Dr.WEB®
с 1992 года

Обзор вирусной активности в январе 2016 года

Обзор вирусной активности в январе 2016 года

29 января 2016 года

Первый месяц 2016 года ознаменовался появлением значительного количества новых вредоносных программ для ОС Linux, в том числе очередной версии троянца-энкодера, а также опасного бэкдора, способного создавать на инфицированном устройстве снимки экрана, фиксировать нажатия клавиш и выполнять поступающие от злоумышленников команды. Кроме того, в январе был обнаружен Android-троянец, распространяющийся в прошивке смартфона одного из известных производителей, а в конце месяца аналитики компании «Доктор Веб» выявили множество вредоносных приложений в официальном каталоге Google Play.

Главные тенденции января

- Появление новых вредоносных программ для Linux
- Появление нового троянца-шифровальщика для Linux
- Распространение опасного троянца в прошивке Android

Обзор вирусной активности в январе 2016 года

Угроза месяца

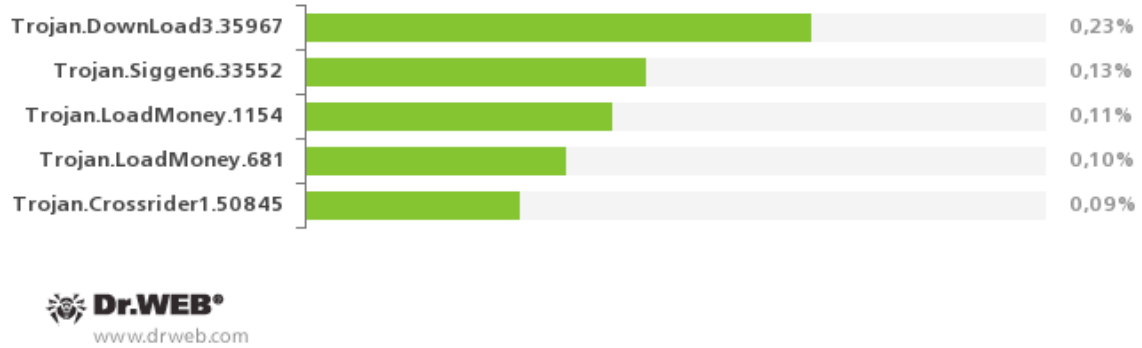
В конце января специалисты компании «Доктор Веб» исследовали многофункционального троянца-бэкдора, способного заражать устройства под управлением ОС Linux. Эта вредоносная программа состоит из двух компонентов: дроппера и полезной нагрузки, которая и выполняет в инфицированной системе основные шпионские функции. В момент своего запуска дроппер демонстрирует на экране атакуемого устройства диалоговое окно:

Если программе удалось стартовать на целевом компьютере, она извлекает из своего тела основной вредоносный компонент — бэкдор — и сохраняет его в одной из папок на жестком диске. Этот модуль способен выполнять более 40 различных команд. В частности, он умеет сохранять нажатия пользователем клавиш (кейлоггинг), загружать и запускать различные приложения, передавать злоумышленникам имена файлов в заданной директории. Также он обладает возможностью загружать на управляющий сервер выбранные файлы, создавать, удалять, переименовывать файлы и папки, создавать снимки экрана (скриншоты), выполнять команды bash, и многое другое. Подробная информация об этом опасном троянце приведена в опубликованной на сайте компании «Доктор Веб» статье.

Обзор вирусной активности в январе 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

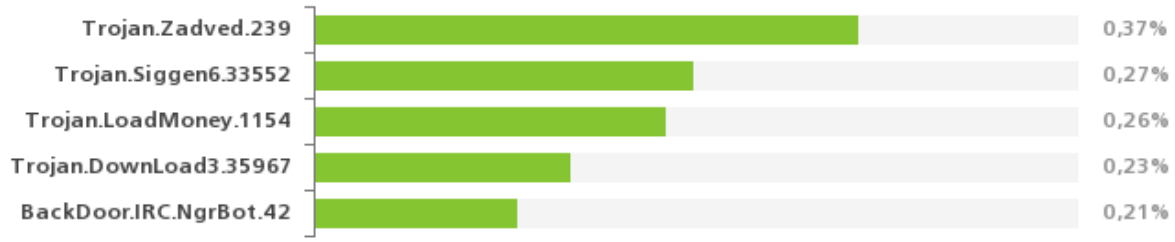


- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Crossrider1.50845**
  Представитель семейства троянцев, предназначенных для демонстрации различной сомнительной рекламы.

