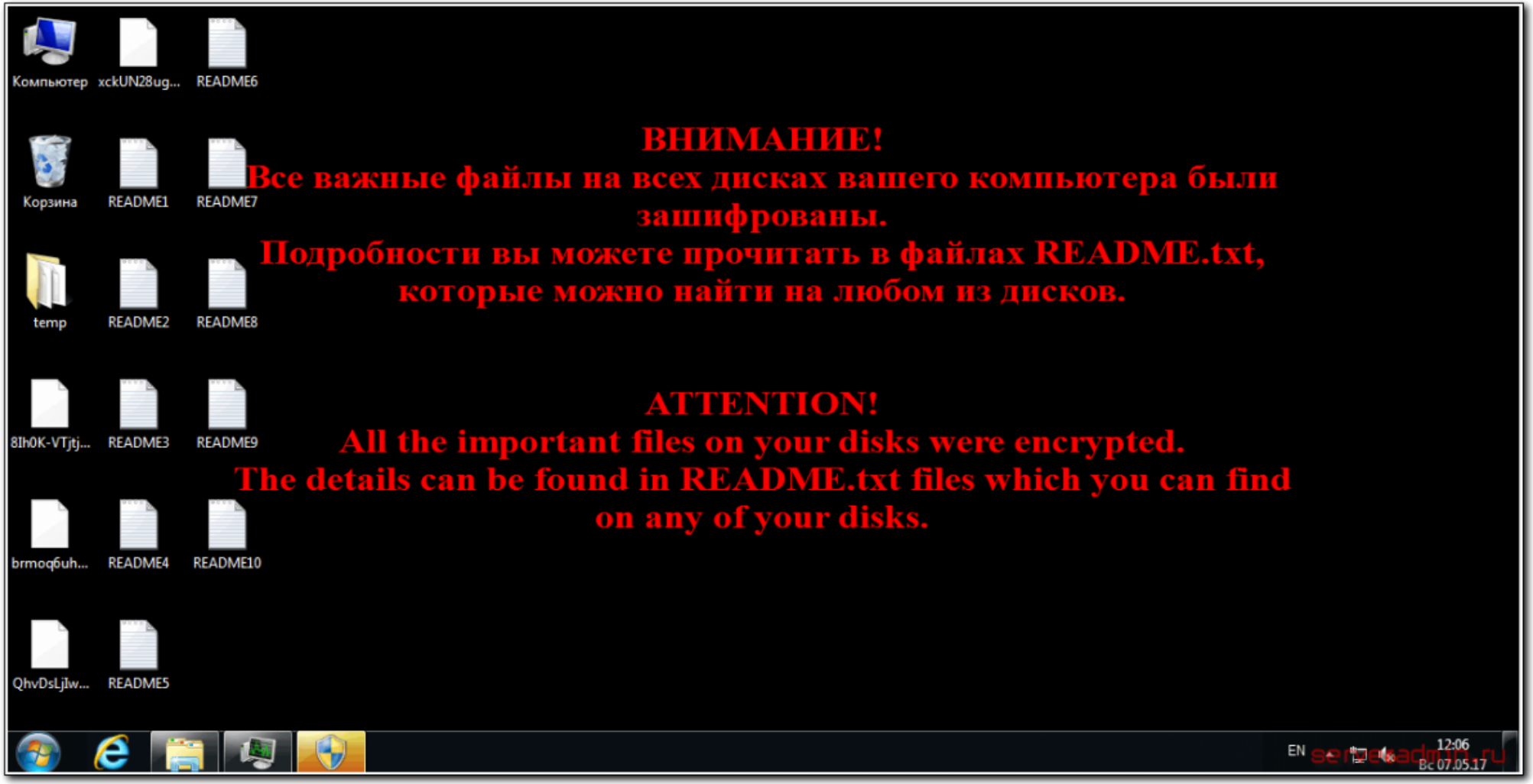


Около недели-двух назад в сети появилась очередная поделка современных вирусоделов, которая шифрует все файлы пользователя. В очередной раз рассмотрю вопрос как вылечить компьютер после вируса шифровальщика **crypted000007** и восстановить зашифрованные файлы. В данном случае ничего

нового и уникального не появилось, просто модификация предыдущей версии.

Содержание:

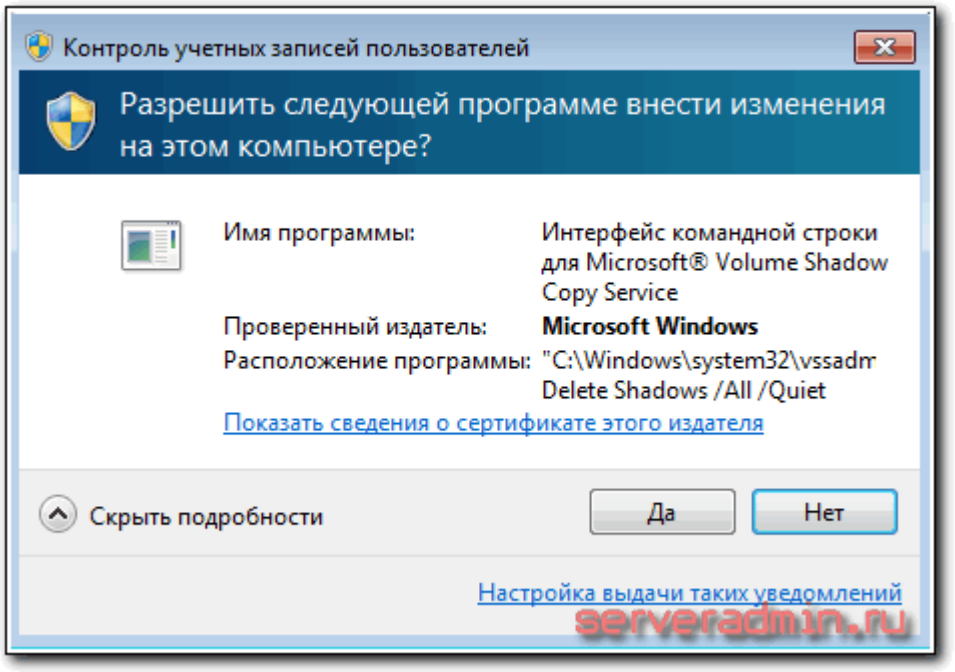
> Гарантированная расшифровка файлов после вируса шифровальщика - dr-shifro.ru. Подробности работы и схема взаимодействия с заказчиком ниже у меня в статье или на сайте в разделе "Порядок работы".

Описание вируса шифровальщика CRYPTED000007

Шифровальщик CRYPTED000007 ничем принципиально не отличается от своих предшественников. Действует он практически один в один как no_more_ransom. Но все же есть несколько нюансов, которые его отличают. Расскажу обо всем по порядку.

Приходит он, как и его аналоги, по почте. Используются приемы социальной инженерии, чтобы пользователь непременно заинтересовался письмом и открыл его. В моем случае в письме шла речь о каком-то суде и о важной информации по делу во вложении. После запуска вложения у пользователя открывается вордовский документ с выпиской из арбитражного суда Москвы.

Параллельно с открытием документа запускается шифрование файлов. Начинает постоянно выскакивать информационное сообщение от системы контроля учетных записей Windows.

