Dr.WEB®
с 1992 года

Обзор вирусной активности в октябре 2017 года

Обзор вирусной активности в октябре 2017 года

27 октября 2017 года

Октябрь 2017 года запомнится не только специалистам по информационной безопасности, но и всем пользователям Интернета появлением нового червя-шифровальщика, получившего имя Trojan.BadRabbit. Этот троянец начал распространяться 24 октября, атаке подверглись в основном компьютеры на территории России и Украины.

В октябре вирусные аналитики «Доктор Веб» исследовали бэкдор, написанный на языке Python. Эта вредоносная программа умеет красть информацию из популярных браузеров, фиксировать нажатия клавиш, скачивать и сохранять на зараженном компьютере различные файлы, а также выполнять ряд других вредоносных функций.

Кроме того, специалисты исследовали новую версию Linux-троянца, способного заражать различные «умные» устройства.

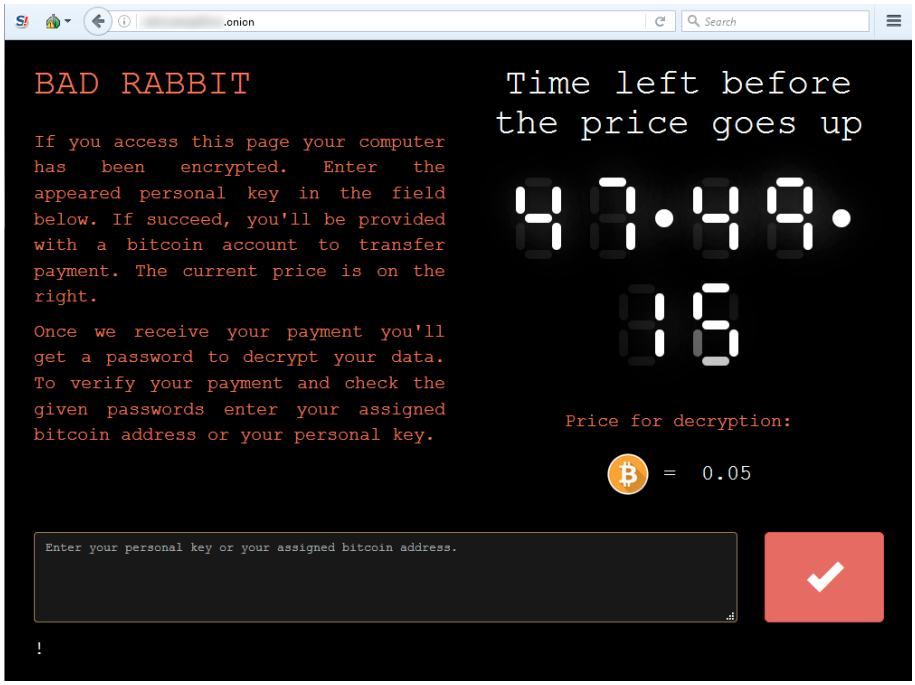
Главные тенденции октября

- Распространение нового червя-шифровальщика BadRabbit
- Появление бэкдора, написанного на Python
- Выявление нового Linux-троянца для IoT

Угроза месяца

Как и ее предшественники, вредоносная программа Trojan.BadRabbit представляет собой червя, способного к самостоятельному распространению без участия пользователя и состоящего из нескольких компонентов: дроппера, шифровальщика-расшифровщика и собственно червя-энкодера. Часть кода этого червя позаимствована у троянца Trojan.Encoder.12544, также известного под именем NotPetya. При запуске энкодер проверяет наличие файла C:\Windows\cscc.dat и, если такой существует, прекращает свою работу (в связи с этим создание файла cscc.dat в папке C:\Windows может предотвратить вредоносные последствия запуска троянца).

