Dr.WEB®
с 1992 года

Обзор вирусной активности в сентябре 2015 года

Обзор вирусной активности в сентябре 2015 года

1 октября 2015 года

С наступлением осени вирусописатели ничуть не снизили своей активности: в сентябре было зафиксировано распространение нескольких установщиков рекламных и нежелательных приложений — причем как для Windows, так и для Mac OS X, нового троянца, способного заражать POS-терминалы, а также различных вредоносных программ для ОС Linux и мобильной платформы Android.

Главные тенденции сентября

- Появление нового троянца, способного заражать POS-терминалы
- Распространение установщиков нежелательных и рекламных приложений для Windows и Mac OS X
- Распространение новых вредоносных программ для Google Android и Linux

Обзор вирусной активности в сентябре 2015 года

Угроза месяца

POS-терминалы, работающие под управлением операционных систем семейства Microsoft Windows, всегда вызывали определенный интерес у киберпреступников, поскольку уже давно известны различные методы хищения треков банковских карт из памяти подобных устройств с использованием вредоносных программ. Одним из таких приложений является исследованный в сентябре специалистами компании «Доктор Веб» трояне Trojan.MWZLesson, представляющий собой модификацию другой опасной программы — BackDoor.Neutrino.50.

Trojan.MWZLesson может выполнять следующие команды:

- CMD – передает поступившую директиву командному интерпретатору CMD;
- LOADER - скачивает и запускает файл (dll – с использованием утилиты regsrv, vbs – с использованием утилиты wscript, exe — осуществляется непосредственный запуск);
- UPDATE – команда обновления;
- rate – задает временной интервал сеансов связи с управляющим сервером;
- FIND - поиск документов по маске;
- DDOS – начать DDoS-атаку методом http-flood.

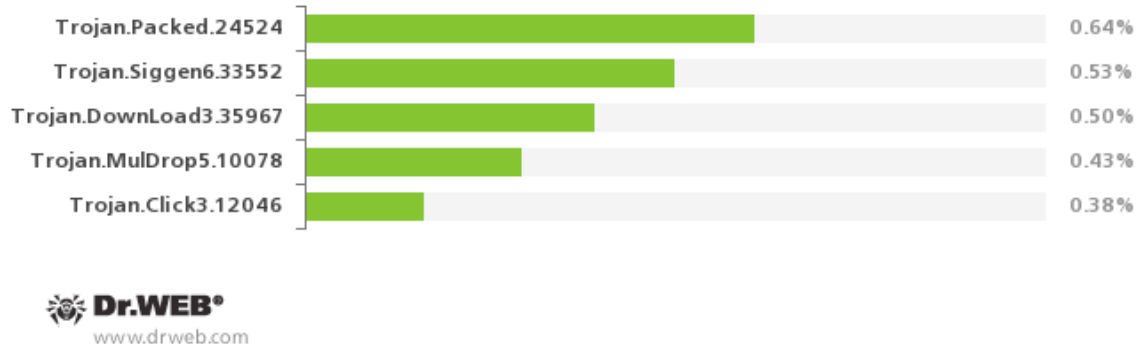
Более подробные сведения об этом троянце можно почерпнуть в опубликованном на сайте компании «Доктор Веб» обзорном материале.

По данным статистики лечащей утилиты Dr.Web CureIt!

В течение сентября с использованием утилиты Dr.Web CureIt! было выявлено 155 554 503 нежелательных, потенциально опасных и вредоносных объекта.

