

Обзор вирусной активности в июне 2016 года



Обзор вирусной активности в июне 2016 года

30 июня 2016 года

Первый летний месяц 2016 года выдался на удивление жарким для специалистов по информационной безопасности — в начале июня вирусные аналитики компании «Доктор Веб» завершили изучение нового банковского вируса Bolik, а вскоре был исследован бестелесный рекламный троянец [Trojan.Kovter.297](#). Кроме того, в июне участились атаки на пользователей российских бухгалтерских программ. Сначала было зафиксировано распространение троянца, написанного на встроенном языке программирования 1С, который запускал на атакованном компьютере опасного шифровальщика. Позже был исследован троянец-шпион [Trojan.PWS.Spy.19338](#), способный фиксировать нажатия клавиш в различных приложениях, в том числе в популярных бухгалтерских программах. Также в течение месяца вирусные аналитики дважды обнаруживали в официальном каталоге Google Play троянцев для мобильной платформы Android.

Главные тенденции июня

- Появление полиморфного банковского вируса Bolik
- Распространение троянца для приложения 1С
- Появление бестелесного рекламного троянца Trojan.Kovter
- Распространение опасного троянца-шпиона Trojan.PWS.Spy.19338

Обзор вирусной активности в июне 2016 года

Угроза месяца

Программы семейства 1С пользуются высокой популярностью среди бухгалтеров и экономистов российских компаний. Проявляют к ним интерес и вирусописатели: аналитикам компании «Доктор Веб» уже встречались вредоносные приложения, написанные на встроенном языке программирования 1С. Троянец [1C.Drop.1](#) отличается от них своей архитектурой и функциональным назначением — это полноценный дроппер, сохраняющий на диск и запускающий опасного шифровальщика [Trojan.Encoder.567](#).

```
ИмяВременногофайла = "D:\ОбновлениеБИКБанка.exe";  
Попытка  
    ДвоичныеДанные.Записать (ИмяВременногофайла);  
Исключение  
ИмяВременногофайла = "C:\ОбновлениеБИКБанка.exe";  
Попытка  
    ДвоичныеДанные.Записать (ИмяВременногофайла);  
Исключение  
ИмяВременногофайла = ПолучитьИмяВременногофайла ("exe");  
    ДвоичныеДанные.Записать (ИмяВременногофайла);  
КонецПопытки;  
КонецПопытки;  
ЗапуститьПриложение (ИмяВременногофайла);
```

Троянец распространяется в сообщениях электронной почты с темой «У нас сменился БИК банка», к которым приложен файл внешней обработки для программы «1С:Предприятие». Если получатель такого письма последует предложенным инструкциям и откроет этот файл в программе «1С:Предприятие», троянец разошлет свою копию по адресам электронной почты, обнаруженным в базе контрагентов, а затем извлечет из своих ресурсов, сохранит на диск и запустит троянца-шифровальщика [Trojan.Encoder.567](#). Этот опасный энкодер, имеющий несколько модификаций, шифрует хранящиеся на дисках зараженного компьютера файлы и требует выкуп за их расшифровку. [1C.Drop.1](#) поддерживает работу с базами следующих конфигураций 1С:

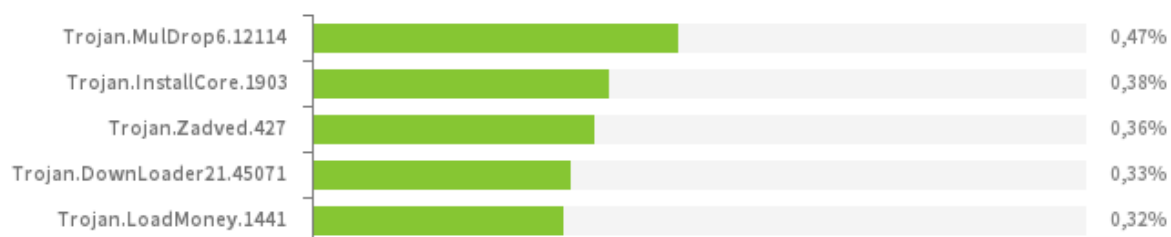
- «Управление торговлей, редакция 11.1»
- «Управление торговлей (базовая), редакция 11.1»
- «Управление торговлей, редакция 11.2»
- «Управление торговлей (базовая), редакция 11.2»
- «Бухгалтерия предприятия, редакция 3.0»
- «Бухгалтерия предприятия (базовая), редакция 3.0»
- «1С:Комплексная автоматизация 2.0»

