Dr.WEB®
с 1992 года

Обзор вирусной активности в сентябре 2016 года

Обзор вирусной активности в сентябре 2016 года

30 сентября 2016 года

В сентябре 2016 года специалисты компании «Доктор Веб» выявили и исследовали несколько вредоносных программ для операционных систем семейства Linux. В начале месяца был изучен троянец, написанный на языке Rust, а вскоре вирусные аналитики обнаружили еще одного троянца для Linux, предназначенного для проведения DDoS-атак. Кроме того, в конце сентября было изучено целое семейство DDoS-троянцев, способных работать в различных версиях Linux. Также вирусные аналитики «Доктор Веб» выявили новую вредоносную программу для мобильной платформы Android. Этот троянец способен встраиваться в системные процессы.

Главные тенденции сентября

- Появление написанного на Rust троянца для Linux
- Распространение новых Linux-троянцев для проведения DDoS-атак
- Появление способного встраиваться в системные процессы троянца для Android

Обзор вирусной активности в сентябре 2016 года

Угроза месяца

Троянцы, предназначенные для проведения атак на отказ в обслуживании, то есть DDoS-атак (англ. Distributed Denial of Service) — не редкость. Некоторые из них могут заражать компьютеры, работающие под управлением не только Microsoft Windows, но и Linux. Одной из таких вредоносных программ является Linux.Mirai.

Первую версию троянца Linux.Mirai вирусные аналитики «Доктор Веб» исследовали еще мае 2016 года. Эта вредоносная программа была добавлена в вирусные базы Dr.Web под именем Linux.DDoS.87. Троянец работает на устройствах с архитектурой x86, ARM, MIPS, SPARC, SH-4 и M68K и имеет сходство с вредоносными программами семейства Linux.BackDoor.Fgt, об одном из представителей которого мы уже писали в 2014 году. Linux.DDoS.87 ищет на зараженном устройстве и прекращает работу других вредоносных программ. По команде злоумышленников он может осуществлять следующие виды атак:

- UDP flood;
- UDP flood over GRE;
- DNS flood;
- TCP flood (несколько разновидностей);
- HTTP flood.

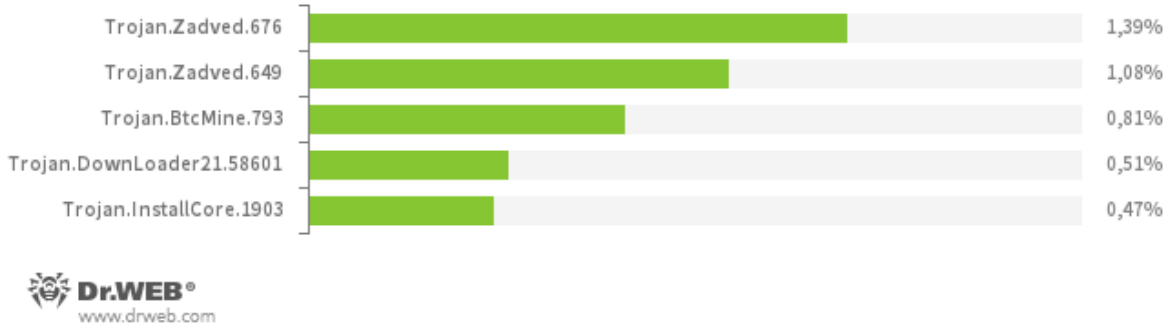
В начале августа 2016 года было зафиксировано распространение следующей модификации этой вредоносной программы, которая получила наименование Linux.DDoS.89. Этот троянец имеет множество общих черт со своим предшественником, однако прослеживаются и характерные отличия от Linux.DDoS.87. Например, в обновленной версии изменился порядок действий при запуске троянца, механизм защиты от самоудаления, а также из списка поддерживаемых типов атак исчез HTTP flood. Кроме того, в Linux.DDoS.89 появился новый компонент — telnet-сканнер, предназначенный для поиска в сети уязвимых устройств и несанкционированного подключения к ним по протоколу telnet.

