Dr.WEB®
с 1992 года

Обзор вирусной активности в апреле 2016 года

Обзор вирусной активности в апреле 2016 года

29 апреля 2016 года

В начале апреля 2016 года вирусные аналитики компании «Доктор Веб» обнаружили новую модификацию банковского троянца Gozi, способную создавать одноранговую бот-сеть. А чуть позже был выявлен бэкдор для Linux, распространяющийся с помощью хакерской утилиты. Также в апреле активизировались сетевые мошенники, создающие фиктивные интернет-магазины с целью обмана покупателей, — от действия киберпреступников уже пострадали многие пользователи Всемирной сети.

Главные тенденции апреля

- Появление новой модификации банковского троянца Gozi
- Распространение вредоносной программы для ОС Linux
- Рост активности сетевых мошенников

Обзор вирусной активности в апреле 2016 года

Угроза месяца

Новые банковские троянцы, предназначенные для хищения денег со счетов своих жертв, появляются нечасто — вирусописатели охотнее модифицируют уже существующие и проверенные в деле вредоносные программы. Одной из таких модификаций стала новая версия троянца Trojan.Gozi, имеющего широкий спектр функциональных возможностей: он может похищать данные, которые пользователи вводят в различные экранные формы, фиксировать нажатия клавиш (кейлоггинг), умеет встраивать постороннее содержимое в веб-страницы на зараженном компьютере (то есть выполнять веб-инжекты). Кроме того, с помощью Trojan.Gozi киберпреступники могут получить удаленный доступ к рабочему столу зараженной машины с использованием технологии Virtual Network Computing (VNC). Этот троянец по команде злоумышленников может запустить на инфицированном ПК прокси-сервер SOCKS, а также загружать и устанавливать различные плагины.

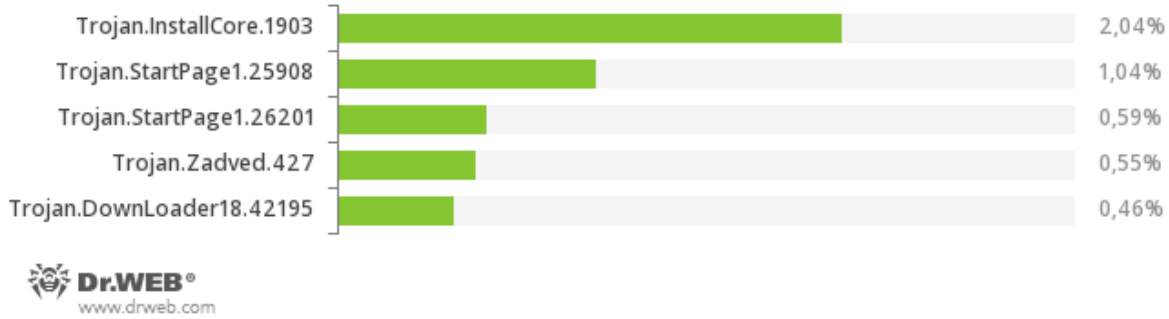
37 45.173629	95.215.111.125	10.0.4.3	UDP	840	Source port: 9772 Destination port: 13888
38 45.174357	10.0.4.3	95.215.111.125	UDP	1340	Source port: 13888 Destination port: 9772
39 45.256337	95.215.111.125	10.0.4.3	UDP	860	Source port: 9772 Destination port: 13888
40 45.261248	173.177.120.102	10.0.4.3	UDP	755	Source port: 29785 Destination port: 13888
41 45.261924	10.0.4.3	173.177.120.102	UDP	315	Source port: 13888 Destination port: 29785
42 45.489461	173.177.120.102	10.0.4.3	UDP	111	Source port: 29785 Destination port: 13888
43 46.093329	10.0.4.3	142.217.75.225	UDP	881	Source port: 13888 Destination port: 31835
44 47.094204	10.0.4.3	109.90.217.159	UDP	767	Source port: 13888 Destination port: 33600
45 52.101663	10.0.4.3	198.53.206.26	UDP	641	Source port: 13888 Destination port: 63599
46 54.104842	10.0.4.3	173.177.120.102	UDP	659	Source port: 13888 Destination port: 29785
47 54.105466	10.0.4.3	173.177.120.102	UDP	831	Source port: 13888 Destination port: 29785
48 54.106034	10.0.4.3	173.177.120.102	UDP	1164	Source port: 13888 Destination port: 29785
49 54.106651	10.0.4.3	173.177.120.102	UDP	342	Source port: 13888 Destination port: 29785
50 54.107504	10.0.4.3	173.177.120.102	UDP	467	Source port: 13888 Destination port: 29785
51 54.248506	173.177.120.102	10.0.4.3	UDP	1003	Source port: 29785 Destination port: 13888
52 54.252619	173.177.120.102	10.0.4.3	UDP	933	Source port: 29785 Destination port: 13888
53 54.256380	173.177.120.102	10.0.4.3	UDP	713	Source port: 29785 Destination port: 13888
54 54.260468	173.177.120.102	10.0.4.3	UDP	953	Source port: 29785 Destination port: 13888
55 54.264843	173.177.120.102	10.0.4.3	UDP	1200	Source port: 29785 Destination port: 13888
56 55.106104	10.0.4.3	173.183.1.166	UDP	264	Source port: 13888 Destination port: 14397
57 55.106666	10.0.4.3	184.64.213.14	UDP	798	Source port: 13888 Destination port: 12294
58 55.286556	184.64.213.14	10.0.4.3	UDP	296	Source port: 12294 Destination port: 13888
59 55.287359	10.0.4.3	184.64.213.14	UDP	887	Source port: 13888 Destination port: 12294
60 55.350810	173.183.1.166	10.0.4.3	UDP	717	Source port: 14397 Destination port: 13888
61 55.351571	10.0.4.3	173.183.1.166	UDP	1123	Source port: 13888 Destination port: 14397
62 55.468797	184.64.213.14	10.0.4.3	UDP	212	Source port: 12294 Destination port: 13888
63 55.608156	173.183.1.166	10.0.4.3	UDP	1081	Source port: 14397 Destination port: 13888
64 56.107339	10.0.4.3	50.69.165.12	UDP	495	Source port: 13888 Destination port: 48090