Обзор вирусной активности в сентябре 2015 года

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

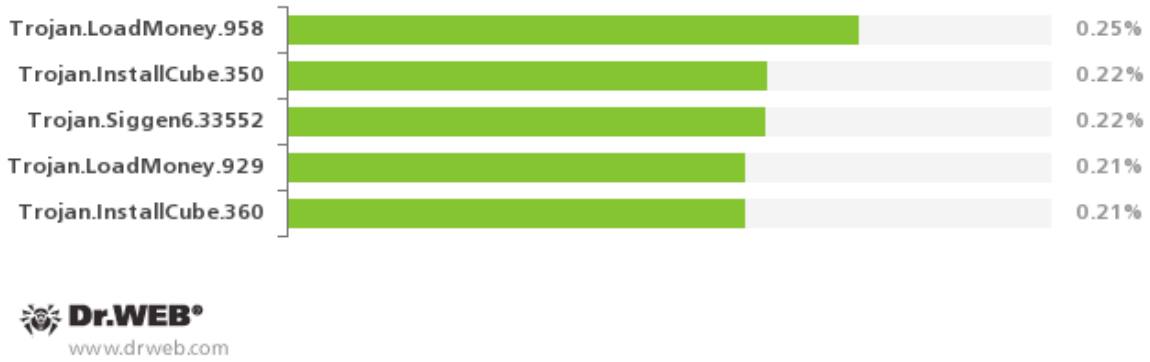


- **Trojan.Packed.24524**
  Установщик рекламных программ и сомнительных приложений, распространяющийся злоумышленниками под видом легитимного ПО.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.MulDrop5.10078**
  Представитель семейства вредоносных программ, предназначенных для доставки и установки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Click**
  Семейство вредоносных программ, предназначенных для накрутки посещаемости различных интернет-ресурсов путем перенаправления запросов жертвы на определенные сайты с помощью управления поведением браузера.

Обзор вирусной активности в сентябре 2015 года

По данным серверов статистики «Доктор Веб»

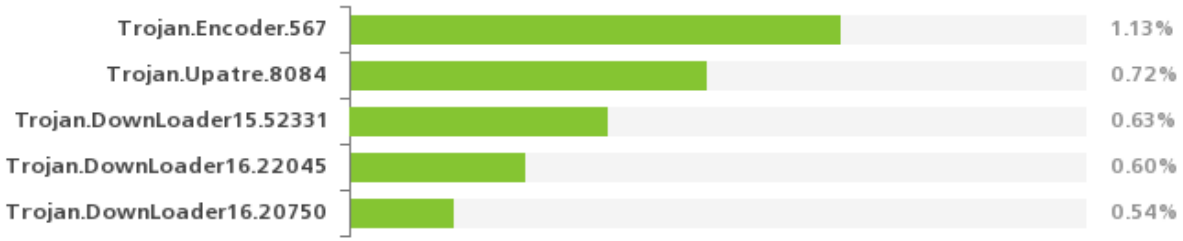
Наиболее распространенные вредоносные программы в сентябре 2015 года
согласно данным серверов статистики Dr.Web



- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **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.

Статистика вредоносных программ в почтовом трафике

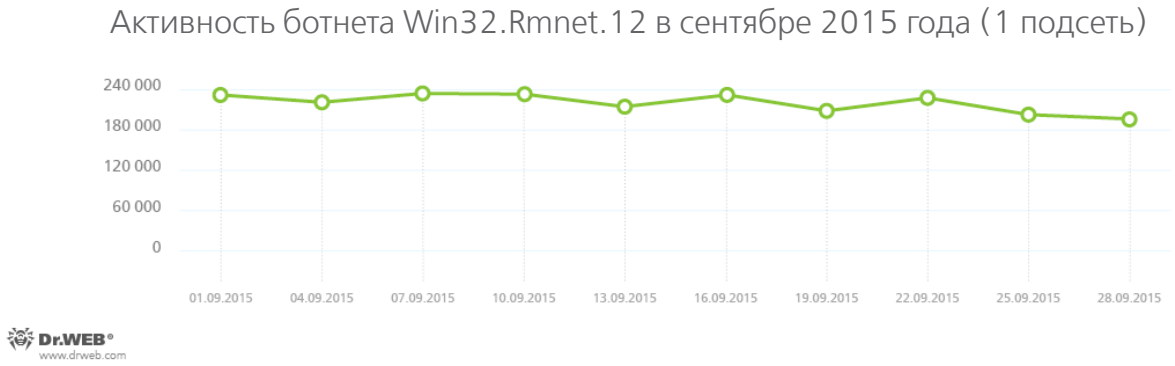
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в сентябре 2015 года

