Dr.WEB®
с 1992 года

Обзор вирусной активности в апреле 2015 года

Обзор вирусной активности в апреле 2015 года

30 апреля 2015 года

В апреле 2015 года произошло сразу несколько ярких событий в сфере информационной безопасности.

Главные тенденции апреля

- Попытки злоумышленников осуществить таргетированную атаку на несколько российских оборонных предприятий.
- Появление нового многокомпонентного банковского троянца, представляющего угрозу для клиентов ряда кредитных организаций.
- Распространение опасных бэкдоров для ОС Windows и Linux.
- Появление новых вредоносных программ для мобильной платформы Google Android.

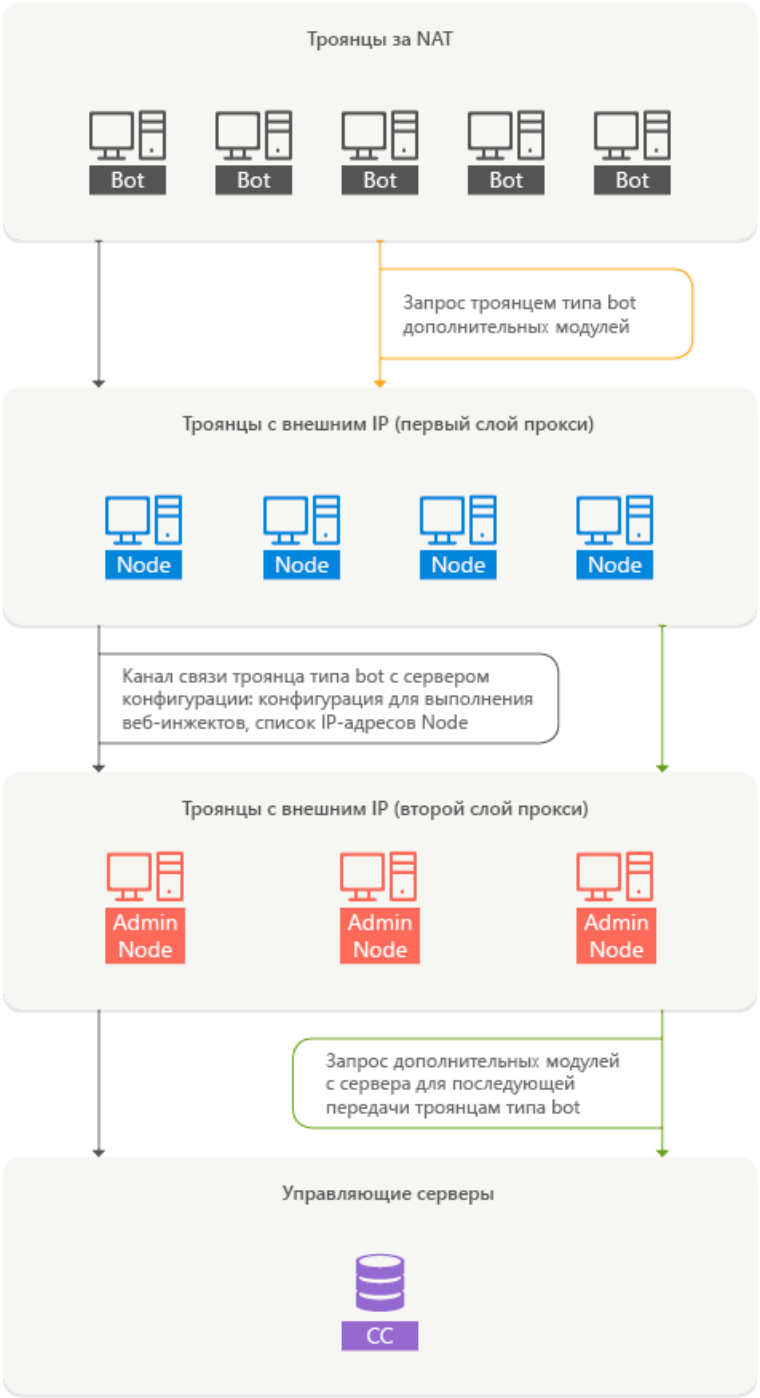
Угроза месяца

В начале апреля специалисты компании «Доктор Веб» завершили исследование опасного многокомпонентного банковского троянца, получившего название Trojan.Dridex.49. Данная вредоносная программа состоит из компонента, формирующего конфигурационные данные, необходимые для работы троянца, и запускающего саму вредоносную программу, ядра и дополнительных модулей. Характерной особенностью данного троянца является то, что для связи с управляющим сервером он использует P2P-протокол.

