Dr.WEB®
с 1992 года

Обзор вирусной активности в декабре 2016 года

Обзор вирусной активности в декабре 2016 года

26 декабря 2016 года

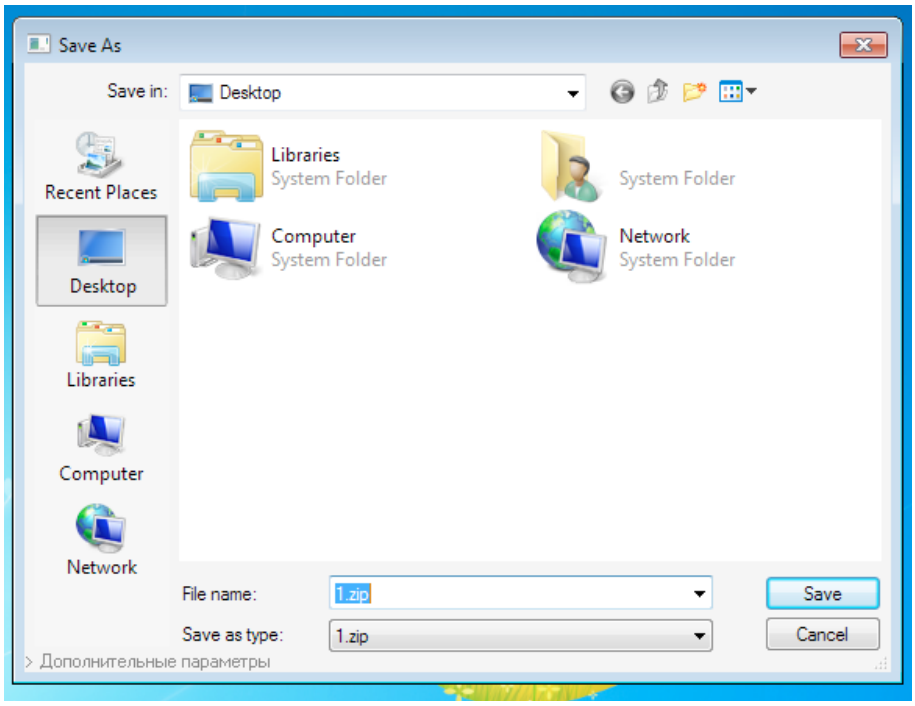
В последнем месяце уходящего года специалисты компании «Доктор Веб» выявили Android-троянца, способного заражать системные библиотеки на инфицированном устройстве, а также исследовали вредоносную программу для Windows, предназначенную для установки нежелательных приложений. Во второй половине декабря специалисты «Доктор Веб» обнаружили Android-троянцев в прошивке множества популярных мобильных устройств.

Главные тенденции ноября

- Распространение вредоносной программы, устанавливающей нежелательные приложения
- Обнаружение трояна в прошивке множества мобильных устройств
- Появление Android-троянца, способного заражать системные библиотеки

Угроза месяца

Многие современные троянцы без ведома пользователя загружают и устанавливают различные приложения на зараженный компьютер: злоумышленники пользуются услугами так называемых «партнерских программ», выплачивающих вознаграждение за инсталляцию ПО. Обычно подобные троянцы устроены примитивно, однако Trojan.Ticno.1537 простым назвать нельзя. После запуска он несколькими способами пытается определить наличие виртуального окружения и средств отладки, и запускается только если ему не удалось обнаружить на атакуемом компьютере ничего для себя подозрительного. После запуска Trojan.Ticno.1537 сохраняет на диск файл с именем 1.zip и открывает диалоговое окно, похожее на стандартное окно сохранения файла Microsoft Windows:

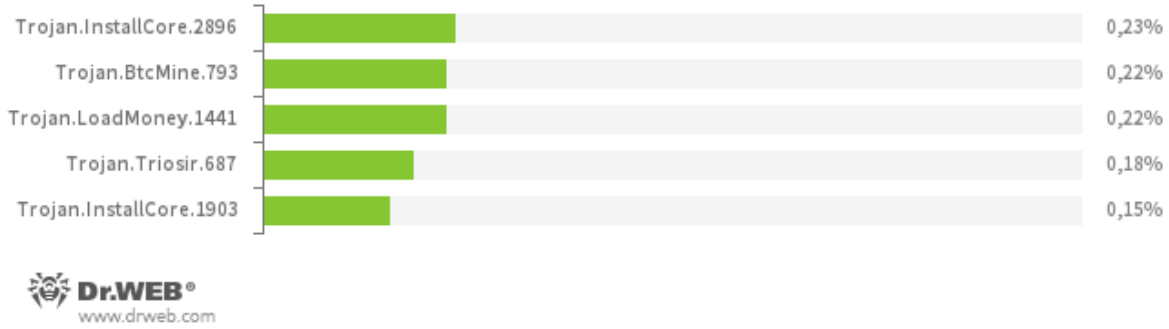


В левом нижнем углу этого окна имеется ссылка «Дополнительные параметры», по нажатии на которую Trojan.Ticno.1537 покажет список программ, которые он собирается установить. Среди них — браузер Amigo и приложение HomeSearch@Mail.ru разработки компании Mail.Ru, а также троянцы Trojan.ChromePatch.1, Trojan.Ticno.1548, Trojan.BPlug.1590, Trojan.Triosir.718, Trojan.Clickmein.1 и Adware.Plugin.1400. Подробнее об устройстве и принципах работы Trojan.Ticno.1537 рассказывается в опубликованной на нашем сайте обзорной статье.

