Dr.WEB®
с 1992 года

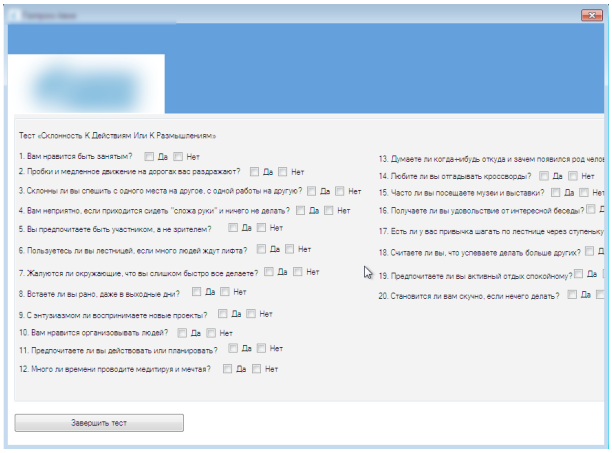
Обзор вирусной активности в июле 2016 года

Обзор вирусной активности в июле 2016 года

30 июля 2016 года

Июль оказался относительно спокойным с точки зрения распространения вирусов: в течение месяца были зафиксированы лишь единичные случаи появления новых вредоносных программ, которые так или иначе являются модификациями уже известных угроз. В конце июня — начале июля в вирусные базы была добавлена запись для очередного шифровальщика **Linux.Encoder.4**, который работает в операционных системах семейства Linux. Судя по информации, опубликованной в одном из зарубежных блогов, эта программа является результатом студенческой исследовательской работы и в «дикой природе» не встречается.

В конце месяца было зафиксировано распространение троянца-дроппера **Trojan.MulDrop6.48664**, устанавливающего на атакуемый компьютер уже известную вредоносную программу BackDoor.TeamViewer.49, о которой мы писали в одном из майских новостных материалов. На сей раз злоумышленники замаскировали дроппера под приложение-опросник, распространяющийся якобы от имени одной из известных российских авиакомпаний.



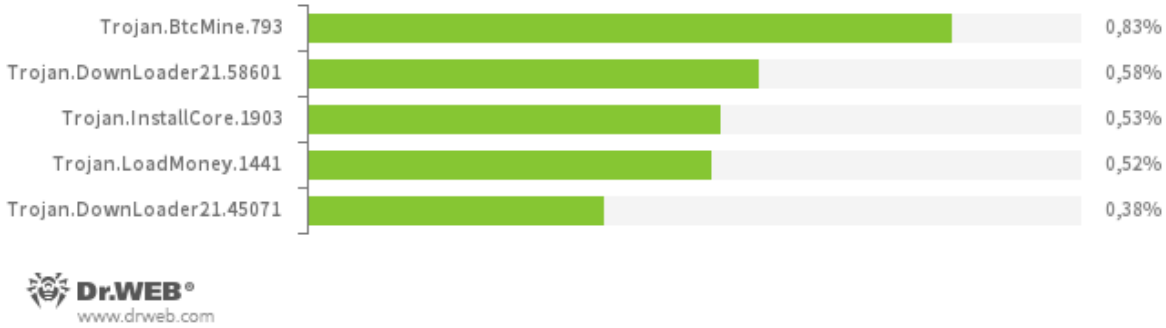
Главные тенденции июля

- Появление полиморфного банковского вируса Bolik
- Распространение троянца для приложения 1С
- Появление бестелесного рекламного троянца Trojan.Kovter
- Распространение опасного троянца-шпиона Trojan.PWS.Spy.19338

Обзор вирусной активности в июле 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

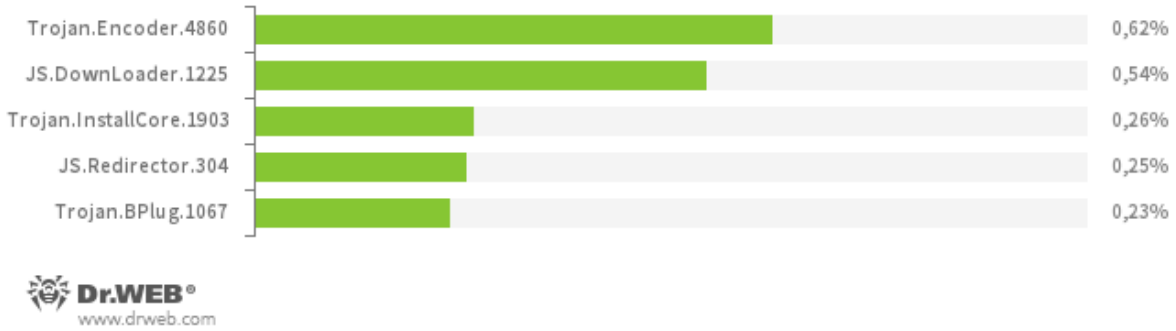


- **Trojan.BtcMine.793**
  Представитель семейства вредоносных программ, предназначенных для негласного использования вычислительных ресурсов зараженного компьютера с целью добычи (майнинга) различных криптовалют, например Bitcoin.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.InstallCore.1903**
  Представитель семейства установщиков нежелательных и вредоносных приложений.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнёрской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.

