Dr.WEB®
с 1992 года

Обзор вирусной активности в ноябре 2016 года

Обзор вирусной активности в ноябре 2016 года

30 ноября 2016 года

Последний месяц осени был отмечен несколькими интересными событиями в сфере информационной безопасности. В ноябре вирусные аналитики компании «Доктор Веб» обнаружили ботнет, атакующий российские банки, а также выявили целенаправленную атаку на компании, выпускающие строительные краны. Также в течение месяца более 1 000 000 пользователей загрузили опасного Android-троянца из каталога приложений Google Play.

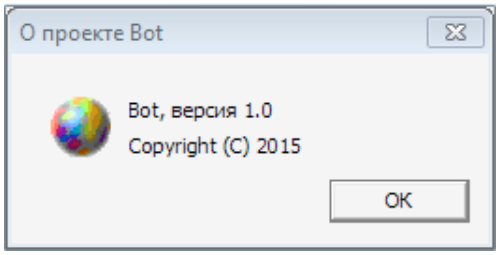
Главные тенденции ноября

- Появление ботнета, атакующего российские банки
- Целенаправленная атака на компании, производящие строительные краны
- Распространение Android-троянца в каталоге приложений Google Play

Угроза месяца

Целенаправленные или, как их еще называют, таргетированные атаки на конкретные интернет-ресурсы или компании удается выявить нечасто. В 2011 году компания «Доктор Веб» рассказывала о распространении троянца BackDoor.Dande, целенаправленно кравшего информацию у аптек и фармацевтических компаний. Спустя четыре года был обнаружен троянец BackDoor.Hser.1, атаковавший оборонные предприятия. А в ноябре 2016 года в вирусные базы Dr.Web был добавлен троянец BackDoor.Crane.1, который похищал важные документы и переписку с компьютеров сотрудников компаний – производителей портальных и грузоподъемных кранов. Кроме того, бэкдор делал снимки экранов зараженных ПК и отправлял их на принадлежащий злоумышленникам управляющий сервер.

Вирусные аналитики «Доктор Веб» предположили, что авторы BackDoor.Crane.1 частично заимствовали код из различных источников – в частности, с сайта rsdn.org. Об этом говорит значение параметра User-Agent, которым троянец представляется при обращении к интернет-ресурсам, – «RSDN HTTP Reader», а также невидимое окно «О проекте Bot», по всей видимости, забытое в его ресурсах.



BackDoor.Crane.1 имеет несколько модулей, каждый из которых решает на зараженной машине одну конкретную задачу:

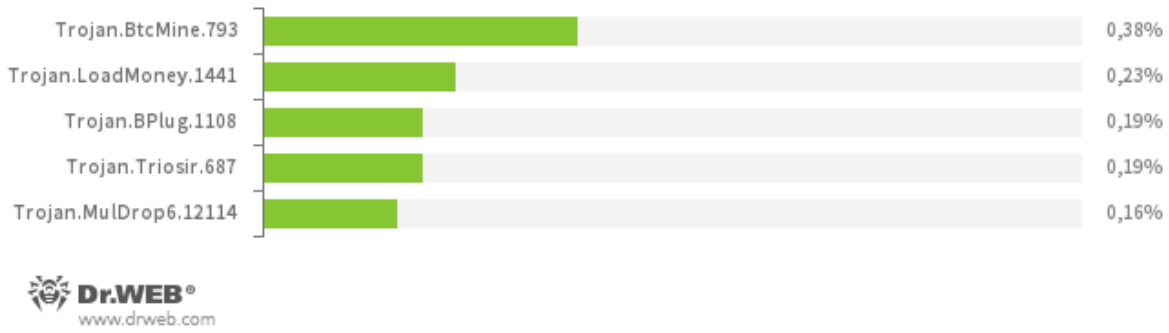
- выполнение переданной с управляющего сервера команды с использованием интерпретатора команд cmd;
- скачивание файла по заданной ссылке и сохранение его в указанную папку на инфицированном компьютере;
- составление и передача на управляющий сервер перечня содержимого заданной директории;
- создание и передача на управляющий сервер снимка экрана;
- загрузка файла на указанный злоумышленниками сервер с использованием протокола FTP;
- загрузка файла на указанный злоумышленниками сервер с использованием протокола HTTP.