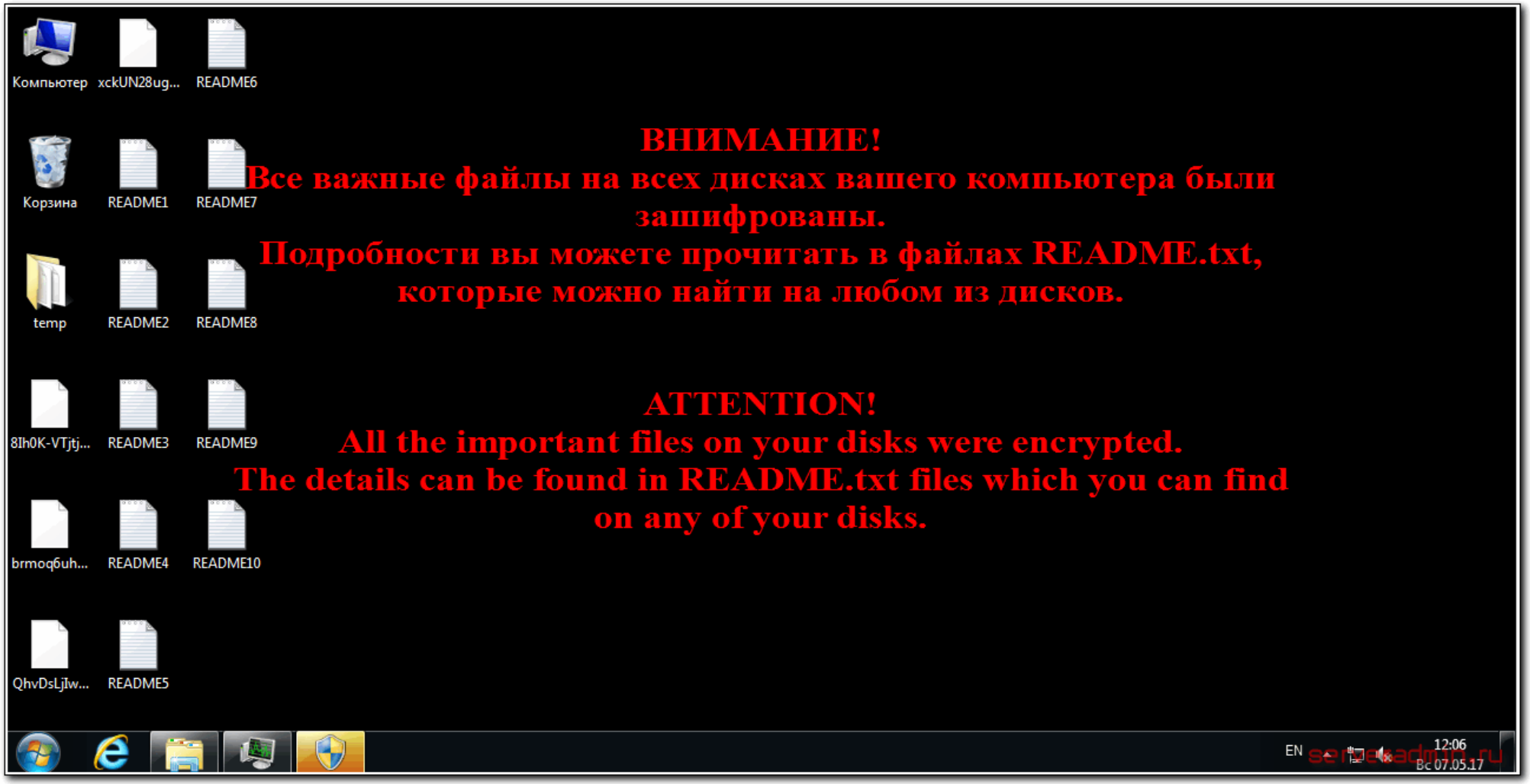


Если согласиться с предложением, то резервные копии файлов в теневых копиях Windows буду удалены и восстановление информации будет очень сильно затруднено. Очевидно, что соглашаться с предложением ни в коем случае нельзя. В данном шифровальщике эти запросы выскакивают постоянно, один за одним и не прекращаются, вынуждая пользователя таки согласиться и удалить резервные копии. Это главное отличие от предыдущих модификаций шифровальщиков. Я еще ни разу не сталкивался с тем, чтобы запросы на удаление теневых копий шли без остановки. Обычно, после 5-10-ти предложений они прекращались.

Дам сразу рекомендацию на будущее. Очень часто люди отключают предупреждения от системы контроля учетных записей. Этого делать

не надо. Данный механизм реально может помочь в противостоянии вирусам. Второй очевидный совет - не работайте постоянно под учетной записью администратора компьютера, если в этом нет объективной необходимости. В таком случае у вируса не будет возможности сильно навредить. У вас будет больше шансов ему противостоять.

Но даже если вы все время отвечали отрицательно на запросы шифровальщика, все ваши данные уже шифруются. После того, как процесс шифрования будет окончен, вы увидите на рабочем столе картинку.



Одновременно с этим на рабочем столе будет множество текстовых файлов с одним и тем же содержанием.

```
Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
329D54752553ED978F94|0
на электронный адрес gervasiy.menyaev@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке: https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/


All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
329D54752553ED978F94|0
to e-mail address gervasiy.menyaev@gmail.com .
Then you will receive all necessary instructions.
All the attempts of decryption by yourself will result only in irrevocable loss of your data.
If you still want to try to decrypt them by yourself please make a backup at first because
the decryption will become impossible in case of any changes inside the files.
If you did not receive the answer from the aforecited email for more than 48 hours (and only in this case!),
use the feedback form. You can do it by two ways:
1) Download Tor Browser from here:
https://www.torproject.org/download/download-easy.html.en
Install it and type the following address into the address bar:
```

```
http://cryptsen7fo43rr6.onion/
Press Enter and then the page with feedback form will be loaded.
2) Go to the one of the following addresses in any browser:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/
```

Почтовый адрес может меняться. Я встречал еще такие адреса:

- Novikov.Vavila@gmail.com
- lukyan.sazonov26@gmail.com

Адреса постоянно обновляются, так что могут быть совершенно разными.

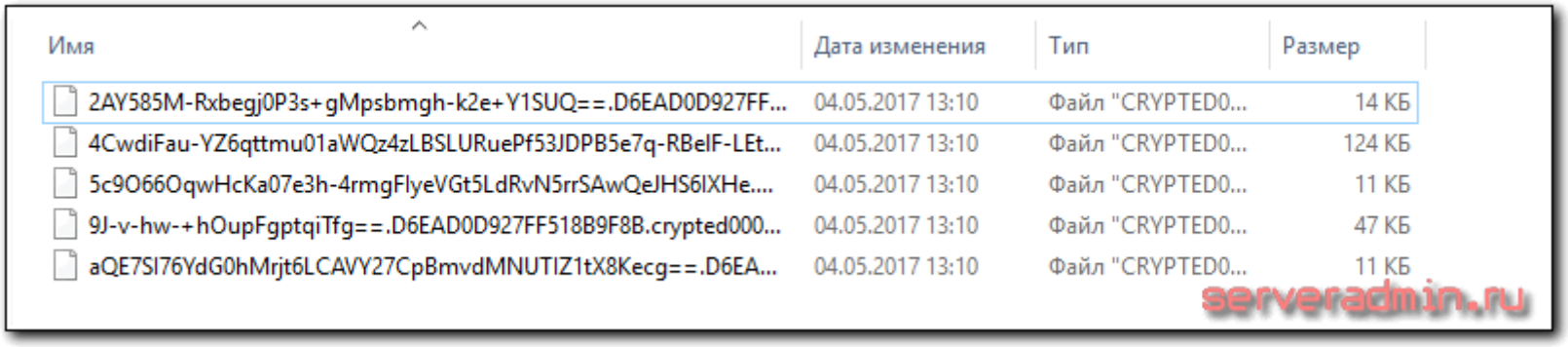
Как только вы обнаружили, что файлы зашифрованы, сразу же выключайте компьютер. Это нужно сделать, чтобы прервать процесс шифрования как на локальном компьютере, так и на сетевых дисках. Вирус-шифровальщик может зашифровать всю информацию, до которой сможет дотянуться, в том числе и на сетевых дисках. Но если там большой объем информации, то ему для этого потребуется значительное время. Иногда и за пару часов шифровальщик не успевал все зашифровать на сетевом диске объемом примерно в 100 гигабайт.

