Dr.WEB®
с 1992 года

Обзор вирусной активности за 2015 год

Обзор вирусной активности за 2015 год

29 декабря 2015 года

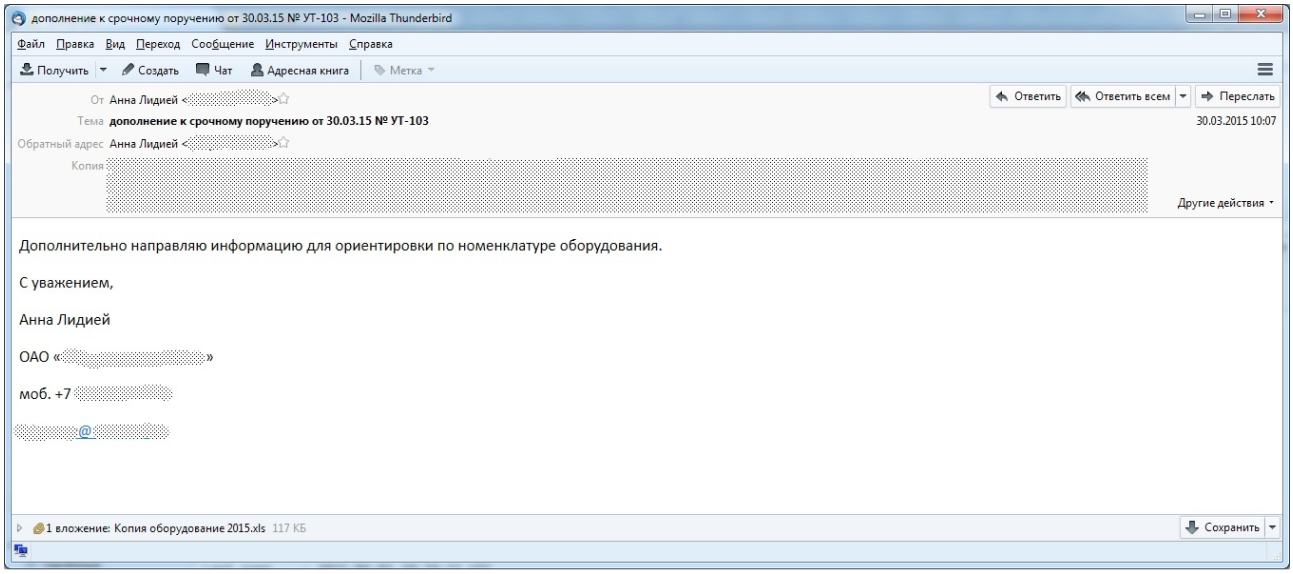
Уходящий год запомнится и простым пользователям, и специалистам по информационной безопасности широким распространением опасного троянца-шифровальщика для операционных систем семейства Linux, сумевшего инфицировать более 3000 веб-сайтов по всему миру. Также 2015 год ознаменовался появлением значительного числа новых вредоносных программ для самой популярной на нашей планете операционной системы — Microsoft Windows. Среди них — новые энкодеры и бэкдоры, шпионские приложения и майнеры криптовалют. Заметно выросло количество троянцев, ориентированных на платформу Apple OS X, — абсолютными лидерами среди них являются приложения, предназначенные для несанкционированного показа рекламы, и всевозможные установщики нежелательных программ. Это обстоятельство красноречиво свидетельствует о росте популярности OS X среди вирусописателей. Пополнились новыми записями и базы Антивируса Dr.Web для мобильной платформы Google Android: по количеству известных угроз эта операционная система уверенно занимает вторую позицию после Windows. В 2015 году продолжали свою деятельность многочисленные сетевые мошенники: они по-прежнему изобретают все новые и новые способы обмана пользователей Интернета. Наконец, в течение минувшего года, как и ранее, функционировали ботнеты — среди них наибольшую активность проявляли сети, созданные злоумышленниками с использованием файловых вирусов Win32.Rmnet.12 и Win32.Sector.

Главные тенденции года

- Распространение опасного троянца-шифровальщика для Linux
- Рост числа вредоносных программ для OS X
- Появление новых троянцев для Google Android
- Распространение новых вредоносных программ для Windows

Наиболее интересные события 2015 года

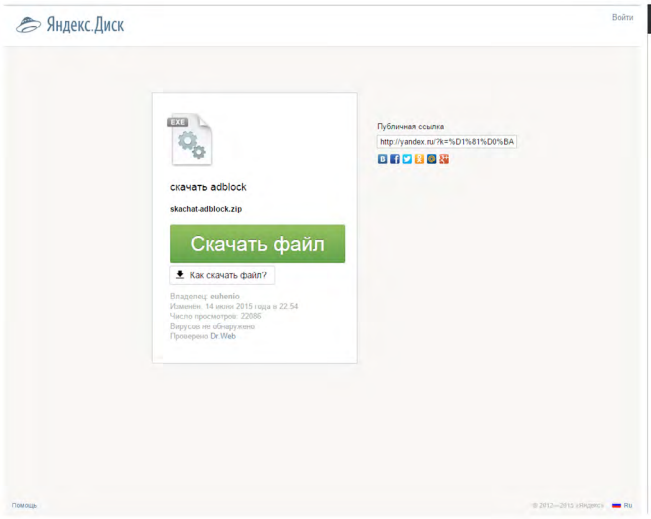
Весной 2015 года специалисты компании «Доктор Веб» исследовали троянца BackDoor.Hser.1, которого злоумышленники использовали для проведения таргетированных атак на российские оборонные предприятия. Эта вредоносная программа распространялась с использованием сообщений e-mail, отправленных киберпреступниками на личные и служебные электронные адреса сотрудников более десяти отечественных предприятий. Все эти компании входят в состав известного российского концерна и имеют оборонный профиль или обслуживают интересы военно-промышленного комплекса.



Вредоносные сообщения имели вложение в виде файла табличного редактора Microsoft Excel, в котором содержался эксплойт для данной программы. С его помощью троянец и проникал на атакуемый компьютер. Среди прочего, данная вредоносная программа способна по команде передавать на удаленный сервер список активных процессов на зараженном ПК, загружать и запускать другие вредоносные приложения, а также открывать командную консоль и выполнять перенаправление ввода-вывода на принадлежащий киберпреступникам сервер, благодаря чему злоумышленники получают возможность дистанционного управления инфицированным компьютером. Более подробная информация о BackDoor.Hser.1 представлена в соответствующем новостном материале.

В июне неизвестные взломали интернет-портал Всероссийского центра изучения общественного мнения (ВЦИОМ): злоумышленники разместили на сервере ВЦИОМ веб-страницы, с которых посетителям предлагалось скачать вредоносную программу под видом различных «полезных» файлов. Этот инцидент также подробно освещался компанией «Доктор Веб» в одной из информационных статей.

Обзор вирусной активности за 2015 год



Все размещенные злоумышленниками на сайте ВЦИОМ архивы содержали вредоносную программу, относящуюся к семейству Trojan.DownLoader — такие троянцы предназначены для скрытой загрузки и установки на атакуемый компьютер различных опасных приложений. С помощью данного загрузчика злоумышленники распространяли программу-майнер, предназначенную для добычи криптовалют, а также иной нежелательный софт. Поскольку сайт ВЦИОМ является достаточно популярным интернет-ресурсом, количество пострадавших в результате действия злоумышленников по оценкам специалистов компании «Доктор Веб» исчислялось десятками тысяч.

В августе вирусные аналитики компании «Доктор Веб» обнаружили опасного троянца, предназначенного для добычи криптовалют с использованием ресурсов компьютера-жертвы. Особенность этой вредоносной программы, получившей имя Trojan.BtcMine.737, заключалась в том, что она умела самостоятельно, без участия пользователя перемещаться по сети и заражать подключенные к ней компьютеры подобно сетевому червю.

Осенью было зафиксировано распространение вредоносной программы Trojan.MWZLesson, способной заражать POS-терминалы. Помимо прочих шпионских и вредоносных функций, этот троянец умеет сохранять и передавать на принадлежащий злоумышленникам управляющий сервер треки банковских пластиковых карт. Исследование показало, что он является модификацией другого вредоносного приложения — BackDoor.Neutrino.50. Помимо функций троянца для POS-терминалов, BackDoor.Neutrino.50 обладает возможностью красть информацию из почтового клиента Microsoft, а также учетные данные для доступа к ресурсам по протоколу FTP с использованием ряда популярных FTP-клиентов, способен осуществлять несколько типов DDoS-атак и заражать компьютеры, доступные в локальной сети.

Обзор вирусной активности за 2015 год

В сентябре 2015 года вирусописатели попытались распространить опасного троянца Trojan.PWS.Stealer.13052 с помощью почтовой рассылки 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»

Защити созданное

«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. Антивирусная защита Dr.Web позволяет информационным системам клиентов эффективно противостоять любым, даже неизвестным угрозам.

