Dr.WEB®
с 1992 года

Обзор вирусной активности в ноябре 2015 года

Обзор вирусной активности в ноябре 2015 года

30 ноября 2015 года

Ноябрь 2015 войдет в историю благодаря появлению информации о распространении шифровальщика для операционных систем семейства Linux, получившего наименование Linux.Encoder.1. Этот энкодер — далеко не первый из тех, что представляли опасность для пользователей ОС Linux: еще в августе 2014 года компания «Доктор Веб» сообщала о появлении троянца Trojan.Encoder.737, способного шифровать хранящиеся в сетевых хранилищах производства компании Synology файлы. Кроме того, распространению Linux.Encoder.1 предшествовало появление еще как минимум двух версий этой вредоносной программы. Вместе с тем именно деструктивная деятельность Linux.Encoder.1 имела наиболее массовый характер: согласно данным поисковой системы Google, этот энкодер сумел заразить более 3000 веб-сайтов по всему миру.

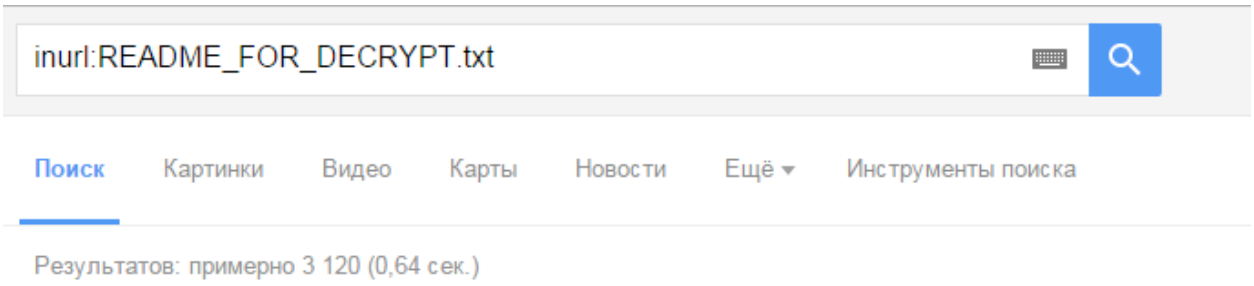
Главные тенденции ноября

- Заражение более 3000 сайтов опасным троянцем-шифровальщиком Linux.Encoder.1
- Распространение вредоносных программ, открывающих несанкционированный доступ к инфицированному компьютеру
- Появление новых троянцев для Microsoft Windows и мобильной платформы Google Android

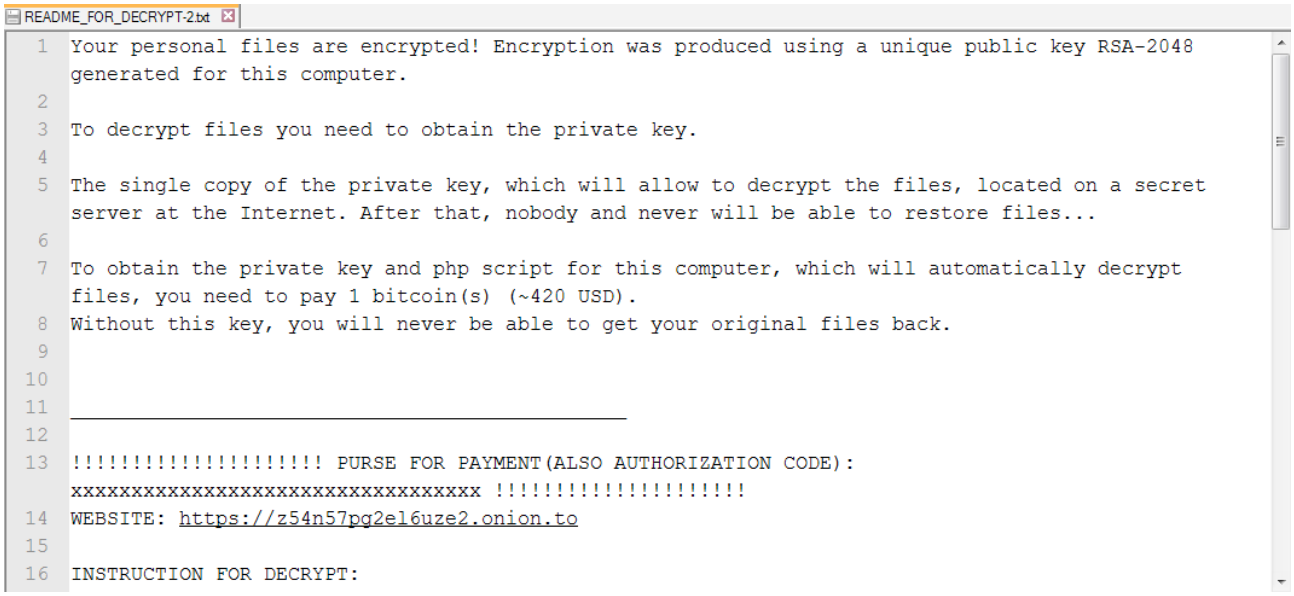
Обзор вирусной активности в ноябре 2015 года

