Dr.WEB®
с 1992 года

Обзор вирусной активности в январе 2017 года

Обзор вирусной активности в январе 2017 года

31 января 2017 года

В первом месяце наступившего 2017 года специалисты компании «Доктор Веб» обнаружили червя, заражающего архивы и удаляющего другие вредоносные программы. Также вирусные аналитики выявили несколько тысяч Linux-устройств, зараженных новым троянцем. Кроме того, в январе в вирусные базы Dr.Web был добавлен целый ряд опасных вредоносных программ для мобильной платформы Google Android. Один из этих троянцев внедрял в приложение Play Маркет модуль, скачивавший различные приложения из каталога Google Play. Другой относится к категории банковских троянцев — злоумышленники опубликовали в свободном доступе его исходный код, в связи с чем аналитики «Доктор Веб» прогнозируют в ближайшем будущем широкое распространение созданных на его основе банкеров.

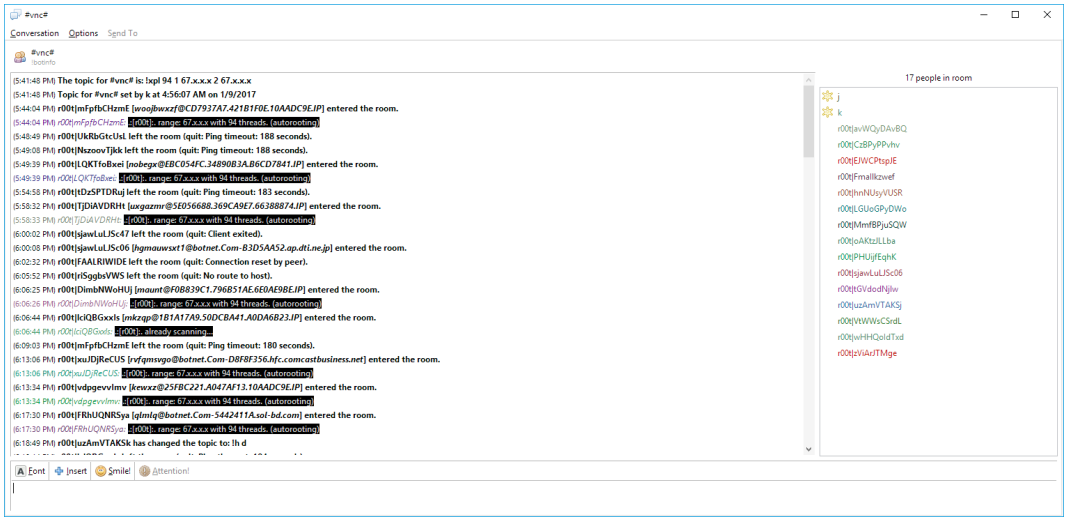
Главные тенденции января

- Распространение червя, способного заражать архивы и удалять другое вредоносное ПО
- Обнаружение нескольких тысяч зараженных Linux-устройств
- Появление Android-троянца, встраивающего свой модуль в программу Play Маркет
- Распространение банковского троянца для Android, попавшего в открытый доступ

Обзор вирусной активности в январе 2017 года

Угроза месяца

Червями обычно называют разновидность троянских программ, способных распространяться самостоятельно, без участия пользователя, но не умеющих заражать исполняемые файлы. В январе аналитики «Доктор Веб» обнаружили нового червя – BackDoor.Ragebot.45. Он получает команды с помощью протокола обмена текстовыми сообщениями IRC (Internet Relay Chat), а заразив компьютер, запускает на нем FTP-сервер. С его помощью троянец скачивает на атакуемый ПК свою копию.