Наконец, совсем недавно был обнаружен еще один представитель этого семейства троянцев, получивший наименование Linux.Mirai. Троянец научился отключать предотвращающий зависание операционной системы сторожевой таймер watchdog (чтобы исключить перезагрузку устройства), а в перечень выполняемых типов атак вернулся HTTP flood. Подробную информацию об этом семействе вредоносных программ можно получить, ознакомившись с опубликованной на сайте компании «Доктор Веб» обзорной статьей.

Обзор вирусной активности в сентябре 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

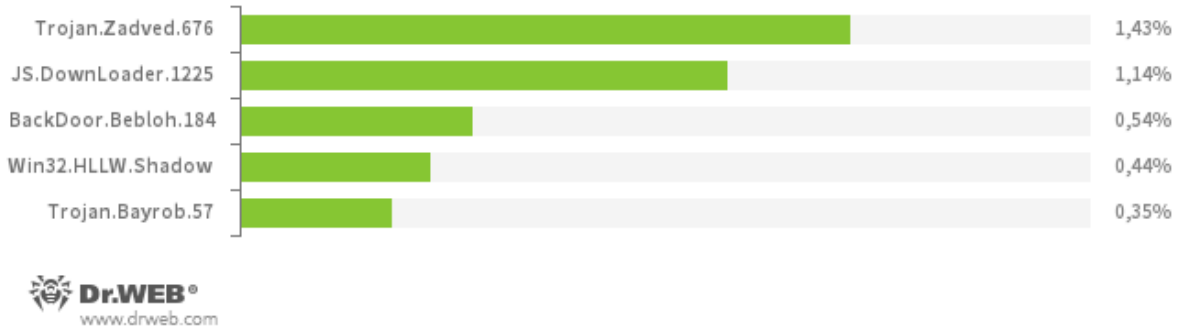


- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **Trojan.BtcMine.793**
  Представитель семейства вредоносных программ, который втайне от пользователя использует вычислительные ресурсы зараженного компьютера для 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.

Обзор вирусной активности в сентябре 2016 года

По данным серверов статистики «Доктор Веб»

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

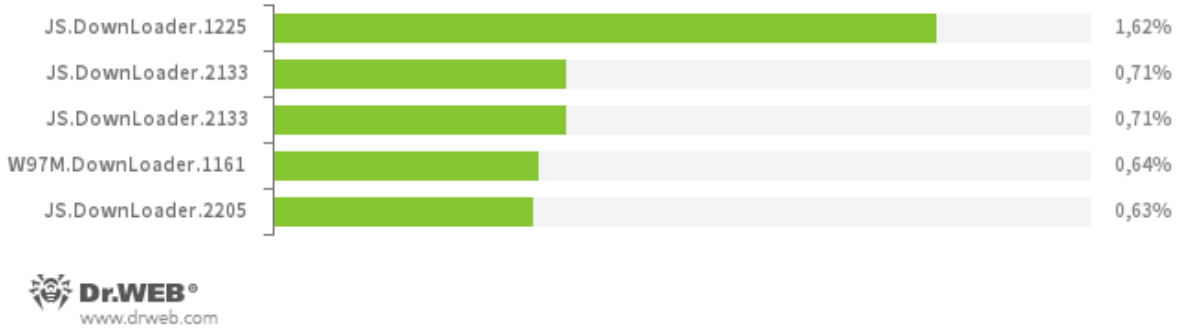


- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **BackDoor.Bebloh.184**
  Один из представителей троянцев-бэкдоров, способных встраиваться в процессы других приложений и выполнять поступающие от злоумышленников команды.
- **Win32.HLLW.Shadow**
  Червь, использующий для своего распространения съемные носители и сетевые диски. Кроме того, может распространяться по сети с использованием стандартного протокола SMB. Способен загружать с управляющего сервера и запускать исполняемые файлы.
- **Trojan.Bayrob.57**
  Троянец, способный похищать конфиденциальную информацию и выполнять на инфицированном компьютере другие нежелательные для пользователя действия.

