Вновь пришлось столкнуться с проблемой пользователя – потеря рабочих файлов из-за нового вирусняка с говорящим названием. Рассмотрим вопрос — как лечить компьютер после вируса шифровальщика da_vinci_code и расшифровать файлы с расширением код да винчи. В очередной раз повторим правила безопасности для защиты компьютеров и данных от такого рода зловредов.

> Гарантированная расшифровка файлов после вируса шифровальщика — dr.shifro.ru. Подробности работы и схема взаимодействия с заказчиком ниже в статье в соответствующем разделе под номером 7 в Содержании.

Содержание:

> Вышла новая модификация вируса шифровальщика, похожего на да винчи — no_more_ransom. Подробное описание вируса, методы лечения компьютера и варианты восстановления файлов читайте по ссылке.

Описание вируса шифровальщика da_vinci_code

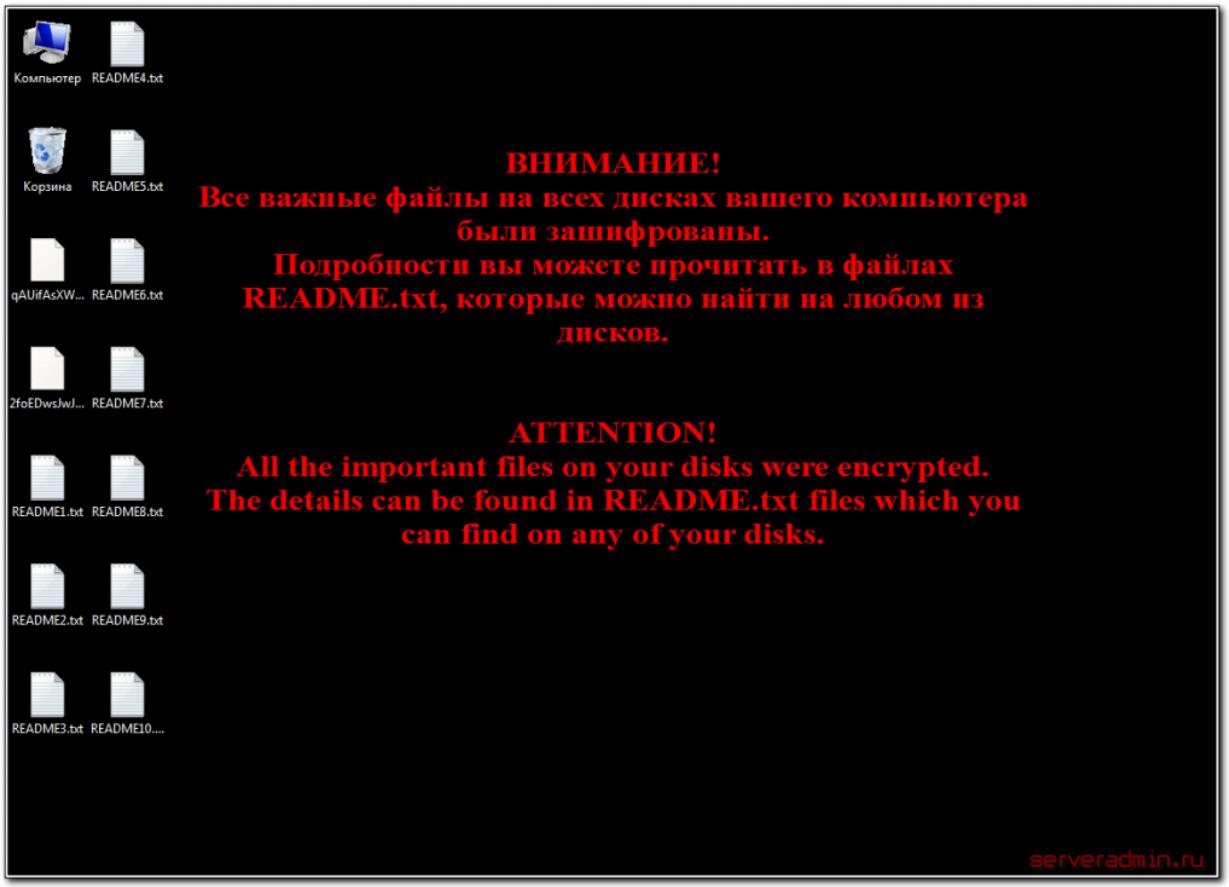
Довелось на днях познакомиться с очередным вирусом шифровальщиком — **da_vinci_code**. На шифровальщиков мне везет, я уже очень хорошо с ними

знаком. Все было как обычно:

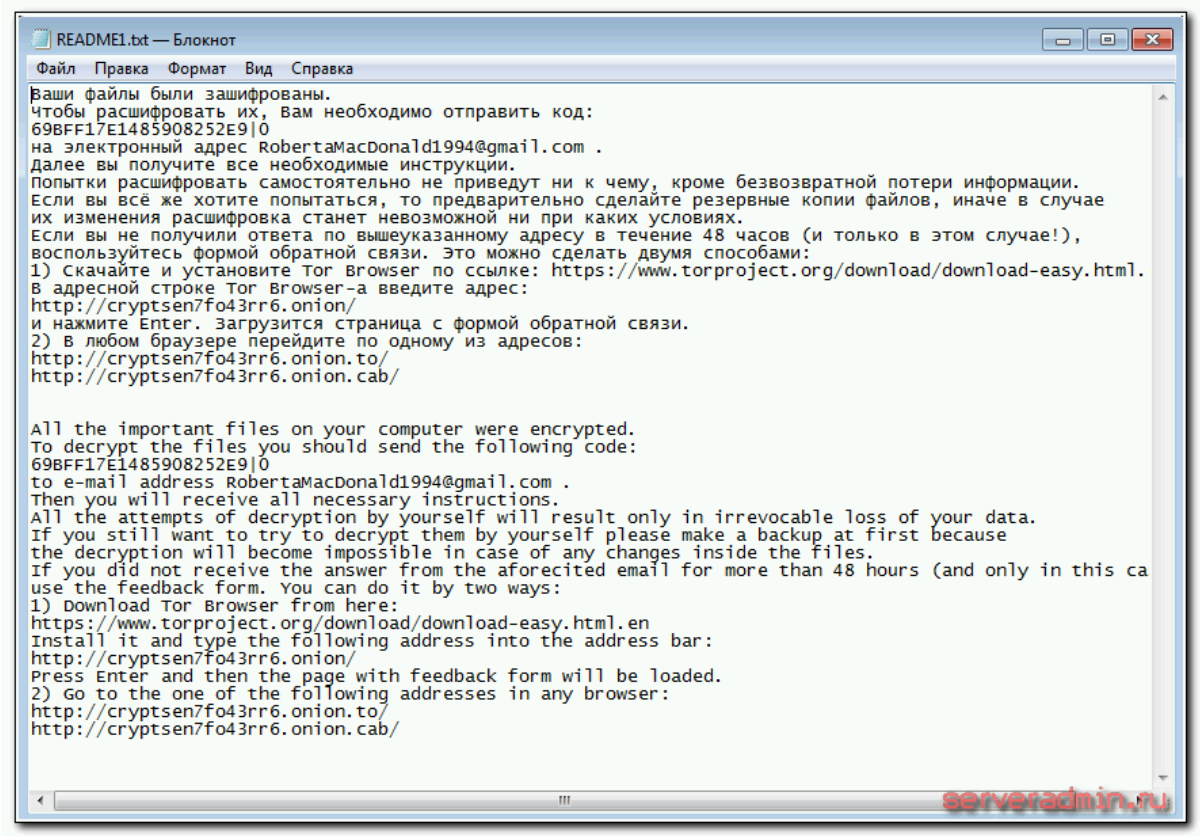
1. Письмо пользователю от якобы контрагента с просьбой проверить там какую-то информацию, акт сверки или что-то еще. Письмо с вложением.
2. Пользователь открывает вложение, там архив, в архиве js скрипт. Открывает архив со скриптом и запускает его.
3. Скрипт качает из интернета сам вирус и начинает шифровать все файлы на локальных дисках, до которых успевает дотянуться.
4. На финише у пользователя меняется картинка на рабочем столе, где говорится о том, что все файлы зашифрованы.