Более подробную информацию об этой вредоносной программе можно почерпнуть в опубликованной на сайте компании «Доктор Веб» [обзорной статье](#).

Обзор вирусной активности в июне 2016 года

По данным статистики лечащей утилиты Dr.Web CureIt!

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



- **Trojan.MulDrop**

Представитель семейства троянцев, предназначенных для установки на инфицированный компьютер других вредоносных программ.

- **Trojan.InstallCore.1903**

Представитель семейства установщиков нежелательных и вредоносных приложений.

- **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.

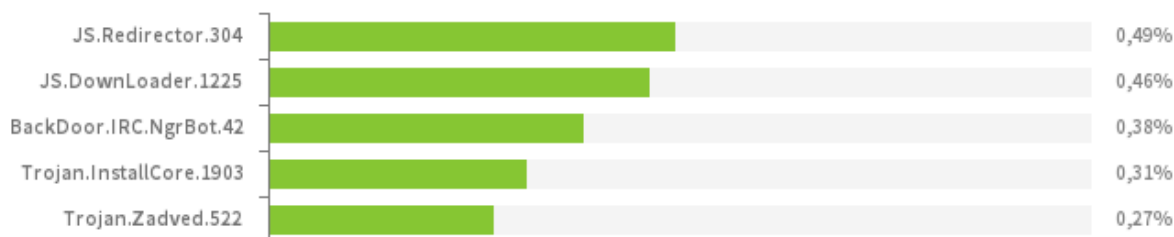
- **Trojan.LoadMoney**

Семейство программ-загрузчиков, генерируемых серверами партнёрской программы LoadMoney. Данные приложения загружают и устанавливают на компьютер жертвы различное нежелательное ПО.

Обзор вирусной активности в июне 2016 года

По данным серверов статистики «Доктор Веб»

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



- **JS.Redirector**

Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для автоматического перенаправления пользователей браузеров на другие веб-страницы.

- **JS.Downloader**

Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для загрузки и установки на компьютер других вредоносных программ.

- **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.InstallCore.1903**

Представитель семейства установщиков нежелательных и вредоносных приложений.

- **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.

Обзор вирусной активности в июне 2016 года

Статистика вредоносных программ в почтовом трафике

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



- **JS.Redirector**

Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для автоматического перенаправления пользователей браузеров на другие веб-страницы.

- **JS.Downloader**

Семейство вредоносных сценариев, написанных на языке JavaScript, предназначенных для загрузки и установки на компьютер других вредоносных программ.

- Один из представителей семейства вредоносных программ, относящихся к категории банковских троянцев. Данное приложение представляет угрозу для пользователей систем дистанционного банковского обслуживания (ДБО), поскольку позволяет злоумышленникам красть конфиденциальную информацию путем перехвата заполняемых в браузере форм и встраивания в страницы сайтов некоторых банков.

- **Trojan.PWS.Turist**

Троянская программа, предназначенная для хищения паролей и другой конфиденциальной информации, прежде всего необходимой для доступа к системам дистанционного банковского обслуживания (в том числе использующим механизм авторизации с применением смарт-карт).

- **Trojan.Encoder.858**

Представитель семейства троянцев-вымогателей, шифрующих файлы на компьютере и требующих от жертвы выкуп за расшифровку.