Обзор вирусной активности в июле 2016 года

По данным серверов статистики «Доктор Веб»

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

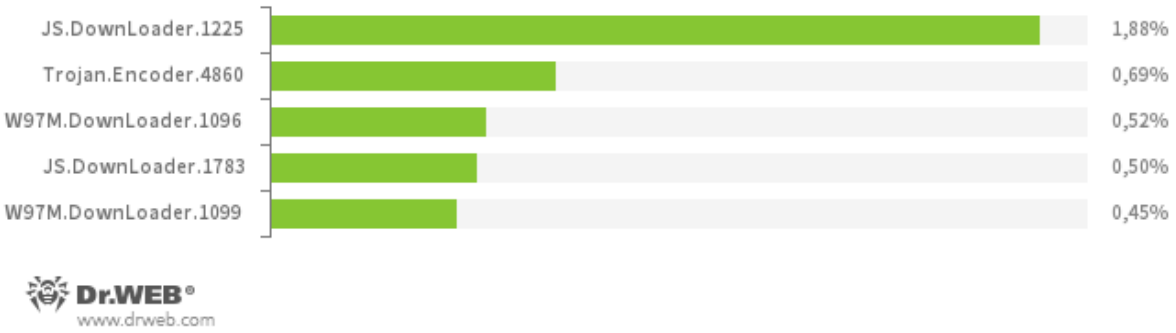


- **Trojan.Encoder.4860**
  Троянец-шифровальщик, также известный под именем JS.Crypt, полностью написанный на языке JScript. Троянец имеет самоназвание — «вирус RAA», а зашифрованные файлы получают расширение *.locked.
- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для загрузки и установки на компьютер других вредоносных программ.
- **Trojan.InstallCore.1903**
  Представитель семейства установщиков нежелательных и вредоносных приложений.
- **JS.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для автоматического перенаправления пользователей браузеров на другие веб-страницы.
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.

Обзор вирусной активности в июле 2016 года

Статистика вредоносных программ в почтовом трафике

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



- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для загрузки и установки на компьютер других вредоносных программ.
- **Trojan.Encoder.4860**
  Троянец-шифровальщик, также известный под именем JS.Crypt. Этот энкодер примечателен тем, что целиком написан на языке JScript. Троянец имеет самоназвание — «вирус RAA», а зашифрованные файлы получают расширение *.locked.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Обзор вирусной активности в июле 2016 года

Троянцы-шифровальщики

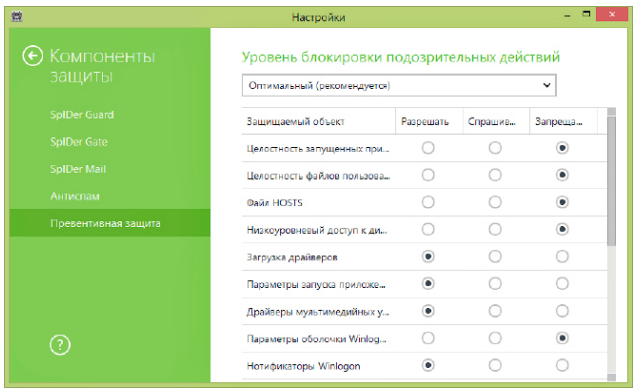
Количество запросов на расшифровку, поступивших в службу технической поддержки «Доктор Веб»

:

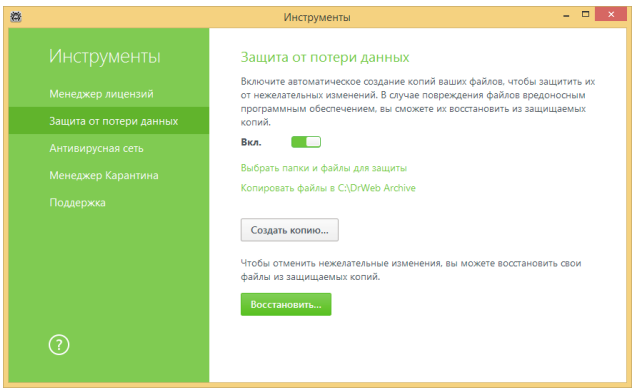
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

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 июля 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 1 716 920 интернет-адресов.

Июнь 2016	Июль 2016	Динамика
+ 1 716 920	+ 139 803	-91,8%

В настоящее время компания «Доктор Веб» осуществляет очистку баз Dr.Web SpIDer Gate и Родительского контроля от ссылок на более не работающие и прекратившие свое существование сайты, что позволит уменьшить объем загружаемых на компьютеры пользователей файлов. Именно с этим связан спад количества адресов, добавленных в июле в базы нерекомендуемых и вредоносных сайтов.

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для мобильных устройств

В июле вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play более 150 приложений, в которые был встроен рекламный троянец Android.Spy.305.origin. Он способен показывать баннеры поверх интерфейса программ и операционной системы, выводить рекламные сообщения в панель уведомлений, а также красть конфиденциальную информацию. Кроме того, в прошедшем месяце была обнаружена троянская программа Android.Spy.178.origin, которую злоумышленники встроили в модифицированную версию популярной игры Pokemon Go. Это вредоносное приложение предназначено для сбора и передачи злоумышленникам конфиденциальной информации.

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

- Обнаружение в каталоге Google Play троянца, предназначенного для показа навязчивой рекламы, а также кражи конфиденциальной информации;
- Обнаружение троянца-шпиона, которого злоумышленники встроили в модифицированную версию игры Pokemon Go.

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

Обзор вирусной активности в июле 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