Дальше нужно хорошенько подумать, как действовать. Если вам во что бы то ни стало нужна информация на компьютере и у вас нет резервных копий, то лучше в этот момент обратиться к специалистам. Не обязательно за деньги в какие-то фирмы. Просто нужен человек, который хорошо разбирается в информационных системах. Необходимо оценить масштаб бедствия, удалить вирус, собрать всю имеющуюся информацию по ситуации, чтобы понять, как действовать дальше.

Неправильные действия на данном этапе могут существенно усложнить процесс расшифровки или восстановления файлов. В худшем случае могут сделать его невозможным. Так что не торопитесь, будьте аккуратны и последовательны.

Как вирус вымогатель CRYPTED000007 шифрует файлы

После того, как вирус у вас был запущен и закончил свою деятельность, все полезные файлы будут зашифрованы, переименованы с **расширением .crypted000007**. Причем не только расширение файла будет заменено, но и имя файла, так что вы не узнаете точно, что за файлы у вас были, если сами не помните. Будет примерно такая картина.



В такой ситуации будет трудно оценить масштаб трагедии, так как вы до конца не сможете вспомнить, что же у вас было в разных папках. Сделано это специально, чтобы сбить человека с толка и побудить к оплате расшифровки файлов.

А если у вас были зашифрованы и сетевые папки и нет полных бэкапов, то это может вообще остановить работу всей организации. Не сразу разберешься, что в итоге потеряно, чтобы начать восстановление.

Как лечить компьютер и удалить вымогатель CRYPTED000007

Вирус CRYPTED000007 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. Сразу обращаю ваше внимание на то, что после того, как вы сами начнете производить какие-то действия со своим компьютером, шансы на расшифровку данных уменьшаются. Если вам во что бы то ни стало нужно восстановить файлы, компьютер не трогайте, а сразу обращайтесь к профессионалам. Ниже я расскажу о них и приведу ссылку на сайт и опишу схему их работы.

А пока продолжим самостоятельно лечить компьютер и удалять вирус. Традиционно шифровальщики легко удаляются из компьютера, так как у вируса нет задачи во что бы то ни стало остаться на компьютере. После полного шифрования файлов ему даже выгоднее самоудалиться и исчезнуть, чтобы было труднее расследовать инцидент и расшифровать файлы.

Описать ручное удаление вируса трудно, хотя я пытался раньше это делать, но вижу, что чаще всего это бессмысленно. Названия файлов и пути размещения вируса постоянно меняются. То, что видел я уже не актуально через неделю-две. Обычно рассылка вирусов по почте идет волнами и каждый раз там новая модификация, которая еще не детектится антивирусами. Помогают универсальные средства, которые проверяют автозапуск и детектят

подозрительную активность в системных папках.

Для удаления вируса CRYPTED000007 можно воспользоваться следующими программами:

1. Kaspersky Virus Removal Tool - утилитой от касперского http://www.kaspersky.ru/antivirus-removal-tool.
2. Dr.Web CureIt! - похожий продукт от др.веб http://free.drweb.ru/cureit.
3. Если не помогут первые две утилиты, попробуйте MALWAREBYTES 3.0 - https://ru.malwarebytes.com.

Скорее всего, что-то из этих продуктов очистит компьютер от шифровальщика CRYPTED000007. Если вдруг так случится, что они не помогут, попробуйте удалить вирус вручную. Методику по удалению я приводил на примере вируса да винчи и spora, можете посмотреть там. Если кратко по шагам, то действовать надо так:

1. Смотрим список процессов, предварительно добавив несколько дополнительных столбцов в диспетчер задач.
2. Находим процесс вируса, открываем папку, в которой он сидит и удаляем его.
3. Чистим упоминание о процессе вируса по имени файла в реестре.
4. Перезагружаемся и убеждаемся, что вируса CRYPTED000007 нет в списке запущенных процессов.