Обзор вирусной активности в июне 2016 года

Троянцы-шифровальщики

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



Наиболее распространенным шифровальщиком в июне 2016 года является

- Trojan.Encoder.858
- Trojan.Encoder.2843
- Trojan.Encoder.4860

В июне 2016 года получил широкое распространение троянец-шифровальщик **Trojan.Encoder.4860**, также известный под наименованием JS.Crypt. Этот энкодер примечателен тем, что целиком написан на языке JScript. Троянец имеет самоназвание — «вирус RAA», а зашифрованные файлы получают расширение *.locked. После завершения шифрования пользовательских файлов **Trojan.Encoder.4860** размещает в корневых папках дисков RTF-документ следующего содержания:

*****ВНИМАНИЕ!*****

Ваши файлы были **зашифрованы вирусом RAA**.
При шифровании был применен алгоритм AES-256, используемый для защиты информации, представляющей государственную тайну.
Это значит, что **восстановить данные можно только купив ключ у нас**.

Покупка ключа - **простейшее** дело.
Все, что вам надо:

1. Скинуть ваш ID **6DDF4405-8C1A-4E29E122C0** на почтовый адрес **raa-consult1@keemail.me**.
2. Тестово расшифровать несколько файлов для того, чтоб убедиться, что у нас действительно есть ключ.
3. Перевести **0.39 BTC (250 долларов)** на Bitcoin-адрес **1NXwDRyEFvEjPkRuXqbw77SwuvUoToc3A**.
О том, как купить Bitcoin за рубли с любой карты - <https://www.bitcoin-masters.com/rub-to-bitcoin.html>
4. **Получить ключ и программу для расшифровки файлов.**
5. Предпринять меры по предотвращению подобных ситуаций в дальнейшем.

Важно (1).
Не пытайтесь подобрать ключ, это бесполезно, и может уничтожить ваши данные окончательно.

Важно (2).
Если по указанному адресу (raa-consult1@keemail.me) вами не был получен ответ в течение 3х часов, вы можете воспользоваться для связи сервисом Bitmessage (наш адрес - BM-2cVCd439eH5kTS9PzG4NxGUAtSCxLywsmv).
Подробнее о программе - https://bitmessage.org/wiki/Main_Page

Важно (3).
Мы **НЕ МОЖЕМ** хранить ваши ключи вечно. **Все ключи**, за которые не было выплачено вознаграждение, **удаляются в течение недели с момента заражения**.

README файлы расположены в корне каждого диска.

ВАШ ID - **6DDF4405-8C1A-4E29E122C0**

Узнайте больше

Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека

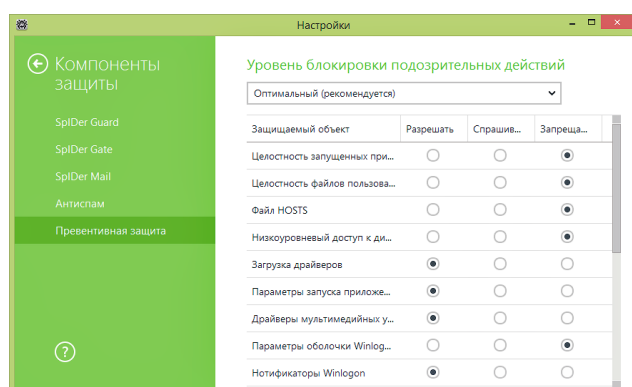
Обзор вирусной активности в июне 2016 года

К сожалению, в настоящее время специалисты компании «Доктор Веб» не располагают инструментарием для расшифровки файлов, поврежденных этой версией троянца-шифровальщика.