Такая вот простая и банальная последовательность действий, которую до сих пор пользователи успешно выполняют. Причем установленные антивирусы на их компьютерах не предотвращают шифрование файлов. Толку от них в случае вируса-шифровальщика никакого нет.

Название этого зловреда весьма оригинальное — код да винчи, или da_vinci_code. Прозвали его так за то, что он ставит соответствующее расширение на зашифрованные файлы. После того, как вирус шифратор поработает на компе и закончит шифрование, вы увидите сообщение на рабочем столе в виде обоев:



На рабочем столе и дисках системы появится множество текстовых файлов с информацией о том, что все ваши файлы были зашифрованы. Текст сообщения будет примерно следующий:



Сразу, как только вы это увидите, отключите компьютер от сети и завершите его работу. Это позволит избежать шифрования сетевых папок, если вирус имеет такую возможность. Я сталкивался с шифровальщиками, которые шифровали все сетевые папки, например vault, но были и такие, которые работали только с локальным компьютером, как вирус enigma. Что конкретно делает этот вирус, я не знаю, так как модификаций может быть много. Поэтому обязательно выключайте компьютер. Ниже я расскажу, как действовать далее для лечения компьютера и расшифровки файлов.

Вирус ставит расширение da_vinci_code на файлы

Итак, вы словили вирус и обнаружили, что все файлы поменяли не только свое расширение на da_vinci_code, но и имена файлов стали вида:

- FCLz7Bp-+HIHOCKm0rlMfw==.8C29FA8A8AC85257C10F.da_vinci_code
- 3Aag8evVDM6H8IWIiRpnhf2XXI6NMbGpB9XQTAKQ==.B604CC12F53D945AF080.da_vinci_code
- 1Fy-zfjTwpz95HtypRQ—Fo8nCVaEECEB+tBgJ4Z7604CC12F53D945AF080.da_vinci_code

Шифрует он почти все полезные файлы. В моем случае он зашифровал все документы, архивы, картинки, видео. Вообще вся полезная информация на компьютере превратилась вот в такую зашифрованную кашу. Прочитать файлы стало невозможно. Даже понять, что это за файлы нельзя. Это, кстати, существенный минус. Все предыдущие модификации шифровальщика, что ко мне попадали, оставляли оригинальное имя файла. Этот же не только расширение поменял, но и заменил все имена файлов. Стало невозможно понять, что конкретно ты потерял. Понимаешь только, что ВСЕ!

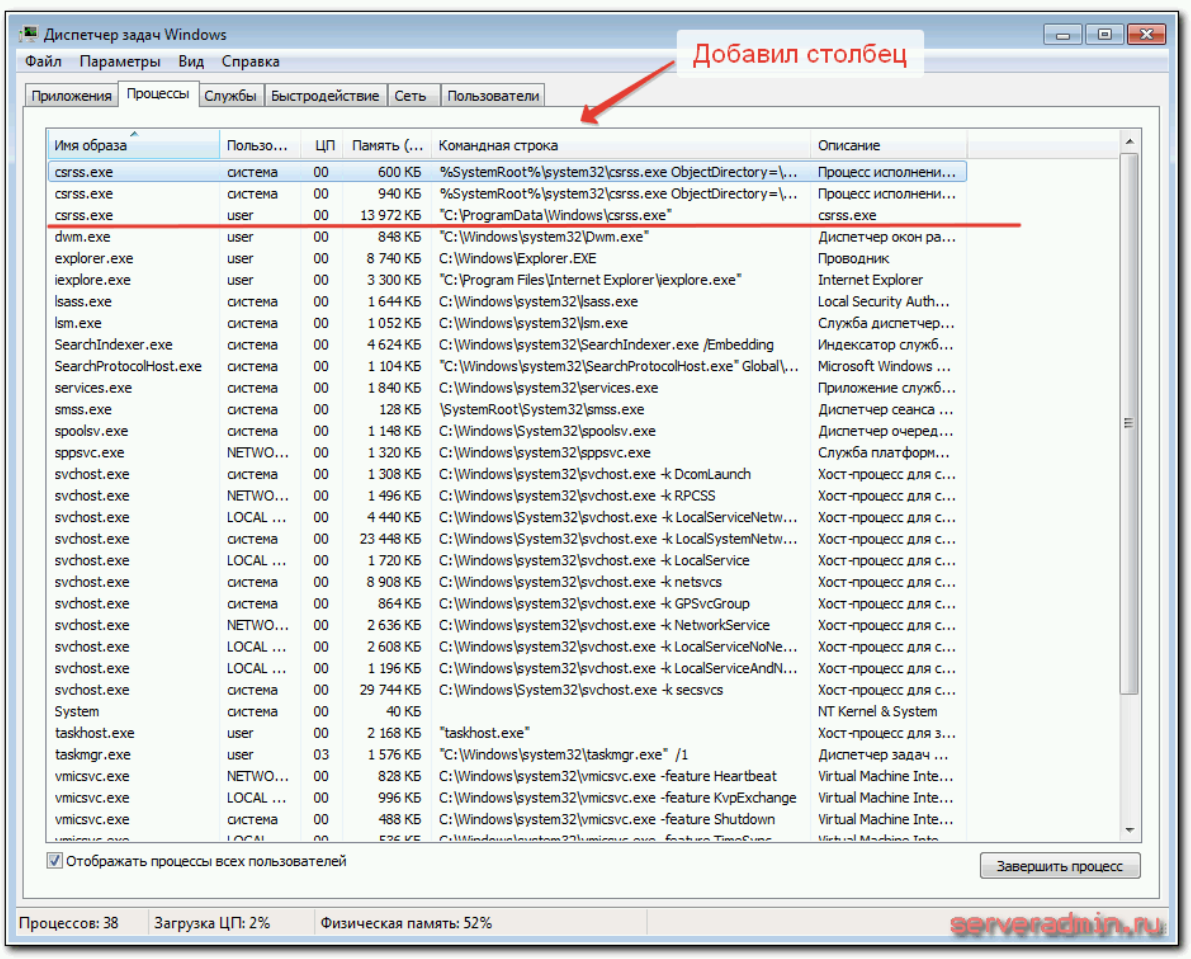
Вам повезло, если файлы зашифрованы только на локальном компьютере, как в моем случае. Хуже, если вирус шифровальщик да винчи повредит файлы и на сетевых дисках, например, организации. Это вообще способно полностью парализовать работу компании. С таким я тоже сталкивался и не раз. Приходилось платить злоумышленникам, чтобы возобновить работу.