Обзор вирусной активности в январе 2016 года

По данным серверов статистики «Доктор Веб»

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

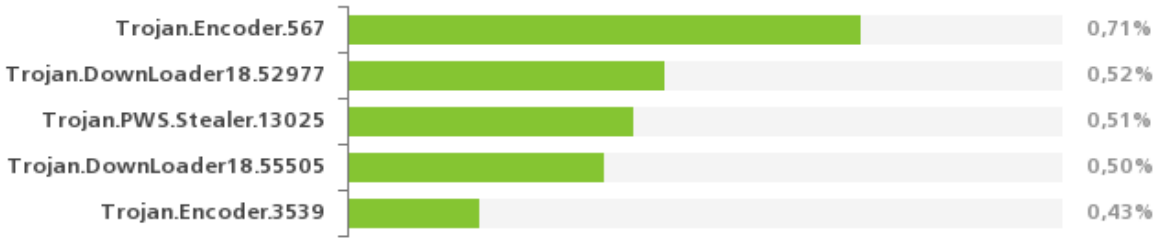


Dr.WEB®
www.drweb.com

- **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.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской 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.
- **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).

Статистика вредоносных программ в почтовом трафике

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



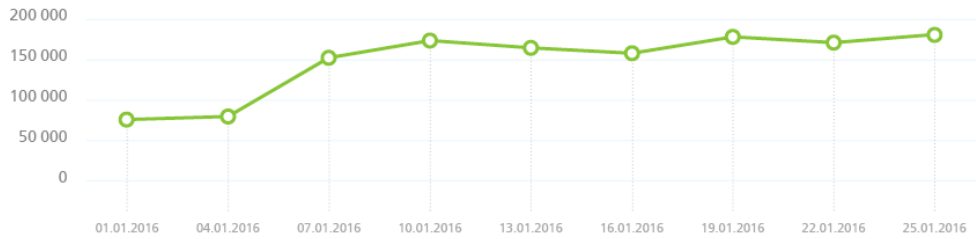
Dr.WEB®
www.drweb.com

- **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.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **Trojan.Encoder.3539**
  Представитель семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку.

Ботнеты

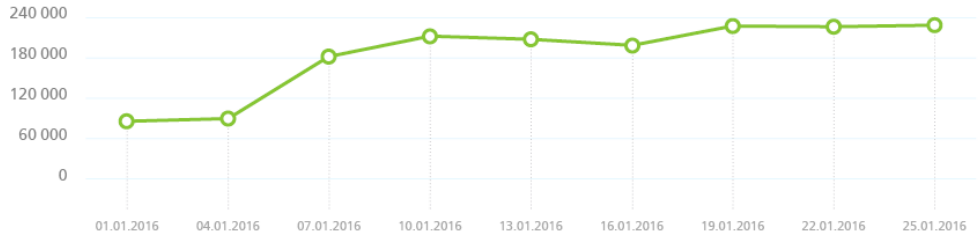
Вирусные аналитики компании «Доктор Веб» продолжают отслеживать активность ботнетов, созданных злоумышленниками с использованием файлового вируса Win32.Rmnet.12.

Активность ботнета Win32.Rmnet.12 в январе 2016 года (1 подсеть)



Dr.WEB®
www.drweb.com

Активность ботнета Win32.Rmnet.12 в январе 2016 года (2 подсеть)



Dr.WEB®
www.drweb.com

Rmnet — это семейство файловых вирусов, распространяющихся без участия пользователя, способных встраивать в просматриваемые пользователям веб-страницы постороннее содержимое (это теоретически позволяет киберпреступникам получать доступ к банковской информации жертвы), а также красть файлы cookies и пароли от наиболее популярных FTP-клиентов и выполнять различные команды, поступающие от злоумышленников.

Обзор вирусной активности в январе 2016 года

Также проявляет активность бот-сеть, состоящая из инфицированных файловым вирусом Win32.Sector. компьютеров. Эта вредоносная программа обладает следующими функциями:

- загрузка из P2P-сети и запуск на зараженной машине различных исполняемых файлов;
- встраивание в запущенные на инфицированном компьютере процессы;
- возможность останавливать работу некоторых антивирусных программ и блокировать доступ к сайтам их разработчиков;
- инфицирование файловых объектов на локальных дисках и сменных носителях (где в процессе заражения создает файл автозапуска autorun.inf), а также файлов, хранящиеся в общедоступных сетевых папках.

