Dr.WEB®
с 1992 года

Обзор вирусной активности в мае 2017 года

Обзор вирусной активности в мае 2017 года

31 мая 2017 года

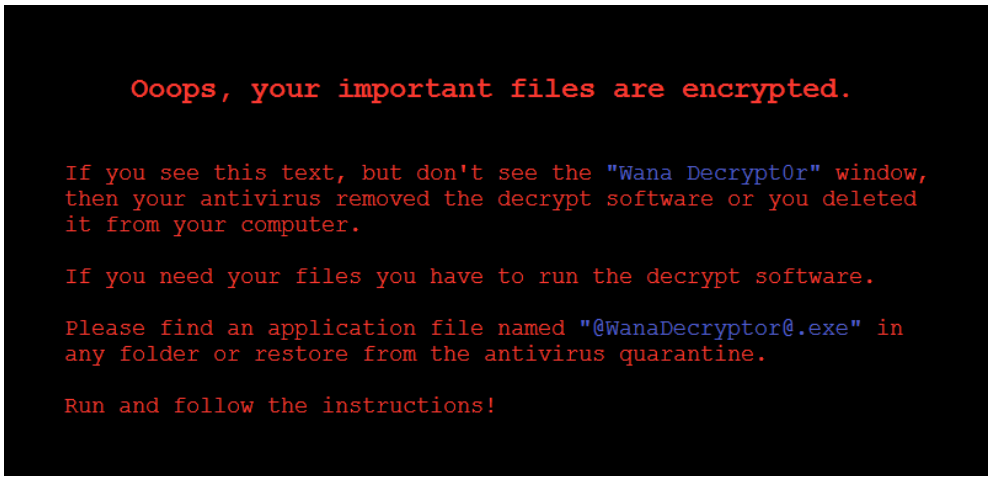
Самым значительным событием мая 2017 года стало массовое распространение вредоносной программы WannaCry, детектируемой Антивирусом Dr.Web как Trojan.Encoder.11432. Этот червь распространялся самостоятельно, заражая сетевые узлы с использованием уязвимости в протоколе SMB. Затем он шифровал файлы на компьютере своей жертвы и требовал выкуп за расшифровку. Кроме того, в мае специалисты «Доктор Веб» исследовали сложного многокомпонентного троянца для Linux, написанного на языке Lua. Также был обнаружен новый бэкдор, угрожающий пользователям macOS.

Главные тенденции мая

- Распространение опасного шифровальщика WannaCry
- Обнаружение бэкдора для macOS
- Появление многокомпонентного троянца для ОС Linux

Угроза месяца

О вредоносной программе, получившей известность под именем WannaCry, рассказывали многие средства массовой информации. Это опасное приложение представляет собой сетевого червя, способного заражать компьютеры под управлением Microsoft Windows. Его распространение началось примерно в 10 утра 12 мая 2017 года. В качестве полезной нагрузки червь несет в себе троянца-шифровальщика. Антивирус Dr.Web детектирует все компоненты червя под именем Trojan.Encoder.11432.

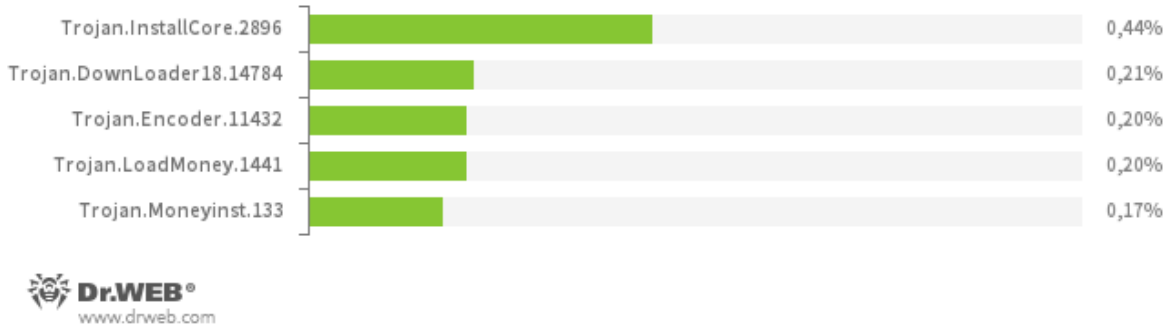


При запуске червь регистрирует себя в качестве системной службы и начинает опрашивать сетевые узлы в локальной сети и в Интернете со случайными IP-адресами. Если установить соединение удалось, червь предпринимает попытку заразить эти компьютеры. В случае успешного заражения червь запускает троянца-шифровальщика, который шифрует файлы на компьютере со случайным ключом. В процессе работы Trojan.Encoder.11432 удаляет теневые копии и отключает функцию восстановления системы. Троянец создает отдельный список файлов, которые шифруются с использованием другого ключа: их вредоносная программа может расшифровать для своей жертвы бесплатно. Поскольку эти тестовые файлы и все остальные файлы на компьютере шифруются с использованием разных ключей, нет никакой гарантии успешной расшифровки файлов даже в случае уплаты выкупа злоумышленникам. Более подробная информация об этом троянце изложена в опубликованной нами статье, а также в подробном техническом описании червя.