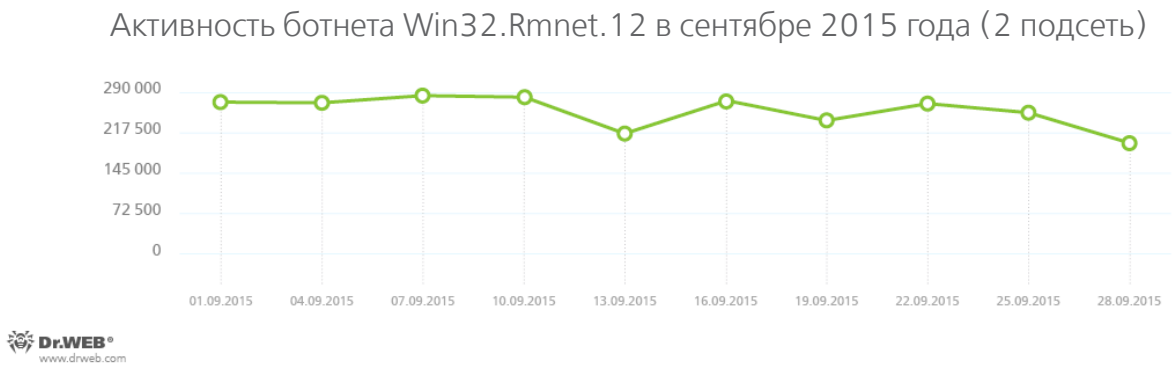


- **Trojan.Encoder.567**
  Один из представителей семейства троянцев-вымогателей, шифрующих файлы на дисках компьютера жертвы и требующих выкуп за их расшифровку. Этот троянец способен зашифровывать важные пользовательские файлы, в том числе следующих типов: .jpg, .jpeg, .doc, .docx, .xls, xlsx, .dbf, .1cd, .psd, .dwg, .xml, .zip, .rar, .db3, .pdf, .rtf, .7z, .kwm, .arj, .xlsm, .key, .cer, .accdb, .odt, .ppt, .mdb, .dt, .gsf, .ppsx, .pptx.
- **Trojan.Upatre**
  Семейство троянцев-загрузчиков, предназначенных для скачивания на инфицированный компьютер и скрытной установки других вредоносных приложений.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Ботнеты

Вирусные аналитики компании «Доктор Веб» продолжают наблюдать за функционированием бот-сетей, созданных злоумышленниками с использованием опасного файлового вируса Win32.Rmnet.12. Активность этих ботнетов в сентябре 2015 года показана на следующих иллюстрациях:





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.

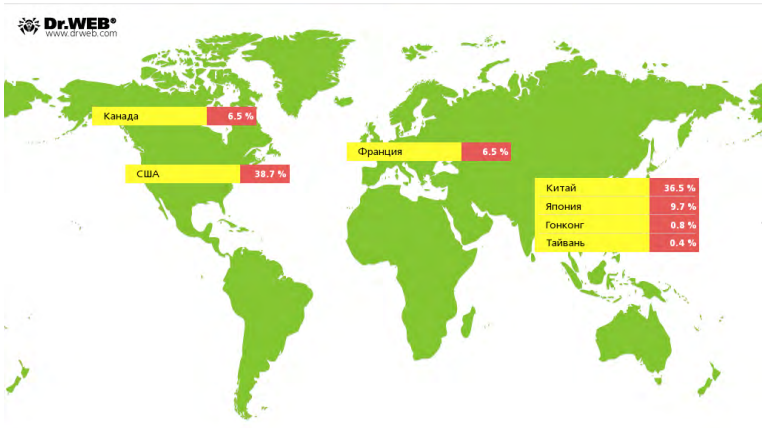
Обзор вирусной активности в сентябре 2015 года

Как и прежде, активен ботнет, состоящий из персональных компьютеров, инфицированных файловым вирусом Win32.Sector., — график этой активности показан на следующей иллюстрации:

Вирус Win32.Sector. располагает следующими функциональными возможностями:

- 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.