Угроза месяца

Основной целью вирусописателей, распространявших троянца-энкодера Linux.Encoder.1, стали владельцы веб-сайтов, работающих под управлением таких популярных CMS, как WordPress, Magento и других. При проведении атак использовалась неустановленная пока уязвимость. Как выяснили эксперты, данному шифровальщику для работы не требуются права root — вполне достаточно привилегий пользователя www-data, то есть прав приложения, работающего от имени веб-сервера. По данным на 12 ноября Linux.Encoder.1 предположительно инфицировал более 2000 сайтов — такой вывод можно сделать, выполнив в Google поиск по имени файла с требованиями злоумышленников. Однако уже к 24 ноября число подобных интернет-ресурсов превысило 3000.



Троянец запускается на сервере, где расположен атакуемый веб-сайт, с помощью ранее внедренного в систему управления контентом шелл-скрипта. С использованием этого скрипта злоумышленники размещают на сервере в той же папке другой файл, представляющий собой дроппер троянца-энкодера Linux.Encoder.1. Активизировавшись по команде киберпреступников, дроппер определяет архитектуру работающей на сервере операционной системы (32- или 64-разрядная версия Linux), извлекает из собственного тела соответствующий экземпляр шифровальщика и запускает его, после чего удаляется. Запустившись на атакуемом сервере, троянец шифрует файлы в папках, для которых у него имеются права на запись. После этого он сохраняет на диске сервера файл с именем README_FOR_DECRYPT.txt, содержащий инструкции по расшифровке файлов и требования злоумышленников. Если по каким-либо причинам у шифровальщика окажутся более высокие привилегии, он не ограничится одной лишь папкой веб-сервера.


README_FOR_DECRYPT-2.txt

```
1  Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
   generated for this computer.
2
3  To decrypt files you need to obtain the private key.
4
5  The single copy of the private key, which will allow to decrypt the files, located on a secret
   server at the Internet. After that, nobody and never will be able to restore files...
6
7  To obtain the private key and php script for this computer, which will automatically decrypt
   files, you need to pay 1 bitcoin(s) (~420 USD).
8  Without this key, you will never be able to get your original files back.
9
10
11 ----------------------------------------------
12
13 !!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!
14 WEBSITE: https://z54n57pg2el6uze2.onion.to
15
16 INSTRUCTION FOR DECRYPT:
```