В зависимости от заданных параметров Trojan.Dridex.49 встраивается в процессы Проводника (explorer.exe) или браузеров (chrome.exe, firefox.exe, iexplore.exe). Все сообщения, которыми он обменивается с управляющим сервером, шифруются. На инфицированном компьютере эта вредоносная программа может играть одну из трех возможных ролей:

- bot — так называется троянец, работающий на компьютере, не имеющем внешнего IP-адреса;
- node — троянцы на компьютерах с внешним IP, принимающие сообщения от троянцев первого типа и передающие их троянцам третьего типа;
- admin node — троянцы на компьютерах с внешним IP, передают сообщения от троянцев второго типа другим admin node или на управляющий сервер.

Иными словами, для обмена сообщениями ботнет Trojan.Dridex.49 использует цепочку вида bot -> node -> admin node -> другие admin node -> управляющий сервер.
Для обеспечения безопасности соединения троянцы осуществляют обмен ключами.
В целом схема взаимодействия внутри бот-сети выглядит следующим образом:



Обзор вирусной активности в апреле 2015 года

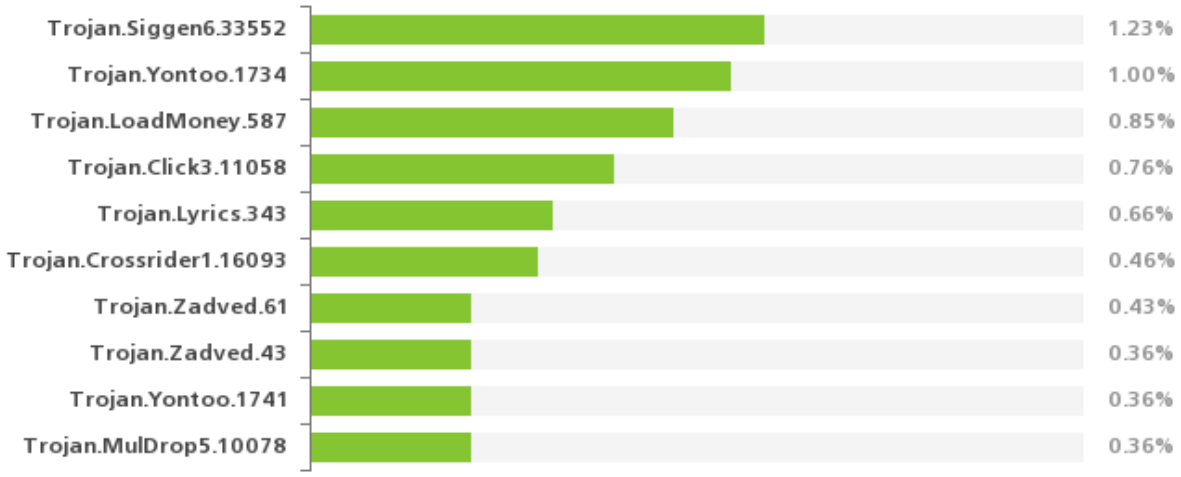
Основное предназначение **Trojan.Dridex.49** заключается в выполнении веб-инжектов, то есть встраивании постороннего содержимого в просматриваемые пользователем страницы различных финансовых организаций.

Троянец может похищать вводимые пользователем в различные формы конфиденциальные данные и позволяет злоумышленникам получить доступ к банковским счетам жертвы с целью кражи хранящихся там средств. Специалистам компании «Доктор Веб» известно более 80 банковских сайтов и других интернет-ресурсов, на которых **Trojan.Dridex.49** может красть информацию, среди них – такие известные финансовые организации, как Royal Bank of Scotland, TCB, Santander, Bank of Montreal, Bank of America, HSBC, Lloyds Bank, Barclays и многие другие. Сигнатура Trojan.**Dridex.49** добавлена в вирусные базы, поэтому пользователи антивирусных продуктов Dr.Web защищены от действия данной вредоносной программы.

По данным статистики лечащей утилиты Dr.Web CureIt!

Всего в течение месяца выявлено 73 149 430 вредоносных и потенциально опасных объектов.