В сентябре 2015 года вновь активизировались злоумышленники, осуществляющие массированные DDoS-атаки с использованием Linux-троянца Linux.BackDoor.Gates.5. По сравнению с предыдущим месяцем количество таких атак увеличилось на 263.5% и составило 7572. При этом страны-лидеры по числу атакованных узлов в сравнении с данными за август поменялись местами: на первое место вышли США, а Китай занял уверенную вторую позицию. Географическое распределение целей злоумышленников, организующих DDoS-атаки с применением Linux.BackDoor.Gates.5. показано на следующей иллюстрации:



Обзор вирусной активности в сентябре 2015 года

Троянцы-шифровальщики

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

Август 2015	Сентябрь 2015	Динамика
1425	1310	- 8 %

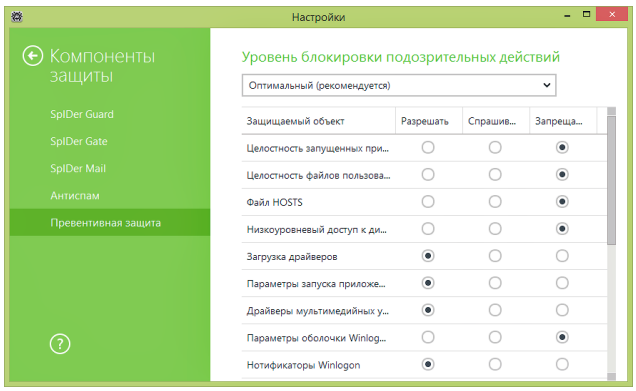
Наиболее распространенные шифровальщики в сентябре 2015 года:

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

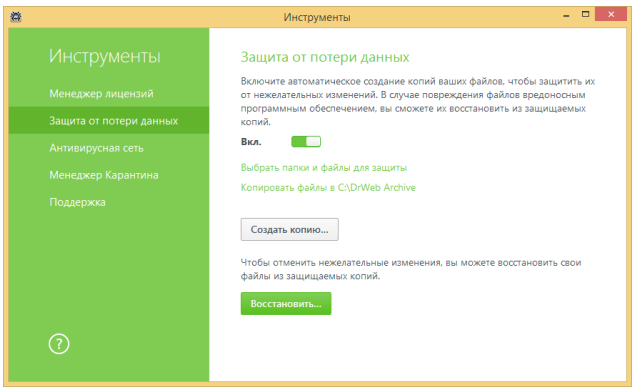
Dr.Web Security Space 10.0 для Windows защищает от троянцев-шифровальщиков

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

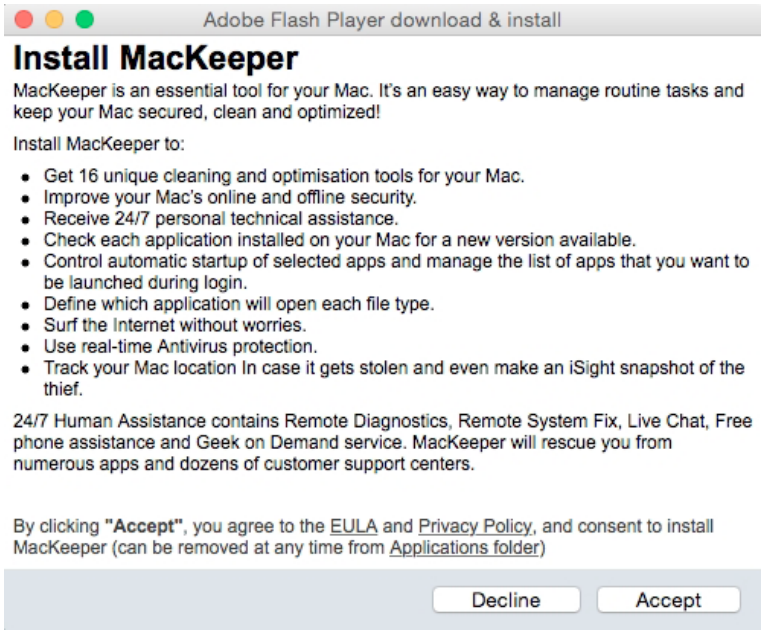
В сентябре специалистам компании «Доктор Веб» вновь пришлось столкнуться с троянцами для операционных систем семейства Linux. Наиболее интересными среди таковых оказались Linux.Ellipsis.1 и Linux.Ellipsis.2. Второй из них предназначен для взлома различных устройств методом перебора логинов и паролей по словарю. Чтобы обеспечить анонимность в процессе доступа к взломанным с его помощью устройствам, злоумышленники используют троянца Linux.Ellipsis.1. Примечательно и то, что эта вредоносная программа обладает весьма своеобразным поведением, которое вирусные аналитики компании «Доктор Веб» назвали «параноидальным».