Как лечить компьютер и удалить вирус da_vinci_code

Вирус уже у вас на компьютере. Первый и самый главный вопрос — как вылечить компьютер и как удалить из него вирус, чтобы предотвратить дальнейшее шифрование, если оно еще не было закончено. Надежнее удалить шифровальщик да винчи вручную, но тут без специальных знаний не обойтись и не всегда это можно сделать быстро. Вирусы постоянно меняются, меняют название исполняемых файлов и место их расположения. Я расскажу про ту модификацию, что попалась мне. Покажу, как вылечить компьютер вручную и автоматически с помощью антивирусных утилит по удалению вирусов.

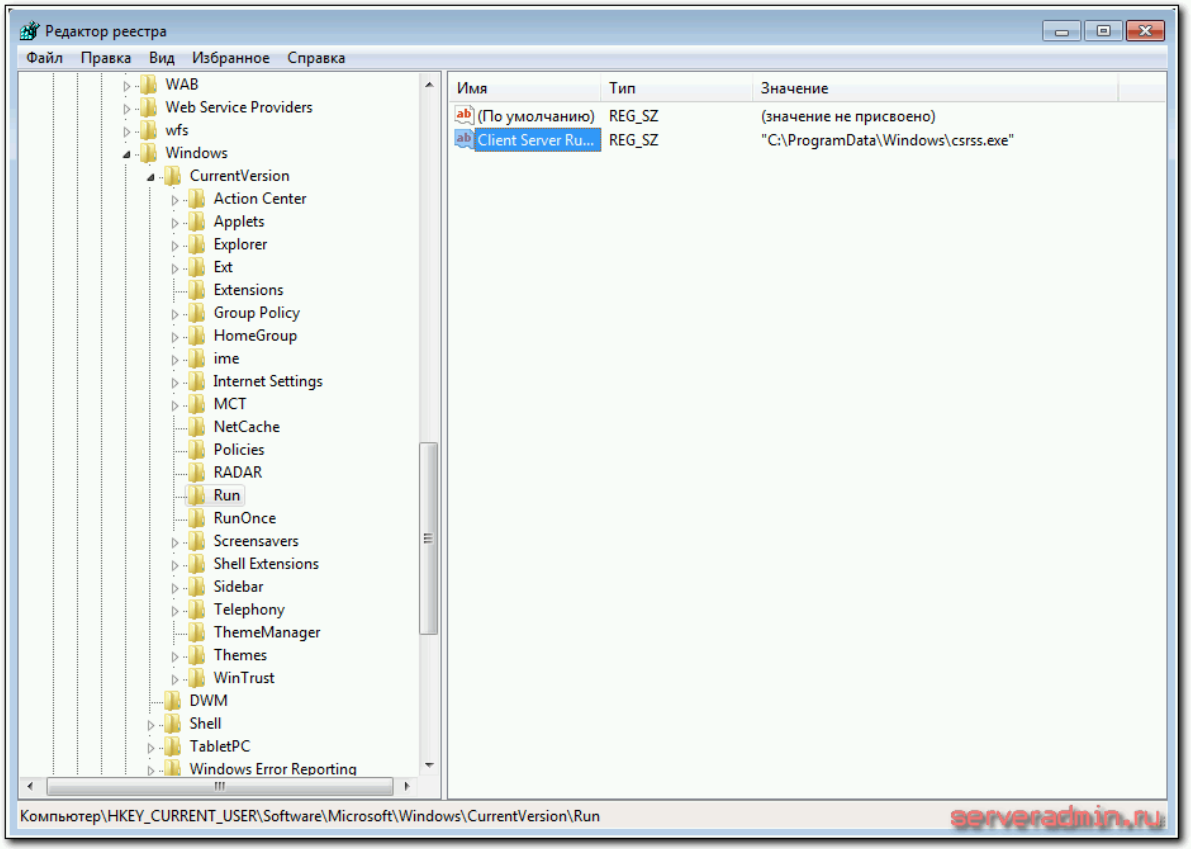
> Хочу сразу сделать важное предупреждение. Если вы хотите во что бы то ни стало восстановить свои файлы и готовы обратиться в организации, занимающиеся расшифровкой или в антивирусную компанию, если у вас есть платная подписка на антивирусы, то не предпринимайте сами ничего. Либо перед этим сделайте полный образ системы и только потом что-то делайте. Иначе ваша работа может существенно осложнить или вообще сделать невозможным восстановление информации.

Сначала проведем удаление вируса код да винчи вручную. Как я уже говорил раньше, компьютер нужно обязательно отключить от сети. Если вы уже видите на рабочем столе картинку с информацией о том, что все важные файлы на всех дисках вашего компьютера были зашифрованы, то скорее всего вирус уже все зашифровал, так что торопиться нам некуда. Я обнаружил вирус практически сразу, просто запустив диспетчер задач и добавив столбец под названием «Командная строка».



Процесс **csrss.exe** расположен в подозрительном месте, маскируется под системный, но при этом не имеет описания. Это и есть вирус. Завершаем процесс в диспетчере задач и удаляем его из папки *C:\ProgramData\Windows*. В моем случае папка была скрытая, поэтому нужно включить отображение скрытых папок и файлов. В поиске легко найти как это сделать.

Дальше запускаем редактор реестра и ищем все записи с найденным путем: «*C:\ProgramData\Windows*» и удаляем их.