Где скачать дешифратор CRYPTED000007

Вопрос простого и надежного дешифратора встает в первую очередь, когда дело касается вируса-шифровальщика. Первое, что я посоветую, это воспользоваться сервисом https://www.nomoreransom.org. А вдруг вам повезет у них будет дешифратор под вашу версию шифровальщика CRYPTED000007. Скажу сразу, что шансов у вас не много, но попытка не пытка. На главной странице нажимаете Yes:

Затем загружаете пару зашифрованных файлов и нажимаете Go! Find out:

На момент написания статьи дешифратора на сайте не было.

Возможно вам повезет больше. Можно еще ознакомиться со списком дешифраторов для скачивания на отдельной странице - https://www.nomoreransom.org/decryption-tools.html. Может быть там найдется что-то полезное. Когда вирус совсем свежий шансов на это мало, но со временем возможно что-то появится. Есть примеры, когда в сети появлялись дешифраторы к некоторым модификациям шифровальщиков. И эти примеры есть на указанной странице.

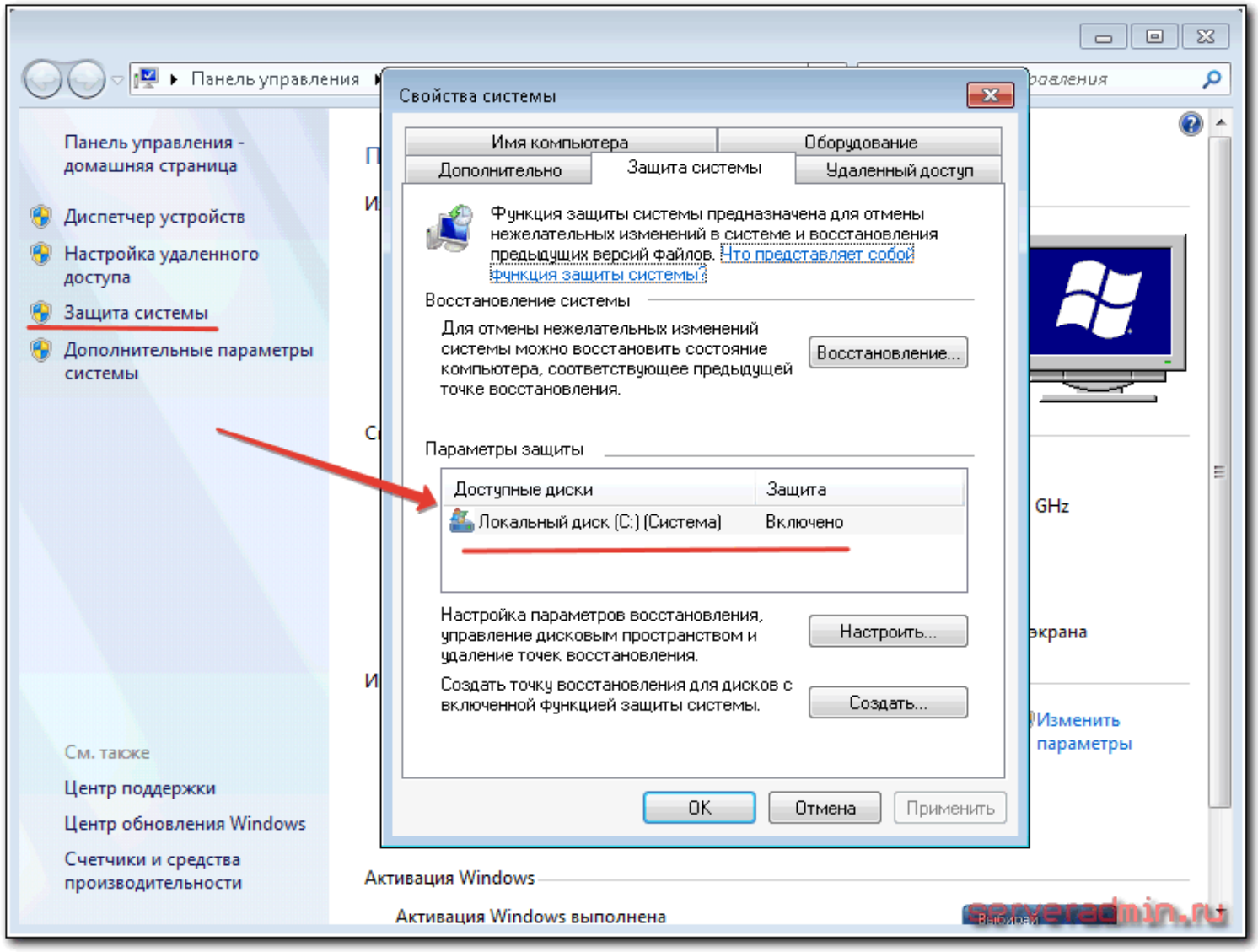
Где еще можно найти дешифратор я не знаю. Вряд ли он реально будет существовать, с учетом особенностей работы современных шифровальщиков. Полноценный дешифратор может быть только у авторов вируса.