Основное предназначение Linux.Ellipsis.1 заключается в организации на инфицированном компьютере прокси-сервера: его киберпреступники и используют для несанкционированного доступа к скомпрометированным устройствам, чтобы «замести следы». Для этой цели троянец контролирует соединения по заданному локальному адресу и порту, проксируя весь транслируемый через этот адрес и порт трафик.

«Параноидальность» поведения Linux.Ellipsis.1 заключается в том, что он располагает довольно обширным списком характерных строк, обнаруживая которые в сетевом трафике, троянец блокирует обмен данными с соответствующим удаленным сервером. Кроме того, эта вредоносная программа проверяет все сетевые подключения компьютера и отсылает на управляющий сервер IP-адрес, с которым установлено соединение. Если сервер отвечает командой «kill», троянец прекращает работу приложения, которое установило соединение, а заодно блокирует этот IP-адрес на два часа. Более детальную информацию об архитектуре и принципах работы этих вредоносных программ можно получить, ознакомившись с опубликованной нами обзорной статьей.

Опасные программы для Mac OS X

Установщиками рекламных и нежелательных приложений для ОС Windows в наши дни никого уже не удивишь, однако в сентябре вирусные аналитики компании «Доктор Веб» познакомились с очередной такой программой, предназначенной для операционной системы Mac OS X. Данный образец, получивший наименование Adware.Mac.WeDownload.1, представляет собой поддельный дистрибутив проигрывателя Adobe Flash Player и распространяется с использованием ресурсов партнерской программы, ориентированной на монетизацию файлового трафика.



После отсылки соответствующего запроса Adware.Mac.WeDownload.1 получает от управляющего сервера список приложений, которые будут предложены пользователю для установки. Среди них замечены как нежелательные, так и откровенно вредоносные программы, в том числе Program.Unwanted.MacKeeper, Mac.Trojan.Crossrider, Mac.Trojan.Genieo, Mac.BackDoor.OpinionSpy, различные представители семейства Trojan.Conduit и некоторые другие опасные приложения, при этом количество и состав устанавливаемых программ зависит от географической «привязки» IP-адреса жертвы.

Более подробно об этом установщике нежелательных программ читайте в нашей информационной статье.

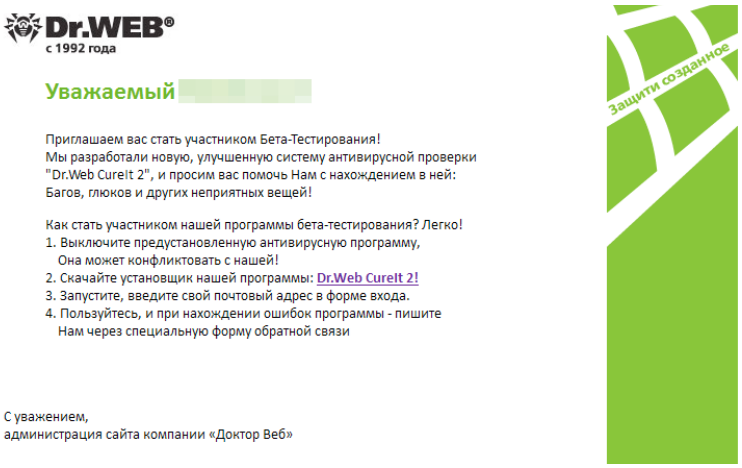
Другие вредоносные программы

Сентябрь 2015 года запомнится специалистам по информационной безопасности широким распространением установщиков нежелательных, рекламных и даже опасных приложений, создаваемых злоумышленниками в рамках различных партнерских программ, направленных на монетизацию файлового трафика.