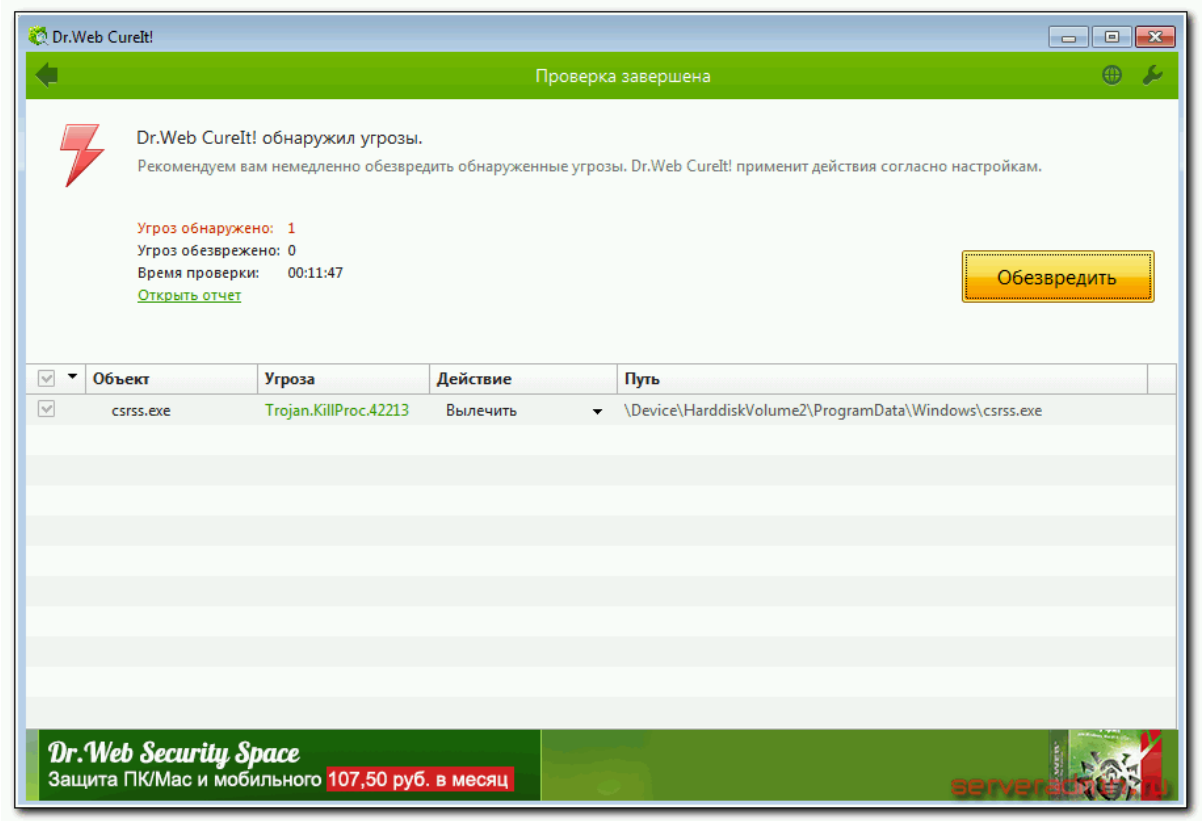
Теперь можно поменять обои на рабочем столе стандартным образом. Установленная картинка с информацией находится по адресу *C:\Users\user\AppData\Roaming*, можете удалить или оставить на память.

Дальше рекомендую очистить временную папку пользователя *C:\Users\user\AppData\Local\Temp*. Конкретно da_vinci там свои экзешники не располагал, но другие частенько это делают.

На этом удаление вируса код да винчи в ручном режиме завершено. Традиционно, вирусы шифровальщики легко удаляются из системы, так как им нет

смысла в ней сидеть после того, как они сделали свое дело.

Теперь я покажу, как вылечить компьютер с помощью утилиты **CureIt** от Dr.web. Идете на сайт https://free.drweb.ru/cureit/ и скачиваете утилиту. Копируете ее на флешку, подсоединяете флешку к компьютеру, предварительно удалив с нее все нужные документы, так как вирус их может зашифровать. И запускаете на флешке программу. Выполняете полное сканирование системы. Антивирус обнаружит установленный шифровщик и предложит его удалить.



Если у вас новая модификация вируса, которую еще не знают антивирусы, то они вам помочь не могут. Тогда остается только ручной вариант лечения компьютера от шифровальщика. Думаю, это не составит большого труда, так как они не сильно маскируются в системе. Как я уже сказал, им это и не нужно. Обычного диспетчера задач и поиска по реестру бывает достаточно.

Будем считать, что лечение прошло успешно и шифровальщик да винчи удален с компьютера. Приступаем к восстановлению файлов.

Где скачать дешифратор da_vinci_code

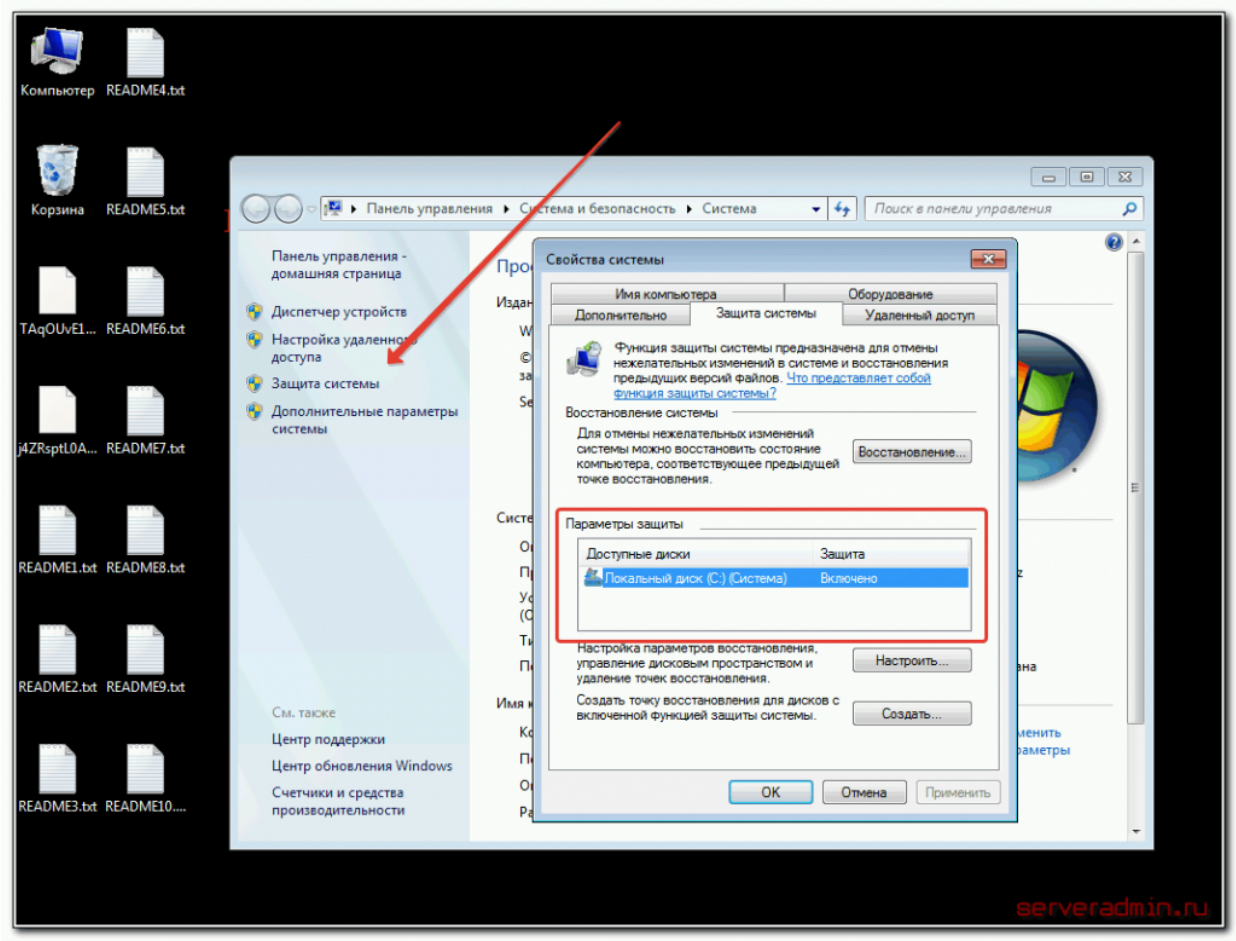
Вопрос простого и надежного дешифратора встает в первую очередь, когда дело касается вируса-шифровальщика. Мне встречались дешифраторы к отдельным модификациям вируса, которые можно было скачать и проверить. Но чаще всего они не работают. Дело в том, что сам принцип rsa шифрования не позволяет создать дешифратор без ключа, который находится у злоумышленников. Если дешифратор da_vinci_code и существует, то только у авторов вируса или аффилированных лиц, которые как-то связаны с авторами. По крайней мере так я понимаю принцип работы. Возможно я в чем-то ошибаюсь. Сейчас слишком много фирм развелось, которые занимаются расшифровкой. С одной из них я знаком, расскажу о ней позже, но как они работают, мне не говорят.

