Dr.WEB®
с 1992 года

Обзор вирусной активности в феврале 2016 года

Обзор вирусной активности в феврале 2016 года

29 февраля 2016 года

В феврале 2016 года произошел целый ряд событий, имеющих самое непосредственное отношение к вопросам информационной безопасности. Так, в начале месяца специалисты «Доктор Веб» обнаружили опасного Android-троянца, способного встраиваться в системные процессы, а во второй половине февраля было выявлено сразу несколько опасных вредоносных программ для ОС Windows.

Главные тенденции февраля

- Появление Android-троянца, способного встраиваться в системные процессы
- Распространение трояна, обманывающего клиентов российских банков
- Появление вредоносной программы для Windows, не работающей в странах СНГ

Обзор вирусной активности в феврале 2016 года

Угроза месяца

Наиболее интересной с технической точки зрения вредоносной «новинкой» среди прочих, обнаруженных в феврале, можно назвать набор из трех действующих совместно Android-троянцев, получивших наименования Android.Loki.1.origin, Android.Loki.2.origin и Android.Loki.3. Эти программы используют в своей работе библиотеку liblokih.so (ее Антивирус Dr.Web детектирует как Android.Loki.6) — компонент Android.Loki.3 встраивает ее в системные процессы, благодаря чему основной модуль, Android.Loki.1.origin, получает возможность действовать на зараженном устройстве с привилегиями пользователя system.

Следует отметить, что раньше Android-троянцы не могли похвастаться умением выполнять инжекты в процессы системных приложений, в связи с чем эта находка вирусных аналитиков компании «Доктор Веб» выглядит по-настоящему интересной. Android.Loki.1.origin обладает широким спектром функциональных возможностей, среди которых:

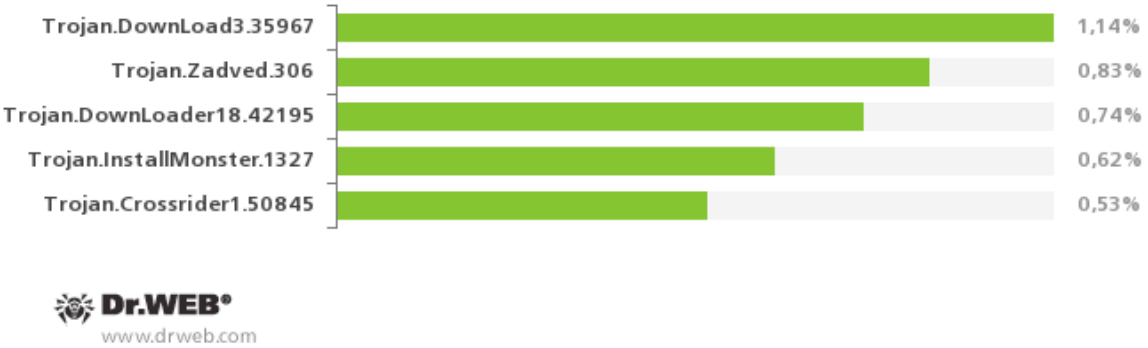
- установка и удаление приложений;
- включение и отключение приложений, а также их компонентов;
- остановка процессов;
- показ уведомлений;
- регистрация приложений как Accessibility Service (службы, отслеживающей нажатия на экран устройства);
- обновление своих компонентов, а также загрузка плагинов по команде с управляющего сервера.

Входящий в комплект вредоносных программ троянец Android.Loki.2.origin предназначен для установки на зараженное устройство различных приложений по команде с управляющего сервера, а также для показа рекламы. Однако обладает он и весьма обширным набором шпионских функций, позволяющих злоумышленникам собирать большой объем информации о зараженном устройстве. Более подробные сведения об этих троянцах для Android можно получить, ознакомившись с соответствующей обзорной статьей.

Обзор вирусной активности в феврале 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

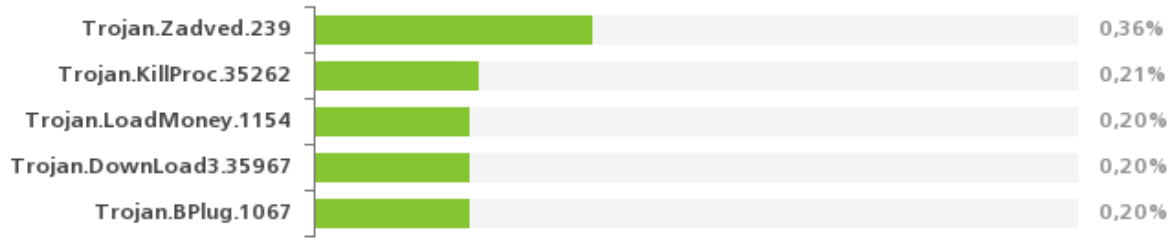


- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Installmonster**
  Семейство вредоносных программ, созданных с использованием партнёрской программы installmonster. Данные приложения устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Crossrider1.50845**
  Представитель семейства троянцев, предназначенных для показа различной сомнительной рекламы.