По мнению некоторых исследователей, источником заражения Trojan.BadRabbit стал ряд скомпрометированных веб-сайтов, в HTML-код которых был внедрен вредоносный сценарий на языке JavaScript. Энкодер шифрует файлы с расширениями .3ds, .7z, .accdb, .ai, .asm, .asp, .aspx, .avhd, .back, .bak, .bmp, .brw, .c, .cab, .cc, .cer, .cfg, .conf, .cpp, .crt, .cs, .ctl, .cxx, .dbf, .der, .dib, .disk, .djvu, .doc, .docx, .dwg, .eml, .fdb, .gz, .h, .hdd, .hpp, .hxx, .iso, .java, .jfif, .jpe, .jpeg, .jpg, .js, .kdbx, .key, .mail, .mdb, .msg, .nrg, .odc, .odf, .odg, .odi, .odm, .odp, .ods, .odt, .ora, .ost, .ova, .ovf, .p12, .p7b, .p7c, .pdf, .pem, .pfx, .php, .pmf, .png, .ppt, .pptx, .ps1, .pst, .pvi, .py, .pyc, .pyw, .qcow, .qcow2, .rar, .rb, .rtf, .scm, .sln, .sql, .tar, .tib, .tif, .tiff, .vb, .vbox, .vbs, .vcb, .vdi, .vfd, .vhd, .vhdx, .vmc, .vmdk, .vmsd, .vmtm, .vmx, .vsdx, .vsv, .work, .xls, .xlsx, .xml, .xvd, .zip. В результате работы троянца на экране зараженного компьютера демонстрируется требование выкупа в криптовалюте Bitcoin, а на сайте злоумышленников в TOR жертве отводится для оплаты 48 часов, по истечении которых сумма выкупа будет увеличена.

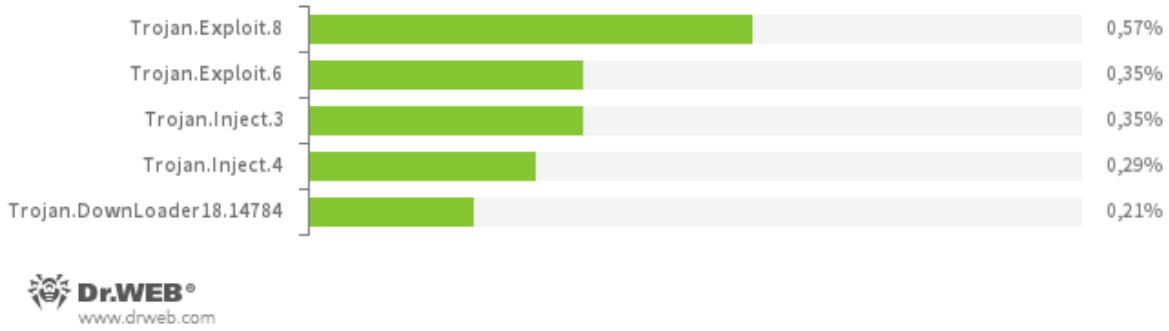


Обзор вирусной активности в октябре 2017 года

В настоящее время исследования Trojan.BadRabbit продолжаются, однако Антивирус Dr.Web успешно определяет и удаляет эту вредоносную программу. Кроме того, анализ троянца показал, что он проверяет присутствие в системе антивирусов Dr.Web и McAfee. При обнаружении нашего продукта Trojan.BadRabbit пропускает этап шифрования в пользовательском режиме, однако пытается запустить полное шифрование диска после перезагрузки системы. Эта функция вредоносной программы блокируется Антивирусом Dr.Web, таким образом, от действия шифровальщика не пострадают пользователи Антивируса Dr.Web версии 9.1 и выше и Dr.Web KATANA, при условии что они не меняли настройки превентивной защиты и не отключили ее.