График среднесуточной активности этого ботнета в январе 2016 года показан на следующей иллюстрации:

Активность ботнета Win32.Sector в январе 2016 года

Обзор вирусной активности в январе 2016 года

Трояны-шифровальщики

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

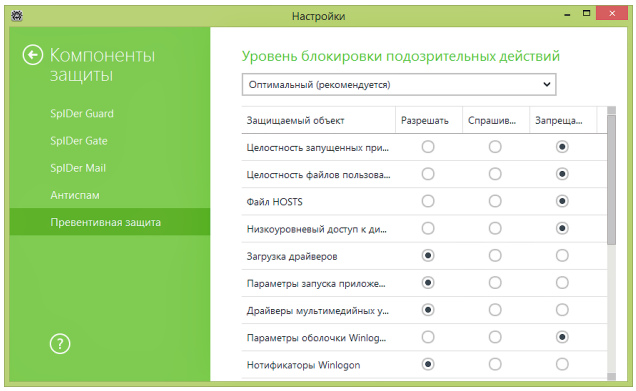
Наиболее распространенные шифровальщики в январе 2016 года:

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

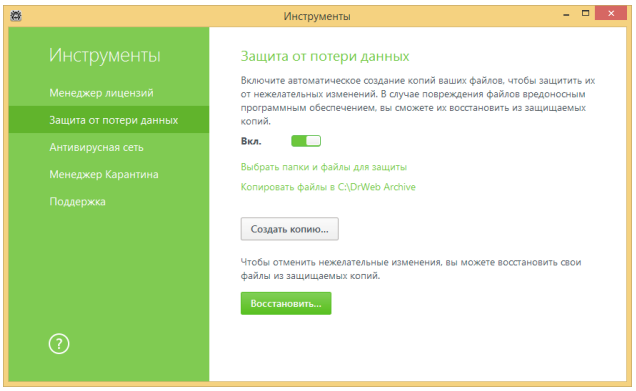
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Вредоносные программы для Linux

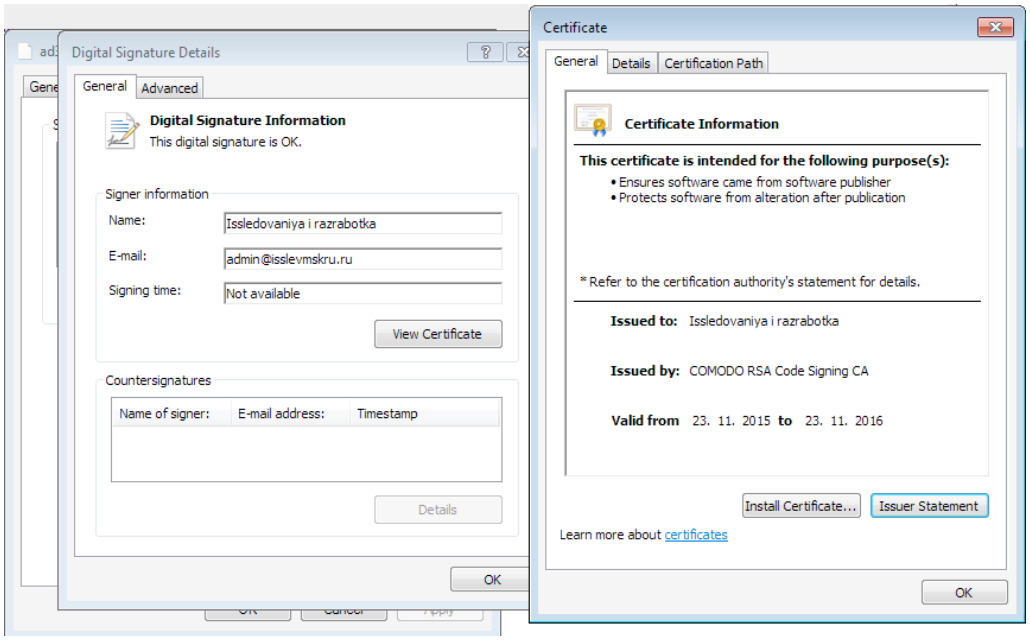
Январь 2016 года стал месяцем вредоносных программ для Linux — количество троянцев для этой операционной системы, выявленных в начале года, можно назвать рекордным. Вскоре после завершения новогодних каникул специалисты компании «Доктор Веб» исследовали новую версию троянца-шифровальщика для ОС Linux, получившего наименование Linux.Encoder.3. В этой модификации вредоносной программы злоумышленники исправили все ошибки и недочеты, характерные для предыдущих реализаций Linux-шифровальщиков, однако несмотря на это ряд архитектурных особенностей Linux.Encoder.3 позволяет расшифровывать поврежденные в результате действий троянца файлы.