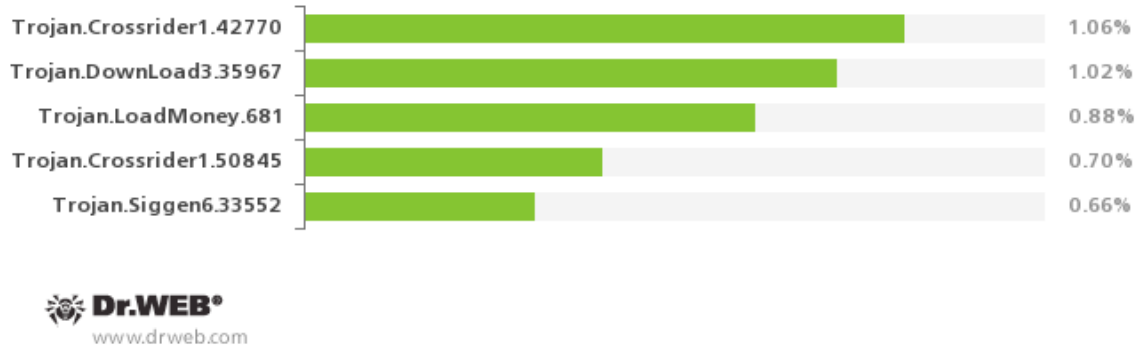
Причин, по которым веб-сайт может оказаться инфицированным данной вредоносной программой, может быть несколько: неправильная настройка администраторами веб-сервера, несвоевременная установка обновлений безопасности систем управления контентом, использование устаревших версий CMS, а также «взломанных» коммерческих компонентов или модулей WordPress, Magento и пр.

В силу того, что создатели Linux.Encoder.1 допустили в коде шифровальщика ряд существенных ошибок, данные, поврежденные этим энкодером, поддаются расшифровке. Об особенностях работы этой вредоносной программы можно узнать, ознакомившись с опубликованной на сайте компании «Доктор Веб» информационной статьей и более подробным исследованием данного троянца.

Обзор вирусной активности в ноябре 2015 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

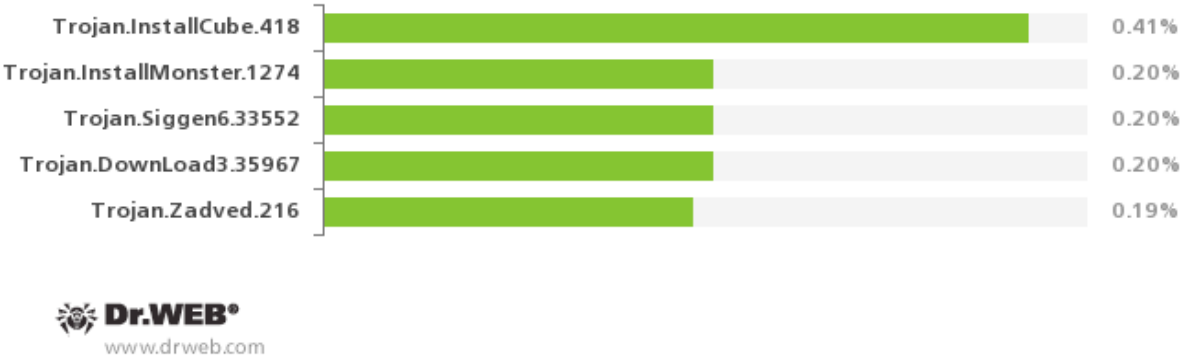


- **Trojan.Crossrider1.42770, Trojan.Crossrider1.50845**
  Представители семейства троянцев, предназначенных для демонстрации различной сомнительной рекламы.
- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.

Обзор вирусной активности в ноябре 2015 года

По данным серверов статистики «Доктор Веб»

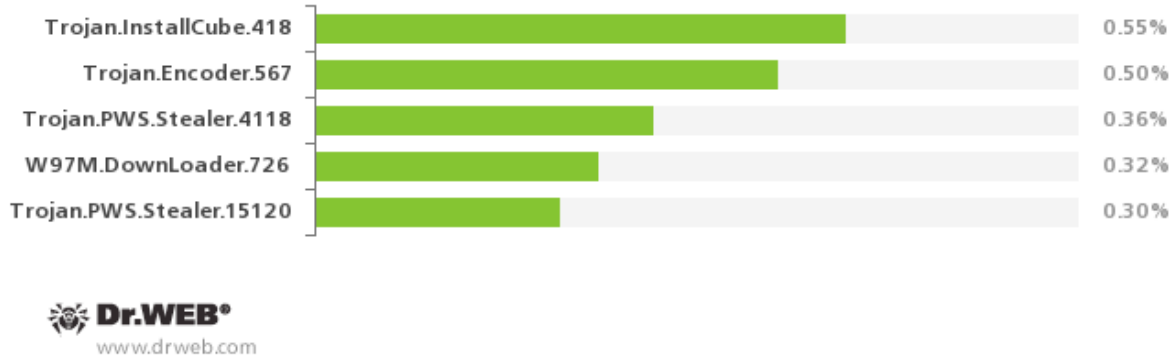
Наиболее распространенные вредоносные программы в ноябре 2015 года
согласно данным серверов статистики Dr.Web