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web

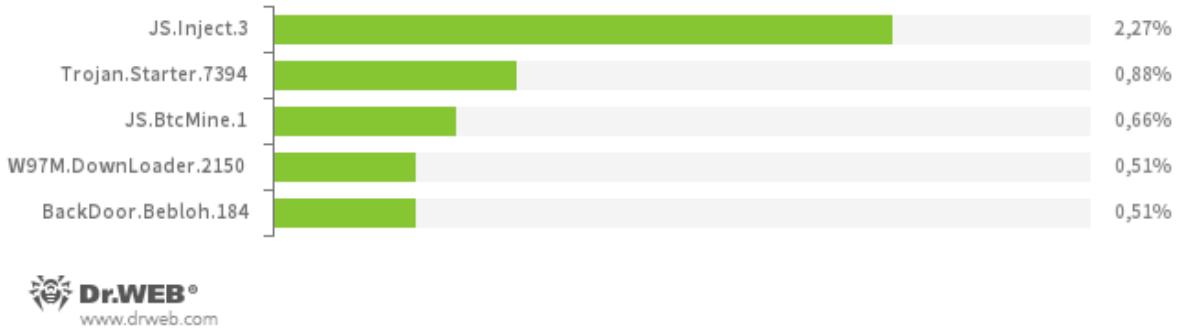


- **Trojan.Exploit**
  Эвристический детект для эксплойтов, использующих различные уязвимости для компрометации легитимных приложений.
- **Trojan.Inject**
  Семейство вредоносных программ, встраивающих вредоносный код в процессы других программ.

Обзор вирусной активности в октябре 2017 года

По данным серверов статистики «Доктор Веб»

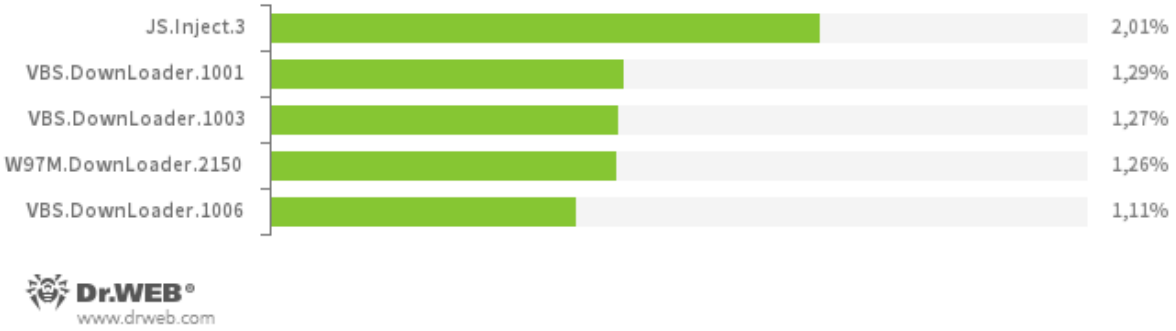
Наиболее распространенные вредоносные программы в октябре 2017 года согласно данным серверов статистики Dr.Web



- **JS.Inject.3**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **Trojan.Starter.7394**
  Представитель семейства троянцев, основное назначение которых — запуск в инфицированной системе исполняемого файла с определенным набором вредоносных функций.
- **JS.BtcMine.1**
  Сценарий на языке JavaScript, предназначенный для скрытой добычи (майнинга) криптовалют.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.
- **BackDoor.Bebloh.184**
  Один из представителей семейства вредоносных программ, относящихся к категории банковских троянцев. Данное приложение представляет угрозу для пользователей систем дистанционного банковского обслуживания (ДБО), поскольку позволяет злоумышленникам красть конфиденциальную информацию путем перехвата заполняемых в браузере форм и встраивания в страницы сайтов некоторых банков.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике во ктябре 2017 года

