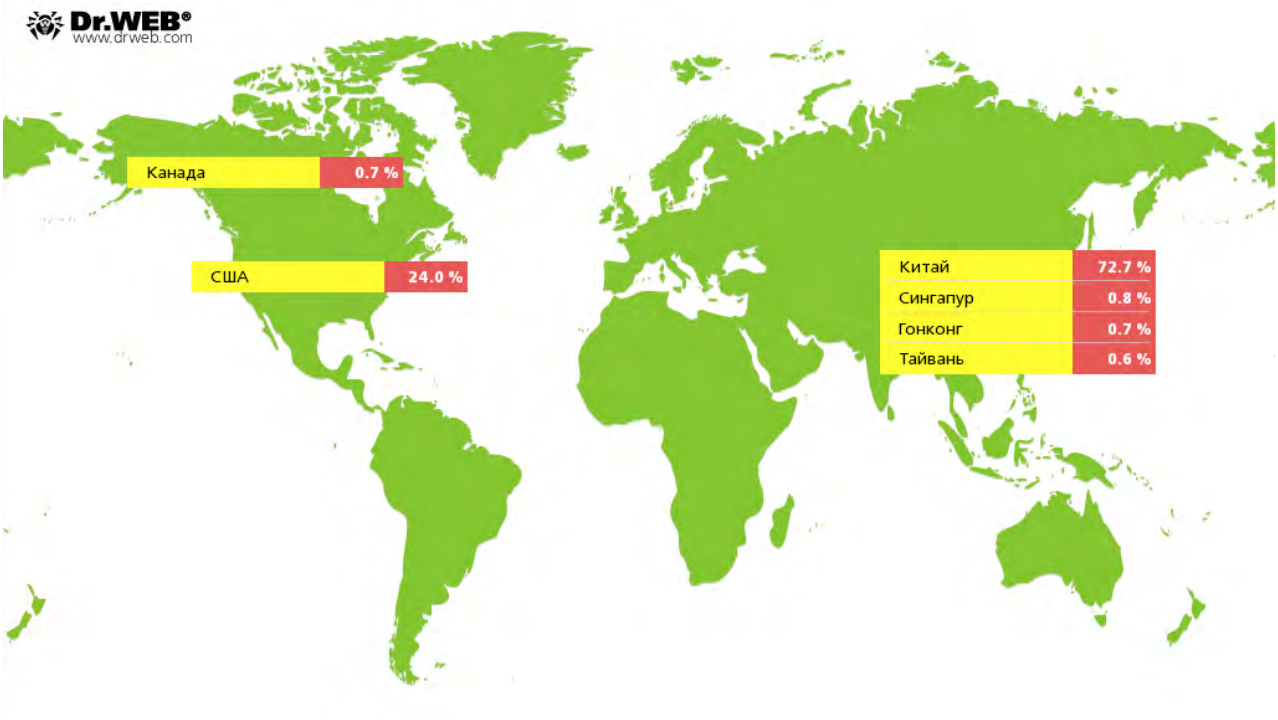
- загрузка из P2P-сети и запуск на зараженной машине различных исполняемых файлов;
- встраивание в запущенные на инфицированном компьютере процессы;
- возможность останавливать работу некоторых антивирусных программ и блокировать доступ к сайтам их разработчиков;
- инфицирование файловых объектов на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

Активность ботнета Win32.Sector в мае 2015 года



Обзор вирусной активности в мае 2015 года

По сравнению с апрелем 2015 года значительно возросло количество атак на различные веб-сайты, осуществляемых злоумышленниками с использованием троянца **Linux.BackDoor.Gates.5**. Так, в мае число уникальных IP-адресов, на которые осуществлялись атаки, выросло на 65,5% и составило 5498. Вновь изменились и цели проводимых злоумышленниками атак: на первое место по количеству атакованных интернет-ресурсов вновь вышел Китай, а вторую позицию по этому показателю занимают США:



Троянцы-шифровальщики

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

Апрель 2015	Май 2015	Динамика
1359	1200	- 11.6%

Обзор вирусной активности в мае 2015 года

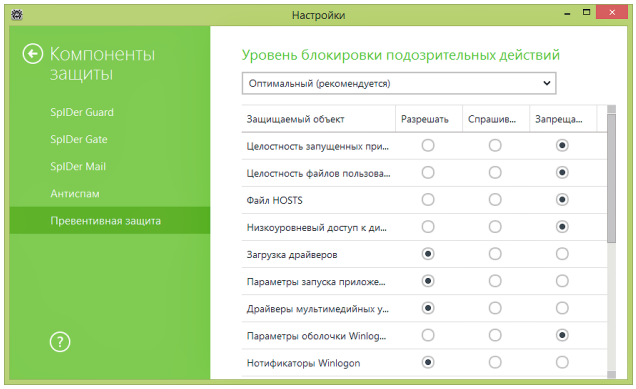
Наиболее распространенные шифровальщики в мае 2015 года:

- BAT.Encoder;
- Trojan.Encoder.858;
- Trojan.Encoder.567;
- Trojan.Encoder.263;
- Trojan.Encoder.741.