- **Trojan.InstallCube**
  Семейство программ-загрузчиков, инсталлирующих на компьютер пользователя различные ненужные и нежелательные приложения.
- **Trojan.Installmonster**
  Семейство вредоносных программ, созданных с использованием партнерской программы installmonster. Данные приложения устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.DownLoad3.35967**
  Один из представителей семейства троянцев-загрузчиков, скачивающих из Интернета и запускающих на атакуемом компьютере другое вредоносное ПО.
- **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.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в ноябре 2015 года

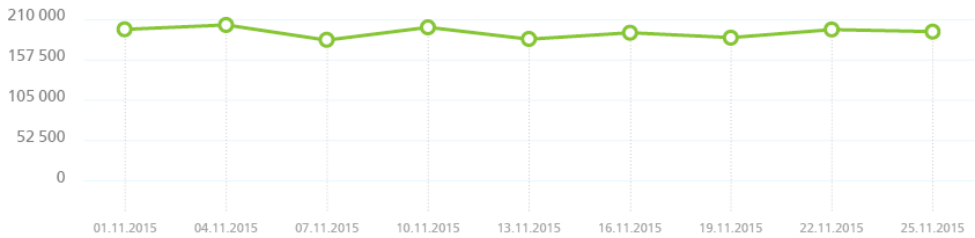


- **Trojan.InstallCube**
  Семейство программ-загрузчиков, инсталлирующих на компьютер пользователя различные ненужные и нежелательные приложения.
- **Trojan.Encoder.567**
  Один из представителей семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку. 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.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.
- **W97M.DownLoader.726**
  Один из представителей троянцев-загрузчиков, использующих в своей работе уязвимости офисных приложений. Предназначен для загрузки на атакуемый компьютер других вредоносных программ.

Ботнеты

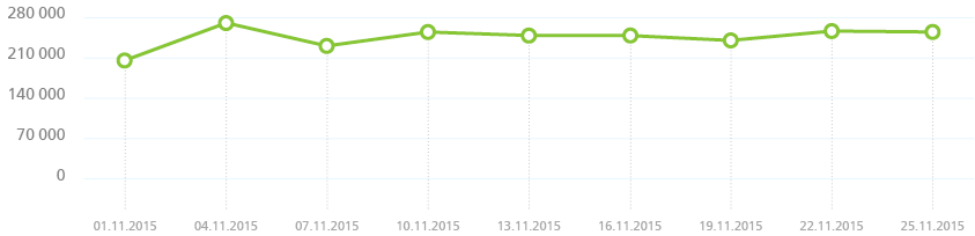
Специалисты компании «Доктор Веб» продолжают внимательно следить за деятельностью двух подсетей ботнета, состоящего из компьютеров, инфицированных файловым вирусом Win32.Rmnet.12. Активность этих бот-сетей в ноябре 2015 года демонстрируют следующие графики:

Активность ботнета Win32.Rmnet.12 в ноябре 2015 года (1 подсеть)



Dr.WEB®
www.drweb.com

Активность ботнета Win32.Rmnet.12 в ноябре 2015 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.