Обзор вирусной активности в феврале 2016 года

По данным серверов статистики «Доктор Веб»

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

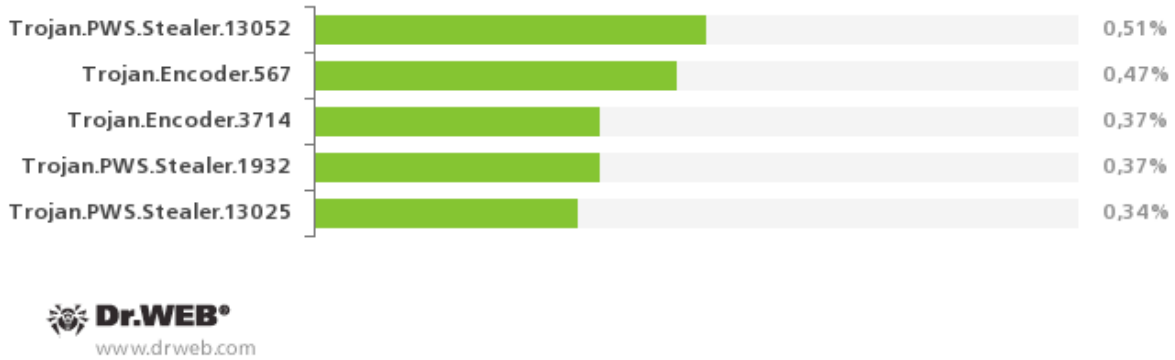


Dr.WEB®
www.drweb.com

- **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.KillProc.35262**
  Представитель семейства вредоносных программ, способных останавливать запущенные процессы других приложений, а также выполнять на инфицированном компьютере иные задачи злоумышленников.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнёрской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.

Статистика вредоносных программ в почтовом трафике

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



- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **Trojan.Encoder.567**
  Один из представителей семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку. Способен 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.
- **Trojan.Encoder.3714**
  Представитель семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку.

Обзор вирусной активности в феврале 2016 года

Троянцы-шифровальщики

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

Наиболее распространенные шифровальщики в феврале 2016 года:

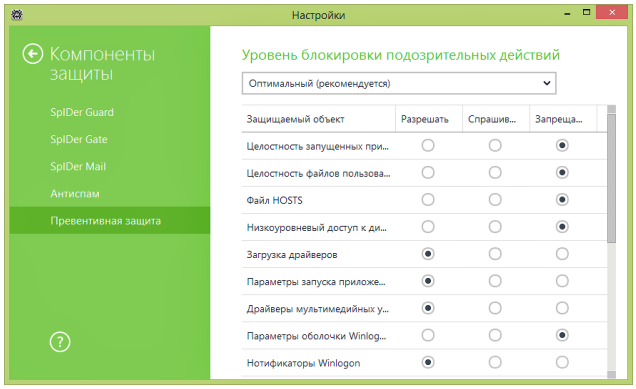
- Trojan.Encoder.567
- Trojan.Encoder.858
- Trojan.Encoder.3564
- Trojan.Encoder.761

Следует отметить, что почти половина зарегистрированных в феврале обращений в службу технической поддержки компании «Доктор Веб» от пользователей, файлы которых были зашифрованы троянцами-энкодерами, поступили из зарубежных стран.

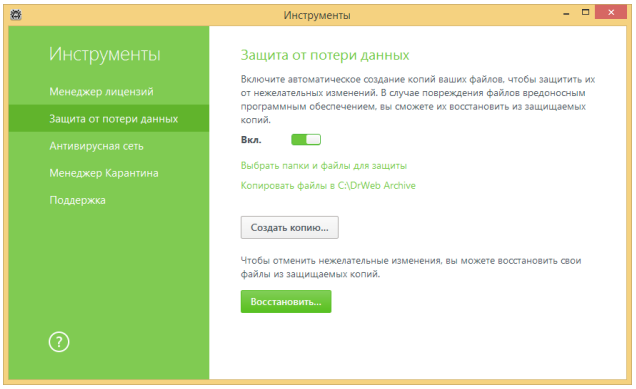
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