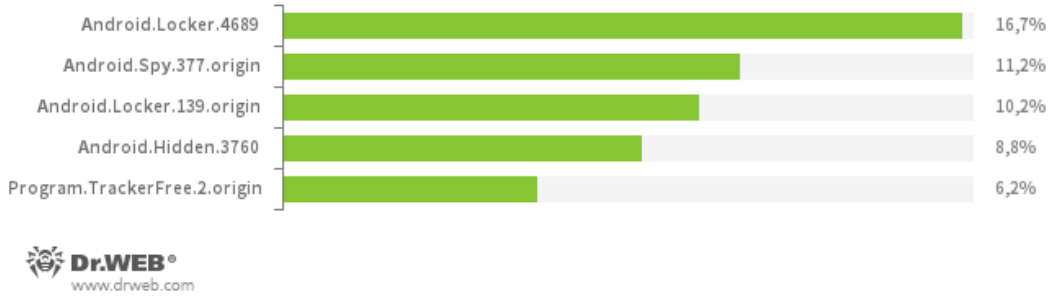


- **JS.Inject.3**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Встраивают вредоносный скрипт в HTML-код веб-страниц.
- **VBS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке VBScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Обзор вирусной активности в октябре 2017 года

По данным бота Dr.Web для Telegram

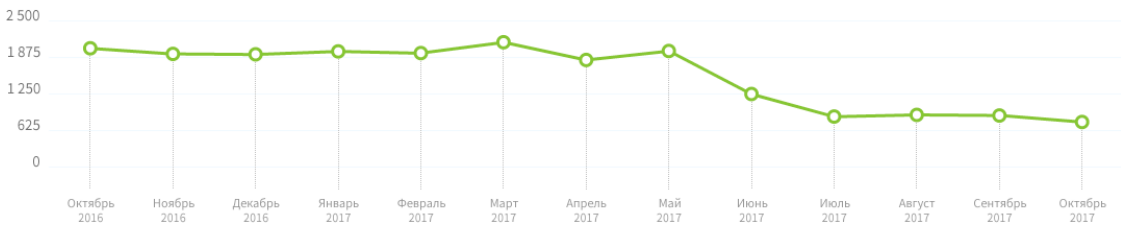
Наиболее распространенные вредоносные программы, обнаруженные ботом Dr.Web для Telegram



- **Android.Locker**
  Семейство Android-троянцев, предназначенных для вымогательства. Они показывают навязчивое сообщение якобы о нарушении закона и о последовавшей в связи с этим блокировке мобильного устройства, для снятия которой пользователю предлагается заплатить определенную сумму.
- **Android.Spy.337.origin**
  Представитель семейства троянцев для ОС Android, способных похищать конфиденциальную информацию, в том числе пользовательские пароли.
- **Android.Hidden**
  Семейство Android-троянцев, способных скрывать свой значок в списке приложений инфицированного устройства.
- **Program.TrackerFree.2.origin**
  Детект приложения для слежки за детьми Mobile Tracker Free.

Шифровальщики

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



Обзор вирусной активности в октябре 2017 года

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

- **Trojan.Encoder.858** — 23,49% обращений;
- **Trojan.Encoder.3953** — 17,26% обращений;
- **Trojan.Encoder.858** — 16,67% обращений;
- **Trojan.Encoder.13671** — 5,51% обращений;
- **Trojan.Encoder.2667** — 4,02% обращений;
- **Trojan.Encoder.567** — 2,38% обращений;
- **Trojan.Encoder.3976** — 2,23% обращений.

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

Настрой-ка Dr.Web от шифровальщиков
Обучающий курс
О бесплатном восстановлении

Dr.Web Rescue Pack

Опасные сайты

В течение октября 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 256 429 интернет-адресов.