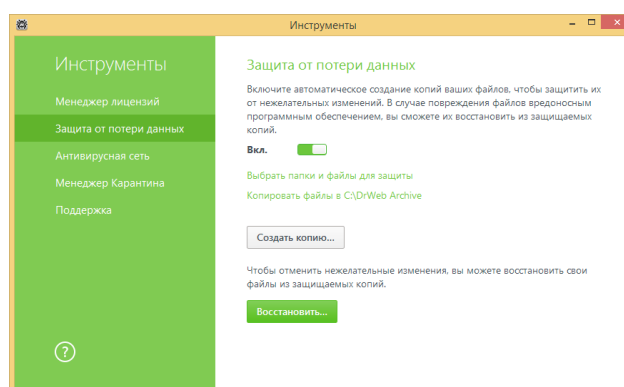
Dr.Web Security Space 11.0 для Windows защищает от троянцев-шифровальщиков

Этого функционала нет в лицензии Антивирус Dr.Web для Windows

Превентивная защита



Защита данных от потери



[Подробнее](#) [Смотрите видео о настройке](#)

Опасные сайты

В начале июня вирусные аналитики компании «Доктор Веб» завершили исследование опасного банковского вируса [Trojan.Bolik.1](#). Он предназначен для кражи денег со счетов клиентов российских банков, похищения конфиденциальной информации и шпионажа. Вирус наследует некоторые технические решения широко известных банковских троянцев Zeus (Trojan.PWS.Panda) и Carberp, но в отличие от них умеет распространяться без участия пользователя и заражать исполняемые файлы.

По команде киберпреступников [Trojan.Bolik.1](#) ищет исполняемые файлы в сетевых папках и на подключенных к компьютеру USB-устройствах, после чего заражает их. Зараженные этим вирусом программы детектируются Антивирусом Dr.Web под именем [Win32.Bolik.1](#). Внутри каждой такой программы хранится в зашифрованном виде сам банковский троянец [Trojan.Bolik.1](#), а также другая необходимая вирусу информация.

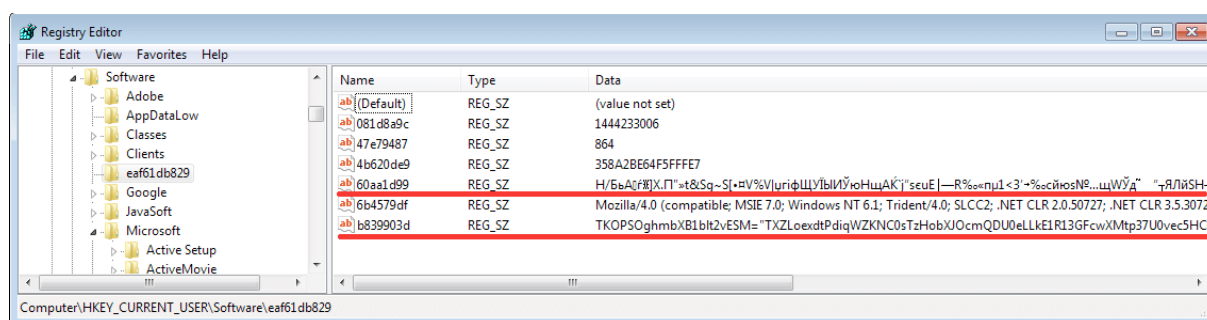
Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

Обзор вирусной активности в июне 2016 года

[Trojan.Bolik.1](#) может контролировать данные, передаваемые и отправляемые браузерами Microsoft Internet Explorer, Chrome, Opera и Mozilla Firefox (благодаря этому он способен похищать информацию, которую пользователь вводит в экранные формы). Кроме того, вирус умеет делать снимки экрана, фиксировать нажатия клавиш, создавать на зараженной машине собственный прокси-сервер и веб-сервер, позволяющий обмениваться файлами со злоумышленниками. Подробности об этой вредоносной программе изложены в подготовленной компанией «Доктор Веб» [обзорной статье](#).

Еще одна новинка июня — бестелесный троянец [Trojan.Kovter.297](#). Эта вредоносная программа незаметно для пользователя запускает в фоновом режиме несколько экземпляров браузера Microsoft Internet Explorer, посещает с их помощью указанные злоумышленниками сайты и накручивает количество просмотров рекламы, нажимая на рекламные ссылки и баннеры. Отличительной чертой троянца является то, что он не присутствует на инфицированном компьютере в виде отдельного файла, а работает непосредственно в оперативной памяти, используя для своего хранения системный реестр Windows.