Однако основное отличие новой версии Trojan.Gozi от предшественников — появившаяся возможность формировать одноранговые ботнеты, то есть обмениваться данными с другими зараженными машинами напрямую, посредством создания P2P-сети. Подробнее об этой вредоносной программе читайте в обзорной статье на сайте компании «Доктор Веб».

Обзор вирусной активности в апреле 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

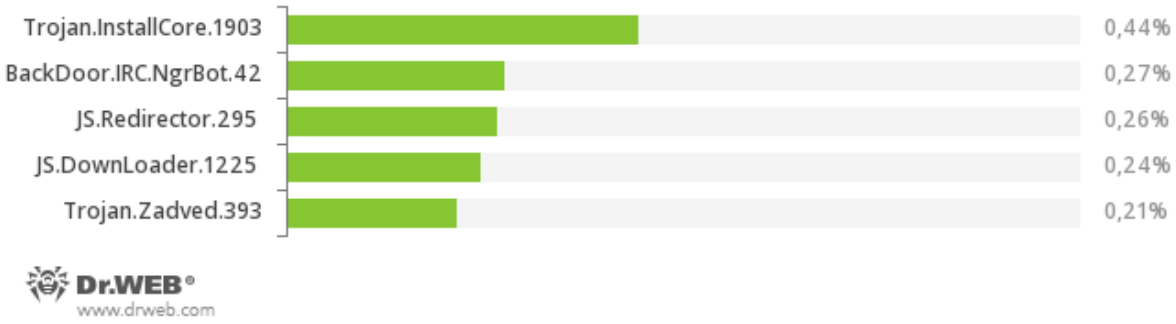


- **Trojan.InstallCore.1903**
  Представитель семейства установщиков нежелательных и вредоносных приложений.
- **Trojan.StartPage**
  Семейство вредоносных программ, способных подменять стартовую страницу в настройках браузера.
- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера 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.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.