Сентябрь 2017	Октябрь 2017	Динамика
+ 298 324	+ 256 429	-14,0%

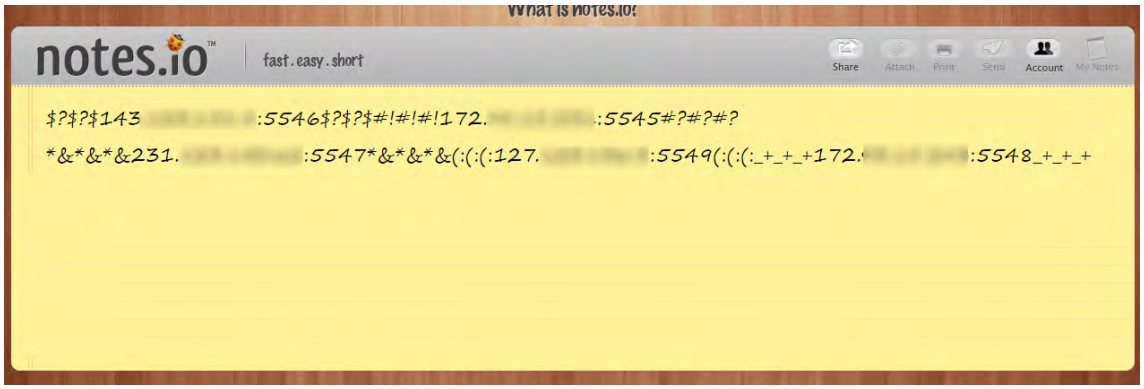
Нерекомендуемые сайты

Вредоносные программы для ОС Linux

В октябре вирусные аналитики «Доктор Веб» исследовали троянца, способного заражать «умные» устройства под управление ОС Linux. Вредоносная программа получила наименование Linux.IotReapper. Это очередная модификация уже давно известного специалистам Linux.Mirai. Вместо перебора логинов и паролей по словарю для взлома устройств Linux.IotReapper запускает эксплойты и проверяет результат их выполнения. Затем троянец ожидает получения команд от управляющего сервера. Он может скачивать и запускать на инфицированном устройстве различные приложения, а также содержит два модуля: интерпретатор Lua и сервер, работающий на порту 8888, который также может выполнять различные команды. Троянец Linux.IotReapper успешно детектируется Антивирусом Dr.Web для Linux.

Другие события в сфере информационной безопасности

В середине месяца вирусные базы Dr.Web пополнились записью Python.BackDoor.33, с использованием которой детектируется бэкдор, написанный на языке Python. Эта вредоносная программа обладает способностью к самораспространению: после установки на инфицированном устройстве и его перезагрузки Python.BackDoor.33 пытается заразить все подключенные к устройству накопители с именами от C до Z. Затем троянец определяет IP-адрес и доступный порт управляющего сервера, отправляя запрос к нескольким серверам в Интернете, включая pastebin.com, docs.google.com и notes.io. Полученное значение имеет следующий вид:



Обзор вирусной активности в октябре 2017 года

При определенных условиях Python.BackDoor.33 скачивает с управляющего сервера и запускает на инфицированном устройстве сценарий на языке Python, в котором реализованы функции кражи паролей (стилер), перехвата нажатия клавиш (кейлоггер) и удаленного выполнения команд (бэкдор). Этот сценарий позволяет выполнять на зараженной машине следующие действия:

- красть информацию из браузеров Chrome, Opera, Yandex, Amigo, Torch, Spark;
- фиксировать нажатия клавиш и делать снимки экрана;
- загружать дополнительные модули на Python и исполнять их;
- скачивать файлы и сохранять их на носителе инфицированного устройства;
- получать содержимое заданной папки;
- перемещаться по папкам;
- запрашивать информацию о системе.

Более подробная информация о Python.BackDoor.33 изложена в размещенной на нашем сайте обзорной статье.

Вредоносное и нежелательное ПО для мобильных устройств

В октябре в средствах массовой информации появились сообщения об обнаружении опасного троянца-вымогателя, который детектируется антивирусом Dr.Web как Android.Banker.184.origin. Эта вредоносная программа, известная вирусным аналитикам «Доктор Веб» с августа 2017 года, изменяет PIN-код разблокировки экрана зараженных Android-смартфонов и планшетов, шифрует файлы и требует выкуп за восстановление работоспособности устройств. Кроме того, в прошедшем месяце в каталоге Google Play был найден троянец Android.SockBot.5, позволявший киберпреступникам использовать мобильные устройства в качестве прокси-серверов.

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

- появление информации о распространении троянца-вымогателя, изменяющего PIN-код разблокировки экрана Android-устройств и шифрующего файлы;
- обнаружение в каталоге Google Play троянца, который превращал зараженные Android-устройства в прокси-серверы.

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

Обзор вирусной активности в октябре 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
125040, 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