Обзор вирусной активности в мае 2017 года

По данным статистики Антивируса Dr.Web

Наиболее распространенные вредоносные программы согласно статистике Антивируса Dr.Web

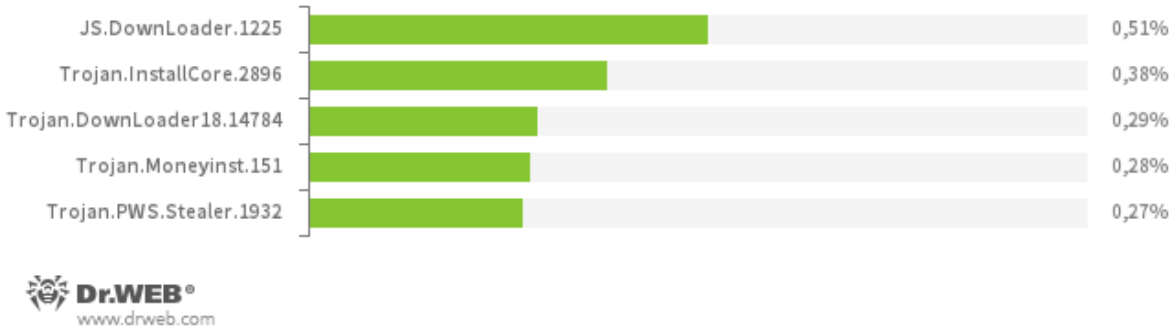


- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Encoder.11432**
  Сетевой червь, запускающий на компьютере жертвы опасного троянца-шифровальщика. Известен также под именем WannaCry.
- **Trojan.LoadMoney**
  Семейство программ-загрузчиков, генерируемых серверами партнерской программы LoadMoney. Эти приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.
- **Trojan.Moneyinst.133**
  Вредоносная программа, устанавливающая на компьютер жертвы различное ПО, в том числе других троянцев.

Обзор вирусной активности в мае 2017 года

По данным серверов статистики «Доктор Веб»

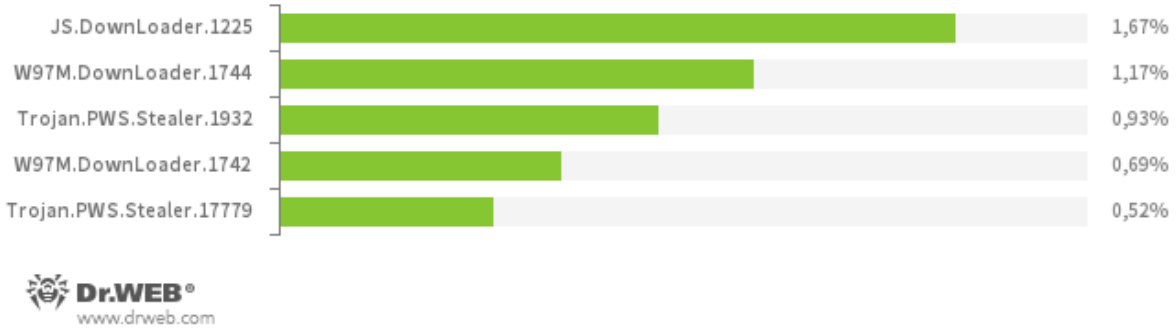
Наиболее распространенные вредоносные программы в мае 2017 года
согласно данным серверов статистики Dr.Web



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. Загружают и устанавливают на компьютер другие вредоносные программы.
- **Trojan.InstallCore**
  Семейство установщиков нежелательных и вредоносных приложений.
- **Trojan.DownLoader**
  Семейство троянцев, предназначенных для загрузки на атакуемый компьютер других вредоносных приложений.
- **Trojan.Moneyinst.151**
  Вредоносная программа, устанавливающая на компьютер жертвы различное ПО, в том числе других троянцев.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в мае 2017 года



- **JS.DownLoader**
  Семейство вредоносных сценариев, написанных на языке JavaScript. 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.
- **Trojan.PWS.Stealer**
  Семейство троянцев, предназначенных для хищения на инфицированном компьютере паролей и другой конфиденциальной информации.

