Dr.WEB®
с 1992 года

Обзор вирусной активности в мае 2016 года

Обзор вирусной активности в мае 2016 года

31 мая 2016 года

Последний весенний месяц 2016 года был отмечен распространением нового бэкдора, предназначенного для слежки за пользователями Microsoft Windows, и прежде всего — для кражи с зараженных компьютеров различных документов. Не снижается активность злоумышленников, создающих вредоносные программы для мобильной платформы Android: в мае вирусные аналитики зафиксировали всплеск распространения мобильных банковских троянцев. Также специалисты «Доктор Веб» исследовали троянца, реализующего на инфицированной машине функции прокси-сервера.

Главные тенденции мая

- Появление опасного троянца-шпиона для Windows
- Появление троянца, превращающего зараженный компьютер в прокси-сервер
- Распространение банковских троянцев для ОС Android

Обзор вирусной активности в мае 2016 года

Угроза месяца

Троянцы-шпионы представляют особую опасность, поскольку способны похищать конфиденциальную информацию, представляющую высокую ценность для пользователей. Одной из таких вредоносных программ является троянец BackDoor.Apper.1, исследованный специалистами «Доктор Веб» в начале мая.

Этот бэкдор распространяется с помощью дроппера, представленного в виде документа Microsoft Excel, в который встроен специальный макрос. Макрос собирает по байтам и запускает самораспаковывающийся архив. В архиве, в свою очередь, содержится исполняемый файл, позаимствованный злоумышленниками из комплекта поставки популярного продукта корпорации Symantec. Этот файл имеет действительную цифровую подпись Symantec и в момент своего запуска загружает в память компьютера динамическую библиотеку, где и реализованы основные вредоносные функции троянца.

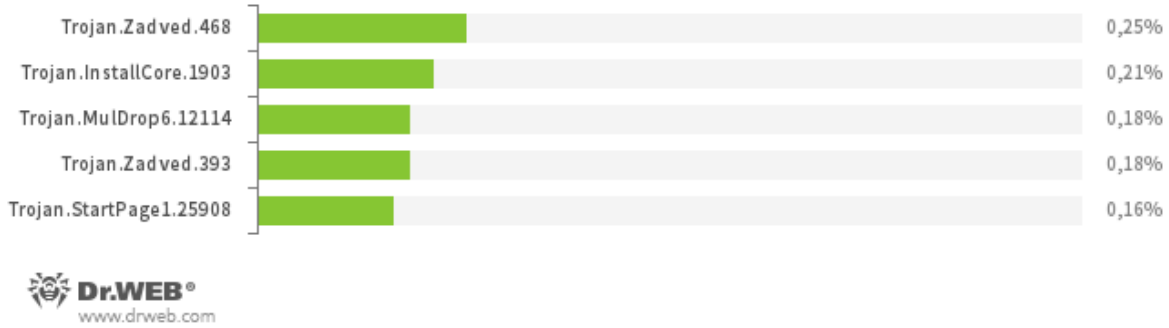
```
signed int __usercall sub_401940@<eax>(int a1@<esi>)
{
  HMODULE v1; // eax@1
  HMODULE v2; // eax@2
  FARPROC v3; // eax@3
  FARPROC v4; // eax@4
  FARPROC v5; // eax@5
  FARPROC v6; // eax@6
  WCHAR wnd_dir[260]; // [esp+8h] [ebp-414h]@1
  WCHAR LibFileName; // [esp+210h] [ebp-20Ch]@2

  GetWindowsDirectoryW(wnd_dir, 0x104u);
  v1 = LoadLibraryW(L"RasTls.dll");
  *(_DWORD *)(a1 + 4) = v1;
  if ( v1
    || (swprintf_s(&LibFileName, 0x104u, L"%s\\system32\\%s", wnd_dir, L"RasTls.dll"),
        v2 = LoadLibraryW(&LibFileName),
        (*(_DWORD *)(a1 + 4) = v2) != 0) )
  {
    v3 = GetProcAddress(*(HMODULE *)(a1 + 4), "RasEapGetInfo");
    *(_DWORD *)(a1 + 12) = v3;
    if ( v3 )
    {
      v4 = GetProcAddress(*(HMODULE *)(a1 + 4), "RasEapFreeMemory");
      *(_DWORD *)(a1 + 20) = v4;
      if ( v4 )
      {
        v5 = GetProcAddress(*(HMODULE *)(a1 + 4), "RasEapGetIdentity");
        *(_DWORD *)(a1 + 8) = v5;
        if ( v5 )
        {
          v6 = GetProcAddress(*(HMODULE *)(a1 + 4), "RasEapInvokeInteractiveUI");
          *(_DWORD *)(a1 + 24) = v6;
          if ( v6 )
            return 1;
        }
      }
    }
  }
}
```

Основное предназначение BackDoor.Apper.1 — кража с инфицированного компьютера различных документов, но этот троянец может выполнять и другие команды злоумышленников. Более подробные сведения о BackDoor.Apper.1 приведены в опубликованной на сайте компании «Доктор Веб» статье.