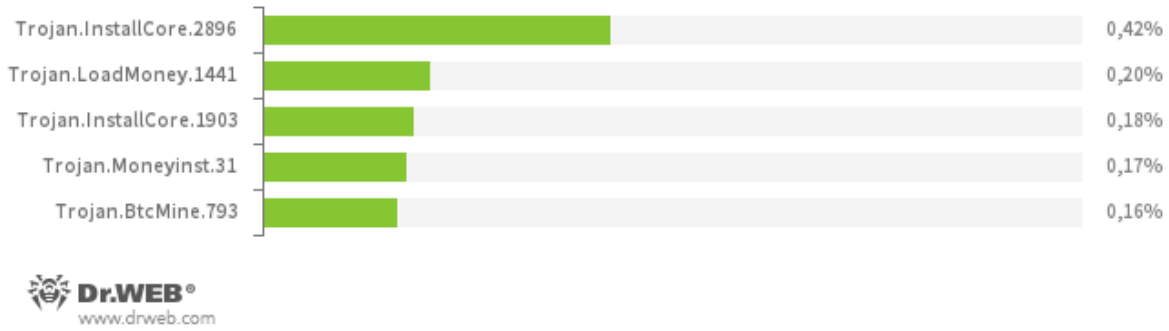
Червь подключается к другим компьютерам в сети при помощи системы удаленного доступа к рабочему столу Virtual Network Computing (VNC), перебирая пароли по словарю. Если взлом удался, он устанавливает с удаленным компьютером VNC-соединение. Затем троянец отправляет сигналы нажатия клавиш, с помощью которых запускает интерпретатор команд CMD и выполняет в нем код для загрузки по протоколу FTP собственной копии. Так червь распространяется автоматически.

Кроме того, BackDoor.Ragebot.45 умеет искать и заражать RAR-архивы на съемных носителях и копировать себя в папки целого ряда программ. Но основная его особенность заключается в том, что эта вредоносная программа по команде злоумышленников ищет в системе других троянцев, при обнаружении которых завершает их процессы и удаляет исполняемые файлы. Более подробно об этом троянце и принципах его работы рассказано в опубликованной нами обзорной статье.

Обзор вирусной активности в январе 2017 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

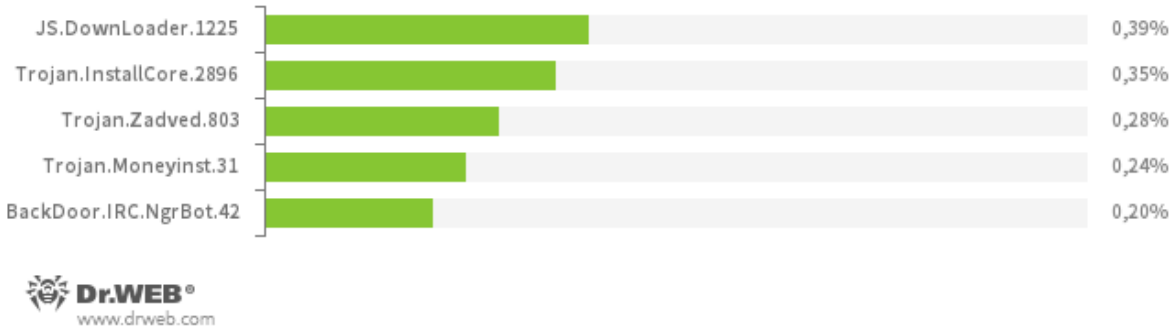


- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Moneyinst.31**
  Вредоносная программа, устанавливающая на компьютер жертвы различное ПО, в том числе других троянцев.
- **Trojan.BtcMine.793**
  Представитель семейства вредоносных программ, который втайне от пользователя применяет вычислительные ресурсы зараженного компьютера для добычи (майнинга) различных криптовалют – например, Bitcoin.

Обзор вирусной активности в январе 2017 года

По данным серверов статистики «Доктор Веб»

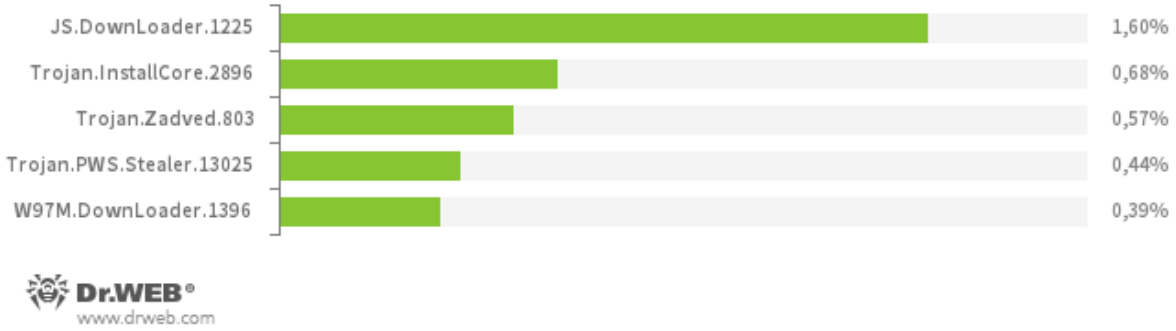
Наиболее распространенные вредоносные программы в январе 2017 года
согласно данным серверов статистики Dr.Web



- **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).