Более детальную информацию о Trojan.Kovter.297 можно получить в соответствующем новостном материале.

В конце месяца вирусные аналитики «Доктор Веб» выявили целую группу вредоносных программ, среди которых оказался [Trojan.PWS.Spy.19338](#) — троянец-шпион, нацеленный на бухгалтеров. Основное предназначение этого троянца — отслеживание нажатий клавиш в окнах ряда приложений, среди которых — 1С различных версий и СБИС++. Также он собирает информацию об инфицированной системе и передает злоумышленникам данные из буфера обмена инфицированного компьютера. Читайте подробности о [Trojan.PWS.Spy.19338](#) в нашей [новостной статье](#).

В июне было зафиксировано распространение Linux-троянца **Linux.BackDoor.Irc.13**. Эта вредоносная программа является модификацией [Linux.BackDoor.Tsunami](#), однако не содержит функций для выполнения DDoS-атак. Команды этот троянец получает с использованием протокола IRC (Internet Relay Chat), предназначенного для обмена текстовыми сообщениями в Интернете.

Обзор вирусной активности в июне 2016 года

Не обошли своим вниманием вирусописатели и пользователей компьютеров Apple: в июне специалисты «Доктор Веб» выявили нового троянца для OS X, получившего наименование **Mac.BackDoor.SynCloud.1**. При запуске он извлекает логины и пароли всех авторизованных в системе на данный момент пользователей OS X и отправляет эту информацию на управляющий сервер. По команде злоумышленников **Mac.BackDoor.SynCloud.1** может загрузить с командного сервера и запустить на инфицированном компьютере исполняемый файл или сценарий на языке Python, а также выполнить иные действия, например, обновить свою версию. Вся информация, которой **Mac.BackDoor.SynCloud.1** обменивается с управляющим сервером, шифруется.

Опасные сайты

В течение июня 2016 года в базу nereкомендуемых и вредоносных сайтов было добавлено 1 716 920 интернет-адресов.

Май 2016	Июнь 2016	Динамика
+ 550 258	+ 1 716 920	+212%

[Nereкомендуемые сайты](#)

Обзор вирусной активности в июне 2016 года

Вредоносное и нежелательное ПО для мобильных устройств

В июне вирусные аналитики компании «Доктор Веб» обнаружили несколько вредоносных приложений, которые распространялись в каталоге Google Play. Одно из них получило имя [Android.Valeriy.1.origin](#). Этот троянец загружал сомнительные веб-сайты и показывал их в виде рекламных баннеров, которые предлагали пользователям указать номер телефона для доступа к различным сервисам и услугам, однако после ввода номера с абонентского счета жертв начинала списываться плата. Также троянец мог скачивать другие вредоносные приложения и выполнять JavaScript-сценарии.

Еще одна вредоносная программа, обнаруженная в каталоге Google Play, была добавлена в вирусную базу как [Android.PWS.Vk.3](#). Этот троянец представлял собой аудиоплеер для прослушивания музыки, размещенной в социальной сети «ВКонтакте». [Android.PWS.Vk.3](#) запрашивал у пользователей логин и пароль от учетной записи, после чего передавал эти данные злоумышленникам.

Наиболее заметные события, связанные с мобильной безопасностью в июне:

- обнаружение в каталоге Google Play троянца, который открывал сомнительные веб-сайты и показывал их в виде рекламных баннеров;
- обнаружение в каталоге Google Play троянца, крадущего логины и пароли от учетных записей «ВКонтакте».

Более подробно о вирусной обстановке для мобильных устройств в мае читайте в нашем [обзоре](#).

Обзор вирусной активности в июне 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

[ВебОметр](#) | [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](#)



© ООО «Доктор Веб»,
2003-2016

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)