Как расшифровать и восстановить файлы после вируса CRYPTED000007

Что делать, когда вирус CRYPTED000007 зашифровал ваши файлы? Техническая реализация шифрования не позволяет выполнить расшифровку файлов без ключа или дешифратора, который есть только у автора шифровальщика. Может быть есть какой-то еще способ его получить, но у меня нет такой информации. Нам остается только попытаться восстановить файлы подручными способами. К таким относится:

- Инструмент **теневых копий** windows.
- Программы по восстановлению удаленных данных

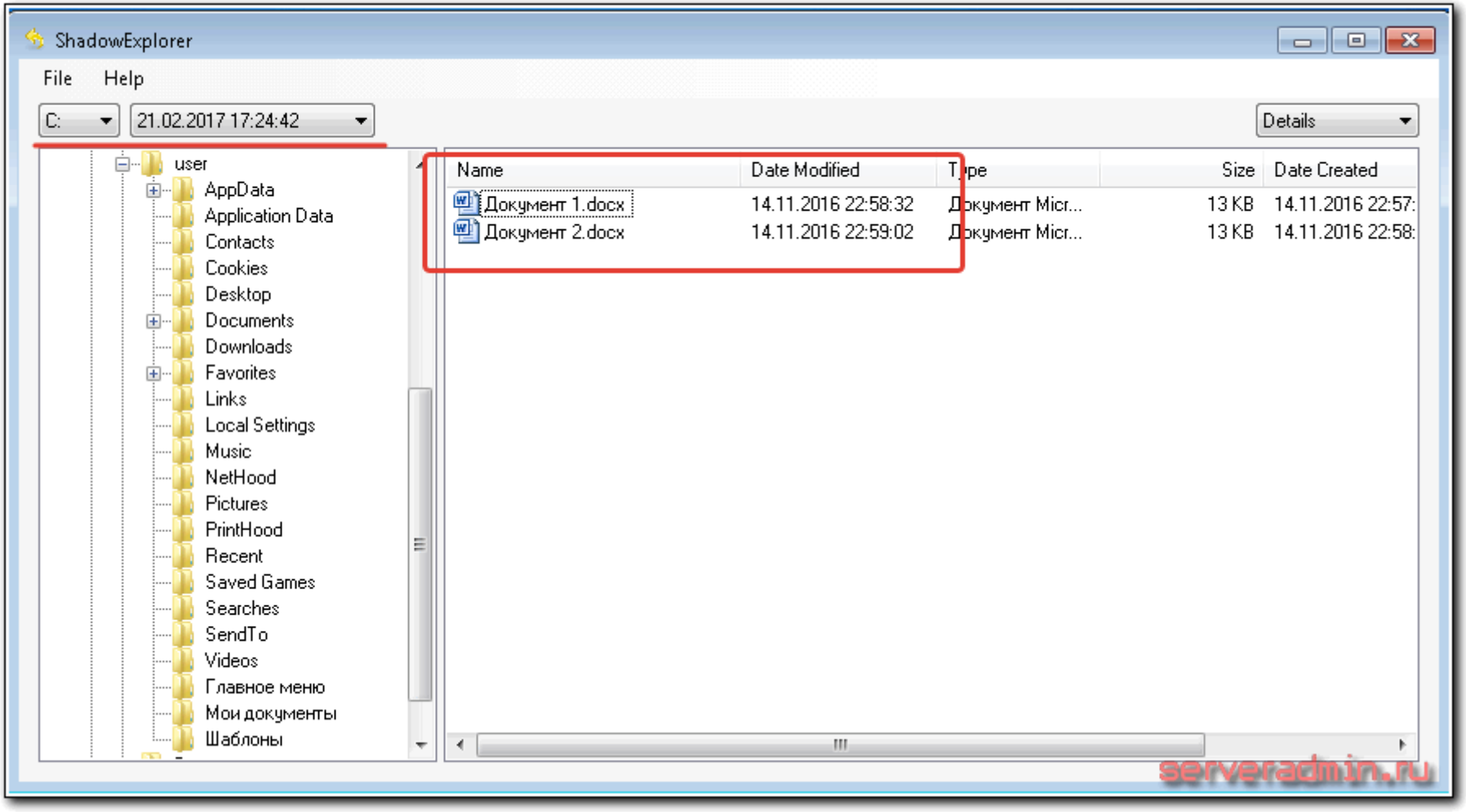
Для начала проверим, включены ли у нас теневые копии. Этот инструмент по-умолчанию работает в windows 7 и выше, если вы его не отключили вручную. Для проверки открываем свойства компьютера и переходим в раздел защита системы.


