Dr.WEB®
с 1992 года

Обзор вирусной активности в октябре 2016 года

Обзор вирусной активности в октябре 2016 года

27 октября 2016 года

В октябре аналитики компании «Доктор Веб» исследовали первого троянца-шифровальщика, написанного на языке Go, и разработали дешифровку для поврежденных этим энкодером файлов. Во второй половине месяца был изучен бэкдор для операционных систем семейства Linux, способный выполнять на зараженном устройстве поступающие от злоумышленников команды. Не остались без внимания киберпреступников и пользователи мобильных устройств: в октябре продолжили распространяться вредоносные программы для Android.

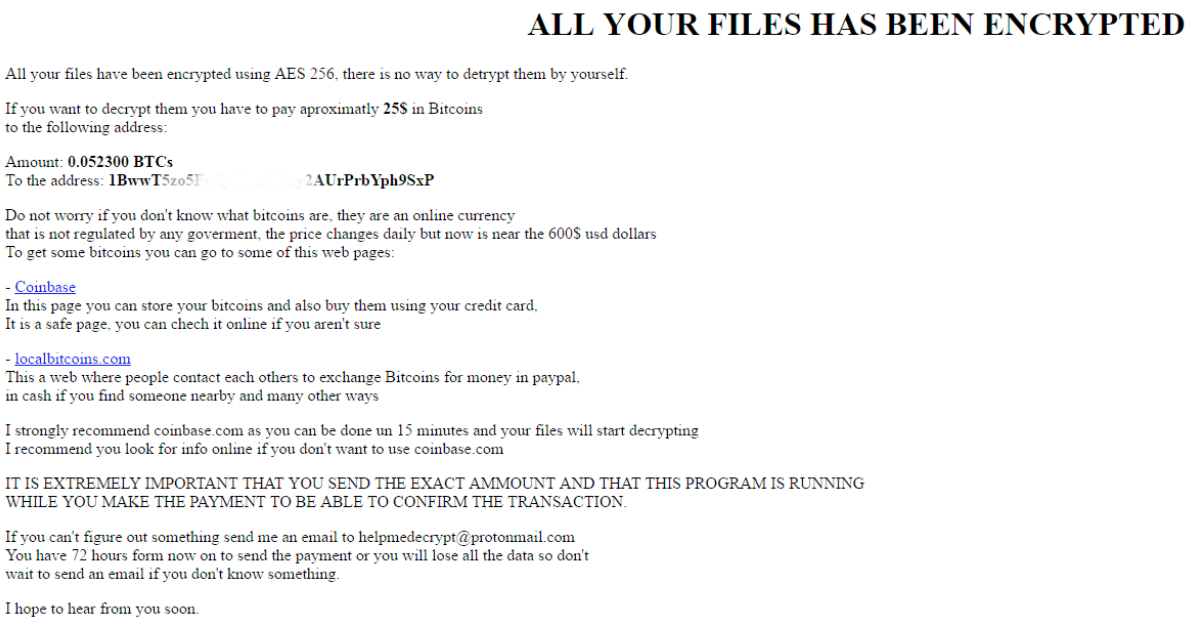
Главные тенденции октября

- Появление первого троянца-шифровальщика, написанного на Go
- Распространение новых троянцев для Linux
- Распространение вредоносных программ для мобильной платформы Android

Угроза месяца

Троянцы-шифровальщики по праву считаются одними из самых опасных вредоносных программ. Новые версии энкодеров появляются ежемесячно, однако до недавнего времени аналитикам компании «Доктор Веб» были неизвестны шифровальщики, написанные на языке Go. Первая такая вредоносная программа была добавлена в вирусные базы в октябре под именем **Trojan.Encoder.6491**.

Троянец шифрует хранящиеся на дисках файлы 140 различных типов с помощью алгоритма AES. **Trojan.Encoder.6491** кодирует оригинальные имена файлов методом Base64, а затем присваивает зашифрованным файлам расширение .enc. В результате, например, файл с именем Test_file.avi получит имя VGVzdF9maWxlLmF2aQ==.enc. Затем шифровальщик открывает в окне браузера файл Instructions.html с требованием выкупа в криптовалюте Bitcoin:



ALL YOUR FILES HAS BEEN ENCRYPTED

All your files have been encrypted using AES 256, there is no way to detrypt them by yourself.