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



Dr.WEB®
www.drweb.com

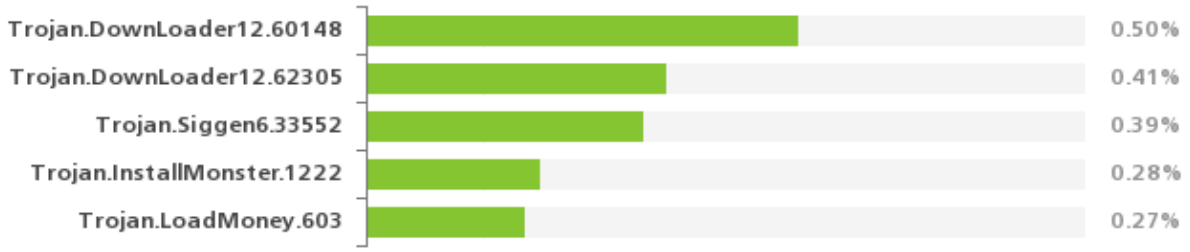
Обзор вирусной активности в апреле 2015 года

- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.Yontoo**
  Семейство надстроек для популярных браузеров, назначение которых заключается в демонстрации пользователю рекламы при просмотре веб-страниц.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Click**
  Семейство вредоносных программ, предназначенных для накрутки посещаемости различных интернет-ресурсов путем перенаправления запросов жертвы на определенные сайты с помощью управления поведением браузера.
- **Trojan.Lyrics**
  Семейство троянцев, способных демонстрировать на экране назойливую рекламу и открывать в окне браузера веб-сайты сомнительного содержания без ведома пользователя.
- **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.MulDrop5.10078**
  Устанавливает на инфицированный компьютер различные нежелательные и рекламные приложения.
- **Trojan.Crossrider1.16093**
  Троянская программа, предназначенная для демонстрации пользователям Интернета различной сомнительной рекламы.

Обзор вирусной активности в апреле 2015 года

По данным серверов статистики «Доктор Веб»

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

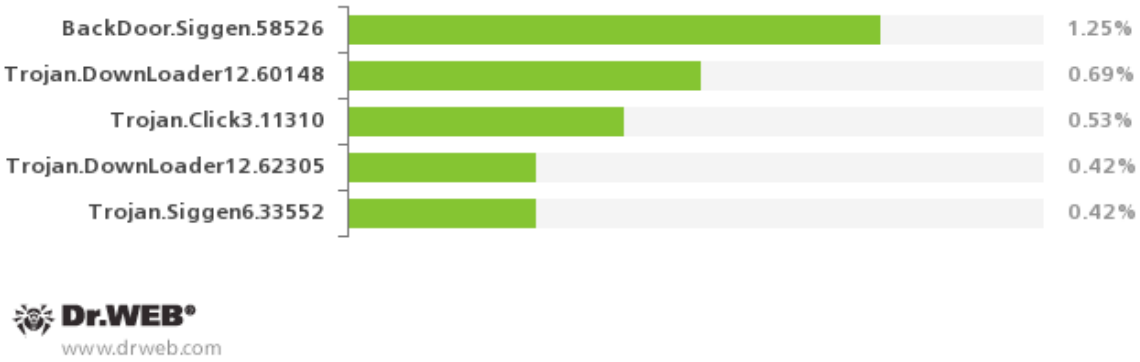


Dr.WEB®
www.drweb.com

- **Trojan.DownLoader**
  Семейство вредоносных программ, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Installmonster**
  Семейство вредоносных программ, созданных с использованием партнерской программы Installmonster. Данные приложения устанавливают на компьютер жертвы различное нежелательное ПО.