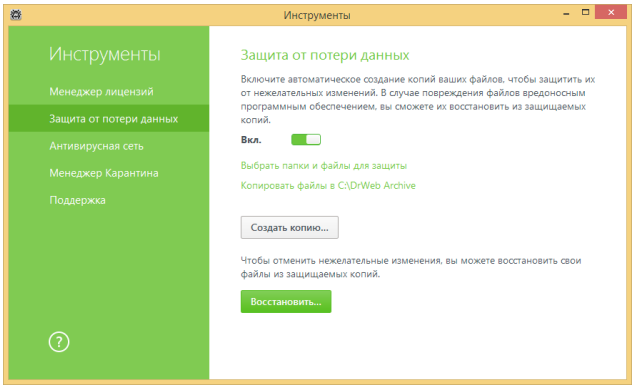
Dr.Web Security Space 10.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



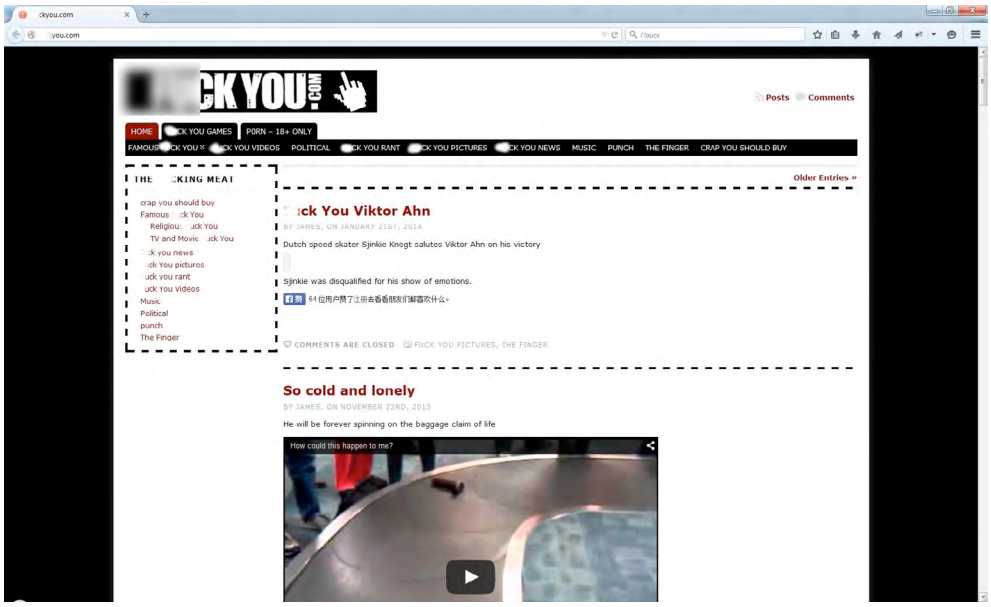
Защита данных от потери



Подробней Смотрите видео о настройке

Угрозы для Linux

В течение мая 2015 года специалистами компании «Доктор Веб» было исследовано несколько вредоносных программ, способных заражать компьютеры под управлением операционных систем семейства Linux. Одна из них, получившая наименование Linux.Kluh.1, является очередным продуктом творчества известной китайской хакерской группы ChinaZ и создана исключительно для заражения роутеров, работающих под управлением Linux. Как и другие вредоносные программы, созданные этими вирусописателями, Linux.Kluh.1предназначен для организации DDoS-атак, при этом троянец способен реализовать несколько разновидностей подобных атак: среди них — HTTP Flood (в случае получения определенной команды с управляющего сервера Linux.Kluh.1 способен выдавать себя за робота китайской поисковой системы Baidu), Spoofed SYN Flood, SYN Flood, а также несколько разновидностей атак, использующих принцип массированной отправки запросов на DNS-серверы. Среди характерных особенностей троянца можно отметить адрес интернет-ресурса, на котором располагается его управляющий сервер:



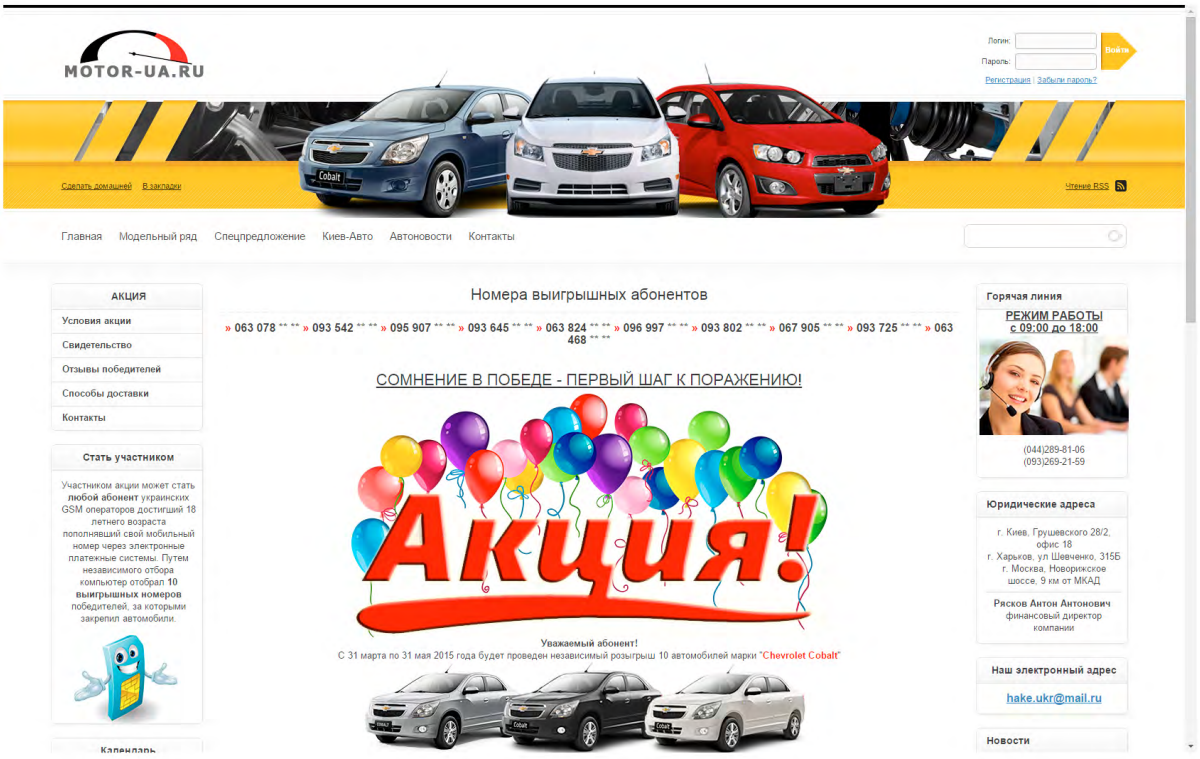
Еще одна опасная программа для Linux получила наименование Linux.Iframe.4 — она представляет собой вредоносный плагин для веб-сервера Apache, который встраивает в передаваемые пользователям html-страницы объект Iframe, а тот, в свою очередь, перенаправляет жертву на принадлежащую злоумышленникам веб-страницу с эксплойтами. С целью избежать ложных срабатываний злоумышленники предусмотрели в архитектуре троянца проверку параметра UserAgent, определяющего версию браузера потенциальной жертвы, а также ее IP-адреса.

Сигнатуры всех обнаруженных в мае вредоносных программ для данного семейства операционных систем добавлены в вирусные базы Антивируса Dr.Web для Linux.

Обзор вирусной активности в мае 2015 года

Опасные сайты

В мае вновь активизировались сетевые мошенники, под различными предлогами выманивающие деньги у доверчивых пользователей. Для привлечения потенциальных жертв жулики используют массовые СМС-рассылки, в сообщениях которых говорится, что получатель якобы выиграл автомобиль в рамках той или иной рекламной акции. Во всех подобных СМС-сообщениях приводится адрес веб-сайта, который оформлен как официальный интернет-ресурс некоего автосалона и содержит порой довольно подробную информацию о данной «компании», способную усыпить бдительность потенциальной жертвы.



Для получения ценного приза — автомобиля — доверчивым посетителям сайта фальшивого автосалона предлагается в течение короткого времени, как правило, нескольких часов, внести через платежный терминал «налог» в размере 1% от стоимости «приза» или аналогичным способом приобрести страховой полис ОСАГО. Подробнее об этой мошеннической схеме рассказано в опубликованной на нашем сайте информационной статье

Обзор вирусной активности в мае 2015 года

В течение мая 2015 года в базу нерекомендуемых и вредоносных сайтов было добавлено 221 346 интернет-адресов.

Март 2015	Апрель 2015	Динамика
74 108	129 199	+ 74.3%

Вредоносное и нежелательное ПО для Android

В течение мая было зафиксировано появление новых вредоносных программ для Android-устройств. Наиболее заметные события минувшего месяца, связанные с вредоносными Android-приложениями:

- атаки с применением разнообразных банковских троянцев;
- обнаружение новых СМС-троянцев;
- появление новых Android-вымогателей.

Узнайте больше с Dr.Web

Обзор вирусной активности в мае 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