Обзор вирусной активности в декабре 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

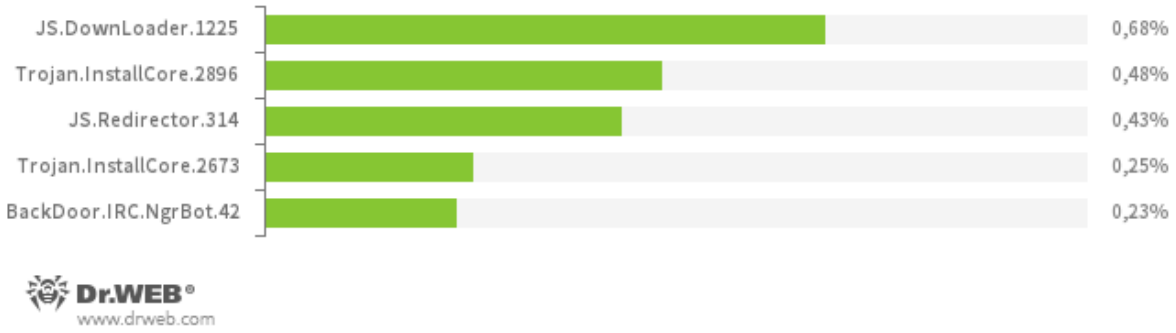


- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.BtcMine.793**
  Представитель семейства вредоносных программ, который втайне от пользователя применяет вычислительные ресурсы зараженного компьютера для добычи (майнинга) различных криптовалют – например, Bitcoin.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнёрской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Triosir.687**
  Представитель семейства троянцев, реализованных в виде плагина (надстройки) для браузеров. Предназначен для демонстрации назойливой рекламы при просмотре веб-страниц.

Обзор вирусной активности в декабре 2016 года

По данным серверов статистики «Доктор Веб»

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

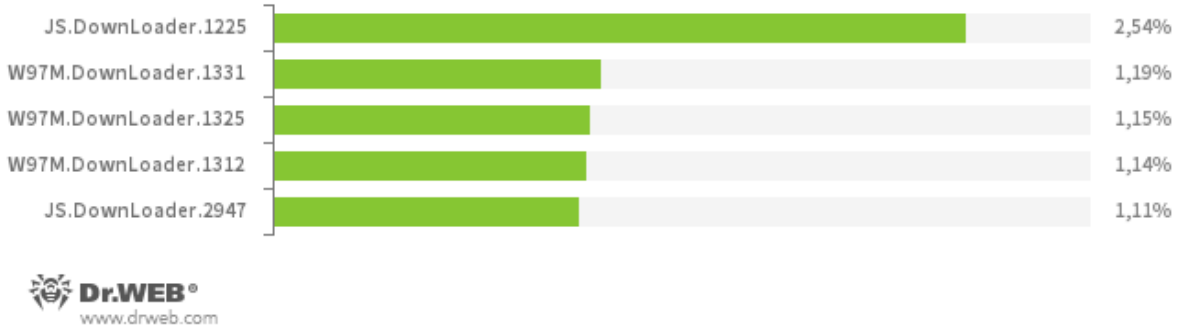


- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **JS.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Автоматически перенаправляют пользователей браузеров на другие веб-страницы.
- **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).

Обзор вирусной активности в декабре 2016 года

Статистика вредоносных программ в почтовом трафике

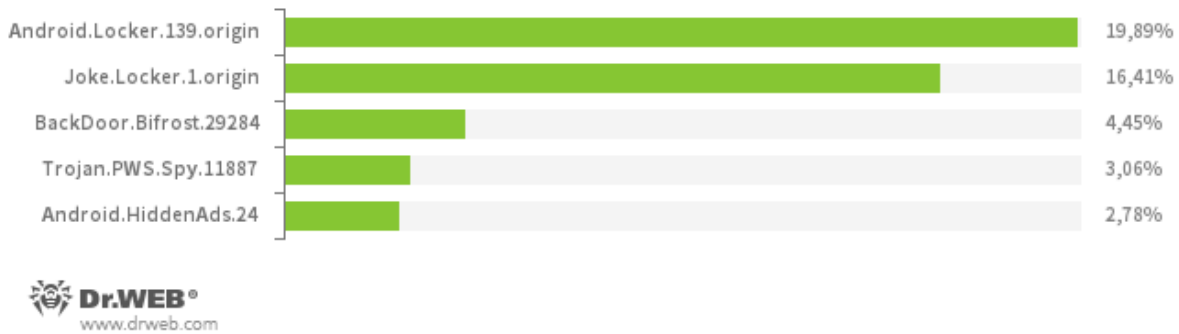
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в декабре 2016 года