Так что дешифратора в полном смысле этого слова я предоставить не смогу. Вместо этого предлагаю пока скачать пару программ, которые нам помогут провести расшифровку и восстановление файлов. Хотя слово расшифровка тут подходит с натяжкой, но смысл в том, что файлы мы можем попытаться получить обратно.

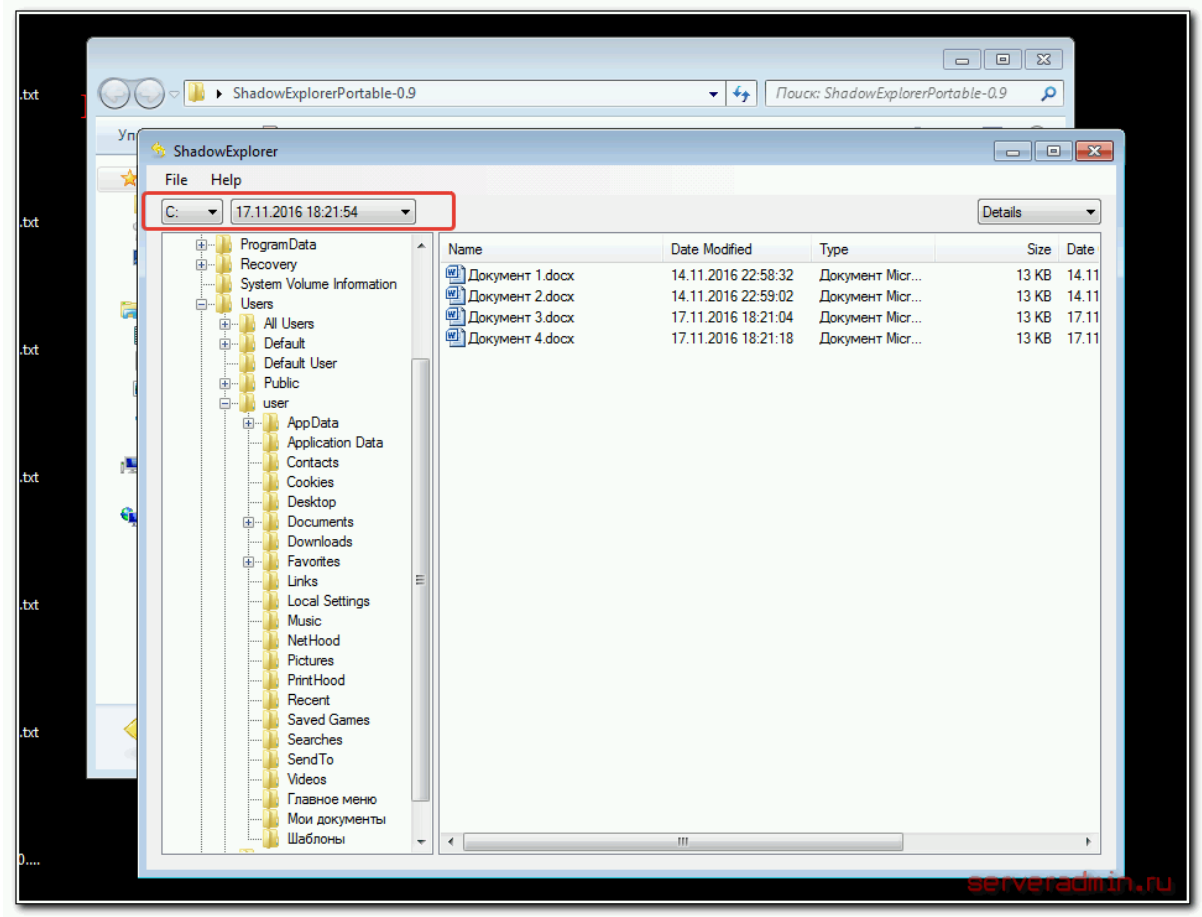
Нам понадобится программа shadow explorer для восстановления файлов из теневых копий. Чтобы попытаться восстановить остальные файлы, воспользуемся программой для восстановления удаленных файлов photorec. Обе программы бесплатные, можно без проблем качать и пользоваться. Дальше расскажу как их использовать.

