Dr.WEB®
с 1992 года

Обзор вирусной активности в марте 2016 года

Обзор вирусной активности в марте 2016 года

31 марта 2016 года

Март 2016 года вполне можно назвать месяцем вредоносных программ для OS X — с началом весны пробудились от спячки вирусописатели, создающие троянцев для компьютеров Apple. В первой половине марта были обнаружены новые представители семейства рекламных троянцев для OS X, а в середине месяца специалисты компании «Доктор Веб» разработали алгоритм расшифровки файлов, поврежденных троянцем-шифровальщиком для этой операционной системы, — Mac.Trojan.KeRanger.2. Кроме того, в марте была выявлена новая вредоносная программа, проникшая в ряд популярных приложений и в прошивку устройств, работающих под управлением мобильной платформы Google Android.

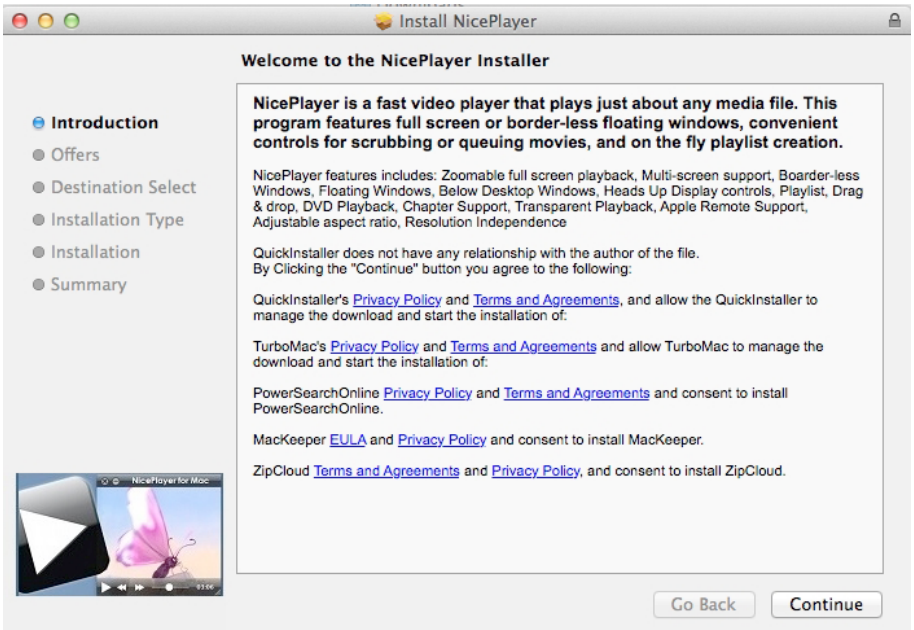
Главные тенденции марта

- Появились новые рекламные троянцы для OS X
- Стала возможной расшифровка файлов, поврежденных энкодером для OS X
- Обнаружен новый троянец в прошивке ряда Android-устройств и в популярных приложениях

Обзор вирусной активности в марте 2016 года

Угроза месяца

В начале марта специалисты компании «Доктор Веб» выявили новых представителей семейства рекламных троянцев, представляющих угрозу для компьютеров Apple под управлением операционной системы OS X. Первым на «мак» проникает установщик троянца Mac.Trojan.VSearch.2, который может быть замаскирован под любое полезное приложение, например, дистрибутив проигрывателя Nice Player.