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

По данным бота Dr.Web для Telegram

Вредоносные программы, обнаруженные ботом Dr.Web для Telegram декабре

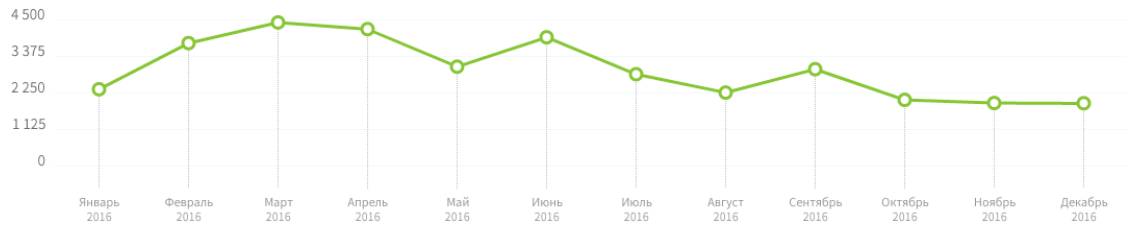


Обзор вирусной активности в декабре 2016 года

- **Android.Locker.139.origin**
  Представитель семейства Android-троянцев, предназначенных для вымогательства денег. Различные модификации этих вредоносных программ могут демонстрировать навязчивое сообщение якобы о нарушении закона и последовавшей в связи с этим блокировкой мобильного устройства, для снятия которой пользователям предлагается заплатить определенную сумму.
- **Joke.Locker.1.origin**
  Программа-шутка для ОС Android, блокирующая экран мобильного устройства и выводящая на него изображение «синего экрана смерти» ОС Windows (BSOD, Blue Screen of Death).
- **BackDoor.Bifrost.29284**
  Представитель семейства троянцев-бэкдоров, способен выполнять на зараженной машине поступающие от злоумышленников команды.
- **Trojan.PWS.Spy.11887**
  Представитель семейства троянцев для ОС Windows, способных похищать конфиденциальную информацию, в том числе пользовательские пароли.
- **Android.HiddenAds.24**
  Троянец, предназначенный для показа навязчивой рекламы.

Троянцы-шифровальщики

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



В декабре в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

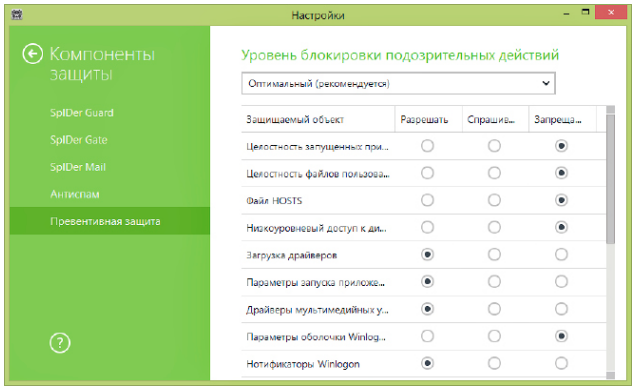
- **Trojan.Encoder.858** — 37,99% обращений;
- **Trojan.Encoder.761** — 12,27% обращений;
- **Trojan.Encoder.567** — 4,11% обращений;
- **Trojan.Encoder.3976** — 3,89% обращений;
- **Trojan.Encoder.3953** — 1,70% обращений.

Обзор вирусной активности в декабре 2016 года

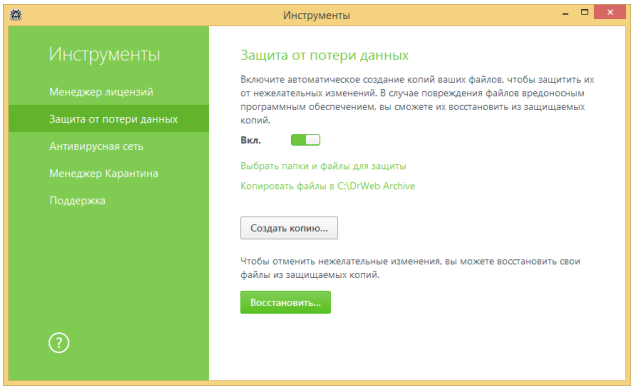
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Обзор вирусной активности в декабре 2016 года

Опасные сайты

В течение декабря 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 226 744 интернет-адреса.

Ноябрь 2016	Декабрь 2016	Динамика
+ 254 736	+ 226 744	-10,98%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В декабре вирусные аналитики компании «Доктор Веб» обнаружили троянца Android.Loki.16.origin, который заражал системные библиотеки Android-устройств, внедрялся в процессы приложений и незаметно загружал и устанавливал программы. Кроме того, были обнаружены троянцы Android.DownLoader.473.origin и Android.Sprovider.7, которых злоумышленники встроили в прошивку десятков моделей мобильных устройств. Эти вредоносные программы также скачивали и пытались установить различное ПО.

Наиболее заметные события, связанные с мобильной безопасностью в декабре:

- обнаружение Android-троянца, который заражает системные библиотеки и внедряется в процессы приложений;
- обнаружение троянцев, предустановленных на множестве мобильных Android-устройств.

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

Обзор вирусной активности в декабре 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