Обзор вирусной активности в ноябре 2016 года

Кроме того, бэкдор по команде злоумышленников может загружать и запускать на атакуемом ПК две другие вредоносные программы, написанные на языке Python: Python.BackDoor.Crane.1 и Python.BackDoor.Crane.2. Подробнее об этих троянцах можно прочитать в опубликованной на сайте «Доктор Веб» обзорной статьей.

По данным статистики лечащей утилиты Dr.Web CureIt!

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

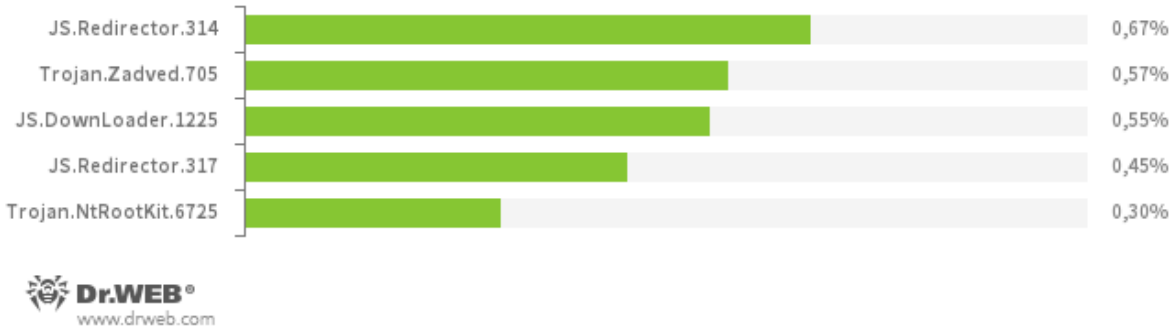


- **Trojan.BtcMine.793**
  Представитель семейства вредоносных программ, который втайне от пользователя применяет вычислительные ресурсы зараженного компьютера для добычи (майнинга) различных криптовалют – например, Bitcoin.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнёрской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.
- **Trojan.Triosir.687**
  Представитель семейства троянцев, представляющих собой плагин (надстройку) для браузеров. Предназначен для демонстрации назойливой рекламы при просмотре веб-страниц.
- **Trojan.MulDrop6.12114**
  Представитель семейства троянцев, предназначенных для установки на инфицированный компьютер других вредоносных программ.

Обзор вирусной активности в ноябре 2016 года

По данным серверов статистики «Доктор Веб»

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

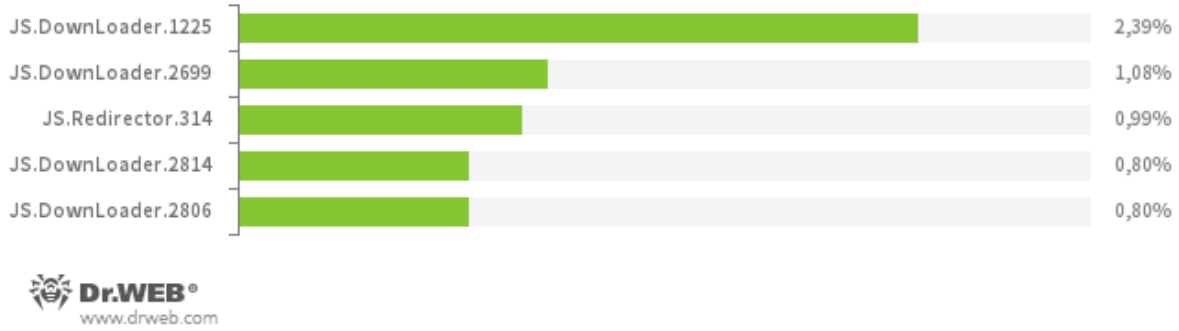


- **JS.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Автоматически перенаправляют пользователей браузеров на другие веб-страницы.
- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных 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.
- **Trojan.NtRootKit.6725**
  Троянец-руткит, способный скрывать свое присутствие в инфицированной системе. Для выполнения вредоносных функций внедряет свой код в другие