Обзор вирусной активности в мае 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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

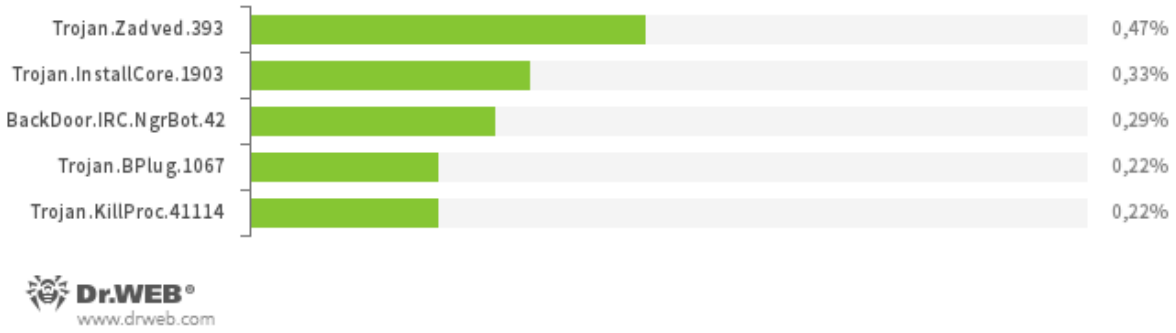


- **Trojan.Zadved**
  Надстройки, предназначенные для подмены в окне браузера результатов выдачи поисковых систем, а также демонстрации поддельных всплывающих сообщений социальных сетей. Кроме того, в их троянский функционал входит замена рекламных сообщений, демонстрируемых на различных сайтах.
- **Trojan.InstallCore.1903**
  Представитель семейства установщиков нежелательных и вредоносных приложений.
- **Trojan.MulDrop**
  Представитель семейства троянцев, предназначенных для установки на инфицированный компьютер других вредоносных программ.
- **Trojan.StartPage**
  Семейство вредоносных программ, способных подменять стартовую страницу в настройках браузера.

Обзор вирусной активности в мае 2016 года

По данным серверов статистики «Доктор Веб»

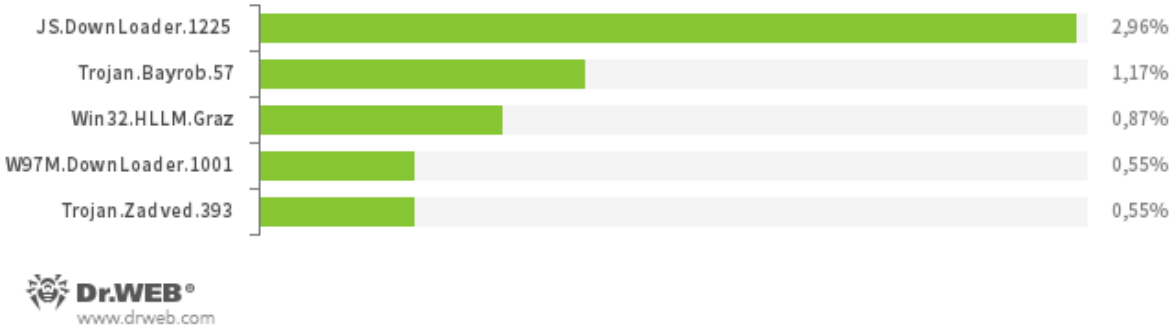
Наиболее распространенные вредоносные программы в мае 2016 года
согласно данным серверов статистики Dr.Web



- **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.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).
- **Trojan.BPlug**
  Это надстройки (плагины) для популярных браузеров, демонстрирующие назойливую рекламу при просмотре веб-страниц.
- **Trojan.KillProc.41114**
  Представитель семейства вредоносных программ, способных останавливать запущенные процессы других приложений, а также выполнять на инфицированном компьютере иные действия.

Статистика вредоносных программ в почтовом трафике

Наиболее распространенные вредоносные программы, выявленные в почтовом трафике в мае 2016 года

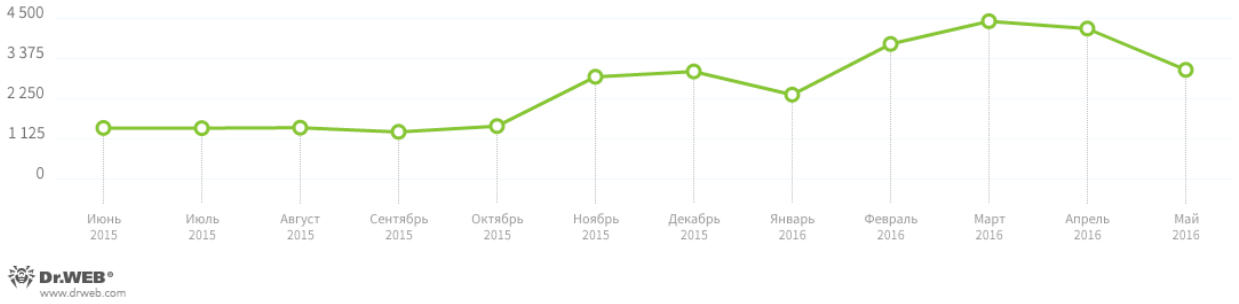


- **JS.Downloader**
  Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для загрузки и установки на компьютер других вредоносных программ.
- **Trojan.Bayrob.57**
  Троянец, способный похищать конфиденциальную информацию и выполнять на инфицированном компьютере другие нежелательные для пользователя действия.
- **Win32.HLLM.Graz**
  Почтовый червь массовой рассылки, отслеживает трафик на определенных портах и разбирает передаваемые данные с целью извлечения паролей; эта информация используется для дальнейшего распространения червя.
- **W97M.DownLoader**
  Семейство троянцев-загрузчиков, использующих в своей работе уязвимости офисных приложений. Предназначены для загрузки на атакуемый компьютер других вредоносных программ.