«Доктор Веб»
2003—2015

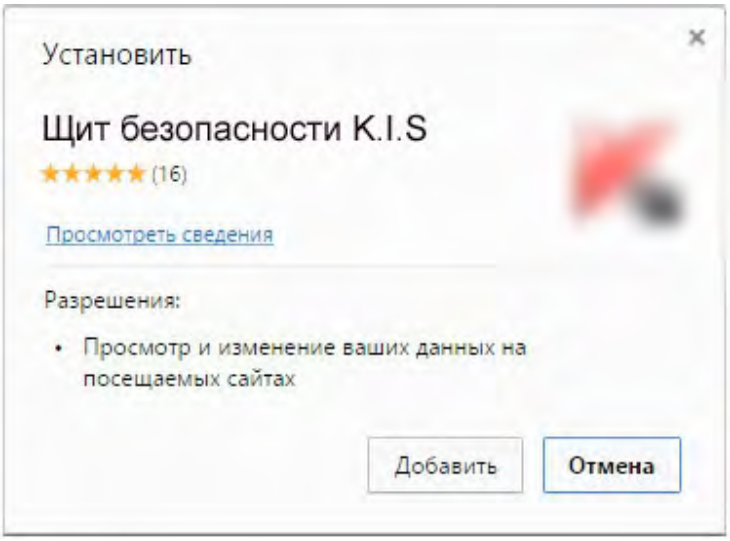
«Доктор Веб» стал первой компанией, предложившей на российском рынке инновационную модель использования антивируса в качестве услуги, и по сей день продолжает оставаться безусловным лидером российского рынка интернет-сервисов безопасности для поставщиков ИТ-услуг. Государственные сертификаты и награды, а также география пользователей Dr.Web свидетельствуют о высоком качестве продуктов, созданных талантливыми российскими программистами.

Вы всегда можете отписаться от нашей рассылки по этой ссылке: Отменить подписку

ООО«Доктор Веб»
Адрес: 125124,
Россия, Москва,
3-я улица
Ямского поля, вл.2,
корп.12А
Телефон:
+7 (495) 789-45-87
(многоканальный)
Факс:
+7 (495) 789-45-97

Пользователям предлагали «протестировать» несуществующую в природе утилиту «Dr.Web CureIt 2», под видом которой на их компьютеры и загружался троянец. Компания «Доктор Веб» своевременно предупредила об этом инциденте своих пользователей, опубликовав подробную информационную статью.

Однако использованием в своих противоправных целях наименования разработчика Антивируса Dr.Web киберзлодеи не ограничились — вскоре они предприняли попытку распространения еще одной вредоносной программы, прикрываясь названием другого производителя антивирусного ПО.

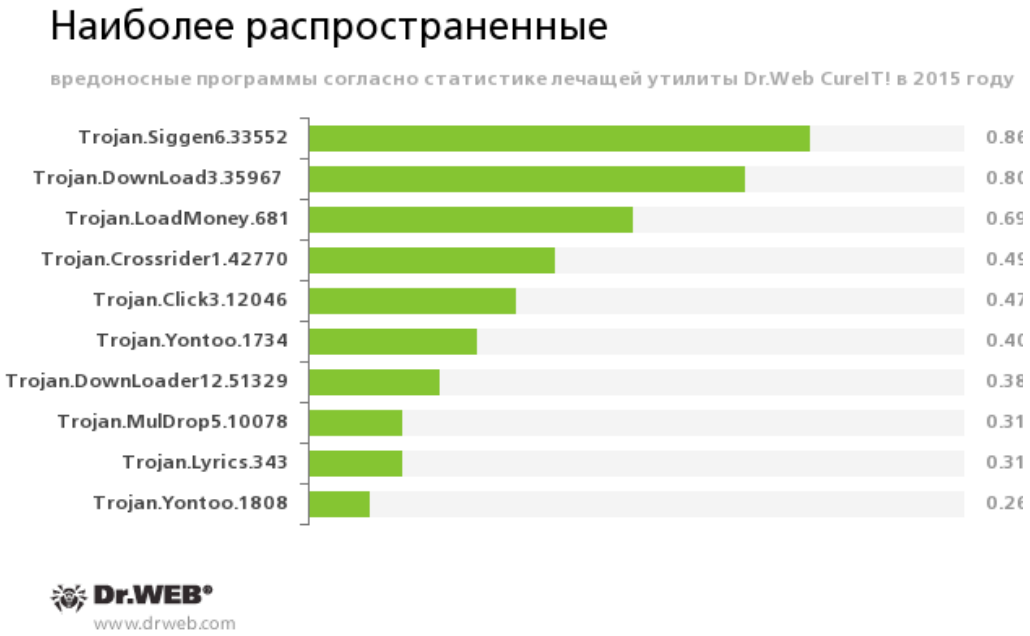


Этой троянской программе, получившей наименование Trojan.BPLug.1041, также была посвящена опубликованная на сайте компании «Доктор Веб» статья.

Наконец, одним из самых громких событий 2015 года стало распространение троянца-шифровальщика Linux.Encoder.1, сумевшего заразить в общей сложности более 3000 веб-сайтов, размещающихся на серверах под управлением ОС Linux. Это далеко не первый известный представитель энкодеров для Linux — еще в августе 2014 года компания «Доктор Веб» сообщала о появлении троянца Trojan.Encoder.737, способного шифровать размещающиеся в сетевых хранилищах производства компании Synology файлы, — однако масштабы распространения Linux.Encoder.1 на сегодняшний день являются рекордными.

Вирусная обстановка

Согласно статистическим данным, собранным с использованием лечащей утилиты Dr.Web CureIt!, в 2015 году чаще всего на компьютерах обнаруживалась вредоносная программа Trojan.Siggen6.33552, предназначенная для установки в атакуемую систему другого опасного ПО. Второе место по количеству обнаружений занимает Trojan.DownLoad3.35967 — один из представителей троянцев-загрузчиков, способных втайне от пользователя скачивать и устанавливать на компьютер различные нежелательные приложения. На третьем месте расположился троянец Trojan.LoadMoney.681 — еще один представитель программ-загрузчиков. Десять вредоносных приложений, обнаруживаемых лечащей утилитой Dr.Web CureIt! в 2015 году наиболее часто, показаны на следующей диаграмме:



- **Trojan.Crossrider1.42770**
  Представитель семейства троянцев, предназначенных для демонстрации различной сомнительной рекламы.
- **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.Yontoo**
  Семейство надстроек для популярных браузеров, назначение которых заключается в демонстрации пользователю рекламы при просмотре веб-страниц.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.MulDrop5.10078**
  Представитель семейства троянцев-дропперов, способных распаковывать и запускать на инфицированном компьютере другие вредоносные программы.
- **Trojan.Lyrics**
  Семейство троянцев, способных демонстрировать на экране назойливую рекламу и открывать в окне браузера веб-сайты сомнительного содержания без ведома пользователя.

Приведенная выше статистика говорит о том, что среди всех выявленных лечащей утилитой Dr.Web CureIt! вредоносных программ в 2015 году преобладают рекламные троянцы, установщики нежелательного ПО и троянцы-загрузчики.

Похожая картина складывается и согласно данным, собранным в течение года серверами статистики Dr.Web: здесь в лидерах также установщик нежелательных программ Trojan.Siggen6.33552, на второй позиции — хорошо известный специалистам по информационной безопасности еще с 2011 года троянец BackDoor.IRC.NgrBot.42. 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). Также среди безоговорочных лидеров по количеству обнаружений — троянцы-загрузчики семейства Trojan.DownLoader. Десять наиболее распространенных в 2015 году вредоносных программ согласно данным серверов статистики Dr.Web показаны на следующей диаграмме:

- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Ormes.69**
  Троянец, демонстрирующий назойливую рекламу при просмотре веб-страниц.
- **Trojan.InstallCore.16**
  Троянец – установщик рекламных и сомнительных приложений, также известный под именем Trojan.Packed.24524.
- **Win32.HLLW.Shadow**
  Сетевой червь, в том числе способный использовать для своего распространения уязвимости в операционных системах семейства Microsoft Windows. Эта вредоносная программа также известна под именами Conficker и Kido.

Данная статистика показывает, что у вирусописателей по-прежнему пользуются весьма высокой популярностью троянцы – установщики нежелательных программ и рекламные троянцы, поскольку они, вероятно, способны приносить злоумышленникам наибольшую прибыль. Аналогичная тенденция прослеживалась и в прошлом, 2014 году.