Панель управления
Панель управления - домашняя страница
Диспетчер устройств
Настройка удаленного доступа
Защита системы
Дополнительные параметры системы
См. также
Центр поддержки
Центр обновления Windows
Счетчики и средства производительности
Свойства системы
Имя компьютера
Оборудование
Дополнительно
Защита системы
Удаленный доступ
Функция защиты системы предназначена для отмены нежелательных изменений в системе и восстановления предыдущих версий файлов. Что представляет собой функция защиты системы?
Восстановление системы
Для отмены нежелательных изменений системы можно восстановить состояние компьютера, соответствующее предыдущей точке восстановления.
Восстановление...
Параметры защиты
Доступные диски
Защита
Локальный диск (C:) (Система)
Включено
Настройка параметров восстановления, управление дисковым пространством и удаление точек восстановления.
Настроить...
Создать точку восстановления для дисков с включенной функцией защиты системы.
Создать...
OK
Отмена
Применить
Изменить параметры
Активация Windows
Активация Windows выполнена
serveradmin.ru

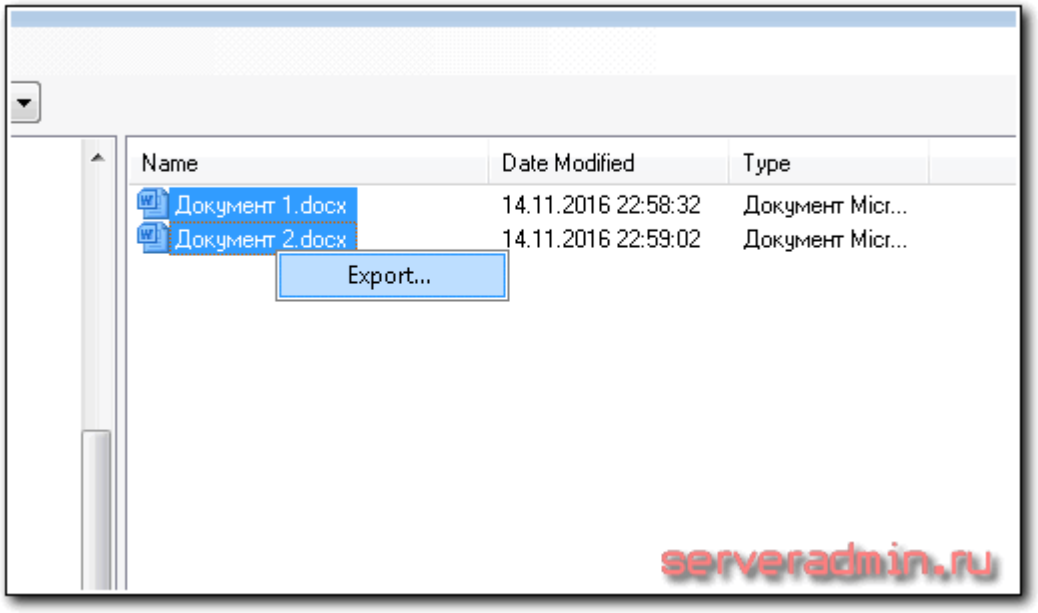
Если вы во время заражения не подтвердили запрос UAC на удаление файлов в теневых копиях, то какие-то данные у вас там должны остаться. Подробнее об этом запросе я рассказал в начале повествования, когда рассказывал о работе вируса.

Для удобного восстановления файлов из теневых копий предлагаю воспользоваться бесплатной программой для этого - ShadowExplorer. Скачивайте архив, распаковывайте программу и запускайте.

Откроется последняя копия файлов и корень диска C. В левом верхнем углу можно выбрать резервную копию, если у вас их несколько. Проверьте разные копии на наличие нужных файлов. Сравните по датам, где более свежая версия. В моем примере ниже я нашел 2 файла на рабочем столе трехмесячной давности, когда они последний раз редактировались.