Обзор вирусной активности в мае 2017 года

По данным бота Dr.Web для Telegram

- **Trojan.Encoder.11432**
  Сетевой червь, запускающий на компьютере жертвы опасного троянца-шифровальщика. Известен также под именем WannaCry.
- **Android.Locker.139.origin**
  Представитель семейства Android-троянцев, предназначенных для вымогательства. Он показывает 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.HiddenAds.24**
  Троянец, предназначенный для показа навязчивой рекламы.
- **Android.Androrat.1.origin**
  Шпионская программа, работающая на устройствах под управлением ОС Android.
- **BackDoor.Bifrost.29284**
  Представитель семейства троянцев-бэкдоров, способных выполнять на зараженной машине поступающие от злоумышленников команды.

Обзор вирусной активности в мае 2017 года

Трояны-шифровальщики

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

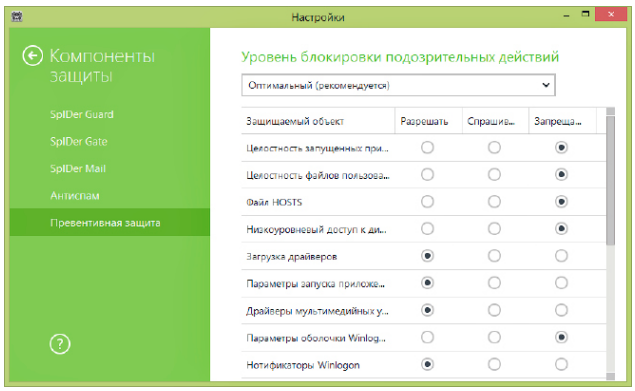
В мае в службу технической поддержки компании «Доктор Веб» чаще всего обращались пользователи, пострадавшие от следующих модификаций троянцев-шифровальщиков:

- **Trojan.Encoder.858** — 14,39% обращений;
- **Trojan.Encoder.11432** — 8.36% обращений;
- **Trojan.Encoder.3953** — 7.41% обращений;
- **Trojan.Encoder.761** — 2.62% обращений;
- **Trojan.Encoder.10144** — 2.60% обращений;
- **Trojan.Encoder.567** — 2.47% обращений.

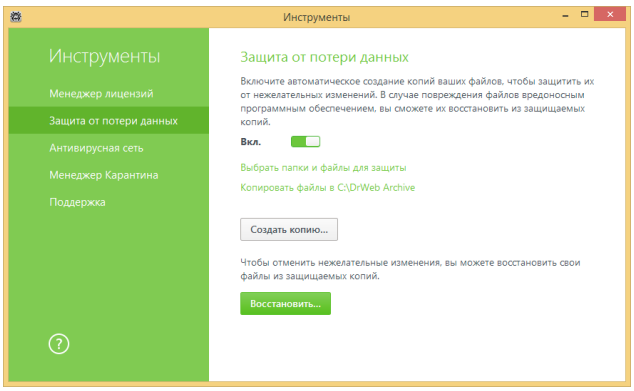
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Опасные сайты

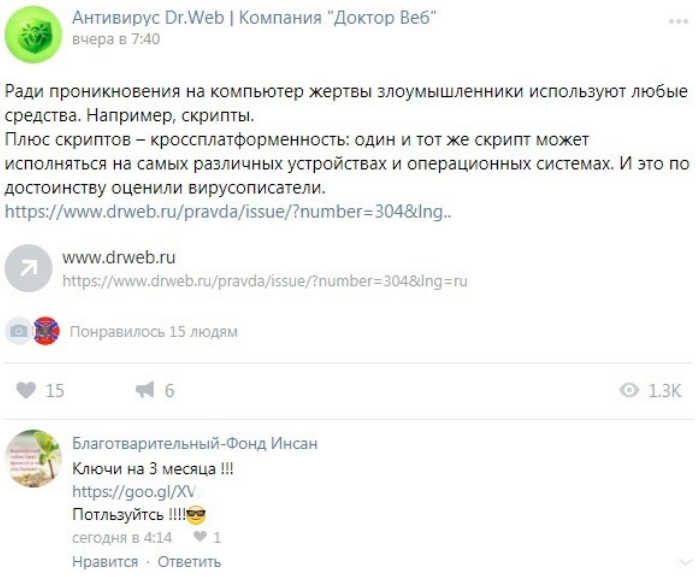
В течение мая 2017 года в базу нерекомендуемых и вредоносных сайтов было добавлено 1 129 277 интернет-адресов.

Апрель 2017	Май 2017	Динамика
+ 568 903	+ 1 129 277	+ 98.5%

Нерекомендуемые сайты

Другие события в сфере информационной безопасности

В начале мая был обнаружен троянец, распространявшийся по ссылкам в комментариях, которые злоумышленники оставляли в официальной группе компании «Доктор Веб» в социальной сети «ВКонтакте». В своих сообщениях киберпреступники предлагали желающим скачать бесплатные ключи к антивирусу Dr.Web, однако в действительности при переходе по ссылке на компьютер жертвы загружался троянец Trojan.MulDrop7.26387.