Как расшифровать и восстановить файлы после вируса код да винчи

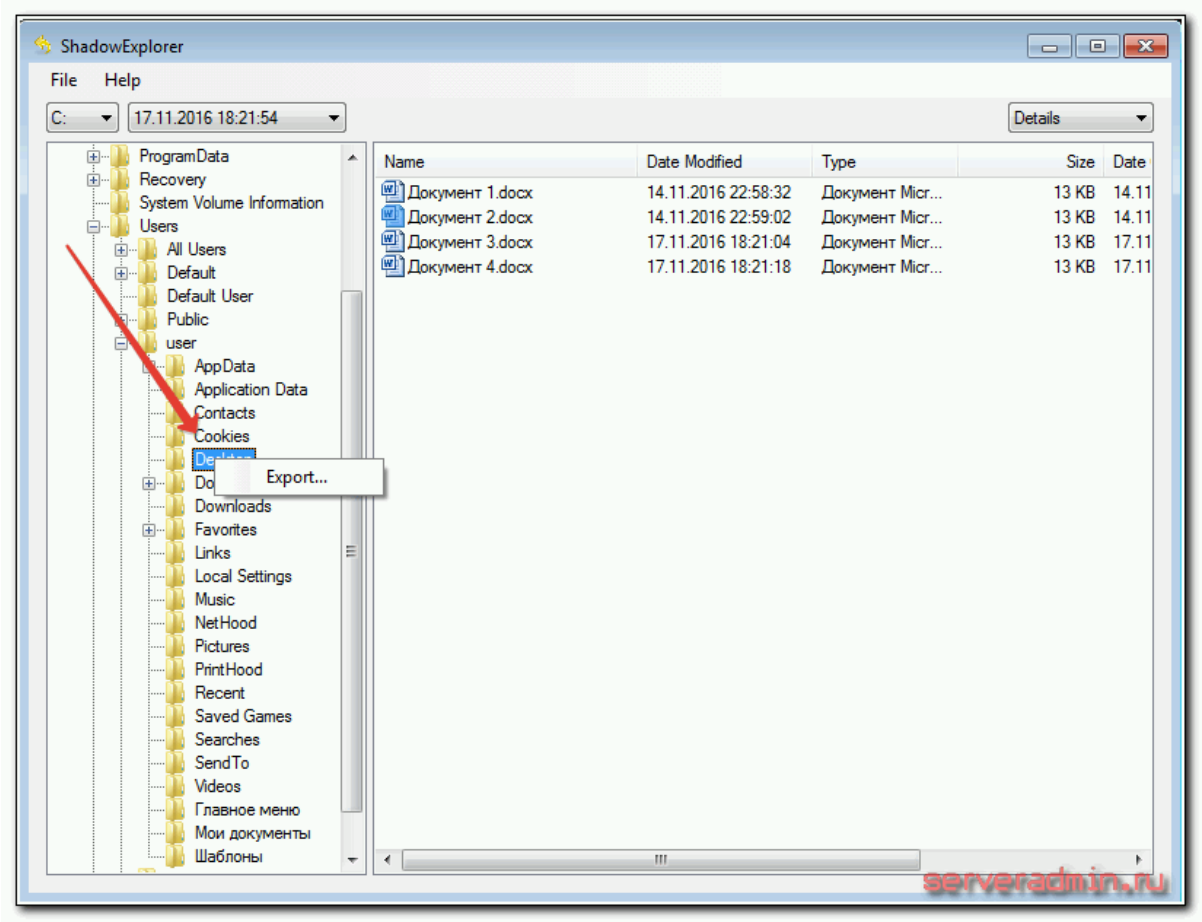
Как я уже говорил ранее, расшифровать файлы после вируса da_vinci_code без ключа невозможно. Поэтому мы воспользуемся альтернативными способами восстановления данных. Для начала попробуем восстановить архивные копии файлов, которые хранятся в **теневых копиях** диска. По-умолчанию, начиная с Windows 7 технология теневых копий включена по умолчанию. Проверить это можно в свойствах компьютера, в разделе защита системы.



Если у вас она включена, то запускайте программу **ShadowExplorer**, которую я предлагал скачать чуть выше. Распаковывайте из архива и запускайте. Нас встречает главное окно программы. В левом верхнем углу можно выбрать диск и дату резервной копии. Скорее всего у вас их будет несколько, нужно выбрать необходимую. Чтобы восстановить как можно больше файлов, проверьте все даты на наличие нужных файлов.



В моем примере на рабочем столе лежат 4 документа, которые там были до работы вируса. Я их могу восстановить. Выделяю нужную папку, в данном случае Desktop и нажимаю правой кнопкой мышки, жму на Export и выбираю папку, куда будут восстановлены зашифрованные файлы.

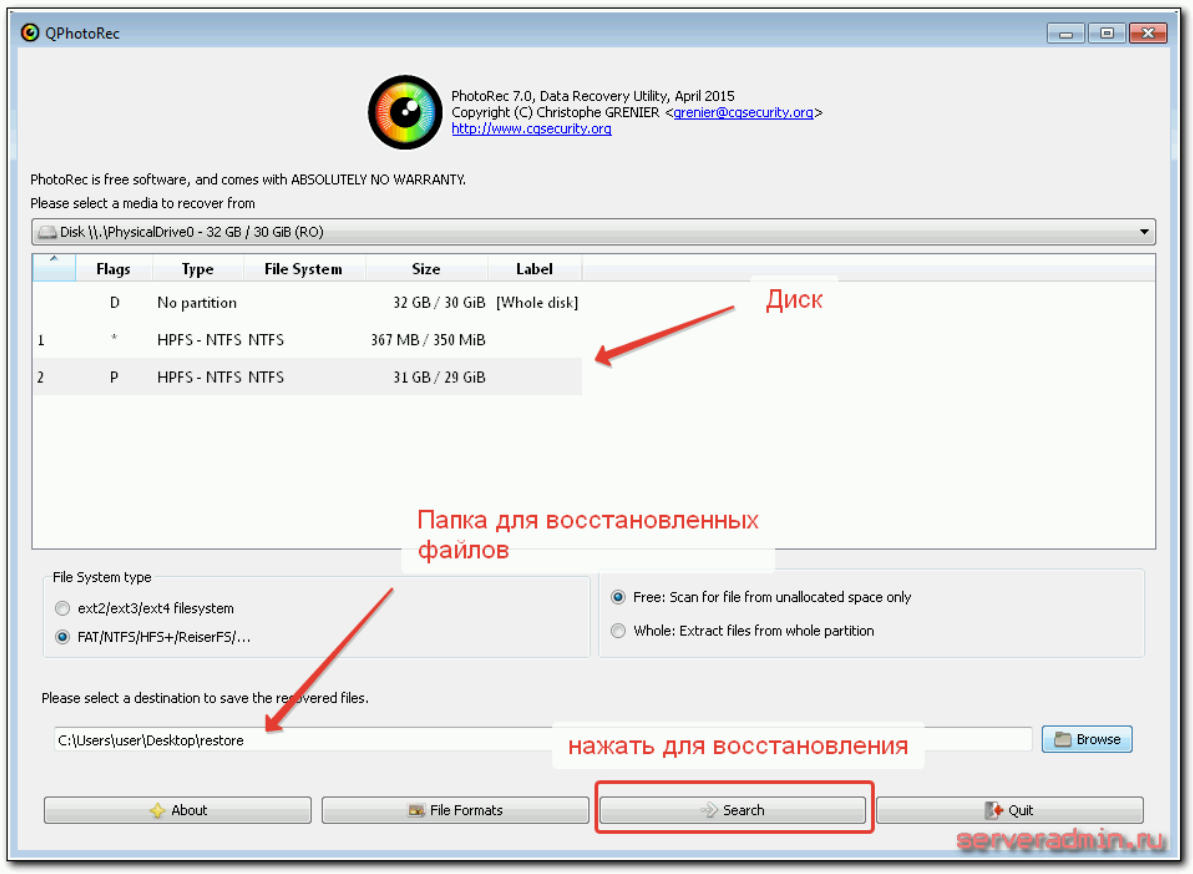


Если у вас не была отключена защита системы, то с большой долей вероятности вы восстановите какую-то часть зашифрованных файлов. Некоторые восстанавливают 80-90%, я знаю такие случаи.