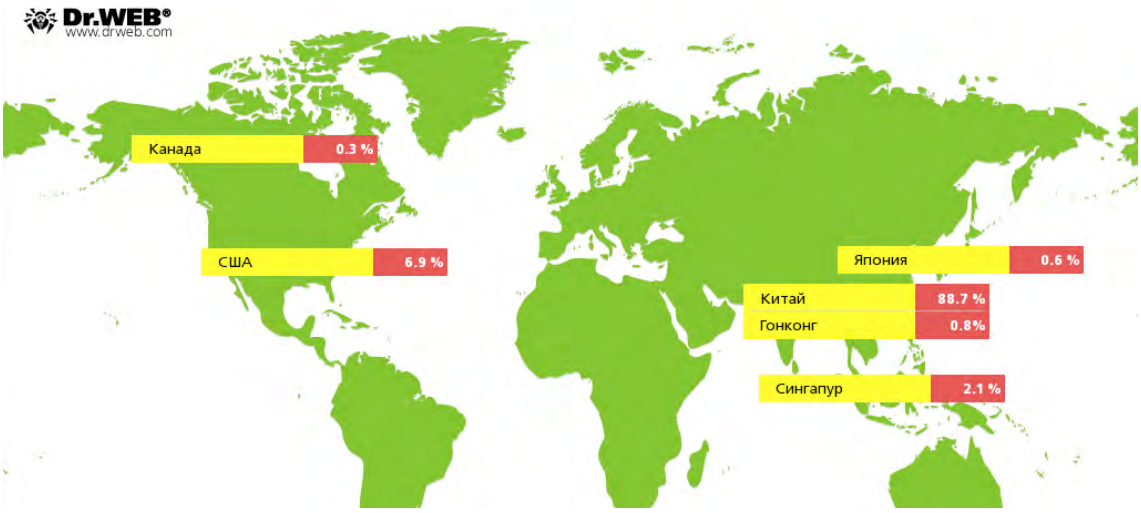
Обзор вирусной активности в ноябре 2015 года

Как и прежде, продолжает действовать бот-сеть, созданная злоумышленниками с использованием файлового вируса Win32.Sector. График среднесуточной активности этого ботнета показан на следующей иллюстрации:

Данная вредоносная программа обладает следующими деструктивными 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.

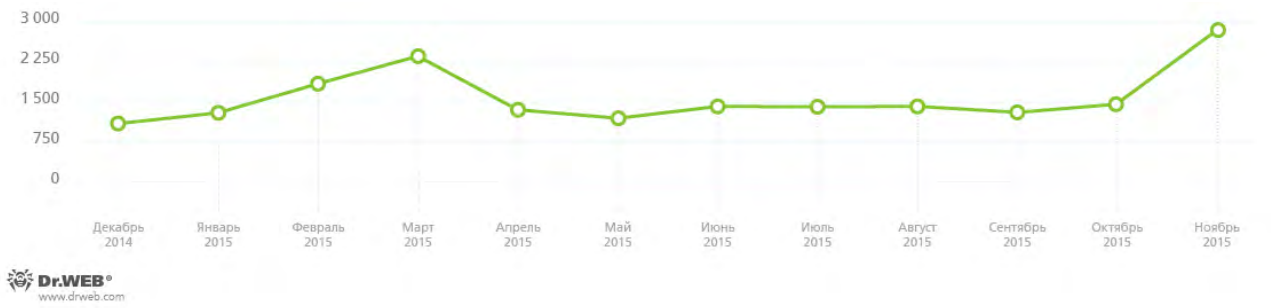
Тенденция к снижению числа DDoS-атак с использованием Linux-троянца Linux.BackDoor.Gates.5, наметившаяся еще в прошлом месяце, продолжилась и в ноябре. Количество атакованных киберпреступниками интернет-ресурсов сократилось на 27.9% и составило 3641. Абсолютным лидером по числу атак является Китай, на втором месте расположились США.



Обзор вирусной активности в ноябре 2015 года

Троянцы-шифровальщики

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



Наиболее распространенные шифровальщики в ноябре 2015 года:

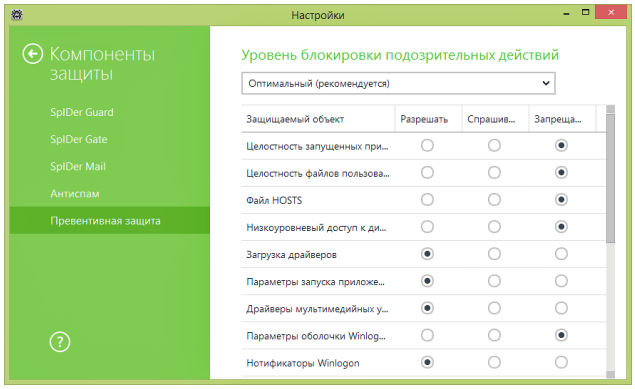
- Trojan.Encoder.2843
- Trojan.Encoder.567
- Trojan.Encoder.858