Статистика вредоносных программ в почтовом трафике

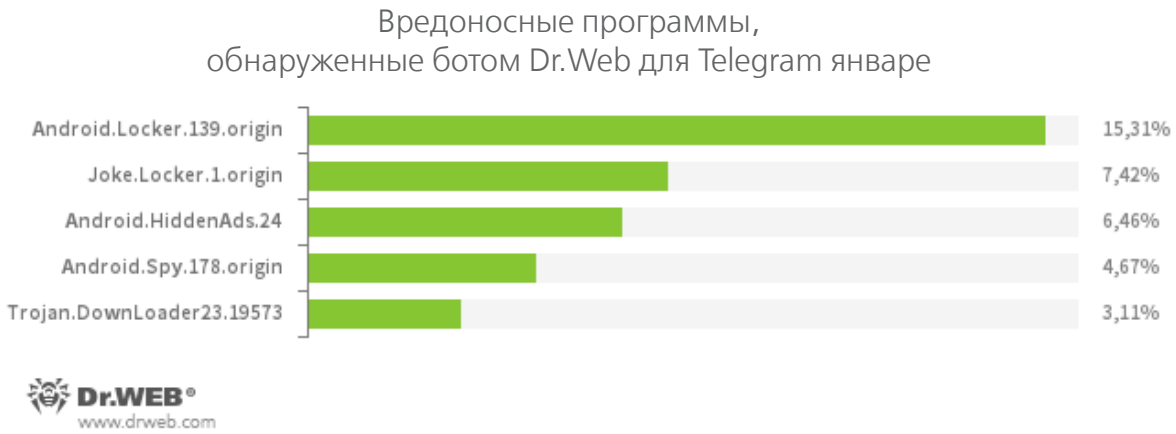
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в январе 2017 года



- **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.
- **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.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Обзор вирусной активности в январе 2017 года

По данным бота Dr.Web для Telegram

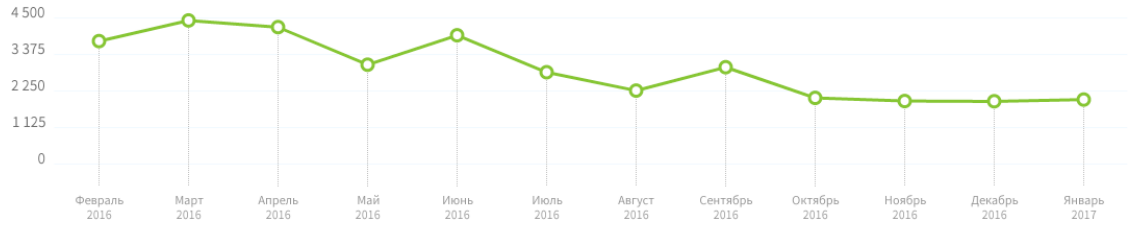


- **Android.Locker.139.origin**
  Представитель семейства Android-троянцев, предназначенных для вымогательства денег. Различные модификации этих вредоносных программ могут демонстрировать навязчивое сообщение якобы о нарушении закона и о последовавшей в связи с этим блокировке мобильного устройства, 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).
- **Android.HiddenAds.24**
  Троянец, предназначенный для показа навязчивой рекламы.
- **Android.Spy.178.origin**
  Представитель семейства троянцев для ОС Windows, способных похищать конфиденциальную информацию, в том числе пользовательские пароли.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Обзор вирусной активности в январе 2017 года

Трояны-шифровальщики

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



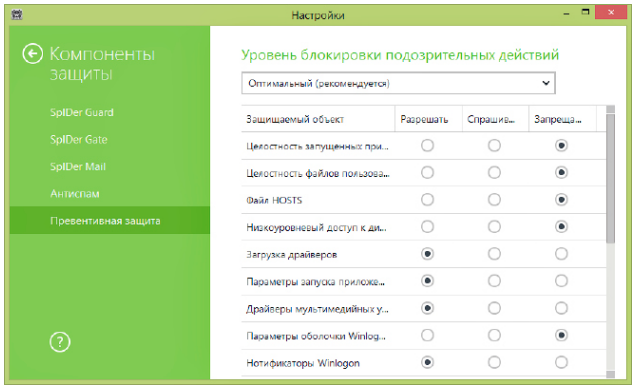
В январе в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- **Trojan.Encoder.858** — 36.71% обращений;
- **Trojan.Encoder.3953** — 5.00% обращений;
- **Trojan.Encoder.567** — 3.97% обращений;
- **Trojan.Encoder.761** — 3.33% обращений;
- **Trojan.Encoder.3976** — 2.88% обращений.