If you want to decrypt them you have to pay aproximatly **25$** in Bitcoins
to the following address:

Amount: **0.052300 BTCs**
To the address: **1BwwT**5zo5F[illegible]2**AUrPrbYph9SxP**

Do not worry if you don't know what bitcoins are, they are an online currency
that is not regulated by any goverment, the price changes daily but now is near the 600$ usd dollars
To get some bitcoins you can go to some of this web pages:

- Coinbase
In this page you can store your bitcoins and also buy them using your credit card,
It is a safe page, you can chech it online if you aren't sure

- localbitcoins.com
This a web where people contact each others to exchange Bitcoins for money in paypal,
in cash if you find someone nearby and many other ways

I strongly recommend coinbase.com as you can be done un 15 minutes and your files will start decrypting
I recommend you look for info online if you don't want to use coinbase.com

IT IS EXTREMELY IMPORTANT THAT YOU SEND THE EXACT AMMOUNT AND THAT THIS PROGRAM IS RUNNING
WHILE YOU MAKE THE PAYMENT TO BE ABLE TO CONFIRM THE TRANSACTION.

If you can't figure out something send me an email to helpmedecrypt@protonmail.com
You have 72 hours form now on to send the payment or you will lose all the data so don't
wait to send an email if you don't know something.

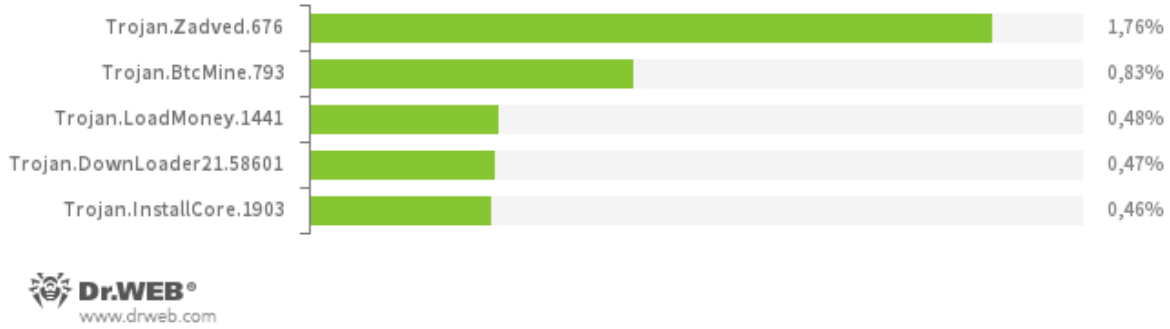
I hope to hear from you soon.

Trojan.Encoder.6491 с определенным интервалом проверяет баланс Bitcoin-кошелька, на который жертва должна перевести средства, и автоматически расшифровывает все зашифрованные ранее файлы, если пострадавший заплатил выкуп. Специалисты компании «Доктор Веб» разработали специальную методику, позволяющую расшифровывать пострадавшие от этого троянца файлы, о чем сообщили в соответствующей обзорной статье.

Обзор вирусной активности в октябре 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

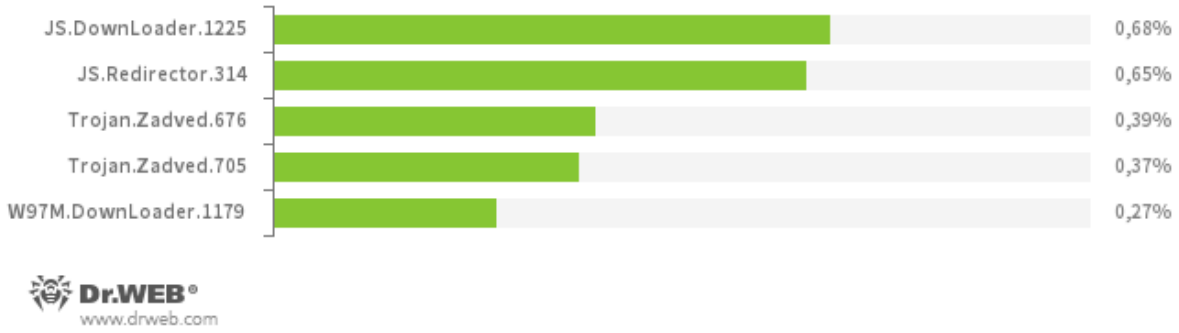


- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **Trojan.BtcMine.793**
  Представитель семейства вредоносных программ, который втайне от пользователя использует вычислительные ресурсы зараженного компьютера для добычи (майнинга) различных криптовалют, например Bitcoin.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **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 октябре 2016 года