Запросы на расшифровку файлов поступают в службу технической поддержки не только из России, но и из-за рубежа. Компания «Доктор Веб» активно помогает пользователям европейских стран, пострадавшим от троянцев-энкодеров. Кроме того, в ноябре в службу технической поддержки компании «Доктор Веб» обращались владельцы сайтов, инфицированных шифровальщиком Linux.Encoder.1. Следует отметить, что известные на сегодняшний день утилиты, предназначенные для расшифровки поврежденных Linux.Encoder.1 файлов, не удаляют внедренный злоумышленниками на инфицированный сервер шелл-скрипт, которым они могут воспользоваться впоследствии для повторного заражения системы. Поэтому специалисты службы технической поддержки компании «Доктор Веб» помогают всем обратившимся за помощью в расшифровке файлов владельцам веб-сайтов очистить систему от посторонних вредоносных объектов и обезопасить ее от возможных атак с использованием этого скрипта в будущем.

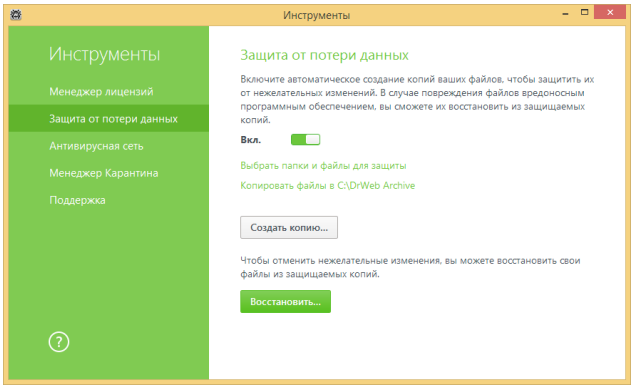
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

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

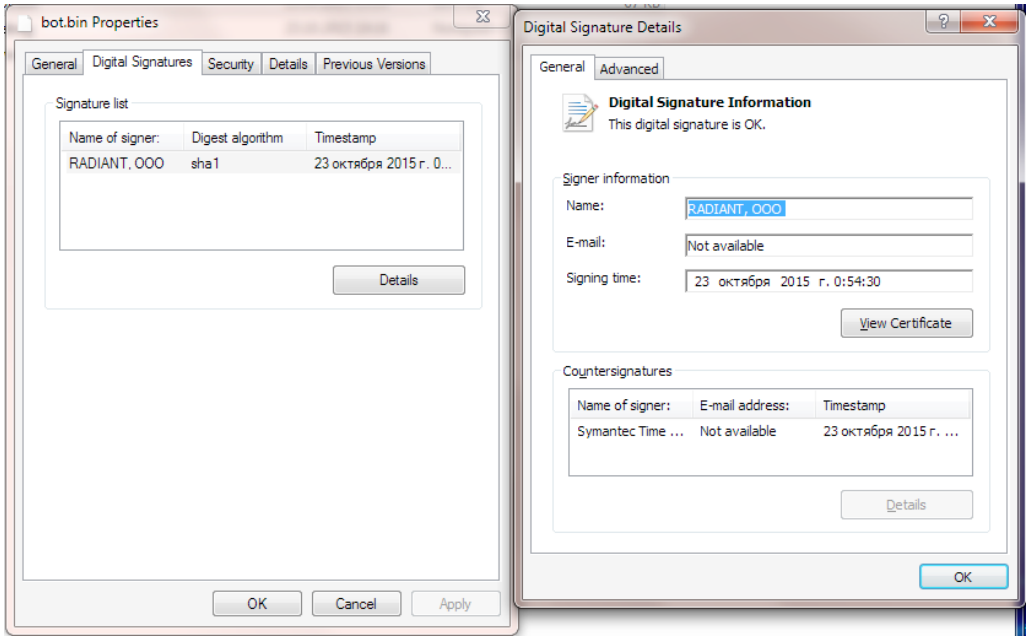
Наделавший много шума троянец-шифровальщик Linux.Encoder.1 оказался далеко не единственным энкодером, угрожающим пользователям данной операционной системы. Специалистам по информационной безопасности стало известно как минимум о двух других представителях этого семейства вредоносных программ, появившихся раньше Linux.Encoder.1, однако в течение длительного времени не попадавших в поле зрения аналитиков антивирусных компаний.