Обзор вирусной активности в сентябре 2016 года

Статистика вредоносных программ в почтовом трафике

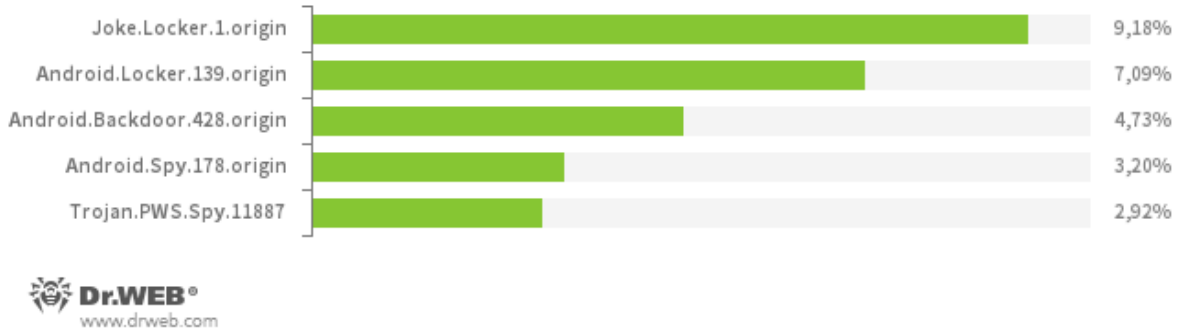
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в сентябре 2016 года



- **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 в сентябре

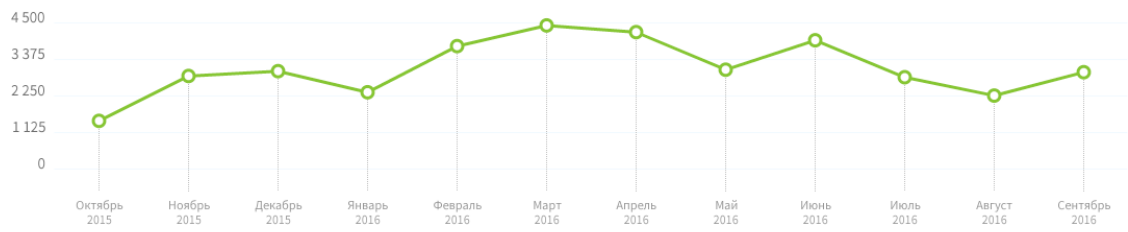


Обзор вирусной активности в сентябре 2016 года

- **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).
- **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.
- **Android.Backdoor.428.origin**
  Представитель семейства Android-троянцев, предназначенных для выполнения поступающих от злоумышленников команд. В зависимости от функционала конкретных модификаций вредоносных приложений среди выполняемых ими действий могут быть отправка СМС-сообщений, открытие определенных URL в браузере, сбор информации об устройстве, включая сведения из телефонной книги, загрузка других программ и т. п.
- **Android.Spy**
  Семейство многофункциональных троянцев, заражающих мобильные устройства под управлением ОС Android. Могут читать и записывать контакты, принимать и отправлять СМС-сообщения, определять GPS-координаты, читать и записывать закладки браузера, получать сведения об IMEI мобильного устройства и номере мобильного телефона.
- **Trojan.PWS.Spy.11887**
  Представитель семейства троянцев для ОС Windows, способных похищать конфиденциальную информацию, в том числе пароли пользователя.