Среди вредоносных вложений, распространяемых киберпреступниками вместе с сообщениями электронной почты, по итогам 2015 года абсолютным лидером является опасный троянец-шифровальщик Trojan.Encoder.567. Этот энкодер способен шифровать файлы на компьютере и требует у жертвы выкуп за расшифровку. Trojan.Encoder.567 может 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.

Обзор вирусной активности за 2015 год

На втором месте по «популярности» в почтовых рассылках по итогам года — BackDoor.Siggen.58526. Это троянец, способный без ведома пользователей загружать и запускать на инфицированном компьютере другие вредоносные программы, а также выполнять поступающие от злоумышленников команды. Ну а третье место занимает BackDoor.Andromeda.404 — троянец-загрузчик, предназначенный для скачивания с удаленных серверов злоумышленников и запуска на инфицированном компьютере других вредоносных программ. Десять вредоносных приложений, наиболее часто обнаруживаемых в течение 2015 года антивирусным ПО Dr.Web в почтовом трафике, представлено на следующей диаграмме:

Помимо уже упоминавшихся ранее в этом обзоре троянцев, среди вложений в сообщения электронной почты в течение 2015 года были обнаружены следующие разновидности вредоносных программ:

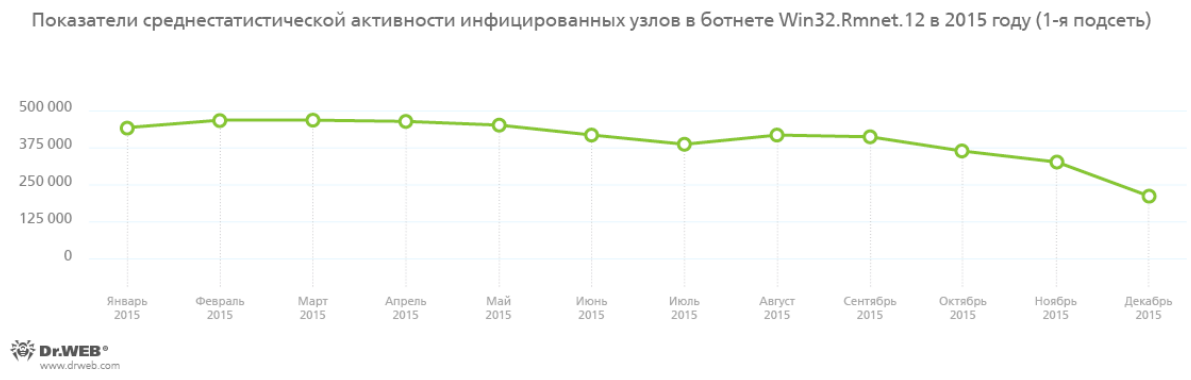
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **Trojan.Oficla**
  Семейство троянцев, распространяющихся преимущественно по каналам электронной почты. При заражении компьютера они скрывают свою вредоносную 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.

- **BackDoor.Bebloh.96**
  Один из представителей семейства вредоносных программ, относящихся к категории банковских троянцев. Данное приложение представляет угрозу для пользователей систем дистанционного банковского обслуживания (ДБО), поскольку позволяет злоумышленникам красть конфиденциальную информацию путем перехвата заполняемых в браузере форм и встраивания в страницы сайтов некоторых банков.
- **Trojan.Packed.24524**
  Троянец-установщик рекламных и сомнительных приложений, также известный под именем Trojan.InstallCore.16.

На основе этих данных можно сделать вывод, что помимо традиционных троянцев-загрузчиков киберпреступники, распространяющие вредоносные программы с помощью почтового спама, в 2015 году сместили фокус своих интересов в сторону троянцев-энкодеров и бэкдоров, способных похищать на зараженном компьютере пароли и иную конфиденциальную информацию.

Ботнеты

На протяжении всего года вирусные аналитики компании «Доктор Веб» внимательно следили за деятельностью нескольких бот-сетей, созданных злоумышленниками с использованием различных вредоносных программ. Так, активность ботнета, состоящего из зараженных файловым вирусом Win32.Rmnet.12 компьютеров, в течение года постепенно снижалась. Этот опасный вирус включает несколько модулей и позволяет встраивать в просматриваемые жертвой веб-страницы посторонний контент, перенаправлять пользователя на указанные злоумышленниками сайты, а также передавать на удаленные узлы содержимое заполняемых на зараженном компьютере форм. Кроме того, Win32.Rmnet.12 может похищать пароли от популярных FTP-клиентов, выполнять различные команды, а также обладает способностью к самокопированию, заражая исполняемые файлы. Вирус также способен распространяться с помощью встраиваемых в веб-страницы сценариев, написанных на языке VBScript. Активность двух подсетей ботнета Win32.Rmnet.12 в 2015 году показана на диаграммах ниже:

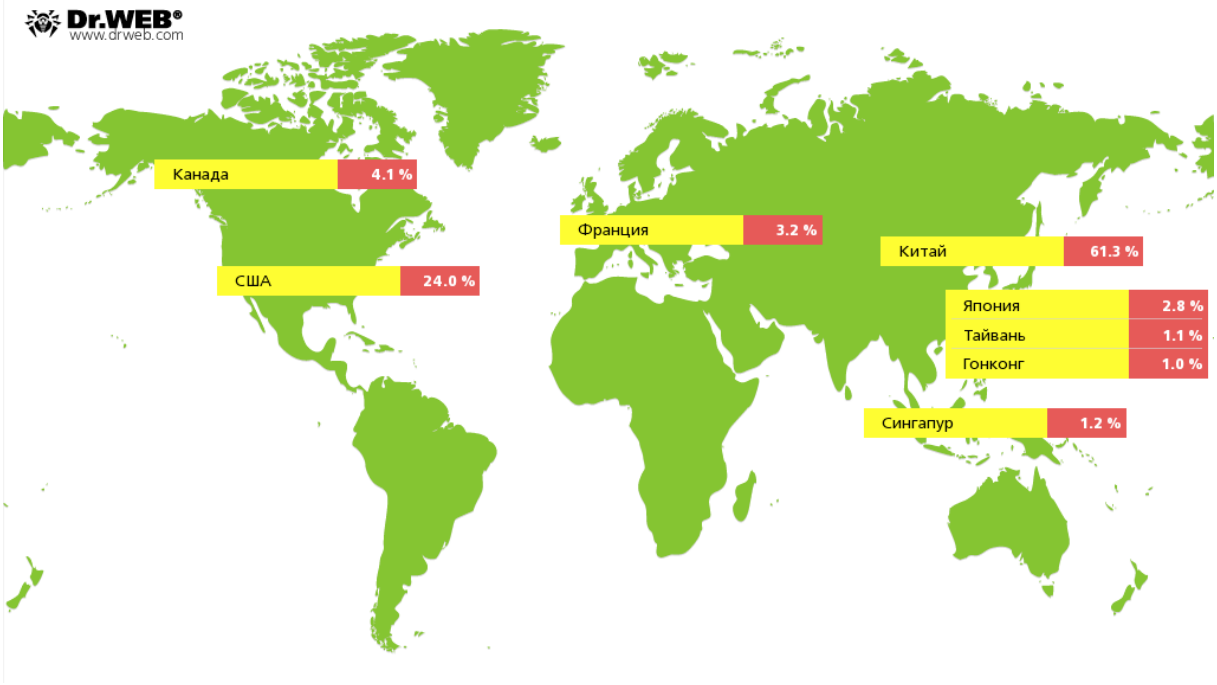


Обзор вирусной активности за 2015 год

Еще один файловый вирус, с использованием которого киберпреступники создали активно действующую бот-сеть, носит наименование Win32.Sector, он известен вирусным аналитикам с 2008 года. Предназначение этого вируса заключается в загрузке из P2P-сети и запуске на зараженной машине различных исполняемых файлов. Вирус может встраиваться в работающие на инфицированном компьютере процессы и самостоятельно распространяться, заражая файлы на локальных дисках и сменных носителях, а также в общедоступных сетевых папках. В первой половине 2015 года активность этой бот-сети продемонстрировала небольшой рост, но ближе к осени возобладала тенденция к ее постепенному снижению:

В течение 2015 года специалисты компании «Доктор Веб» продолжали следить за активностью Linux-троянца Linux.BackDoor.Gates.5, предназначенного для организации DDoS-атак на различные интернет-ресурсы. Всего за прошедший год злоумышленники предприняли 31 880 таких атак, и большая часть подвергшихся DDoS-атакам интернет-ресурсов (более 61%) располагалось на территории Китая. Второе место по числу атакованных серверов занимает США, третье — Канада. Географическое распределение DDoS-атак, организованных киберпреступниками с использованием троянца Linux.BackDoor.Gates.5 в 2015 году, показано на следующей иллюстрации:

Обзор вирусной активности за 2015 год



Месяц от месяца количество предпринятых киберпреступниками атак колебалось, а к декабрю они и вовсе сошли на нет. График интенсивности DDoS-атак, предпринятых с использованием троянца Linux.BackDoor.Gates.5 (по количеству уникальных IP-адресов атакованных узлов) с января по ноябрь 2015 года представлен ниже:

Троянцы-шифровальщики

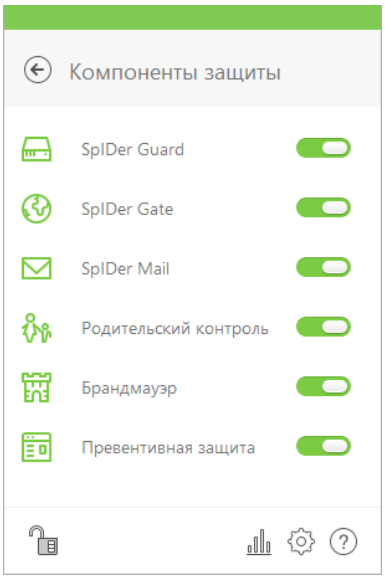
Как и в 2014-м, в уходящем году троянцы-шифровальщики представляли серьезную угрозу для пользователей, они по праву считаются наиболее опасным семейством вредоносных программ из всех ныне существующих. Если год назад среднемесячное число обращений в службу технической поддержки компании «Доктор Веб» от пользователей, пострадавших в результате действия энкодеров, составляло около 1000, то к концу 2015 года оно увеличилось практически втрое, что наглядно демонстрирует представленный ниже график:

Наиболее распространенные шифровальщики в 2015 году:

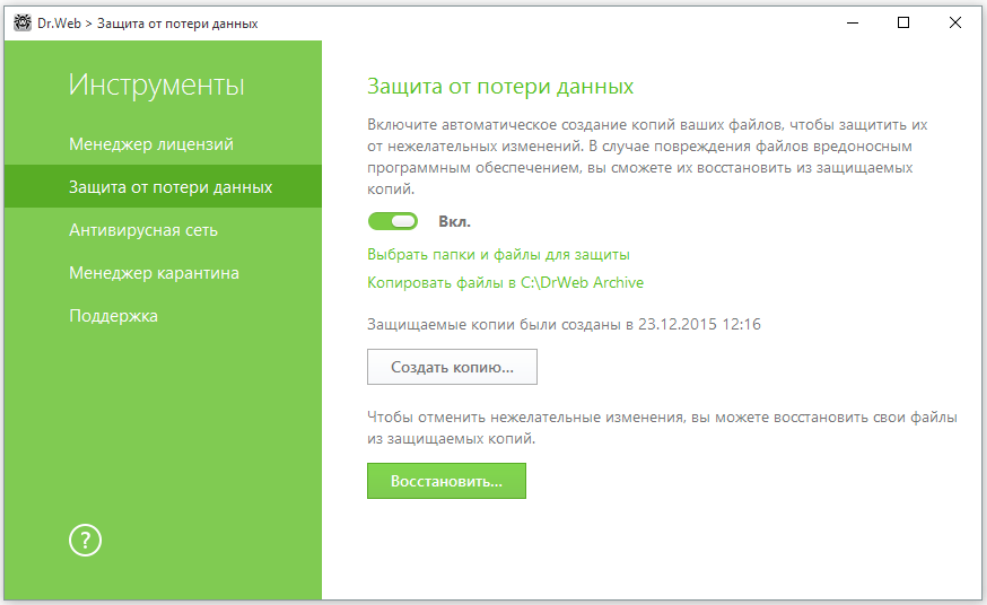
- **Trojan.Encoder.567**
- **Trojan.Encoder.858**
- **BAT.Encoder**
- **Trojan.Encoder.741**
- **Trojan.Encoder.761**
- **Trojan.Encoder.556**
- **Trojan.Encoder.398**
- **Trojan.Encoder.2843**
- **Trojan.Encoder.888**
- **Trojan.Encoder.263**

Чтобы избежать потери ценных файлов, воспользуйтесь следующими советами:

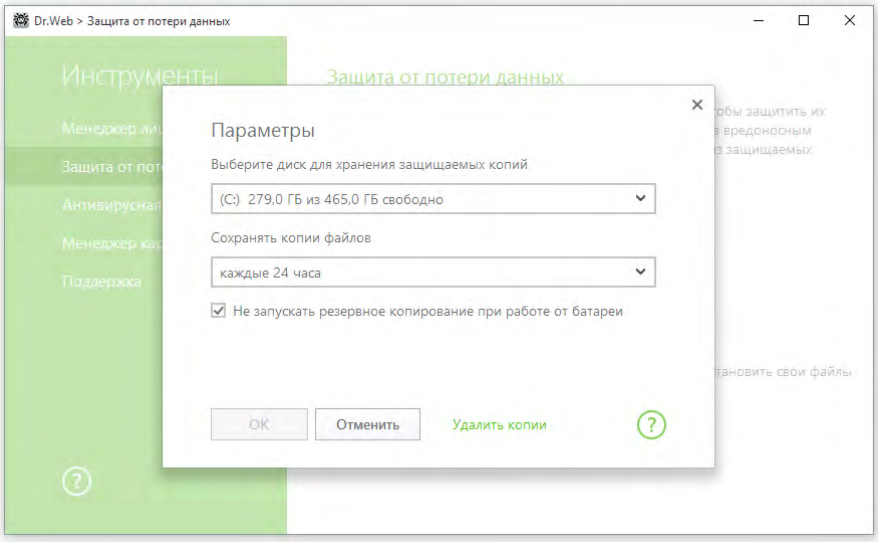
1. Убедитесь, что в настройках Dr.Web Security Space (версии 9, 10 и 11) включена «Превентивная защита», которая бережет ваш ПК от угроз, еще не известных вирусной базе Dr.Web.



2. После этого включите «Защиту от потери данных» в разделе «Инструменты» и настройте параметры хранилища резервной копии важных для вас файлов.



3. Создайте резервную копию ценных данных и настройте их автоматическое сохранение по удобному для вас графику, выбрав подходящий временной интервал.

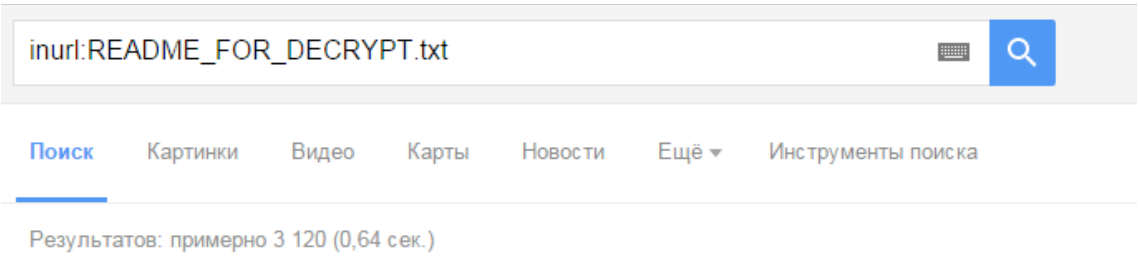


Эти действия в сочетании с определенной осмотрительностью позволят вам защитить вашу операционную систему от большинства современных угроз, включая троянцев-шифровальщиков.

Подробней Смотрите видео о настройке

Вредоносные программы для Linux

Наиболее резонансным событием в сфере информационной безопасности операционных систем семейства Linux стало распространение в ноябре 2015 года трояна-шифровальщика для этой платформы, получившего наименование Linux.Encoder.1. Троянец проникал на работающие под управлением Linux веб-серверы с использованием ряда уязвимостей в популярных системах управления контентом (Content Management Systems, CMS) и к 24 ноября инфицировал более 3000 веб-сайтов.