Так, в начале месяца вирусные аналитики компании «Доктор Веб» исследовали вредоносную программу Trojan.InstallCube.339, которая может быть загружена потенциальными жертвами с различных поддельных файлообменных ресурсов или торрент-трекеров. После запуска этот троянец получает необходимые для своей работы данные с управляющего сервера и демонстрирует пользователю окно с информацией о загружаемом объекте, имеющее значок популярного торрент-клиента mTorrent. Особенность управляющих серверов данной вредоносной программы состоит в том, что они позволяют скачать полезную нагрузку только если обращающийся к ним компьютер имеет российский IP-адрес. Подробнее об этой вредоносной программе рассказано в опубликованной на сайте компании «Доктор Веб» обзорной статье.

Другой опасный установщик, о котором мы рассказывали в середине месяца, носит название Trojan.RoboInstall.1. Как и другие подобные программы, этот троянец распространяется с использованием файлообменных сайтов, поддельных торрентов и иных аналогичных интернет-ресурсов, созданных злоумышленниками. Такие вредоносные программы зачастую используют и сами авторы бесплатных приложений для их монетизации — они получают вознаграждение за каждую дополнительную утилиту, загруженную троянцем на компьютеры пользователей. В отличие от многих других установщиков рекламного ПО, в отображаемых Trojan.RoboInstall.1 диалоговых окнах зачастую отсутствуют флажки, позволяющие отказаться от инсталляции дополнительных программ, поэтому их запуск на исполнение осуществляется без каких-либо условий.

В конце сентября злоумышленники предприняли попытку распространения вредоносной программы в почтовой рассылке, осуществлявшейся якобы от имени компании «Доктор Веб».


Dr.WEB®
с 1992 года

Уважаемый

Приглашаем вас стать участником Бета-Тестирования!
Мы разработали новую, улучшенную систему антивирусной проверки "Dr.Web CureIt 2", и просим вас помочь Нам с нахождением в ней: Багов, глюков и других неприятных вещей!

Как стать участником нашей программы бета-тестирования? Легко!
1. Выключите предустановленную антивирусную программу, Она может конфликтовать с нашей!
2. Скачайте установщик нашей программы: Dr.Web CureIt 2!
3. Запустите, введите свой почтовый адрес в форме входа.
4. Пользуйтесь, и при нахождении ошибок программы - пишите Нам через специальную форму обратной связи

С уважением,
администрация сайта компании «Доктор Веб»

Обзор вирусной активности в сентябре 2015 года

Киберпреступники предлагали своим жертвам принять участие в тестировании несуществующей утилиты Dr.Web CureIt 2, под видом которой с принадлежащего вирусописателям сайта загружался троянец Trojan.PWS.Stealer.13052, предназначенный для хищения паролей. С целью увеличения числа заражений данной вредоносной программой злоумышленники предлагали потенциальным жертвам отключить работающий на их компьютерах антивирус, якобы потому, что «утилита» может конфликтовать с другим антивирусным ПО. Подробнее об этом инциденте мы рассказывали в опубликованном нами новостном материале.

Опасные сайты

В течение сентября 2015 года в базу нерекомендуемых и вредоносных сайтов было добавлено 399 227 интернет-адресов.

Август 2015	Сентябрь 2015	Динамика
+ 834 753	+ 399 227	- 51.39 %

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для Android

Сентябрь оказался чрезвычайно насыщенным на события вирусной тематики, связанные с мобильными устройствами. Так, специалисты по информационной безопасности обнаружили массовое проникновение троянского приложения в каталог App Store, а также многочисленные случаи размещения различных вредоносных программ в каталоге Google Play. В середине месяца вирусные аналитики «Доктор Веб» зафиксировали очередной инцидент с участием троянца, предустановленного злоумышленниками в одну из официальных Android-прошивок. Кроме этого, пользователям вновь угрожали банковские троянцы, Android-вымогатели и другие вредоносные приложения.

Наиболее заметные тенденции в сфере мобильной безопасности в сентябре:

- обнаружение в каталоге App Store большого числа программ, содержащих троянца IPhoneOS.Trojan.XcodeGhost;
- обнаружение множества троянцев в каталоге приложений Google Play;
- новый случай заражения Android-прошивки вредоносным приложением;
- появление новых троянцев-вымогателей для ОС Android;
- распространение злоумышленниками новых Android-банкеров.

Обзор вирусной активности в сентябре 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