Троянцы-шифровальщики

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



Обзор вирусной активности в сентябре 2016 года

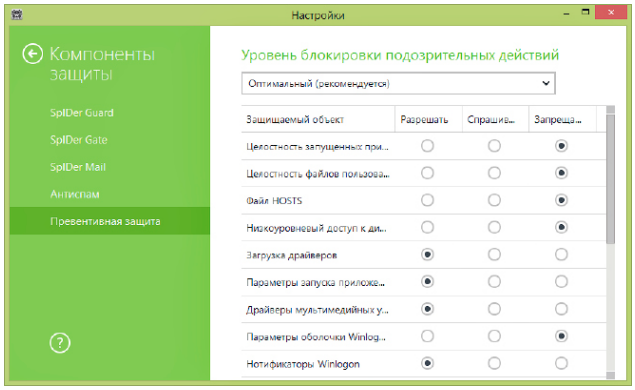
В сентябре в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- **Trojan.Encoder.717** — 25,64% обращений;
- **Trojan.Encoder.602** — 21,53% обращений;
- **Trojan.Encoder.143** — 5,11% обращений;
- **Trojan.Encoder.126** — 4,51% обращений;
- **Trojan.Encoder.119** — 4,26% обращений.

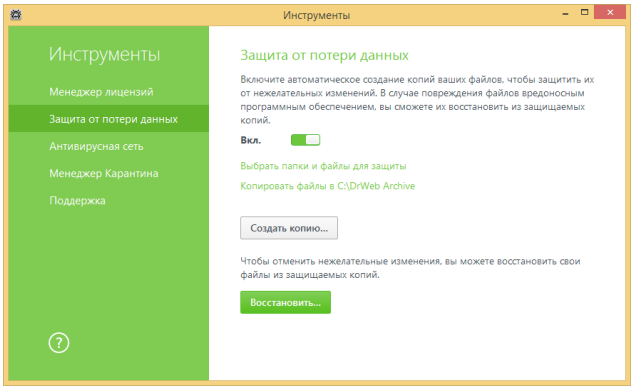
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

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 сентября 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 298 985 интернет-адресов.

Август 2016	Сентябрь 2016	Динамика
+ 245 394	+ 298 985	+21,8%

Нерекомендуемые сайты

Вредоносные программы для Linux

В первой половине сентября вирусные аналитики «Доктор Веб» исследовали вредоносную программу для ОС семейства Linux, получившую название Linux.BackDoor.Irc.16. Особенность этого троянца заключается в том, что он написан на языке Rust, — раньше аналитики не встречали троянцев, созданных с использованием этой технологии. Linux.BackDoor.Irc.16 выполняет поступающие от злоумышленников команды. Для их получения троянец использует протокол обмена текстовыми сообщениями IRC (Internet Relay Chat). Подробнее об этом трояне рассказано в специально подготовленной компанией «Доктор Веб» обзорной статье.

Вскоре было зафиксировано распространение еще одного Linux-троянца: Linux.DDoS.93. Эта вредоносная программа в полном соответствии со своим названием предназначена для осуществления DDoS-атак и может выполнять следующие команды злоумышленников:

- обновить вредоносную программу;
- скачать и запустить указанный в команде файл;
- самоудалиться;
- начать атаку методом UDP flood на указанный порт;
- начать атаку методом UDP flood на случайный порт;
- начать атаку методом Spoofed UDP flood;
- начать атаку методом TCP flood;

- начать атаку методом TCP flood (в пакеты записываются случайные данные длиной 4096 байт);
- начать атаку методом HTTP flood с использованием GET-запросов;
- начать атаку методом HTTP flood с использованием POST-запросов;
- начать атаку методом HTTP flood с использованием HEAD-запросов;
- отправить на 255 случайных IP-адресов HTTP-запросы с указанными параметрами;
- завершить выполнение;
- отправить команду “ping”.

Подробнее о Linux.DDoS.93 рассказано в опубликованном нами обзорном материале.

Вредоносное и нежелательное ПО для мобильных устройств

В сентябре вирусные аналитики компании «Доктор Веб» обнаружили новые версии распространенных троянцев Android.Xiny, предназначенных для незаметной загрузки и установки разнообразного ПО без согласия пользователей. Выявленные троянцы научились внедряться в процессы системных приложений и могут запускать дополнительные программные модули.

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

- обнаружение новых представителей троянцев семейства Android.Xiny, которые могут встраиваться в процессы системных приложений и запускать вредоносные плагины.

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

Обзор вирусной активности в сентябре 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