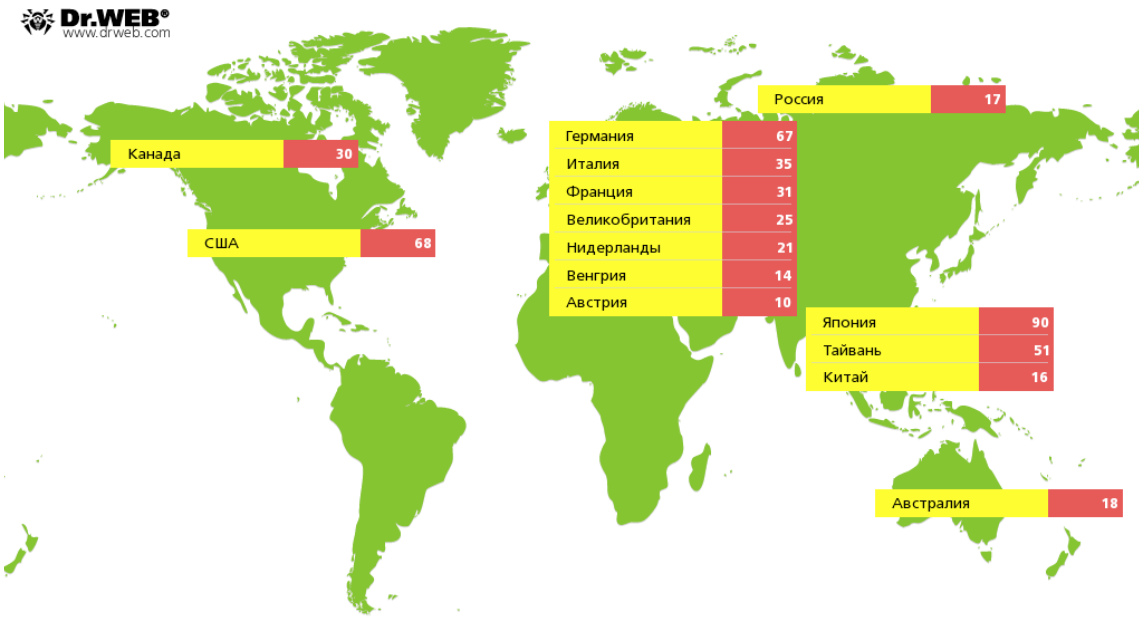
При помощи неустановленной уязвимости злоумышленники размещали на взломанном сайте специальный шелл-скрипт, который позволял им дистанционно выполнять различные команды. С его помощью на скомпрометированный сервер загружался дроппер троянца-энкодера Linux.Encoder.1, который, определив архитектуру операционной системы (32- или 64-разрядная версия Linux), извлекал из собственного тела соответствующий экземпляр шифровальщика и запускал его, после чего удалялся. Примечательно, что шифровальщик успешно функционировал в системе с привилегиями веб-сервера – иными словами, для работы ему не требовалось прав суперпользователя (root). Более подробно об этой вредоносной программе рассказано в соответствующей статье.

Вскоре после данного инцидента вирусные аналитики компании «Доктор Веб» установили факт существования еще нескольких более ранних модификаций данного шифровальщика, одна из которых получила имя Linux.Encoder.2. Об особенностях работы и отличиях этого энкодера от более распространенной его версии рассказано в опубликованном на сайте компании обзорном материале.

Впрочем, атаки на работающие под управлением ОС Linux веб-серверы наблюдались еще весной этого года – так, обнаруженный в апреле троянец Linux.BackDoor.Sessox.1 получал команды от злоумышленников по протоколу IRC (Internet Relay Chat) и обладал способностью атаковать заданный веб-узел Интернета путем отправки на него повторяющихся GET-запросов. Также по команде Linux.BackDoor.Sessox.1 мог выполнять сканирование атакуемого сервера на наличие ShellShock-уязвимости, которая позволяет удаленно выполнить в системе произвольный код. Подробнее о данной вредоносной программе рассказывается в опубликованной компанией «Доктор Веб» информационной статье.

В 2015 году вирусными аналитиками компании «Доктор Веб» было обнаружено несколько троянцев-бэкдоров для Linux. Об одном из них, Linux.BackDoor.Xnote.1, мы рассказывали в своей публикации еще в феврале. Способ распространения этого троянца вполне традиционен для подобных вредоносных программ: подбирая пароль, злоумышленники взламывали учетные записи для доступа к атакуемой системе по протоколу SSH и устанавливали в нее Linux.BackDoor.Xnote.1. Функциональное назначение этого троянца также стандартно для бэкдора: он может выполнять поступающие от киберпреступников команды. Кроме того, Linux.BackDoor.Xnote.1 может запустить командную оболочку (shell) с заданными переменными окружения и предоставить управляющему серверу доступ к ней, запустить на зараженном компьютере SOCKS proxy или собственную реализацию сервера portmap.

Другой Linux-бэкдор, получивший наименование Linux.BackDoor.Dklkt.1, специалисты «Доктор Веб» выявили в июле. Основное предназначение этого троянца — выполнение нескольких видов DDoS-атак. А в августе вирусные аналитики компании «Доктор Веб» сообщили об обнаружении большой группы вредоносных программ, способных заражать работающие под управлением Linux роутеры. Всего вирусным аналитикам компании «Доктор Веб» стало известно о 1439 случаях заражения устройств с использованием данных инструментов, при этом в 649 из них было выявлено географическое положение инфицированных устройств. Большинство располагалось на территории Японии, чуть меньше – в Германии, США и Тайване:

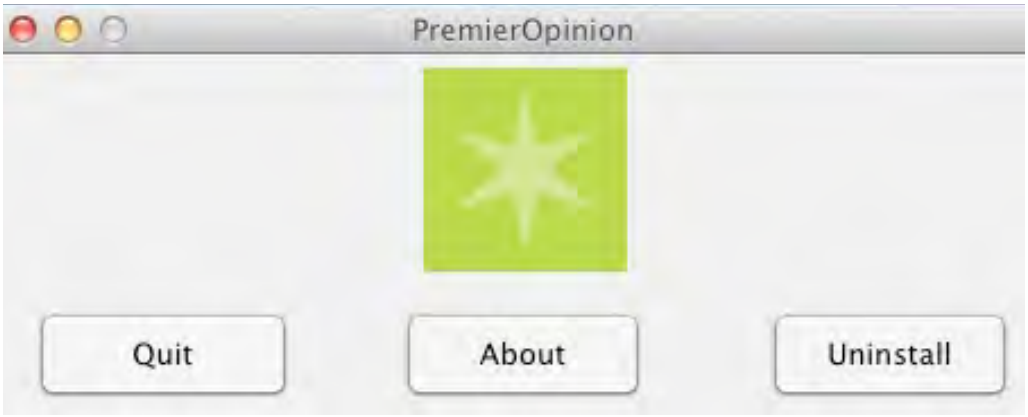


В сентябре компания «Доктор Веб» опубликовала новостной материал о распространении троянца Linux.Ellipsis.1, отличавшегося «параноидальным» поведением. Он был разработан злоумышленниками для создания на атакованной машине прокси-сервера, который использовался в целях обеспечения собственной анонимности для доступа к устройствам, взломанным при помощи другой вредоносной программы, — Linux.Ellipsis.2. По ряду характерных признаков эта вредоносная программа является творением того же самого автора и предназначенного для подбора паролей методом грубой силы («брутфорс»).

В целом можно сказать, что интерес злоумышленников к операционным системам семейства Linux понемногу растет, и в будущем можно ожидать появления новых троянцев для этой платформы.

Вредоносные программы для Apple OS X

Злоумышленники по-прежнему проявляют внимание и к компьютерам производства корпорации Apple, работающим под управлением операционной системы OS X. Причем подавляющее большинство обнаруженных в 2015 году вредоносных программ для этой системы — рекламные троянцы и установщики нежелательных приложений. Редким исключением стала обнаруженная в начале года новая версия давно известного троянца Mac.BackDoor.OpinionSpy, знакомого специалистам по информационной безопасности еще с 2010 года.



Несмотря на то, что разработчики данного приложения позиционируют его как утилиту для проведения маркетинговых исследований, Mac.BackDoor.OpinionSpy является полноценным троянцем-шпионом: он отслеживает активность пользователя и передает на управляющий сервер сведения о посещенных сайтах, открываемых вкладках и ссылках, по которым выполнялся переход. Также троянец осуществляет мониторинг трафика, передаваемого через сетевую карту компьютера Apple, в том числе трафика клиентов для обмена мгновенными сообщениями (Microsoft Messenger, Yahoo! Messenger, AIM, iChat). Более подробные сведения об этом бэкдоре можно почерпнуть в опубликованной на сайте компании «Доктор Веб» статье.

Среди более распространенных установщиков нежелательных программ для OS X следует упомянуть обнаруженный специалистами «Доктор Веб» в мае 2015 года Adware.Mac.InstallCore.1, который загружал и инсталлировал на атакуемый «мак» вредоносные надстройки для браузеров Safari, Firefox и Chrome, детектируемые как троянцы семейства Trojan.Crossrider. Другой установщик получил название Adware.Mac.WeDownload.1 — о нем компания «Доктор Веб» рассказала в сентябре. Данный загрузчик распространяется с использованием ресурсов партнерской программы, ориентированной на монетизацию файлового трафика, как и его аналог Adware.Mac.Tuguu.1, исследованный вирусными аналитиками в декабре 2015 года.

Судя по тому, что подобные приложения выявляются в «живой природе» с завидной регулярностью, в следующем году также вряд ли удастся избежать появления новых образцов подобных вредоносных программ.