По данным серверов статистики «Доктор Веб»

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

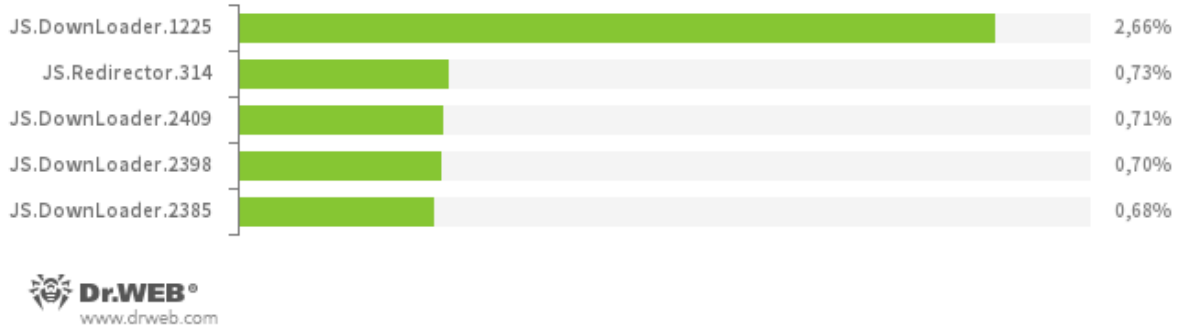


- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **JS.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Автоматически перенаправляют пользователей браузеров на другие веб-страницы.
- **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.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Обзор вирусной активности в октябре 2016 года

Статистика вредоносных программ в почтовом трафике

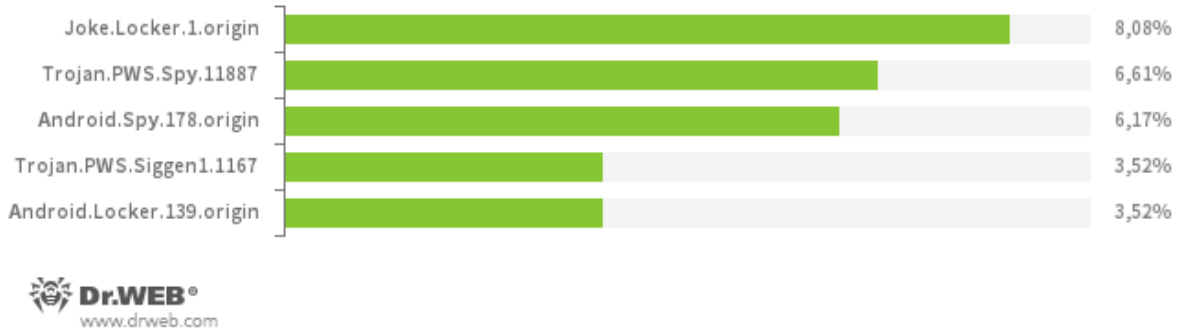
Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в октябре 2016 года



- **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

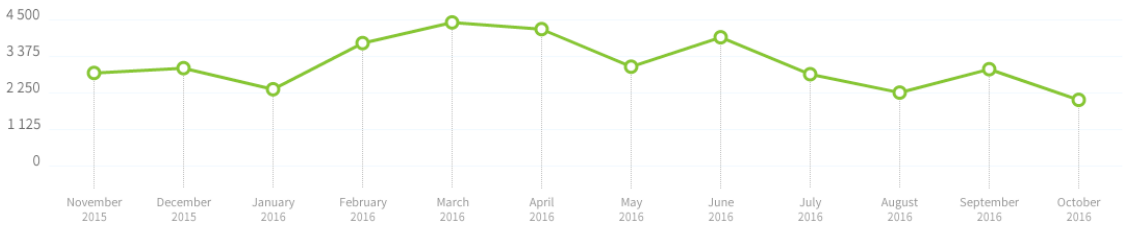
Вредоносные программы, обнаруженные ботом Dr.Web для Telegram в октябре