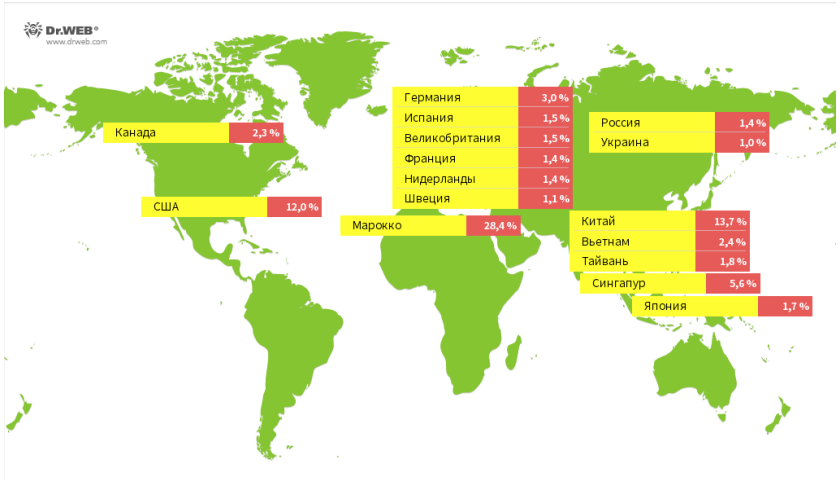


Эта вредоносная программа может выполнять различные команды злоумышленников: например, менять обои Рабочего стола Windows, открывать и закрывать лоток оптического привода, менять местами функции кнопок мыши, воспроизвести с помощью динамиков заданную фразу, используя голосовой синтезатор, или даже продемонстрировать на экране компьютера пугающие видеоролики. Подробности об этом инциденте изложены в опубликованной на нашем сайте статье.

Вредоносные программы для Linux

В мае вирусные аналитики компании «Доктор Веб» исследовали многокомпонентного троянца для ОС Linux, написанного на языке Lua. Эта вредоносная программа, получившая имя Linux.LuaBot, состоит из 31 Lua-сценария и может заражать не только компьютеры, но и различные «умные» устройства: сетевые хранилища, роутеры, телевизионные приставки, IP-камеры, и т. д. Троянец генерирует список IP-адресов, которые будет атаковать, а затем пытается соединиться с удаленными устройствами по созданному списку и авторизоваться путем перебора логинов и паролей по словарю. В случае успеха он загружает на инфицированное устройство свою копию и запускает ее.

Этот троянец фактически является бэкдором – то есть способен выполнять поступающие от злоумышленников команды. Кроме того, он запускает на зараженном устройстве веб-сервер, позволяющий злоумышленникам скачивать и загружать различные файлы. Вирусные аналитики «Доктор Веб» собрали статистику об уникальных IP-адресах устройств, зараженных Linux.LuaBot, – они представлены на следующей иллюстрации.



Более подробную информацию об этом многокомпонентном троянце можно получить, ознакомившись с нашей новостью или подробным техническим описанием вредоносной программы.

Вредоносные программы для Linux

Последний весенний месяц 2017 года ознаменовался распространением бэкдора для macOS. Троянец был добавлен в вирусные базы Dr.Web под именем Mac.BackDoor.Systemd.1. Бэкдор способен выполнять следующие команды:

- получить список содержимого заданной директории;
- прочитать файл;
- записать в файл;
- получить содержимое файла;
- удалить файл или папку;
- переименовать файл или папку;
- изменить права для файла или папки (команда chmod);
- изменить владельца файлового объекта (команда chown);
- создать папку;
- выполнить команду в оболочке bash;
- обновить троянца;
- переустановить троянца;
- сменить IP-адрес управляющего сервера;
- установить плагин.

Более подробные сведения об этой вредоносной программе изложены в опубликованной на нашем сайте статье.

Вредоносное и нежелательное ПО для мобильных устройств

В мае в каталоге Google Play был обнаружен троянец Android.RemoteCode.28, который скачивал другие программы и передавал на управляющий сервер конфиденциальную информацию. Кроме того, в каталоге были выявлены приложения, скрывающие в себе троянца Android.Spy.308.origin. Он загружал и запускал дополнительные программные модули, а также показывал рекламу. В минувшем месяце вирусописатели под видом MMC-сообщений распространяли банковского троянца Android.BankBot.186.origin, крадущего деньги со счетов пользователей.

- обнаружение Android-троянцев в каталоге Google Play;
- распространение банковского троянца, который незаметно переводил деньги пользователей на счета киберпреступников.

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

Обзор вирусной активности в мае 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