Обзор вирусной активности в ноябре 2016 года

Статистика вредоносных программ в почтовом трафике

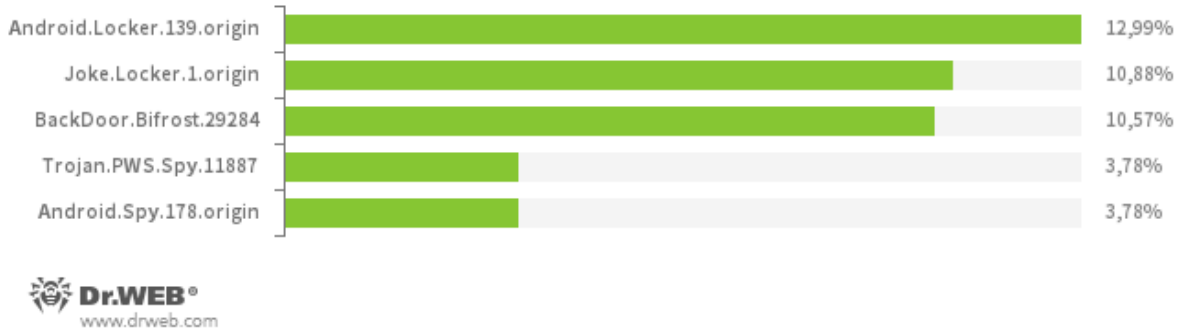
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в ноябре 2016 года



- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Автоматически перенаправляют пользователей браузеров на другие веб-страницы.

По данным бота Dr.Web для Telegram

Вредоносные программы, обнаруженные ботом Dr.Web для Telegram ноябре

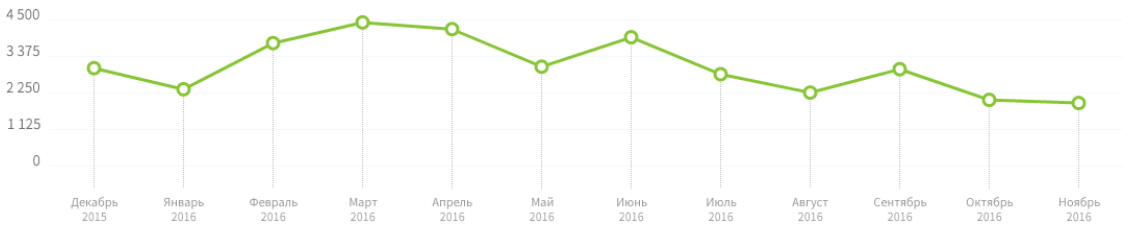


Обзор вирусной активности в ноябре 2016 года

- **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.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.

Троянцы-шифровальщики

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



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

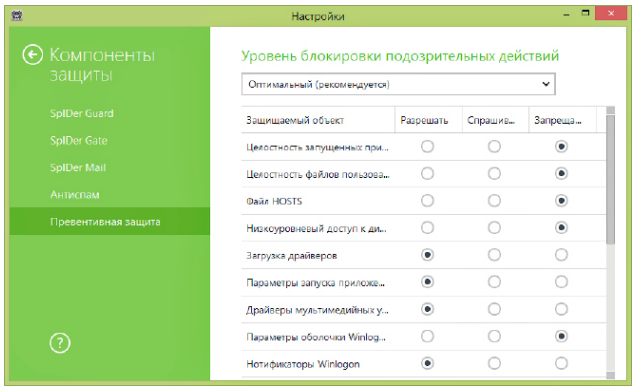
Обзор вирусной активности в ноябре 2016 года

- **Trojan.Encoder.717** — 25,64% обращений;
- **Trojan.Encoder.858** — 16,97% обращений;
- **Trojan.Encoder.761** — 14,54% обращений;
- **Trojan.Encoder.3953** — 5,55% обращений**;**
- **Trojan.Encoder.3976** — 3,79% обращений;
- **Trojan.Encoder.567** — 1,50% обращений.