Обзор вирусной активности в апреле 2016 года

По данным серверов статистики «Доктор Веб»

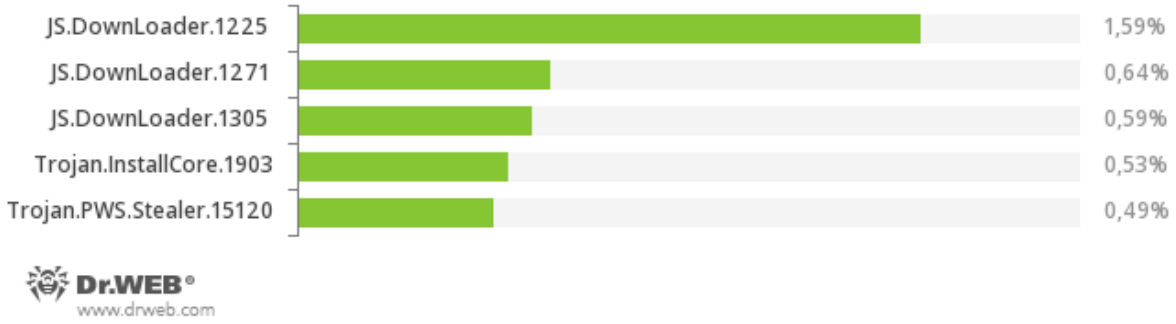
Наиболее распространенные вредоносные программы в апреле 2016 года согласно данным серверов статистики Dr.Web



- **Trojan.InstallCore.1903**
  Представитель семейства установщиков нежелательных и вредоносных приложений.
- **BackDoor.IRC.NgrBot.42**
  Довольно распространенный троянец, известный специалистам по информационной безопасности еще с 2011 года. Вредоносные программы этого семейства способны выполнять на инфицированном компьютере поступающие от злоумышленников команды, а управление ими киберпреступники осуществляют с использованием протокола обмена текстовыми сообщениями IRC (Internet Relay Chat).
- **JS.Redirector**
  Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для перенаправления пользователей браузеров на различные (в том числе вредоносные и мошеннические) веб-страницы.
- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для загрузки и установки на компьютер других вредоносных программ.
- **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 апреле 2016 года

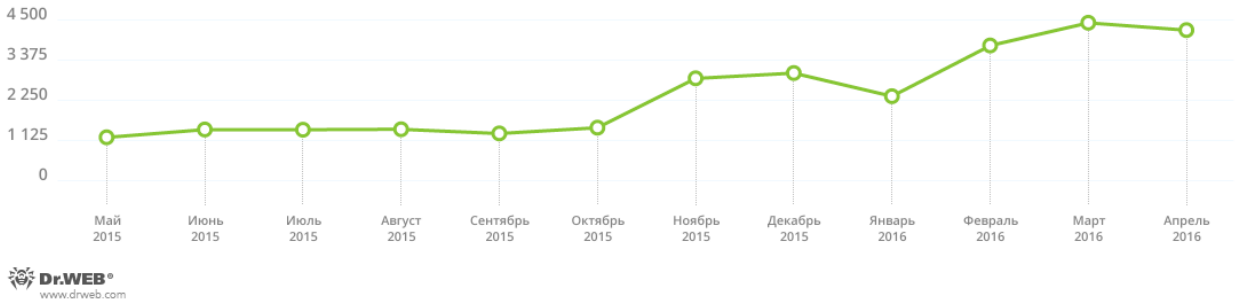


- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для загрузки и установки на компьютер других вредоносных программ.
- **Trojan.InstallCore.1903**
  Представитель семейства установщиков нежелательных и вредоносных приложений.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Обзор вирусной активности в апреле 2016 года