Статистика вредоносных программ в почтовом трафике

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

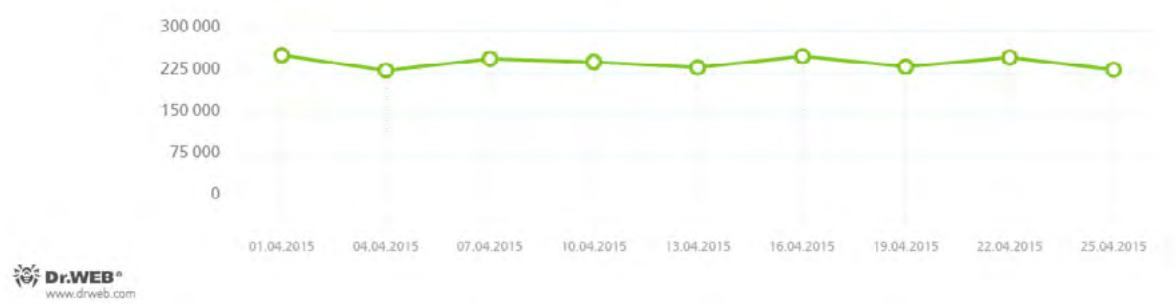


- **BackDoor.Siggen.58526**
  Троянец, способный без ведома пользователей загружать и запускать на инфицированном компьютере другие вредоносные программы, а также выполнять поступающие от злоумышленников команды.
- **Trojan.DownLoader**
  Семейство вредоносных программ, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Click**
  Семейство вредоносных программ, предназначенных для накрутки посещаемости различных интернет-ресурсов путем перенаправления запросов жертвы на определенные сайты с помощью управления поведением браузера.
- **Trojan.Siggen6.33552**
  Детект вредоносной программы, предназначенной для установки другого опасного ПО.

Ботнеты

Специалисты компании «Доктор Веб» продолжают отслеживать деятельность бот-сети, созданной злоумышленниками с использованием файлового вируса **Win32.Rmnet.12.**

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



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.

По-прежнему продолжает функционировать бот-сеть, состоящая из компьютеров, инфицированных файловым вирусом **Win32.Sector.** Данная вредоносная программа обладает следующими 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.

Обзор вирусной активности в апреле 2015 года

Активность ботнета Win32.Sector в апреле 2015 года

Количество компьютеров Apple, инфицированных троянской программой **BackDoor.Flashback.39**, остается практически неизменным и составляет порядка 25 000:

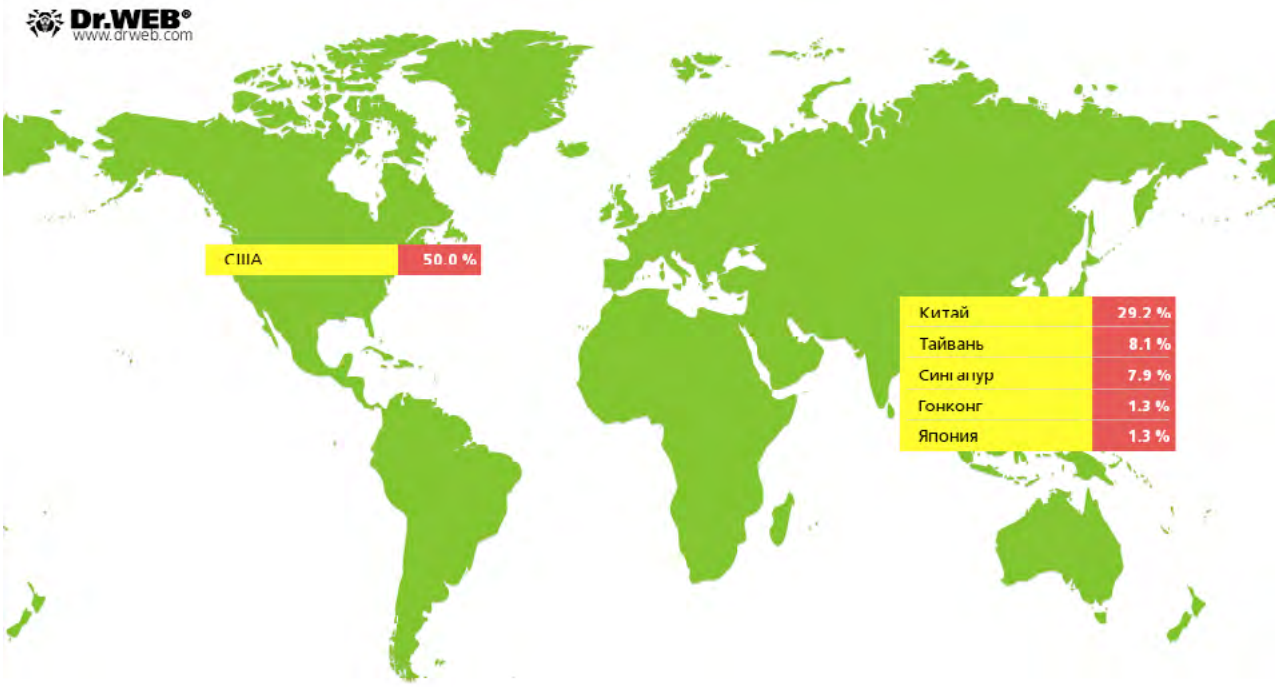
Активность ботнета BackDoor.Flashback. в апреле 2015 года

BackDoor.Flashback.39

Троянская программа для Mac OS X, получившая массовое распространение в апреле 2012 года. Заражение осуществлялось с использованием уязвимостей Java. Предназначение троянца — загрузка и запуск на инфицированной машине полезной нагрузки, в качестве которой может выступать любой исполняемый файл, указанный в полученной троянцем от злоумышленников директиве.