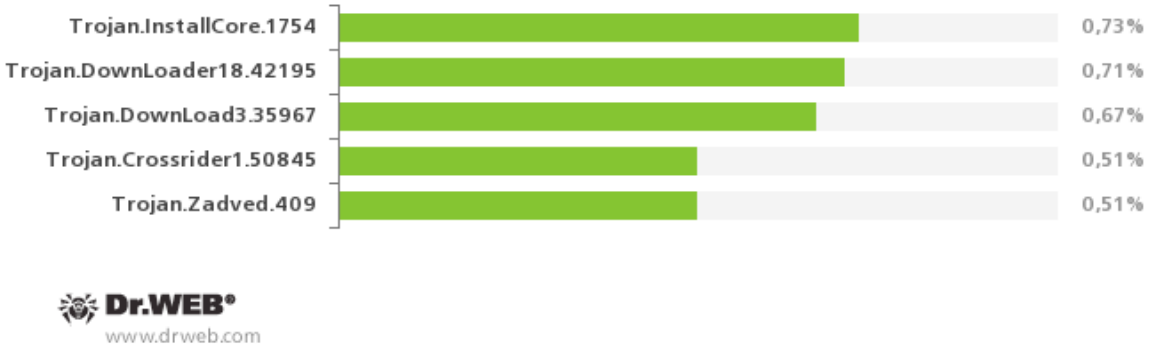
В отличие от других программ-установщиков, Mac.Trojan.VSearch.2 не позволяет пользователю выбрать копируемые на компьютер компоненты — он настроен таким образом, будто пользователь сам отметил флажками все предложенные варианты. Среди других опасных и нежелательных программ этот троянец устанавливает на атакуемый «мак» вредоносное приложение Mac.Trojan.VSearch.4, которое, в свою очередь, внедряет в систему троянца Mac.Trojan.VSearch.7. Запустившись на зараженном компьютере, Mac.Trojan.VSearch.7 создает в операционной системе нового пользователя (который не отображается в окне приветствия OS X) и встраивает во все открываемые в окне браузера веб-страницы сценарий на языке JavaScript, показывающий рекламные баннеры. Помимо этого, он собирает пользовательские запросы в нескольких популярных поисковых системах.

Более подробную информацию об этих вредоносных программах и их функциях можно получить, ознакомившись с опубликованной на нашем сайте обзорной статьей.

Обзор вирусной активности в марте 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

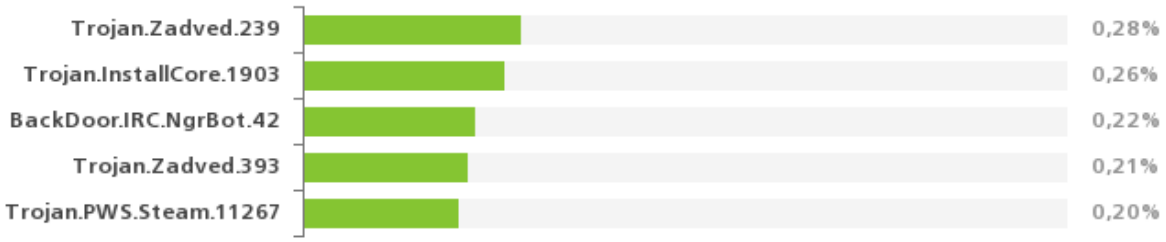


- **Trojan.InstallCore.1754**
  Один из представителей семейства программ-установщиков нежелательных и вредоносных приложений.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, которые скачивают из Интернета и запускают на атакуемом компьютере другое вредоносное ПО.
- **Trojan.Crossrider1.50845**
  Представитель семейства троянцев, предназначенных для показа различной сомнительной рекламы.
- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.

Обзор вирусной активности в марте 2016 года

По данным серверов статистики «Доктор Веб»

Наиболее распространенные вредоносные программы в марте 2016 года
согласно данным серверов статистики Dr.Web

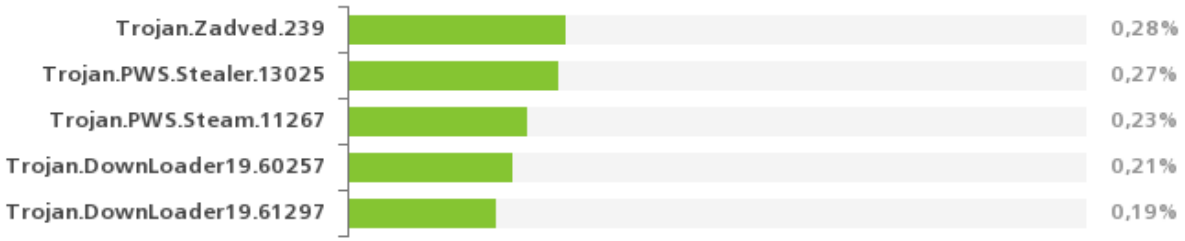


Dr.WEB®
www.drweb.com

- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **Trojan.InstallCore.1903**
  Один из представителей семейства установщиков нежелательных и вредоносных приложений.
- **BackDoor.IRC.NgrBot.42**
  Довольно распространенный троянец, известный специалистам по информационной безопасности еще с 2011 года. Вредоносные программы этого семейства способны выполнять на инфицированном компьютере поступающие от злоумышленников команды, а управление ими киберпреступники осуществляют с использованием протокола обмена текстовыми сообщениями IRC (Internet Relay Chat).
- **Trojan.PWS.Steam.11267**
  Представитель семейства вредоносных программ, предназначенных для хищения на инфицированном компьютере логинов, паролей и другой конфиденциальной информации, в том числе учетных записей из игровой платформы Steam.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в марте 2016 года



- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **Trojan.PWS.Steam.11267**
  Представитель семейства вредоносных программ, предназначенных для хищения на инфицированном компьютере логинов, паролей и другой конфиденциальной информации, в том числе учетных записей из игровой платформы Steam.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Обзор вирусной активности в марте 2016 года

Троянцы-шифровальщики

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

Наиболее распространенные шифровальщики в марте 2016 года:

- Trojan.Encoder.858
- Trojan.Encoder.2843
- Trojan.Encoder.567

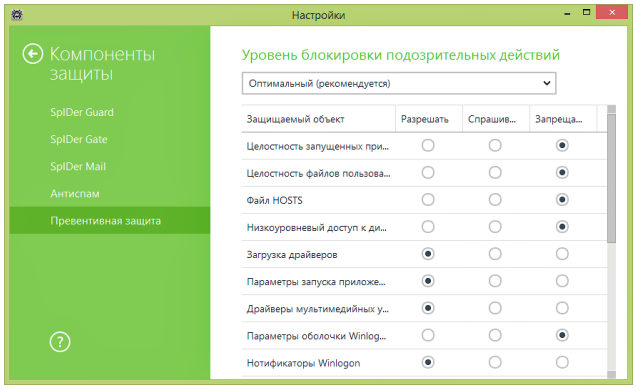
В феврале 2016 года многочисленные средства массовой информации сообщили о появлении первого троянца-шифровальщика, способного действовать на компьютерах Apple с установленной операционной системой OS X. Эта вредоносная программа получила наименование Mac.Trojan.KeRanger.2. В марте специалисты компании «Доктор Веб» разработали технологию, позволяющую расшифровывать файлы, поврежденные этим энкодером. О принципах действия энкодера Mac.Trojan.KeRanger.2, а также о том, какие шаги следует предпринять пользователям, пострадавшим от него, читайте в посвященной этому шифровальщику информационной статье.

Обзор вирусной активности в марте 2016 года

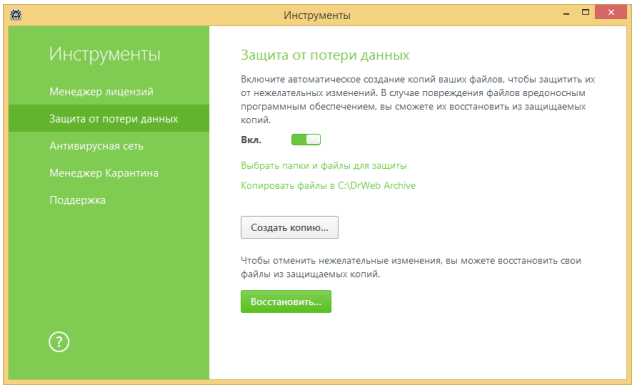
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Опасные сайты

В течение марта 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 458 013 интернет-адресов.

Февраль 2016	Март 2016	Динамика
+ 453 623	+ 458 013	+0.96%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

Первый весенний месяц 2016 года не обошелся без инцидентов с участием вредоносных Android-приложений. Специалисты компании «Доктор Веб» обнаружили рекламного троянца, который проник в приложения известных компаний, а также в прошивку нескольких десятков моделей мобильных устройств. Помимо показа навязчивой рекламы эта вредоносная программа могла загружать, устанавливать и запускать различное ПО, а также передавала на удаленный сервер конфиденциальную информацию. Кроме того, в марте вирусные аналитики «Доктор Веб» завершили анализ опасных троянцев, внедрявшихся в системный процесс ОС Android и процессы запускаемых приложений.

Наиболее заметные события, связанные с «мобильной» безопасностью в марте:

- обнаружение рекламного троянца в ряде программ известных компаний, а также прошивке большого числа мобильных устройств под управлением ОС Android;
- завершение исследования опасных троянцев, встраивающихся в системный процесс Android.

Более подробно о вирусной обстановке для мобильных устройств в марте читайте в нашем обзоре.

Обзор вирусной активности в марте 2016 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