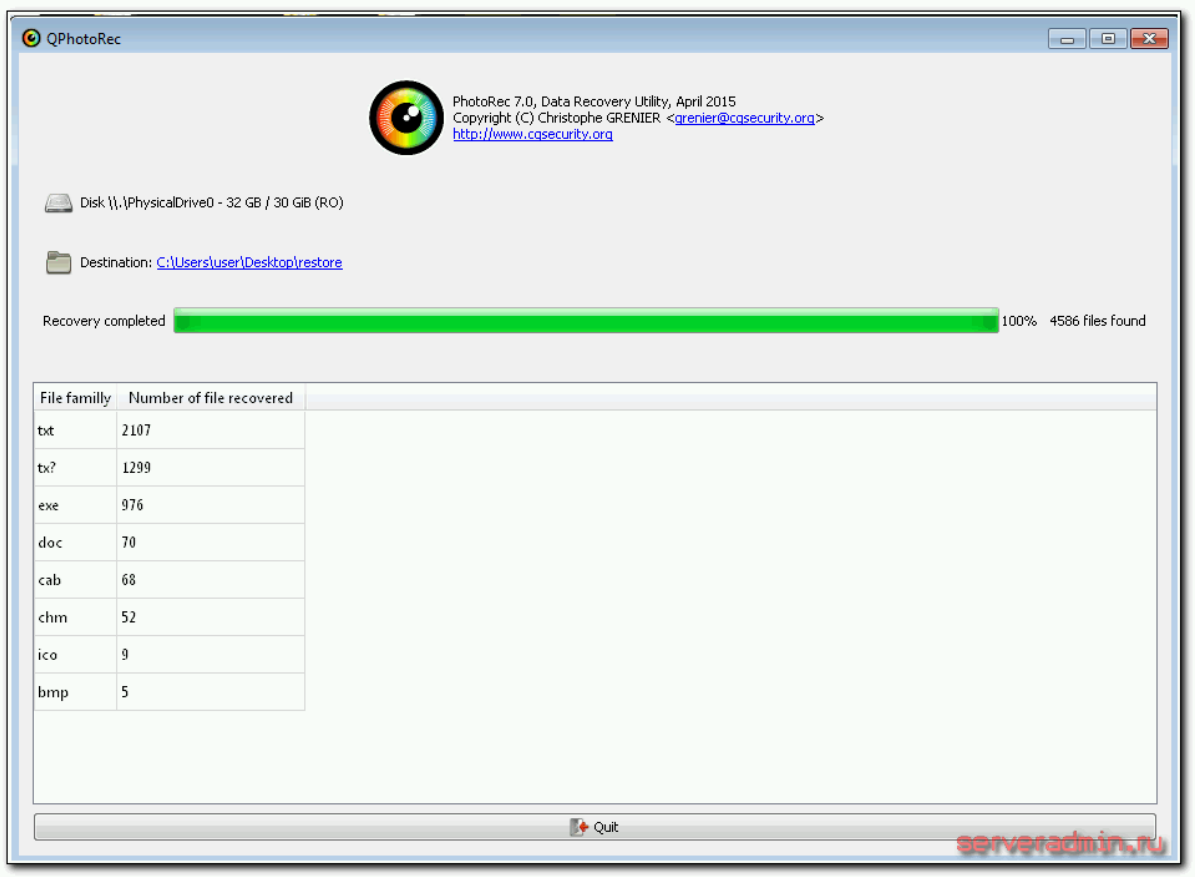
Если у вас по какой-то причине нет теневых копий, то все значительно усложняется. У вас остается последний шанс бесплатно расшифровать свои файлы — восстановить их с помощью программ по поиску и восстановлению удаленных файлов. Я предлагаю воспользоваться бесплатной программой **Photorec**.

Скачивайте ее и запускайте.

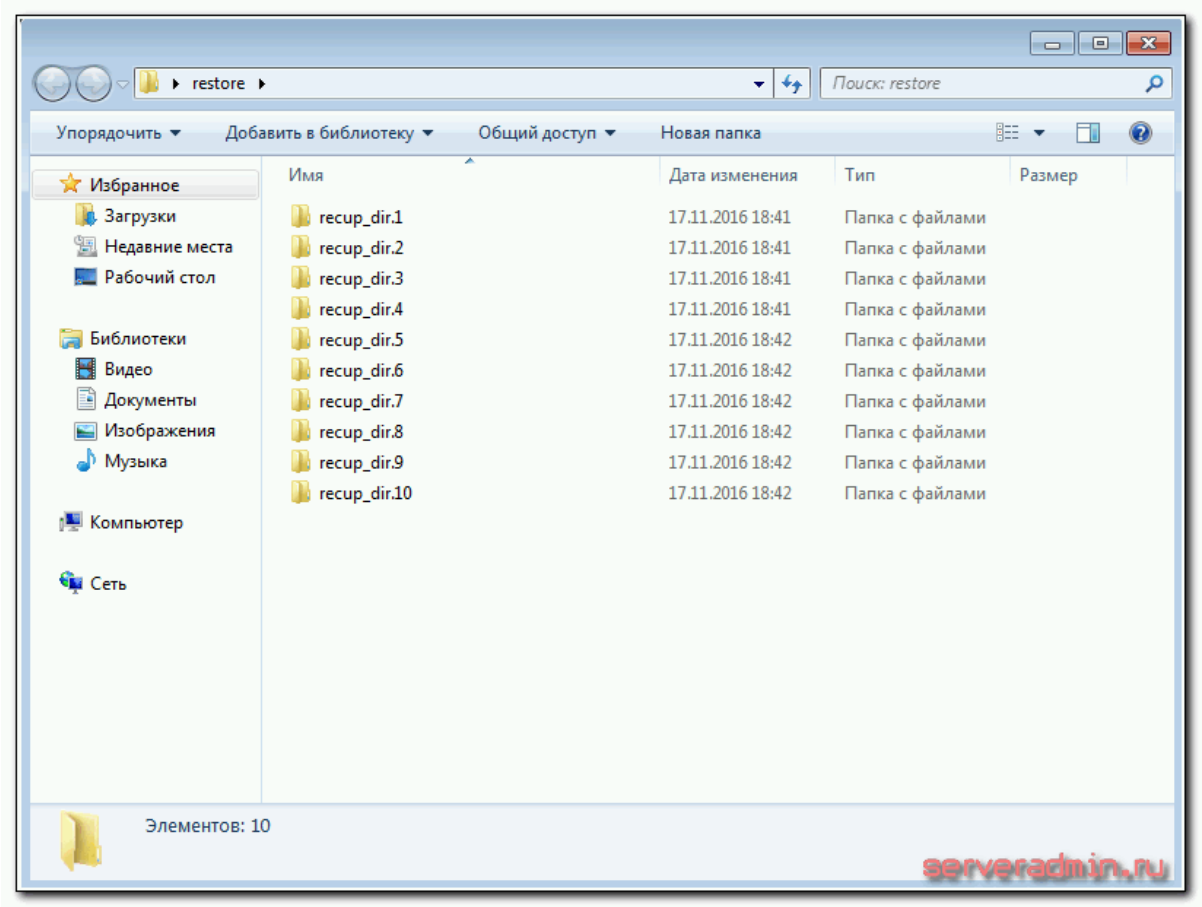
После запуска выберите ваш диск, на котором будем проводить восстановление данных. Затем укажите папку, куда будут восстановлены найденные файлы. Лучше, если это будет какой-то другой диск или флешка, но не тот же самый, где осуществляете поиск.