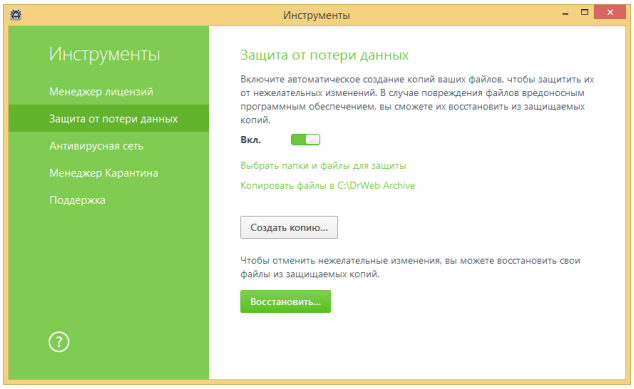
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

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 января 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 223 127 интернет-адресов.

Декабрь 2016	Январь 2017	Динамика
+ 226 744	+ 223 127	-1.59%

Нерекомендуемые сайты

Вредоносные программы для Linux

Массовое распространение вредоносных программ для операционных систем семейства Linux — не слишком частое явление, но вместе с тем оно было зафиксировано специалистами «Доктор Веб» в январе 2017 года. Речь идет о троянце Linux.Proxy.10, предназначенном для запуска на инфицированном устройстве SOCKS5-прокси сервера. Такие скомпрометированные устройства используются злоумышленниками для обеспечения собственной анонимности в Интернете. По информации, имеющейся в распоряжении специалистов «Доктор Веб», на 24 января 2017 года число зараженных Linux-девайсов составило несколько тысяч.

Распространяется Linux.Proxy.10, авторизуясь на уязвимых узлах с заданным сочетанием логина и пароля: пользователей с такими учетными данными обычно создают в системе другие Linux-троянцы (либо они установлены на устройстве по умолчанию). Это означает, что Linux.Proxy.10 атакует в основном устройства, уже зараженные другим вредоносным ПО. Более подробная информация об этой вредоносной программе изложена в опубликованной нами статье.

Также в январе был обнаружен новый представитель семейства вредоносных программ Linux.Lady — Linux.Lady.4. В этой версии троянца вирусописатели удалили функцию скачивания и запуска утилиты для добычи (майнинга) криптовалют, а также добавили возможность осуществления атак на сетевые хранилища данных Redis. Кроме того, в троянце появился дополнительный модуль, способный общаться с удаленными серверами с использованием технологии RPC (Remote Procedure Call), отправлять на них информацию об инфицированной системе и выполнять shell-команды.

Вредоносное и нежелательное ПО для мобильных устройств

В первом месяце 2017 года специалисты компании «Доктор Веб» обнаружили троянца Android.Skyfin.1.origin, который внедрялся в активный процесс приложения Play Маркет и незаметно загружал приложения из каталога Google Play, искусственно увеличивая их популярность. Позднее вирусные аналитики выявили Android-банкера Android.BankBot.149.origin, исходный код которого вирусописатели опубликовали в Интернете. Другой Android-банкер, обнаруженный в январе, получил имя Android.BankBot.140.origin. Он распространялся под видом игры Super Mario Run, которая еще недоступна для Android-устройств. Также в прошлом месяце в каталоге Google Play был найден троянец-вымогатель Android.Locker.387.origin, блокировавший смартфоны и планшеты.

Наиболее заметные события, связанные с мобильной безопасностью в январе:

- обнаружение Android-троянца, который внедрялся в работающий процесс программы Play Маркет и незаметно скачивал приложения из каталога Google Play;
- распространение банковских троянцев;
- появление троянца-вымогателя в каталоге приложений Google Play.

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

Обзор вирусной активности в январе 2017 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