- **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).
- **Trojan.PWS.Spy.11887**
  Представитель семейства троянцев для ОС Windows, способных похищать конфиденциальную информацию, в том числе пароли пользователя.
- **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.Siggen1.1167**
  Представитель семейства троянцев для ОС Windows, способных похищать пароли от различных приложений.
- **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.

Троянцы-шифровальщики

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



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

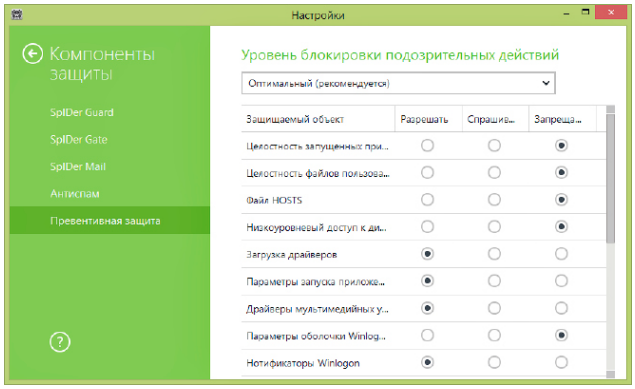
Обзор вирусной активности в октябре 2016 года

- **Trojan.Encoder.858** — 26,85% обращений;
- **Trojan.Encoder.761** — 21,01% обращений;
- **Trojan.Encoder.3953** — 5,25% обращений;
- **Trojan.Encoder.567** — 4,61% обращений;
- **Trojan.Encoder.3976** — 2,92% обращений.

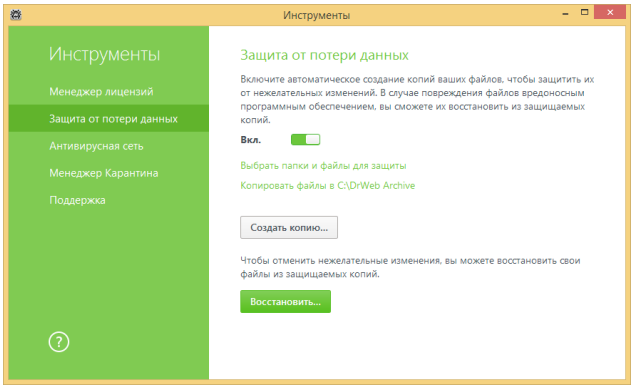
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

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 октября 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 338 670 интернет-адресов.