Троянцы-шифровальщики

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



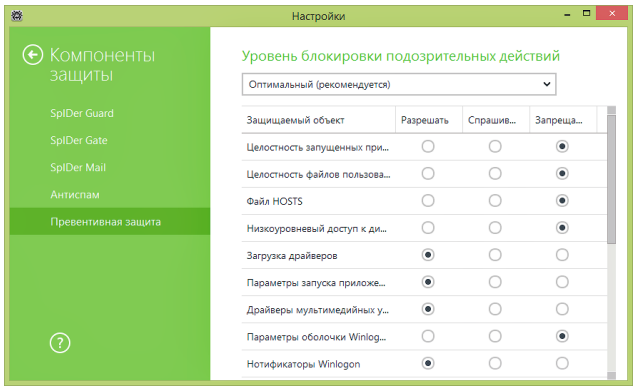
Наиболее распространенным шифровальщиком в апреле 2016 года является

- Trojan.Encoder.858

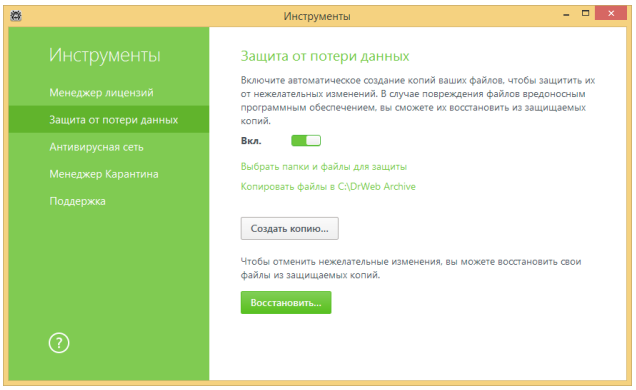
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



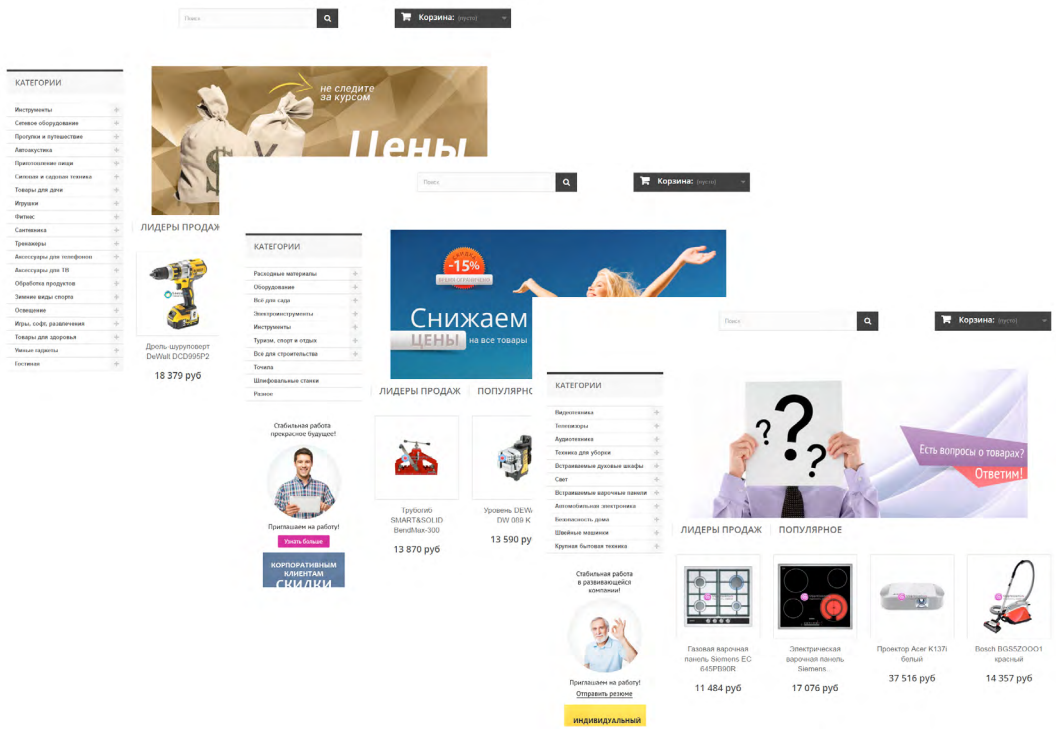
Подробней Смотрите видео о настройке

Опасные сайты

В течение апреля 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 749 173 интернет-адреса.