Опасные и нерекомендуемые сайты

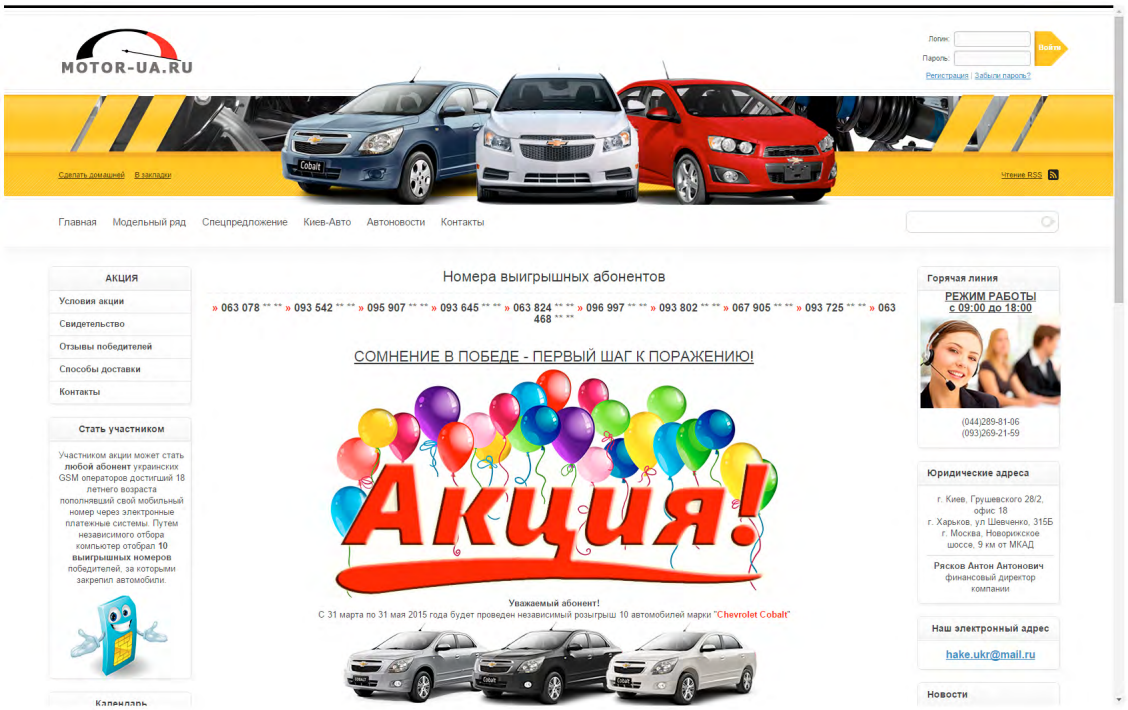
В Интернете существует огромное количество сайтов, посещение которых нежелательно для несовершеннолетних, а то и вовсе может причинить компьютеру вред. Для борьбы с ними предназначены компоненты Антивируса Dr.Web SpIDer Gate и Родительский контроль, в базы которых ежедневно добавляются новые ссылки на вредоносные и нерекомендуемые сайты. Динамику этого процесса в 2015 году можно проследить на представленной ниже диаграмме:

Нерекомендуемые сайты

Обзор вирусной активности за 2015 год

Сетевые мошенничества

Не дремлют и сетевые жулики, стремящиеся нажиться на доверчивости или неопытности пользователей Интернета. В 2015 году компания «Доктор Веб» сообщала об участившихся случаях мошенничества с применением сайтов, оформленных как веб-страницы автосалонов. Для привлечения на них посетителей кибермошенники используют массовые СМС-рассылки, в которых потенциальной жертве сообщается о выигрыше автомобиля в рамках той или иной рекламной акции.



Помимо прочего, подобные сайты содержат отдельную страницу с описанием условий «акции», согласно которым «выигравший» автомобиль участник должен 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. В этом и кроется интерес мошенников: отправив подобным способом платеж, жертва больше не увидит ни своих денег, ни ценного приза.

Обзор вирусной активности за 2015 год

Продолжают процветать и многочисленные интернет-магазины, торгующие всевозможными сомнительными товарами — о подобных интернет-коммерсантах компания «Доктор Веб» рассказывала в 2015 году в своих новостных публикациях. Нет никаких сомнений в том, что грядущий год вряд ли изменит ситуацию с появлением подобных сомнительных торговых площадок.

Для мобильных устройств

В минувшем году злоумышленники сохранили повышенный интерес к пользователям мобильных устройств. Как и следовало ожидать, одной из главных целей киберпреступников в течение последних 12 месяцев вновь стали владельцы Android-смартфонов и планшетов. За последний год вирусные аналитики компании «Доктор Веб» проанализировали множество новых вредоносных, нежелательных и потенциально опасных приложений для ОС Android, в результате чего вирусная база Dr.Web пополнилась 11929 новыми записями и увеличилась в объеме на 210%.

Динамика пополнения вирусной базы Dr.Web записями для вредоносных, нежелательных и потенциально опасных Android-программ

Dr.WEB®
www.drweb.com

Как и прежде, основную массу вредоносных приложений, предназначенных для атаки на Android-устройства, составили всевозможные СМС-троянцы. Согласно вирусным базам Dr.Web, число записей для наиболее многочисленного семейства СМС-сендеров Android.SmsSend за год увеличилось на 164,2% и составило 7 103 единицы. Выросло и количество записей для троянцев семейства Android.SmsBot (+192,8%). В целом можно с уверенностью сказать, что вредоносные программы, отправляющие СМС-сообщения на платные номера и подписывающие пользователей на дорогостоящие услуги, по-прежнему представляют одну из основных угроз для владельцев Android-устройств.

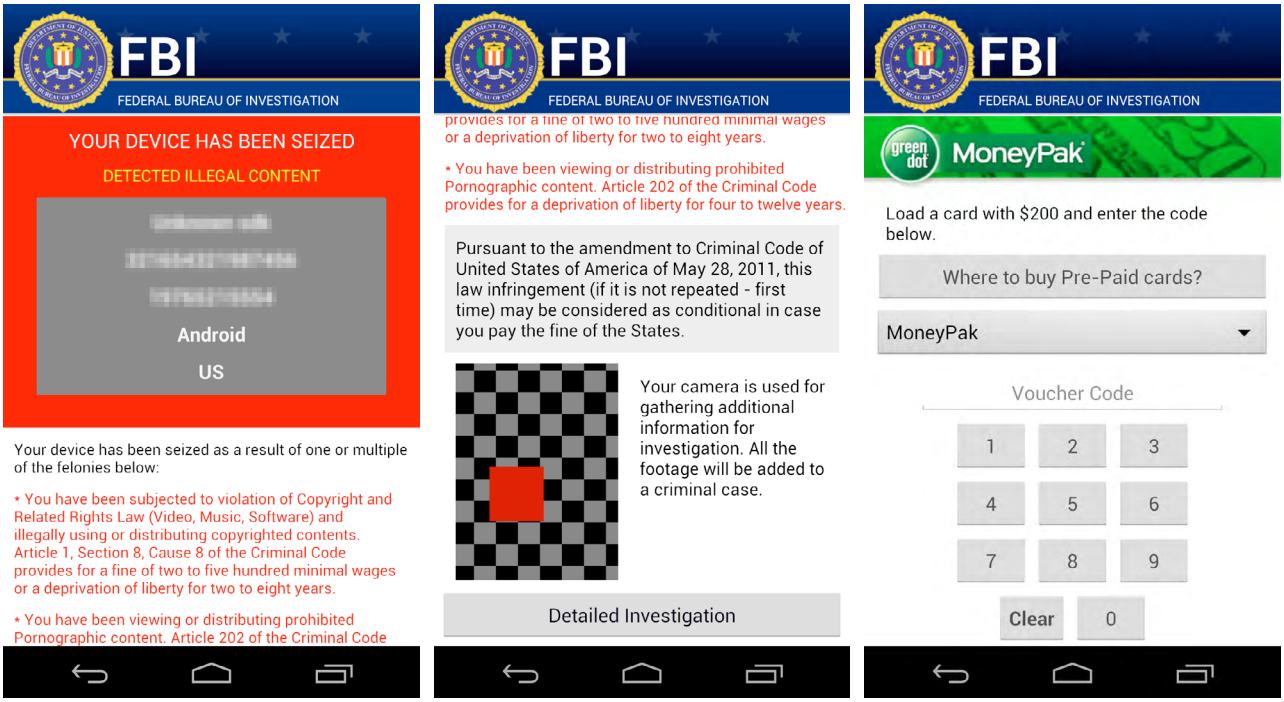
Серьезную опасность для финансового благополучия пользователей ОС Android в 2015 году вновь представляли всевозможные банковские троянцы. Эти вредоносные программы способны похищать логины и пароли для доступа к мобильному банкингу, а также могут незаметно переводить деньги на счета киберпреступников. За прошедшие 12 месяцев специалисты «Доктор Веб» выявили большое число таких троянцев. При этом среди них оказались не только представители уже хорошо известных семейств Android.Banker и Android.BankBot, но также и новые вредоносные приложения данного типа, в частности, банкеры Android.ZBot.