Сентябрь 2016	Октябрь 2016	Динамика
+ 298 985	+ 338 670	+13,27%

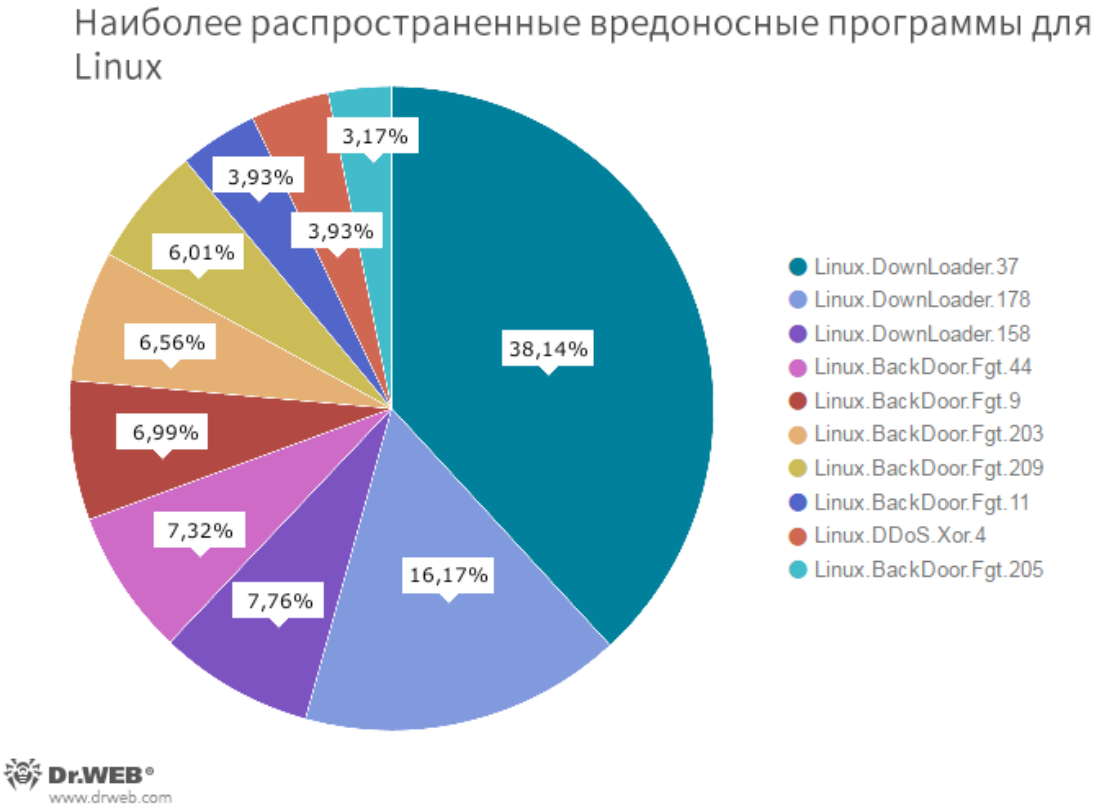
Среди добавленных в базу нерекомендуемых сайтов значительную долю занимают мошеннические интернет-ресурсы. Сетевые жулики придумывают все новые способы обмана пользователей Интернета, и об одном из них мы подробно рассказали в опубликованной на нашем сайте статье.

Создатели мошеннического интернет-ресурса «Детектор Миллионеров» завлекают потенциальных жертв при помощи массовых спам-рассылок. Посетителям предлагают протестировать программу «Детектор Миллионера», с помощью которой создатели сайта якобы уже заработали несколько миллионов долларов. Чтобы использовать «Детектор Миллионера», потенциальной жертве нужно перевести на счет злоумышленников некую денежную сумму. Разумеется, все деньги, внесенные жертвой на так называемый депозит, будут неизбежно проиграны. Кроме того, простой поиск в базе данных регистратора показывает, что администратором домена detektor-millionera.com является некто Bob Douglas, которому принадлежит множество других сомнительных интернет-ресурсов.