Поиск и восстановление файлов будет длиться достаточно долго. После окончания процесса восстановления вам будет показано, сколько и каких файлов было восстановлено.



Можно закрыть программу и пройти в папку, которую указали для восстановления. Там будет набор других папок, в которых будут файлы. Все, что получилось расшифровать, находится в этих папках. Вам придется вручную смотреть, искать и разбирать файлы.



Если результат вас не удовлетворит, то есть другие программы для восстановления удаленных файлов. Вот список программ, которые я обычно использую, когда нужно восстановить максимальное количество файлов:

- R.saver
- Starus File Recovery
- JPEG Recovery Pro

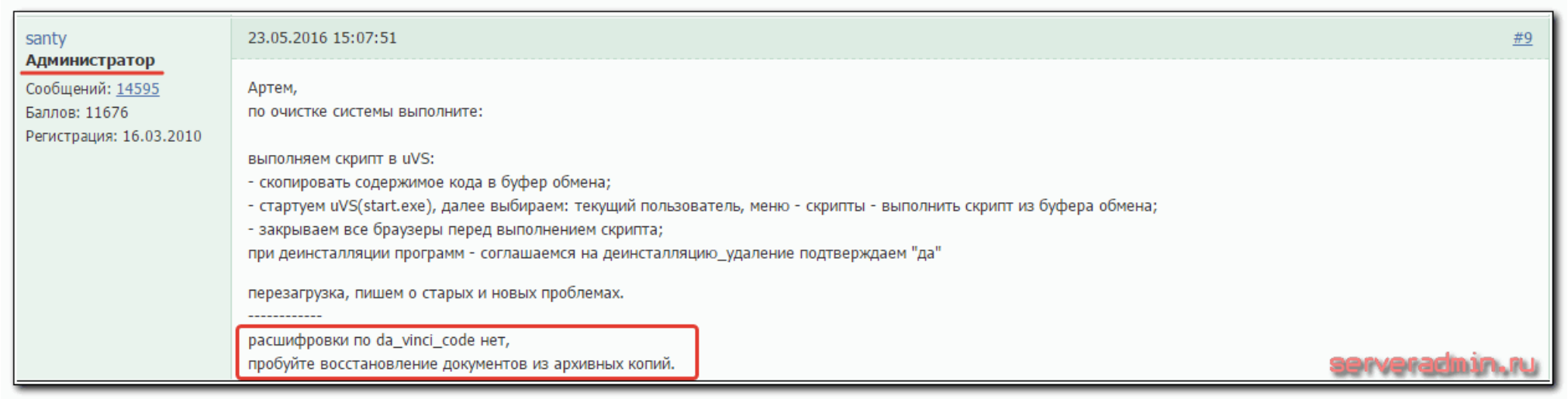
- Active File Recovery Professional

Программы эти не бесплатные, поэтому я не буду приводить ссылок. При большом желании, вы сможете их сами найти в интернете.

Это все, что я знал и мог подсказать на тему того, как расшифровать и восстановить файлы после вируса da_vinci_code. В принципе, шансы на восстановление есть, но не в полном объеме. Наверняка может помочь только своевременно сделанная архивная копия.

Касперский, eset nod32 и другие в борьбе с шифровальщиком код да винчи

Ну а что же наши современные антивирусы скажут насчет расшифровки файлов. Я полазил по форумам самых популярных антивирусов: kaspersky, eset nod32, dr.web. Никакой более ли менее полезной информации там не нашел. Вот что отвечают на форуме eset nod32 по поводу вируса да винчи:



http://forum.esetnod32.ru/messages/forum35/topic13242/message93186/

Нод 32 ничего предложить не может для того, чтобы расшифровать файлы. На форуме антивируса kaspersky схожий ответ: «С расшифровкой помочь не сможем.»

https://forum.kasperskyclub.ru/index.php?showtopic=50109&p=737346

Модератор предлагает обратиться в техническую поддержку. Но лично я не видел информации, чтобы касперский кому-то предложил дешифратор da_vinci_code. На официальном форуме вообще нет полезной информации в открытом виде, только просьбы о помощи с расшифровкой и лечением. Всех отправляют на форум kasperskyclub.

Получается, что спасение утопающих дело рук самих утопающих. Вирус давно гуляет по интернету, а надежного средства восстановления данных нет. С

недавним вирусом enigma была получше ситуация. Там вроде бы Dr.Web предлагал дешифратор. По текущему вирусу информации нет. На форуме доктора веба только запросы на помощь в расшифровке. Но всех отправляют в тех поддержку. Она попытается помочь только в том случае, если на момент заражения у вас была лицензия на антивирус.

Куда еще обратиться за гарантированной расшифровкой

Мне довелось познакомиться с одной компанией, которая реально расшифровывает данные после работы различных вирусов-шифровальщиков, в том числе da vinci code. Их адрес — http://www.dr-shifro.ru . Оплата только после полной расшифровки и вашей проверки. Вот примерная схема работы:

1. Специалист компании подъезжает к вам в офис или на дом, и подписывает с вами договор, в котором фиксирует стоимость работ.
2. Запускает дешифратор и расшифровывает все файлы.
3. Вы убеждаетесь в том, что все файлы открываются, и подписываете акт сдачи/приемки выполненных работ.
4. Оплата исключительно по факту успешного результата дешифрации.

Подробнее о схеме работы- http://www.dr-shifro.ru/11_blog-details.html

Скажу честно, я не знаю, как они это делают, но вы ничем не рискуете. Оплата только после демонстрации работы дешифратора. Просьба написать отзыв об опыте взаимодействия с этой компанией.

Методы защиты от вируса da_vinci_code

Все способы защиты от вирусов шифровальщиков давно уже придуманы и известны. Я их приводил в предыдущих статьях по вирусам, повторяться не хочется. Самое главное — не открывать подозрительные вложения в почте. Все известные мне шифровальщики попали на компьютер пользователя через почту. Если вирус свежий, то ни один антивирус вам не поможет. Злоумышленники, прежде чем начать рассылать вирус, проверяют его всеми известными антивирусами. Они добиваются того, чтобы антивирусы никак не реагировали. После этого начинается рассылка. Так что первые жертвы гарантированно пострадают, если запустят вирусы. Остальным уже как повезет.

Как только эффективность вируса падает, а антивирусы начинают на него реагировать, выходит новая модификация и все начинается снова. И так по кругу уже года два. Именно в этот период я заметил самый расцвет вирусов-шифровальщиков. Раньше это была экзотика и редкость, а сейчас самый популярный тип вирусов, который заменил собой банеры-блокировщики. Но они по сравнению с шифровальщиками, просто детские шалости.

Второй совет по надежной защите от шифровальщиков — резервные копии, которые не подключены к компьютеры. То есть сделали копию и отключили носитель от компьютера, положили в ящик. Только так можно наверняка защитить информацию.

Видео с расшифровкой и восстановлением файлов

Watch this video on YouTube

Помогла статья? Есть возможность отблагодарить автора