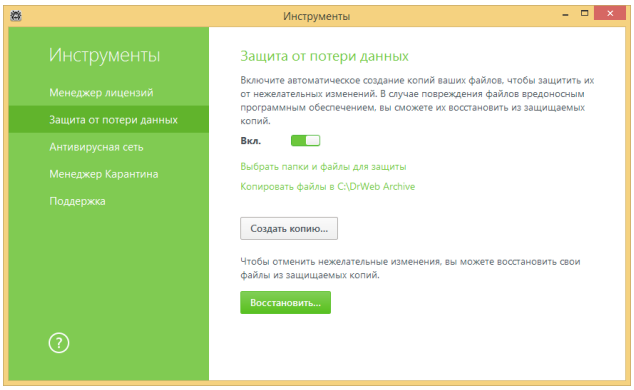
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

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 ноября 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 254 736 интернет-адресов.

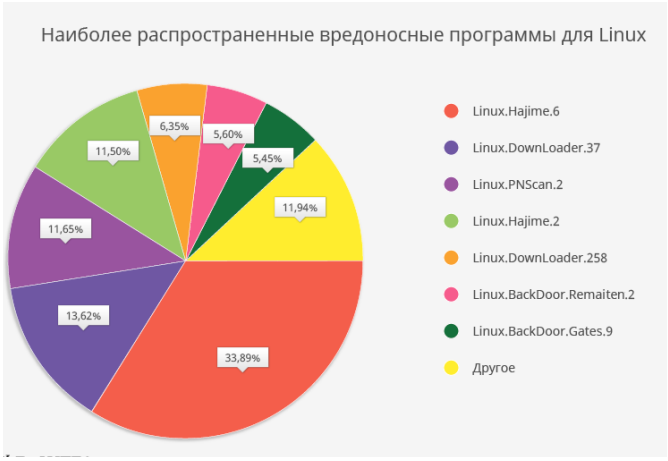
Октябрь 2016	Ноябрь 2016	Динамика
+ 338 670	+ 254 736	-24,78%

В Интернете иногда встречаются сайты, не являющиеся мошенническими, однако копирующие оформление ресурсов официальных государственных структур. Они вводят пользователей в заблуждение с применением методов и средств, в целом аналогичных тем, которые используют создатели фишинговых веб-страниц. Владельцы таких сайтов — коммерческие организации, не гнушающиеся недобросовестных методов рекламы. О поисках грани между рекламой и мошенничеством, а также о том, почему компания «Доктор Веб» добавляет адреса таких ресурсов в базу нерекомендуемых сайтов, читайте в нашей статье.

Нерекомендуемые сайты

Вредоносные программы для Linux

С начала ноября специалисты компании «Доктор Веб» выявили 389 285 атак на различные Linux-устройства, из них 79 447 осуществлялись по протоколу SSH и 309 838 — по протоколу Telnet. Пропорциональное соотношение вредоносных программ, которые киберпреступники загружали на атакованные устройства, показано на следующей диаграмме:

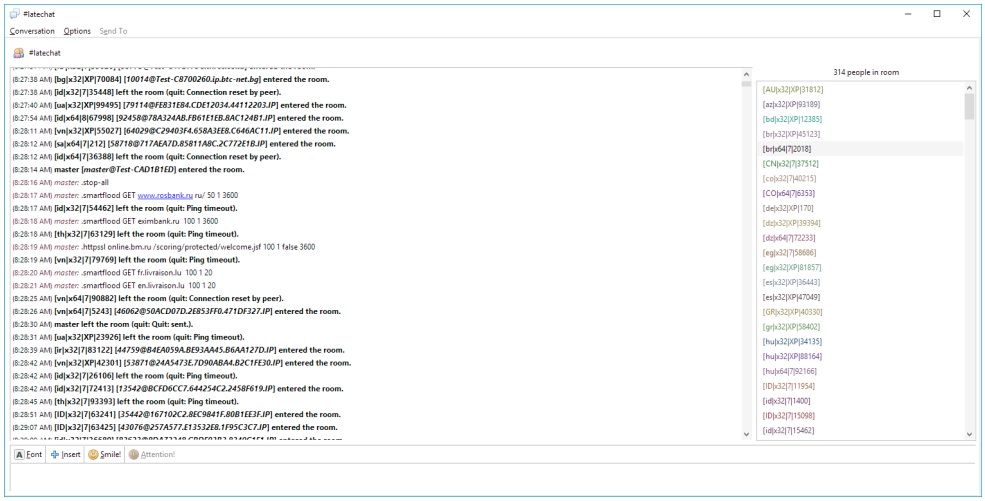


- **Linux.Hajime**
  Семейство сетевых червей для Linux, распространяются с использованием протокола Telnet. После успешной авторизации путем подбора пароля плагин-инфектор сохраняет на устройство хранящийся в нем загрузчик для архитектур MIPS/ARM, написанный на ассемблере. Загрузчик загружает с компьютера, с которого осуществлялась атака, основной модуль троянца, который включает устройство в децентрализованный P2P-ботнет.
- **Linux.DownLoader**
  Семейство вредоносных программ и скриптов для Linux, предназначенных для загрузки и установки на атакуемое устройство других вредоносных программ.
- **Linux.PNScan.2**
  Сетевой червь, предназначенный для заражения роутеров, работающих под управлением ОС семейства Linux. Червь решает следующие задачи: самостоятельное инфицирование устройств, открытие портов 9000 и 1337, обслуживание запросов по этим портам и организация связи с управляющим сервером.
- **Linux.BackDoor.Remaiten**
  Семейство вредоносных программ для Linux, предназначенных для осуществления DDoS-атак. Троянец умеет взламывать устройства по протоколу Telnet методом перебора паролей, в случае успеха сохраняет на устройство загрузчик, написанный на языке Ассемблер. Этот загрузчик предназначен для скачивания и установки на атакуемое устройство других вредоносных приложений.
- **Linux.BackDoor.Gates**
  Семейство Linux-троянцев, которые сочетают функции бэкдора и DDoS-бота. Троянцы способны выполнять поступающие команды, а также осуществлять DDoS-атаки.

Другие события

В ноябре вирусные аналитики компании «Доктор Веб» обнаружили ботнет, предназначенный для проведения массированных атак на отказ в обслуживании (DDoS-атак). Для этой цели злоумышленники использовали троянца BackDoor.IRC.Medusa.1 — вредоносную программу, относящуюся к категории IRC-ботов. Троянец получает команды с помощью протокола обмена текстовыми сообщениями IRC (Internet Relay Chat), присоединяясь к определенному чат-каналу.

Обзор вирусной активности в ноябре 2016 года



BackDoor.IRC.Medusa.1 может выполнять несколько типов DDoS-атак, а также по команде злоумышленников загружать и запускать на зараженной машине исполняемые файлы. Специалисты компании «Доктор Веб» предполагают, что именно эта вредоносная программа использовались в ходе массированных атак на Сбербанк России. В период с 11 по 14 ноября 2016 года злоумышленники неоднократно атаковали с ее помощью веб-сайты rosbank.ru («Росбанк») и eximbank.ru («Росэксимбанк»). Более подробные сведения об этом троянце изложены в опубликованной «Доктор Веб» новостной статье.

Вредоносное и нежелательное ПО для мобильных устройств

В ноябре вирусные аналитики компании «Доктор Веб» обнаружили в каталоге Google Play троянца Android.MulDrop.924, который распространялся под видом безобидной программы и мог загружать вредоносные приложения, а также показывать навязчивую рекламу. В общей сложности эту вредоносную программу установили более 1 000 000 пользователей. Также в ноябре был выявлен троянец Android.Spy.332.origin, предустановленный на некоторых популярных Android-устройствах. Он мог незаметно загружать, устанавливать и удалять приложения, а также передавать на удаленный сервер конфиденциальную информацию.

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

- обнаружение в каталоге Google Play троянца Android.MulDrop.924, который скачивал приложения и предлагал установить их, а также показывал навязчивую рекламу;
- обнаружение троянца Android.Spy.332.origin, который был предустановлен на некоторых мобильных устройствах и мог незаметно загружать, устанавливать и удалять ПО.

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

Обзор вирусной активности в ноябре 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