Примечательно, что атаки с использованием Android-банкеров популярны у злоумышленников по всему миру. В 2015 году такие троянцы широко применялись в том числе и против жителей России и Южной Кореи. Например, опасная вредоносная программа Android.BankBot.65.origin, предназначенная для кражи денег у российских пользователей, была встроена киберпреступниками в настоящее приложение для доступа к мобильному банкингу и распространялась под видом обновления соответствующего ПО на одном из популярных веб-сайтов, посвященных приложениям для смартфонов и планшетов. Подробнее об Android.BankBot.65.origin рассказано в соответствующем материале.

Однако в большинстве случаев банковские троянцы распространяются вирусописателями как самостоятельные вредоносные приложения, и в этом злоумышленникам активно помогает массовая рассылка СМС-сообщений, в которых указывается ссылка на загрузку того или иного банкера. Так, в 2015 году для российских пользователей чаще всего подобные сообщения представляли собой «уведомления» о поступивших ММС, а, например, в Южной Корее пользователям предлагалось посетить свадьбу, отследить почтовое отправление и даже ознакомиться с материалами некоего уголовного дела.

Также в 2015 году продолжили появляться новые троянцы-вымогатели. Эти вредоносные приложения стали известны в середине 2014 года и с тех пор представляют одну из самых серьезных угроз для владельцев Android-устройств. Большинство из них блокирует зараженные мобильные телефоны или планшеты и требует у своих жертв выкуп за их разблокировку. Однако существуют и еще более опасные модификации подобных вымогателей. Например, выявленная в феврале 2015 года новая версия троянца Android.Locker.71.origin шифровала все доступные файлы и требовала у пострадавших пользователей денежную компенсацию в размере $200.

Обзор вирусной активности за 2015 год



Число записей для троянцев-вымогателей семейства Android.Locker в вирусной базе Dr.Web:

2014	2015	Динамика
137	965	+604,4%

Одной из тенденций уходящего года стало появление большого числа троянцев, которые распространялись злоумышленниками в Android-прошивках и даже предустанавливались непосредственно на мобильные устройства. Одна из таких вредоносных программ была обнаружена в январе и получила имя Android.CaPson.1. Этот троянец мог незаметно отправлять и перехватывать СМС-сообщения, открывать интернет-страницы, передавать на удаленный сервер информацию о зараженном мобильном устройстве, а также загружать другие приложения. В сентябре специалисты компании «Доктор Веб» обнаружили троянца Android.Backdoor.114.origin, который был предустановлен на популярном планшете. Эта вредоносная программа могла незаметно загружать, устанавливать и удалять программы по команде киберпреступников. А уже в октябре 2015 года на нескольких мобильных Android-устройствах был обнаружен предустановленный троянец Android.Cooee.1. Эта вредоносная программа находилась

в приложении-лаунчере (графической оболочке Android) и предназначалась для показа рекламы, а также незаметной загрузки и запуска на исполнение как дополнительных рекламных модулей, так и других приложений, включая вредоносные.

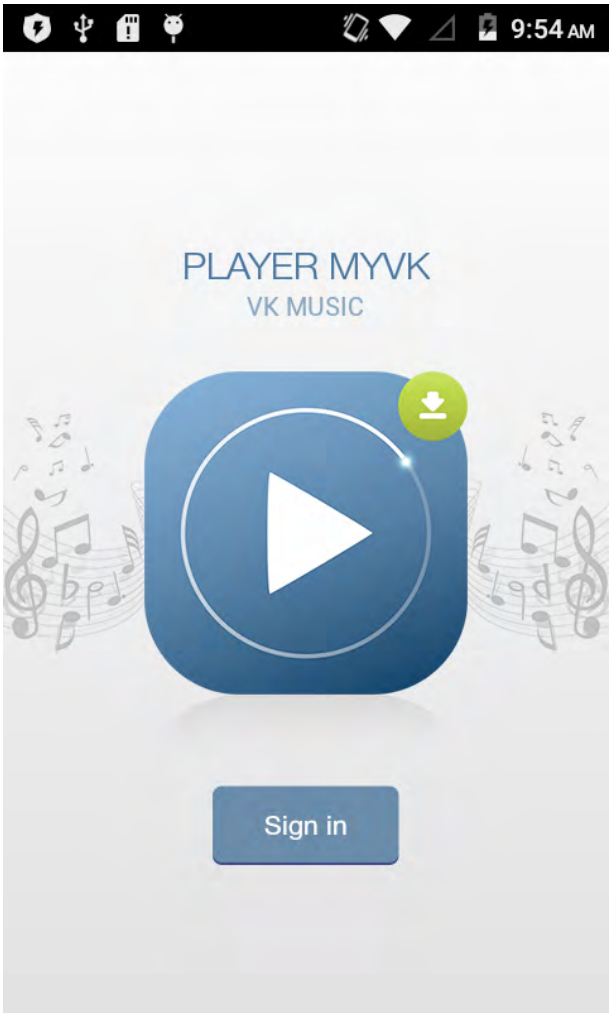
Еще одной опасной тенденцией 2015 года стал рост числа вредоносных программ, пытавшихся получить root-полномочия на Android-устройствах. Например, в апреле специалисты компании «Доктор Веб» обнаружили троянцев семейства Android.Toorch, которые распространялись вирусописателями через популярные в Китае онлайн-сборники ПО, а также при помощи агрессивных рекламных модулей, встроенных в различные приложения. Если данные троянцы получали root-полномочия, они по команде злоумышленников могли без ведома пользователя загружать, устанавливать и удалять различное ПО. Позднее был обнаружен троянец Android.Backdoor.176.origin, а также его модификация Android.Backdoor.196.origin – обе эти вредоносные программы пытались получить root-доступ на заражаемых смартфонах и планшетах с использованием модифицированной версии утилиты Root Master. Основное их предназначение – незаметная установка и удаление приложений по команде вирусописателей. Помимо этих вредоносных программ в 2015 году были выявлены и другие аналогичные троянцы, например, Android.Backdoor.273.origin, распространявшийся через каталог Google Play, а также Android.DownLoader.244.origin, которого потенциальные жертвы могли скачать с популярных сайтов – сборников ПО. Оба эти троянца также предназначались для незаметной загрузки и скрытной инсталляции других вредоносных приложений. Таким образом, в 2015 году наблюдался значительный рост числа всевозможных троянцев, главной задачей которых являлась загрузка и незаметная установка различных программ.

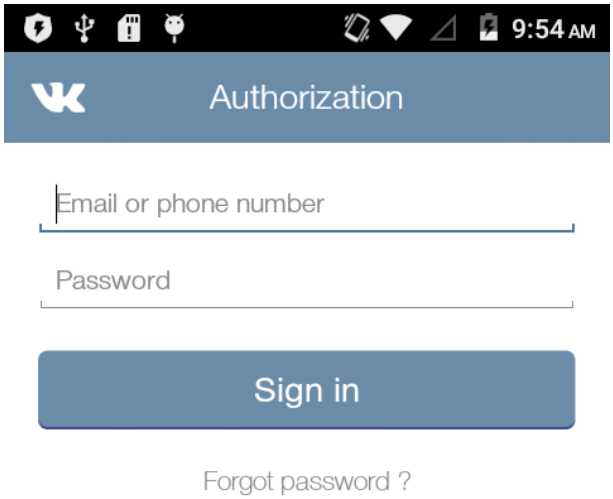
В минувшем году вновь не обошлось без проникновения вредоносных программ в каталог Google Play. В частности, обнаруженные в нем троянцы Android.Spy.134 и Android.Spy.135 могли демонстрировать на экране зараженных устройств поддельное окно аутентификации приложения-клиента Facebook, запрашивая у владельцев смартфонов и планшетов логин и пароль от их учетных записей, и передавать введенные данные на удаленный сервер. В общей сложности эти троянцы были загружены более 500 000 раз.

Также вирусные аналитики «Доктор Веб» обнаружили в каталоге Google Play троянца Android.DownLoader.171.origin, которого скачало более 100 000 пользователей. Злоумышленники распространяли эту вредоносную программу и через популярные сайты – сборники ПО, поэтому общее число загрузок троянца превысило 1 500 000. Основное предназначение Android.DownLoader.171.origin – загрузка и установка различных приложений. Подробнее об этой вредоносной программе рассказано в соответствующем материале.