Так, троянец, получивший название Linux.Encoder.2, отличается от своих аналогов тем, что использует другой генератор псевдослучайных чисел, для шифрования применяет библиотеку OpenSSL (а не PolarSSL, как в Linux.Encoder.1) и шифрует данные в режиме AES-OFB-128. При этом происходит повторная инициализация контекста каждые 128 байт, то есть через 8 блоков AES. Также в Linux.Encoder.2 имеется ряд других существенных отличий от альтернативной реализации этого энкодера. Более подробную информацию об этой вредоносной программе можно почерпнуть в опубликованной нами статье.

Кроме того, в ноябре вирусные аналитики компании «Доктор Веб» обнаружили троянца Linux.Sshcrack.1, предназначенного для получения несанкционированного доступа к различным устройствам путем подбора логина и пароля по словарю (брутфорс).

Другие вредоносные программы

В середине ноября специалисты «Доктор Веб» исследовали целый пакет вредоносных программ, получивших общее наименование BackDoor.RatPack. Киберпреступники распространяли его в виде документа в формате RTF, при попытке открыть который на компьютере жертвы расшифровывался и сохранялся вредоносный файл. Примечательно, что этот файл, представляющий собой программу-установщик, имеет действительную цифровую подпись (как, впрочем, почти все файлы из комплекта BackDoor.RatPack).



При запуске инсталлятор пытается выявить присутствие на атакуемом компьютере виртуальных машин, программ-мониторов и отладчиков, после чего проверяет наличие в системе программ «банк-клиент» нескольких российских кредитных организаций. Полезной нагрузкой установщика является несколько вариантов вполне легальной условно-бесплатной утилиты Remote Office Manager — специалисты компании «Доктор Веб» зафиксировали как минимум три таких варианта с разными конфигурационными настройками. С помощью перехвата ряда системных функций вредоносная программа скрывает значки этой утилиты в области уведомлений и панели задач Windows, чтобы пользователь не мог вовремя ее обнаружить. Можно предположить, что с применением BackDoor.RatPack злоумышленники пытаются получить доступ к банковским счетам и конфиденциальной информации жертв путем удаленного управления зараженным компьютером. Подробности об этом инциденте – в опубликованной на сайте компании «Доктор Веб» информационной статье.

Обзор вирусной активности в ноябре 2015 года

Опасные сайты

В течение ноября 2015 года в базу нерекомендуемых и вредоносных сайтов было добавлено 670 545 интернет-адресов.

Октябрь 2015	Ноябрь 2015	Динамика
+ 264 970	+ 670 545	+ 153 %

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для Android

Последний осенний месяц оказался относительно спокойным для владельцев мобильных устройств. Тем не менее, в ноябре киберпреступники не оставляли попыток заразить смартфоны и планшеты разнообразным вредоносным и нежелательным ПО, которое оперативно вносилось в вирусную базу Dr.Web. В частности, вирусные аналитики компании «Доктор Веб» выявили весьма неприятное рекламное Android-приложение, которое устанавливалось в систему при помощи троянца и демонстрировало навязчивые уведомления поверх запускаемых пользователями программ. Также в течение всего месяца владельцам Android-смартфонов и планшетов угрожали троянцы-вымогатели, банкеры, СМС-троянцы и другие опасные приложения. Помимо этого в ноябре был обнаружен очередной вариант троянца, заражающего устройства под управлением iOS.

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

- Обнаружение нежелательного Android-приложения, которое демонстрировало рекламу поверх окон запускаемых пользователем программ
- Обнаружение новой модификации опасного троянца для iOS

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

Обзор вирусной активности в ноябре 2015 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