Обзор вирусной активности в апреле 2015 года

В апреле активизировались атаки на различные интернет-ресурсы, осуществляемые злоумышленниками с использованием троянца **Linux.BackDoor.Gates.5.** По сравнению с прошлым месяцем число уникальных IP-адресов, на которые осуществлялись атаки, выросло более чем на 48% и составило 3320. Любопытно, что если ранее основные цели злоумышленников располагались на территории Китая, то сейчас в лидеры по этому показателю вышли США. Географическое распределение этих атак показано на следующей иллюстрации:



Троянцы-шифровальщики

Всего в течение месяца выявлено 73 149 430 вредоносных и потенциально опасных объектов.

Март 2015	Апрель 2015	Динамика
2 361	1 359	- 42.4 %

Обзор вирусной активности в апреле 2015 года

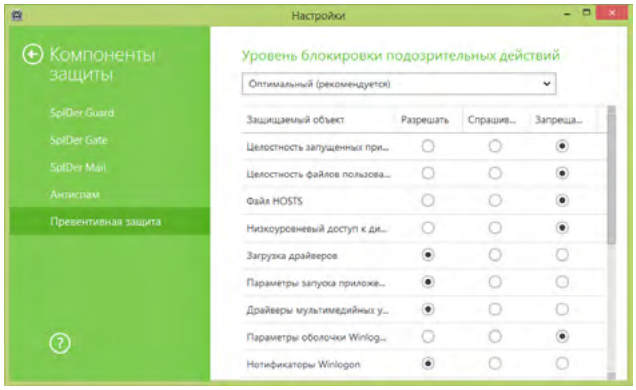
Наиболее распространенные шифровальщики в апреле 2015 года:

- Trojan.Encoder.761;
- Trojan.Encoder.567;
- Trojan.Encoder.741;
- Trojan.Encoder.888;
- BAT.Encoder.

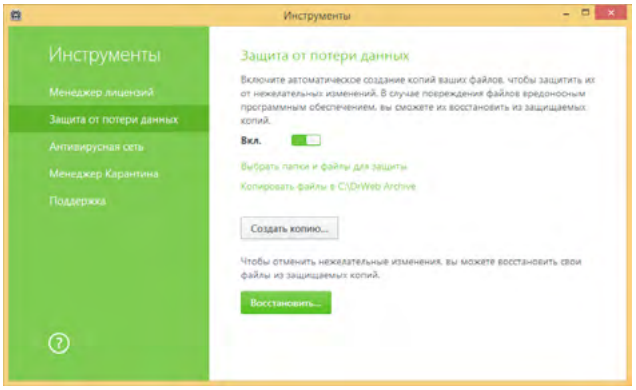
Dr.Web Security Space 10.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Обзор вирусной активности в апреле 2015 года