В сентябре 2015 года в каталоге Google Play был найден троянец Android.MKcap.1.origin, который автоматически подписывал пользователей на платные сервисы. В этом же месяце был обнаружен еще один опасный троянец Android.MulDrop.67, предназначенный для загрузки и инсталляции другого вредоносного ПО, а также показа рекламы.

В октябре в каталоге Google Play был выявлен троянец Android.PWS.3, скрывавшийся во внешне безобидном аудиоплеере. Он требовал от пользователей логин и пароль от их учетной записи в популярной социальной сети, после чего незаметно загружал эти данные на удаленный сервер злоумышленников.



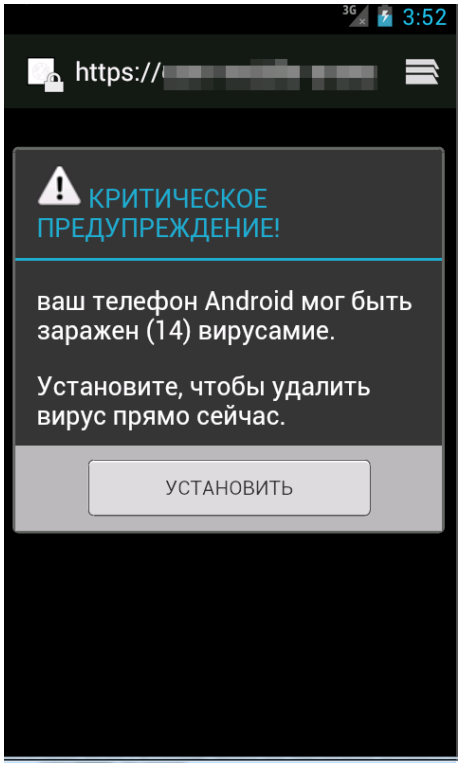


Еще одним поводом для беспокойства пользователей Android-смартфонов и планшетов в 2015 году стала активность всевозможных агрессивных рекламных модулей, встраиваемых злоумышленниками в различные программы. По сравнению с 2014 годом, за 12 месяцев число записей в вирусной базе для них увеличилось на 166% и достигло 290 единиц.

Так, в январе в каталоге Google Play были обнаружены приложения, содержащие рекламный плагин **Adware.HideIcon.1.origin**. Этот нежелательный модуль мог показывать в панели уведомлений мобильных устройств сообщения о доступности неких обновлений, имитировать процесс загрузки важных «файлов», при попытке открыть которые владелец смартфона или планшета перенаправлялся на различные веб-сайты. Также при запуске тех или иных программ **Adware.HideIcon.1.origin** мог выводить на весь экран всевозможную рекламу.

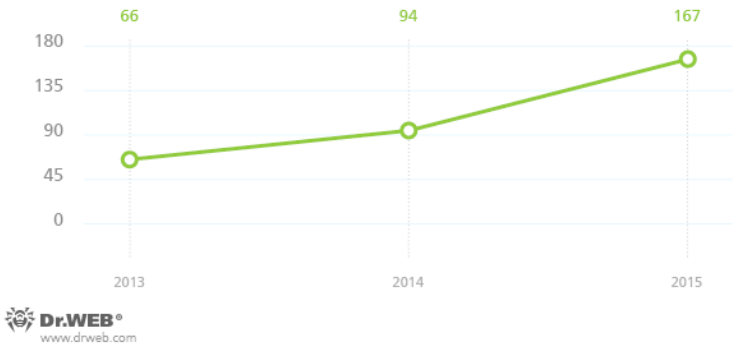
В феврале был обнаружен нежелательный рекламный модуль Adware.MobiDash.1.origin, встроенный в распространяемые через каталог Google Play программы, которые в общей сложности были скачаны десятки миллионов раз. Позже был найден агрессивный рекламный модуль Adware.HiddenAds.1, который инсталлировался на мобильные устройства вредоносным приложением, работал скрытно от пользователей и мог отображать в панели уведомлений всевозможные рекламные сообщения. Другой нежелательный модуль, добавленный в вирусную базу как Adware.Adstoken.1.origin, распространялся в составе разнообразных программ и показывал на экране рекламные баннеры, демонстрировал сообщения в панели уведомлений и мог открывать в веб-браузере сайты с рекламой. А в конце года вирусные аналитики компании «Доктор Веб» обнаружили рекламное ПО Adware.AnonyPlayer.1.origin. Этот нежелательный модуль показывал рекламу поверх большинства запускаемых приложений.

Обзор вирусной активности за 2015 год



Все еще распространенный миф о том, что мобильные устройства от компании Apple не подвержены атакам со стороны вредоносных приложений постепенно развенчивается – с каждым годом для смартфонов и планшетов под управлением iOS появляется все больше троянцев и прочих опасных программ. Так, если в 2014 году вирусная база Dr.Web содержала 94 записи для вредоносных iOS-программ, то за последние 12 месяцев их количество увеличилось на 77% и составило уже 167 единиц.

Динамика пополнения вирусной базы Dr.Web записями для вредоносных, нежелательных и потенциально опасных программ для iOS



Одним из выявленных в 2015 году троянцев для iOS стала вредоносная программа IPhoneOS.BackDoor.KeyRaider, распространявшаяся в модифицированных злоумышленниками программах и заражавшая устройства, подвергнутые процедуре «jailbreak». IPhoneOS.BackDoor.KeyRaider крал различную конфиденциальную информацию с зараженных смартфонов и планшетов и загружал ее на сервер киберпреступников.
В сентябре в официальном магазине iOS-приложений App Store был выявлен опасный троянец IPhoneOS.Trojan.XcodeGhost, основная задача которого – показ поддельных диалоговых окон с целью проведения фишинг-атак, а также открытие заданных злоумышленниками ссылок. В ноябре специалисты компании «Доктор Веб» обнаружили одну из модификаций троянца IPhoneOS.Trojan.XcodeGhost, которая получила имя IPhoneOS.Trojan.XcodeGhost.8 и обладала аналогичным функционалом. А в октябре был обнаружен троянец IPhoneOS.Trojan.YiSpecter.2, загружавшийся при посещении различных веб-сайтов и заражавший не только смартфоны и планшеты с наличием «jailbreak», но и устройства с немодифицированной версией iOS. IPhoneOS.Trojan.YiSpecter.2 устанавливал дополнительные вредоносные модули, имел возможность показывать различную рекламу, а также удалять по команде киберпреступников программы и заменять их поддельными версиями.

В конце года был обнаружен троянец IPhoneOS.Trojan.TinyV, который распространялся в модифицированных вирусописателями приложениях и заражал «взломанные» iOS-устройства. По команде с управляющего сервера IPhoneOS.Trojan.TinyV имел возможность незаметно скачивать и устанавливать различное ПО, а также модифицировать файл hosts, в результате чего злоумышленники перенаправляли пользователей на нежелательные веб-сайты. Также среди выявленных в 2015 году опасных программ для iOS оказалась рекламное приложение Adware.Muda.1, заражавшее устройства с «jailbreak». Оно могло показывать рекламу поверх пользовательских приложений и в панели уведомлений, а также загружать различное ПО без ведома пользователя.

Перспективы и вероятные тенденции

Анализ сложившейся на текущий момент ситуации в сфере информационной безопасности позволяет сделать предположение о том, что в наступающем 2016 году будет по-прежнему наблюдаться рост числа вредоносных программ для операционных систем Linux и OS X. Возможно и расширение их функциональных возможностей: так, поклонники компьютеров Apple помимо рекламных троянцев и установщиков нежелательного ПО вполне могут столкнуться с первыми в истории энкодерами для OS X.

Обзор вирусной активности за 2015 год

Будут появляться все новые вредоносные программы для мобильной платформы Android, при этом значительную часть среди них наверняка будут составлять банковские троянцы. Не стоит расслабляться также пользователям портативных устройств производства компании Apple, работающих под управлением операционной системы iOS — в течение 2015 года для нее было обнаружено несколько троянских программ, и есть основания полагать, что эта тенденция сохранится и в дальнейшем.

Весьма вероятно появление новых ботнетов, причем созданных злоумышленниками с помощью вредоносных программ не только для ОС Windows, но и для альтернативных системных платформ. Наконец, не следует исключать вероятности появления новых способов сетевого мошенничества, в том числе с применением мобильных устройств, а также совершенствования киберпреступниками методик хищения персональных данных пользователей и различной конфиденциальной информации.

Одно можно сказать со всей определенностью: сотрудники компании «Доктор Веб» продолжат внимательно следить за развитием ситуации в сфере информационной безопасности и в 2016 году, как и ранее, будут своевременно информировать своих пользователей о появлении новых актуальных угроз.

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