Март 2016	Апрель 2016	Динамика
+ 458 013	+ 749 173	+63,6%

В апреле заметно активизировались сетевые мошенники, создающие фиктивные интернет-магазины с целью обмануть доверчивых пользователей Интернета. Такие сайты имеют практически все элементы, традиционно присутствующие на страницах онлайн-магазинов, однако сделаны они все с использованием одного и того же стандартного шаблона.



О том, каким образом сетевые жулики обманывают своих покупателей и как уберечься от этого способа мошенничества, читайте в опубликованной нами статье.

Другие события

Чтобы проникнуть в сети различных коммерческих предприятий, злоумышленники используют различные методы. Серьезной «дырой» в безопасности, которой могут воспользоваться хакеры, порой становятся неправильные настройки серверных приложений или других программных средств. В апреле 2016 года специалисты компании «Доктор Веб» обнаружили ошибку в конфигурации оборудования одной из зарубежных компаний, предоставляющих услугу DNS-хостинга. В результате клиенты этой фирмы открывали всему миру список зарегистрированных ими поддоменов, в частности используемых для внутренних целей. Такие домены могут быть задействованы, например, для организации непубличных внутренних веб-серверов, систем контроля версий, баг-трекеров, различных служб мониторинга, вики-ресурсов и т. д. С использованием подобного списка адресов злоумышленникам становится значительно проще исследовать сеть потенциальной жертвы для поиска слабых или незащищенных мест. Более подробно о расследовании этого инцидента рассказано в опубликованном на сайте компании «Доктор Веб» новостном материале.

Также в апреле было зафиксировано распространение троянца-бэкдора для ОС Linux, получившего наименование Linux.BackDoor.Xudp.1. Примечательная особенность этой вредоносной программы заключалась в том, что она проникала на компьютер жертвы при помощи хакерской утилиты, предназначенной для организации одной из разновидностей атак на удаленные узлы путем массовой отправки на заданный адрес UDP-пакетов. Иными словами, пользователь Linux, решивший атаковать какой-либо узел Интернета, сам оказывался жертвой атаки троянца.

Среди команд, которые способен выполнять Linux.BackDoor.Xudp.1, исследователи выявили приказ на непрерывную отправку заданному удаленному узлу различных запросов (флуд), осуществление DDoS-атак, выполнение произвольных команд на зараженном устройстве. Также Linux.BackDoor.Xudp.1 способен по команде сканировать порты в заданном диапазоне IP-адресов, может запускать указанные злоумышленником файлы, выслать им какой-либо файл, а также выполнять иные задачи. О других особенностях работы этого бэкдора можно прочитать в соответствующей информационной статье.

В самом конце апреля была зафиксирована атака на пользователей социальной сети Facebook — вредоносная программа Trojan.BPlug.1074, представляющая собой плагин для браузера Google Chrome, рассылала спам в этой социальной сети. Также с ее помощью злоумышленники распространяли другие опасные надстройки для Chrome. По информации, имеющейся у аналитиков «Доктор Веб», на 29 апреля Trojan.BPlug.1074 загрузили более 12 000 пользователей Facebook. Подробная информация об этом инциденте изложена в опубликованном на сайте «Доктор Веб» новостном материале.

Вредоносное и нежелательное ПО для мобильных устройств

Согласно статистике, собранной с использованием антивирусных продуктов Dr.Web для Android, в апреле наблюдалась активность агрессивных рекламных платформ – в прошедшем месяце они обнаруживались чаще других вредоносных и нежелательных программ. Зачастую такие программные модули могут не только показывать навязчивую рекламу, но и красть конфиденциальную информацию, а также загружать и устанавливать всевозможное ПО, принося неплохую прибыль вирусописателям. Кроме того, в апреле специалисты компании «Доктор Веб» обнаружили нового троянца Android.GPLoader.1.origin, предназначенного для несанкционированной установки приложений.

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

- активность агрессивных рекламных модулей для ОС Android;
- обнаружение нового троянца, способного устанавливать программы без участия пользователя.

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

Обзор вирусной активности в апреле 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