Угрозы для Linux

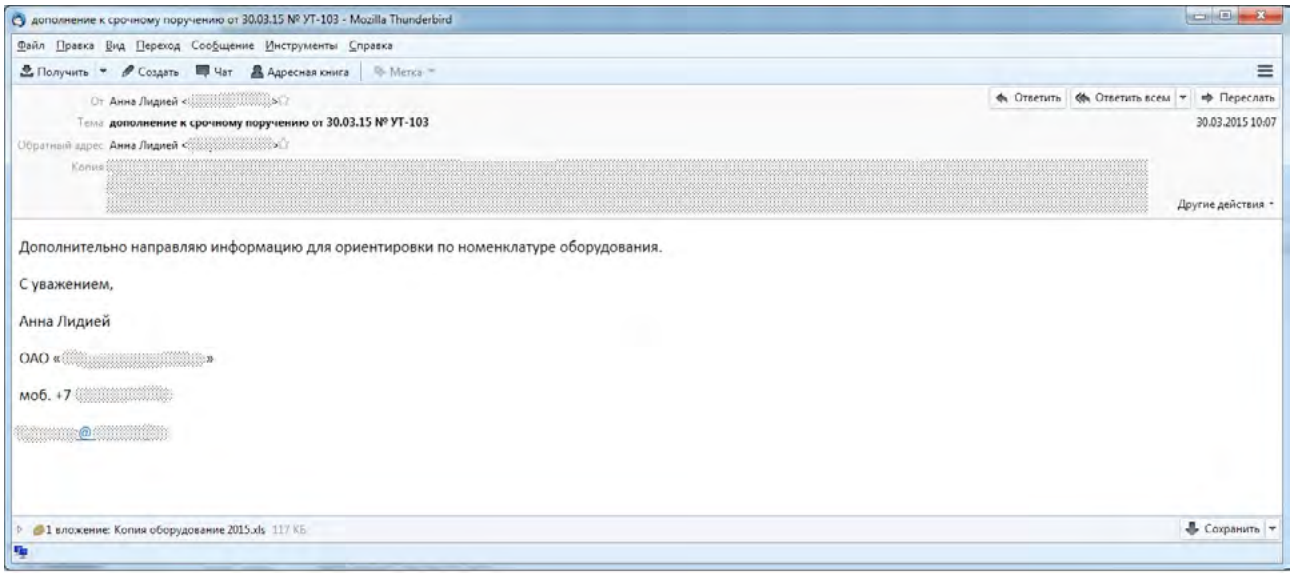
В апреле специалисты компании «Доктор Веб» исследовали нового троянца, способного заражать операционные системы семейства Linux — **Linux.BackDoor.Sessox.1**. Злоумышленники могут управлять этим бэкдором с помощью протокола для обмена текстовыми сообщениями IRC (Internet Relay Chat), — бот получает команды от вирусописателей в работающем на принадлежащем им сервере чате. Троянец распространяется, сканируя удаленные серверы на предмет уязвимости с целью запустить на незащищенном сервере сторонний скрипт, который, в свою очередь, может установить в скомпрометированной системе копию троянца.

Вредоносная программа способна атаковать заданный киберпреступниками веб-узел путем отправки на него повторяющихся GET-запросов.

Подробное описание Linux.BackDoor.Sessox.1

Другие события апреля

В начале месяца специалисты компании «Доктор Веб» зафиксировали целенаправленную почтовую рассылку по личным и служебным адресам сотрудников ряда российских оборонных предприятий, с помощью которой злоумышленники распространяли опасного троянца.



Обзор вирусной активности в апреле 2015 года

Вредоносная программа, получившая наименование **BackDoor.Hser.1**, способна по команде передать на удаленный сервер список активных процессов на зараженном ПК, загрузить и запустить другое вредоносное приложение, а также открыть командную консоль и выполнить перенаправление ввода-вывода на принадлежащий киберпреступникам сервер, благодаря чему злоумышленники получают возможность дистанционного управления инфицированным компьютером. Более подробные сведения об этом инциденте изложены в соответствующем новостном материале.

Также в апреле была исследована новая вредоносная программа **VBS.BackDoor.DuCk.1**, способная выполнять поступающие от злоумышленников команды и передавать на удаленный сервер сделанные на инфицированном компьютере снимки экрана. Бэкдор обладает механизмами проверки наличия на атакуемом компьютере виртуальной среды и антивирусных приложений. Статья, посвященная этому опасному троянцу, опубликована на сайте компании «Доктор Веб».

Опасные сайты

В течение апреля 2015 года в базу нерекомендуемых и вредоносных сайтов Dr.Web было добавлено 129 199 интернет-адресов.

Март 2015	Апрель 2015	Динамика
74 108	129 199	+ 74.3%

Нерекомендуемые сайты

Вредоносное и нежелательное ПО для Android

В апреле злоумышленники продолжили активно атаковать пользователей мобильных Android-устройств, поэтому прошедший месяц вновь оказался насыщенным на события вирусной тематики. Наиболее заметными событиями, связанными с вредоносным и нежелательным ПО для ОС Android, стали:

- обнаружение опасного троянца Android.**Toorch.1.origin**, способного получать root-доступ для незаметной установки и удаления приложений;
- появление в каталоге Google play очередных программ с агрессивным рекламным модулем;
- высокая активность банковских троянцев.

Обзор вирусной активности в апреле 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