Нерекомендуемые сайты

Вредоносные программы для Linux

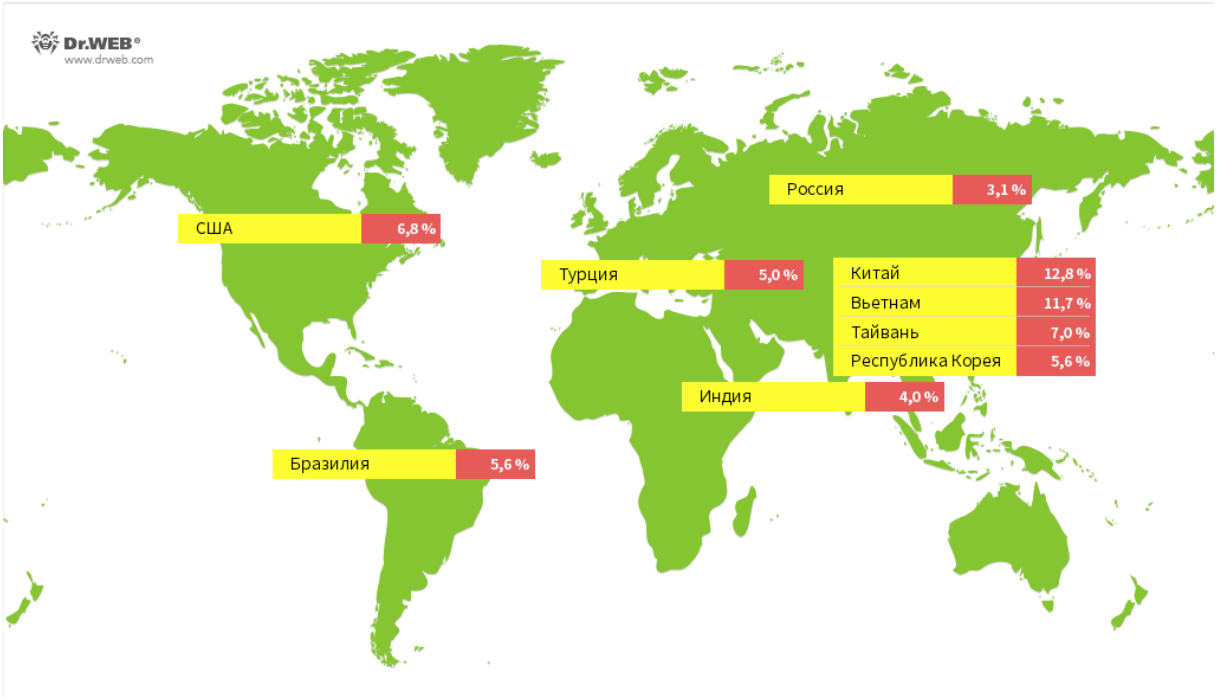
С начала октября специалисты компании «Доктор Веб» выявили 40 756 атак на различные Linux-устройства, из них 35 423 осуществлялись по протоколу SSH и 5 333 — по протоколу Telnet. Пропорциональное соотношение вредоносных программ, которые киберпреступники загружали на атакованные устройства, показано на следующей диаграмме:



- **Linux.DownLoader**
  Семейство вредоносных программ и сценариев (скриптов) для ОС Linux, предназначенных для загрузки и установки в скомпрометированной системе других вредоносных приложений.
- **Linux.BackDoor.Fgt**
  Семейство вредоносных программ для ОС Linux, предназначенных для DDoS-атак. Существуют версии троянцев для различных дистрибутивов Linux, в том числе встраиваемых систем для архитектур MIPS и SPARC.
- **Linux.DDoS.Xor**
  Семейство вредоносных программ для ОС Linux, предназначенных для DDoS-атак на различные сетевые узлы.

Обзор вирусной активности в октябре 2016 года

Ниже представлено географическое распределение IP-адресов, с которых на уязвимые Linux-устройства загружалось вредоносное ПО:



В конце октября вирусные аналитики «Доктор Веб» исследовали троянца-бэкдора, угрожающего пользователям ОС семейства Linux. Троянец, получивший наименование Linux.BackDoor.FakeFile.1, распространялся в архиве под видом PDF-файла, документа Microsoft Office или Open Office. Эта вредоносная программа способна выполнять следующие команды:

- передать на управляющий сервер количество сообщений, отправленных в ходе текущего соединения;
- передать список содержимого заданной папки;
- передать на управляющий сервер указанный файл или папку со всем содержимым;
- удалить каталог;
- удалить файл;
- переименовать указанную папку;
- удалить себя;
- запустить новую копию процесса;
- закрыть текущее соединение;
- организовать backconnect и запустить sh;
- завершить backconnect;
- открыть исполняемый файл процесса на запись;

- закрыть файл процесса;
- создать файл или папку;
- записать переданные значения в файл;
- получить имена, разрешения, размеры и даты создания файлов в указанной директории;
- установить права 777 на указанный файл;
- завершить выполнение бэкдора.

Более подробная информация о Linux.BackDoor.FakeFile.1 представлена в опубликованной нами статье.

Вредоносное и нежелательное ПО для мобильных устройств

В конце сентября — начале октября в каталоге Google Play был обнаружен троянец Android.SockBot.1, который перенаправлял интернет-трафик через зараженные мобильные устройства, используя их в качестве прокси-серверов.

Наиболее заметные события, связанные с мобильной безопасностью в октябре:

- обнаружение в каталоге Google Play троянца Android.SockBot.1, который после заражения мобильных устройств использовал их в качестве прокси-серверов.

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

Обзор вирусной активности в октябре 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