Обзор вирусной активности в мае 2016 года

Троянцы-шифровальщики

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



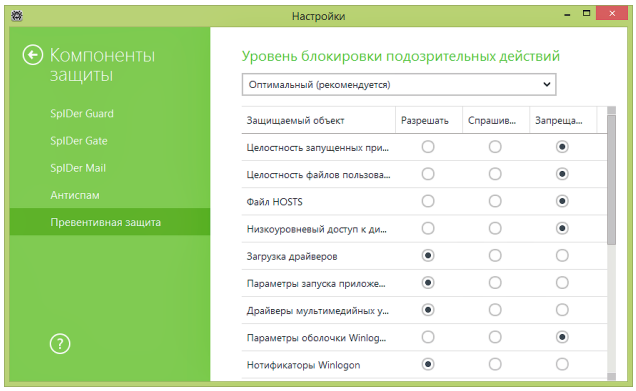
Наиболее распространенным шифровальщиком в мае 2016 года является

- Trojan.Encoder.858
- Trojan.Encoder.761
- Trojan.Encoder.4393

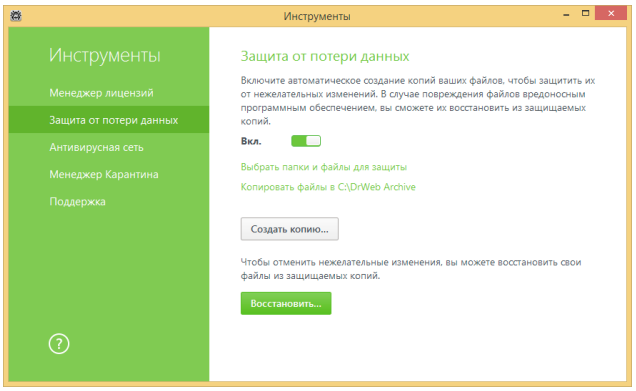
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



Подробней Смотрите видео о настройке

Обзор вирусной активности в мае 2016 года

Опасные сайты

В течение мая 2016 года в базу нерекомендуемых и вредоносных сайтов было добавлено 550 258 интернет-адресов.

Апрель 2016	Май 2016	Динамика
+ 749 173	+ 550 258	-26.55%

Нерекомендуемые сайты

Другие события

TeamViewer является популярной программой для удаленного администрирования — с ее помощью специалисты по компьютерным технологиям и системные администраторы могут получить доступ к операционной системе по сети и выполнить в ней какие-либо действия – например, изменить настройки или передать нужные файлы. Однако этой утилитой иногда пользуются и злоумышленники — они модифицируют TeamViewer таким образом, чтобы его значок не демонстрировался в панели задач Windows, а затем соединяются с атакуемой машиной без ведома пользователя.

Троянец BackDoor.TeamViewer.49 также использует в своих целях TeamViewer, но по другой причине: с его помощью он загружает в память компьютера библиотеку, в которой реализованы основные вредоносные функции троянца. Этот бэкдор превращает зараженный ПК в прокси-сервер, который перенаправляет трафик от управляющего сервера на заданный удаленный узел. Это позволяет злоумышленникам обеспечить собственную анонимность в Интернете, соединяясь с удаленными компьютерами через зараженную машину как через обычный прокси-сервер. Более подробную информацию о способе распространения BackDoor.TeamViewer.49 и его возможностях можно получить, ознакомившись с опубликованной на сайте «Доктор Веб» информационной статьей.

Вредоносное и нежелательное ПО для мобильных устройств

Банковские троянцы, заражающие мобильные устройства под управлением ОС Android, по-прежнему представляют серьезную опасность для пользователей. В прошедшем мае с помощью таких вредоносных программ злоумышленники вновь пытались украсть деньги у владельцев смартфонов и планшетов. Так, продолжилось распространение банкера Android.SmsSpy.88.origin, способного атаковать клиентов кредитных организаций по всему миру. Кроме того, специалисты компании «Доктор Веб» обнаружили большое число мошеннических сайтов, при помощи которых вирусописатели распространяли троянца Android.BankBot.104.origin, а также других Android-банкеров.

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

- новые случаи распространения банковского троянца Android.SmsSpy.88.origin, атакующего клиентов десятков банков по всему миру;
- распространение банковских троянцев при помощи мошеннических веб-сайтов, предлагающих загрузить ПО для взлома игр и получения бесконечных игровых ресурсов.

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

Обзор вирусной активности в мае 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