Linux.Encoder.3 не требует для своей работы привилегий суперпользователя Linux — троянец запускается с правами веб-сервера, которых ему вполне достаточно для того, чтобы зашифровать все файлы в домашней директории сайта. Существенным отличием от предыдущих версий шифровальщика является то обстоятельство, что Linux.Encoder.3 способен запоминать дату создания и изменения исходного файла и подменять ее для измененных им файлов значениями, которые были установлены до шифрования. Также вирусописатели пересмотрели алгоритм шифрования: каждый экземпляр вредоносной программы использует собственный уникальный ключ, создаваемый на основе характеристик шифруемых файлов и значений, сгенерированных случайным образом. Более подробную информацию об этой вредоносной программе можно получить, ознакомившись с опубликованной на сайте компании «Доктор Веб» статьей.

Вскоре после этого вирусные аналитики компании «Доктор Веб» обнаружили троянца Linux.Ekoms.1, общие сведения о котором были опубликованы в соответствующем новостном материале. Этот троянец с периодичностью в 30 секунд делает на зараженном компьютере снимок экрана (скриншот) и сохраняет его во временную папку в формате JPEG. Содержимое временной папки загружается на управляющий сервер по таймеру с определенными временными интервалами. Кроме того, Linux.Ekoms.1 обладает возможностью загружать на сервер злоумышленников файлы с инфицированного устройства, а также умеет скачивать с управляющего сервера другие файлы и сохранять их на диске компьютера.

Следует отметить, что в январе специалистами компании «Доктор Веб» была обнаружена и Windows-совместимая версия Linux.Ekoms.1, получившая наименование Trojan.Ekoms.1. При запуске этот троянец выполняет поиск ряда исполняемых файлов в папке %appdata% с целью предотвратить повторное заражение системы, и, если не обнаруживает их, сохраняет свою копию в этой папке под именем одного из таких файлов. Помимо снимков экрана, Trojan.Ekoms.1 сохраняет данные о нажатиях пользователем клавиш в файле с расширением .kkt, а также списки файлов в папках, которые

записываются в файл с расширением .ddt, и передает эти файлы на сервер злоумышленников. Примечательно, что в Linux.Ekoms.1 встречались упоминания этих файлов, но в Linux-редакции троянца отсутствовал код, отвечающий за их обработку.
Как и в структуре троянца для Linux, в Trojan.Ekoms.1 присутствует специальный механизм, позволяющий записывать звук и сохранять полученную запись в формате WAV, но здесь он тоже никак не используется. Троянец имеет действующую цифровую подпись некой компании «Issledovaniya i razrabotka», а корневой сертификат был выдан компанией Comodo.



Рассказывая о вредоносных программах для ОС Linux, нельзя не упомянуть о том, что в конце января несколько популярных сетевых изданий и блогов опубликовали информацию о распространении якобы принципиально нового Linux-червя под названием «TheMoon». Это опасное приложение детектируется Антивирусом Dr.Web для Linux под именем Linux.DownLoader.69 еще с 14 декабря 2015 года. Ознакомиться с подробным техническим описанием этой вредоносной программы можно в опубликованном компанией «Доктор Веб» материале.

Обзор вирусной активности в январе 2016 года

Опасные сайты

В течение января 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 625 588 интернет-адресов.

Декабрь 2015	Январь 2016	Динамика
+ 210 987	+ 625 588	+ 196%

Узнайте больше о нерекомендуемых Dr.Web сайтах

Вредоносное и нежелательное ПО для мобильных устройств

Минувший январь показал, что интерес злоумышленников к мобильной платформе Google Android по-прежнему высок. Так, в середине месяца вирусные аналитики компании «Доктор Веб» обнаружили в прошивке смартфона Philips s307 опасного троянца Android.Cooee.1, предназначенного для незаметной загрузки и установки всевозможных приложений. А уже в конце января специалисты «Доктор Веб» выявили в каталоге Google Play более 60 игр, содержащих троянца Android.Xiny.19.origin, – эта вредоносная программа способна незаметно запускать полученные от вирусописателей apk-файлы, загружать и предлагать пользователям установить всевозможное ПО, а также показывать навязчивую рекламу.

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

- выявление в каталоге Google Play большого количества игр, в которые был внедрен троянец;
- обнаружение троянца в Android-прошивке смартфона Philips s307.

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

Обзор вирусной активности в январе 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