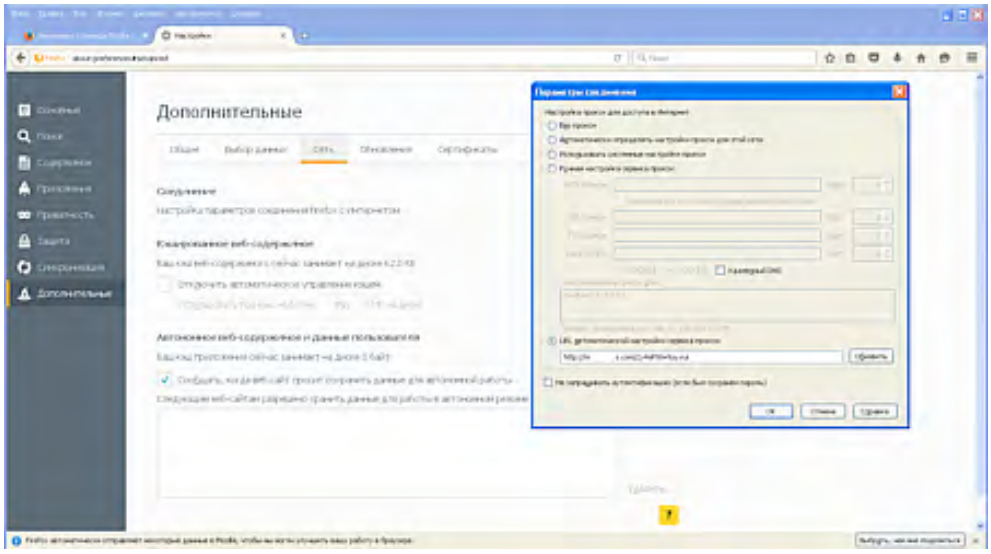
Подробней Смотрите видео о настройке

Другие вредоносные программы

О банковских троянцах семейства Trojan.Dyre многочисленные средства массовой информации сообщали с завидной регулярностью: эти вредоносные программы досаждают пользователям еще с середины 2014 года. Различные модификации Trojan.Dyre распространялись злоумышленниками с использованием партнерских программ по схеме CaaS — crime-as-a-service («преступление как услуга»). Участники программы получали специальный конструктор, с помощью которого генерировали новые образцы троянца. Также злоумышленники предоставляли в распоряжение своих партнеров специальную администраторскую панель, с помощью которой те могли управлять ботами. О том, как специалисты «Доктор Веб» борются с создателями и распространителями Trojan.Dyre, можно прочитать в опубликованной на сайте компании статье.

В середине февраля был обнаружен троянец Trojan.Proxy2.102, угрожающий клиентам нескольких крупных российских банков, — он позволяет злоумышленникам похищать деньги с банковских счетов. Для этого троянец устанавливает в системе корневой цифровой сертификат и изменяет настройки соединения с Интернетом, прописывая в них адрес принадлежащего злоумышленникам прокси-сервера.

Обзор вирусной активности в феврале 2016 года



С помощью этого прокси-сервера в страницы систем «банк-клиент» при открытии на инфицированном компьютере встраивается постороннее содержимое, позволяющее злоумышленникам похищать деньги с банковских счетов жертвы. Более подробная информация о троянце Trojan.Proxy2.102 изложена в соответствующем обзорном материале.

В конце месяца компания «Доктор Веб» сообщила о появлении троянца-загрузчика BackDoor.Andromeda.1407, примечательная особенность которого заключается в том, что он не работает на компьютерах, где установлена русская, украинская, белорусская или казахская национальная раскладка клавиатуры. В настоящее время этот бэкдор замечен в распространении нескольких опасных вредоносных приложений.

Опасные сайты

В течение февраля 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 453 623 интернет-адреса.

Январь 2016	Февраль 2016	Динамика
+ 625 588	+ 453 623	- 27.5%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

Прошедший февраль был отмечен сразу несколькими инцидентами с участием Android-троянцев. Так, в начале месяца вирусные аналитики компании «Доктор Веб» исследовали целую группу многофункциональных вредоносных приложений семейства Android.Loki, предназначенных, в частности, для загрузки и установки различного ПО, показа рекламы, а также сбора конфиденциальной информации. Кроме того, в феврале злоумышленники вновь распространяли банковских троянцев среди пользователей Android-смартфонов и планшетов.

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

- появление многофункциональных троянцев, встраивающихся в системные процессы и обладающих широкими функциональными возможностями;
- очередные случаи распространения банковских троянцев.

Обзор вирусной активности в феврале 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