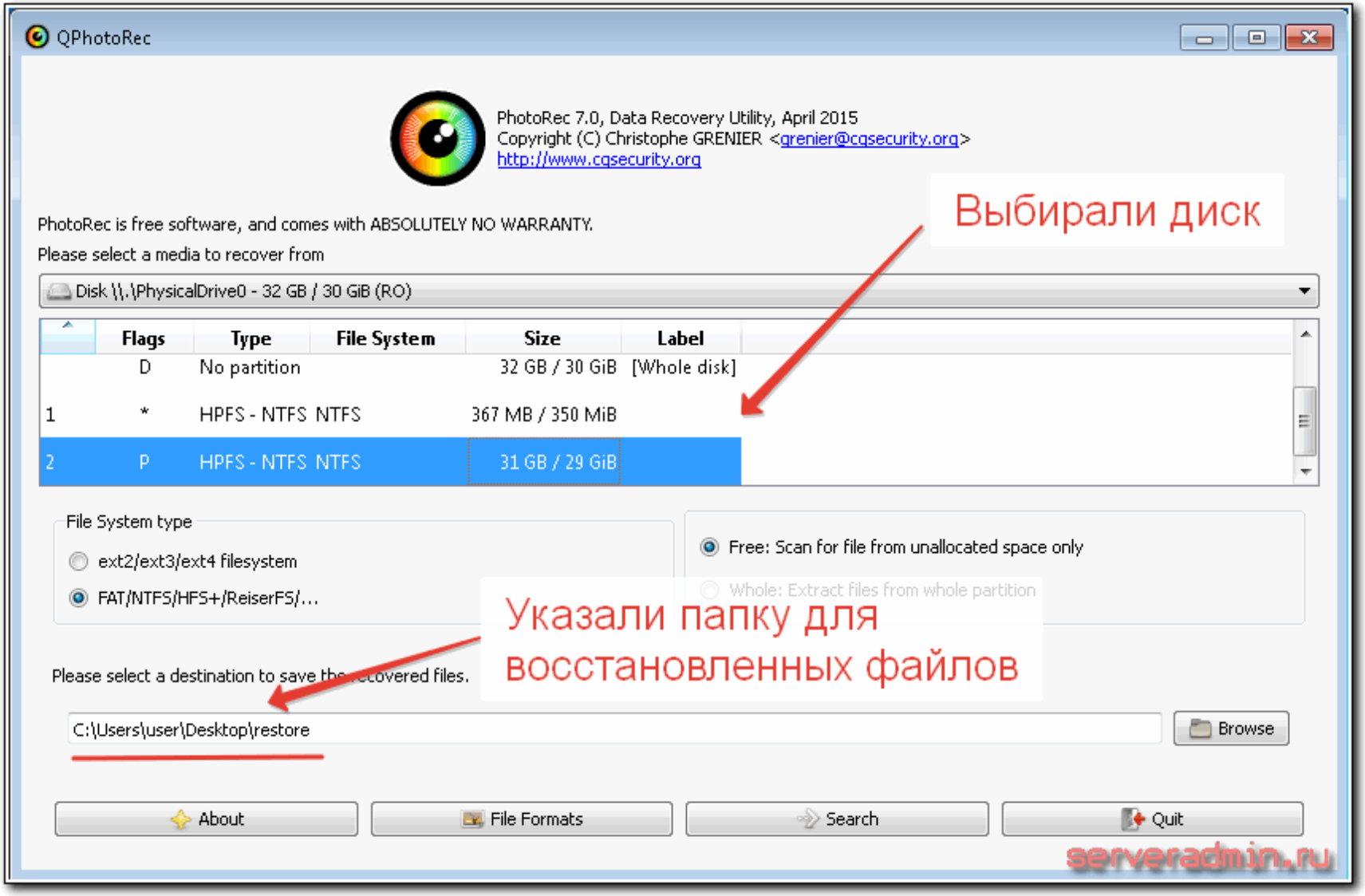
Мне удалось восстановить эти файлы. Для этого я их выбрал, нажал правой кнопкой мыши, выбрал Export и указал папку, куда их восстановить.



Вы можете восстанавливать сразу папки по такому же принципу. Если у вас работали теневые копии и вы их не удаляли, у вас достаточно много шансов восстановить все, или почти все файлы, зашифрованные вирусом. Возможно, какие-то из них будут более старой версии, чем хотелось бы, но тем не менее, это лучше, чем ничего.

Если по какой-то причине у вас нет теневых копий файлов, остается единственный шанс получить хоть что-то из зашифрованных файлов - восстановить их с помощью средств восстановления удаленных файлов. Для этого предлагаю воспользоваться бесплатной программой Photorec.

Запускайте программу и выбирайте диск, на котором будете восстанавливать файлы. Запуск графической версии программы выполняет файл *qphotorec_win.exe*. Необходимо выбрать папку, куда будут помещаться найденные файлы. Лучше, если эта папка будет располагаться не на том же диске, где мы осуществляем поиск. Подключите флешку или внешний жесткий диск для этого.


QPhotoRec
PhotoRec 7.0, Data Recovery Utility, April 2015
Copyright (C) Christophe GRENIER <grenier@cgsecurity.org>
http://www.cgsecurity.org
Выбирали диск
PhotoRec is free software, and comes with ABSOLUTELY NO WARRANTY.
Please select a media to recover from
Disk \\.\PhysicalDrive0 - 32 GB / 30 GiB (RO)
Flags Type File System Size Label
D No partition 32 GB / 30 GiB [Whole disk]
1 * HPFS - NTFS NTFS 367 MB / 350 MiB
2 P HPFS - NTFS NTFS 31 GB / 29 GiB
File System type
ext2/ext3/ext4 filesystem
FAT/NTFS/HFS+/ReiserFS/...
Free: Scan for file from unallocated space only
Whole: Extract files from whole partition
Указали папку для восстановленных файлов
Please select a destination to save the recovered files.
C:\Users\user\Desktop\restore
Browse
About
File Formats
Search
Quit
serveradmin.ru

Процесс поиска будет длиться долго. В конце вы увидите статистику. Теперь можно идти в указанную ранее папку и смотреть, что там найдено. Файлов будет скорее всего много и большая часть из них будут либо повреждены, либо это будут какие-то системные и бесполезные файлы. Но тем не менее, в этом списке можно будет найти и часть полезных файлов. Тут уже никаких гарантий нет, что найдете, то и найдете. Лучше всего, обычно, восстанавливаются изображения.

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

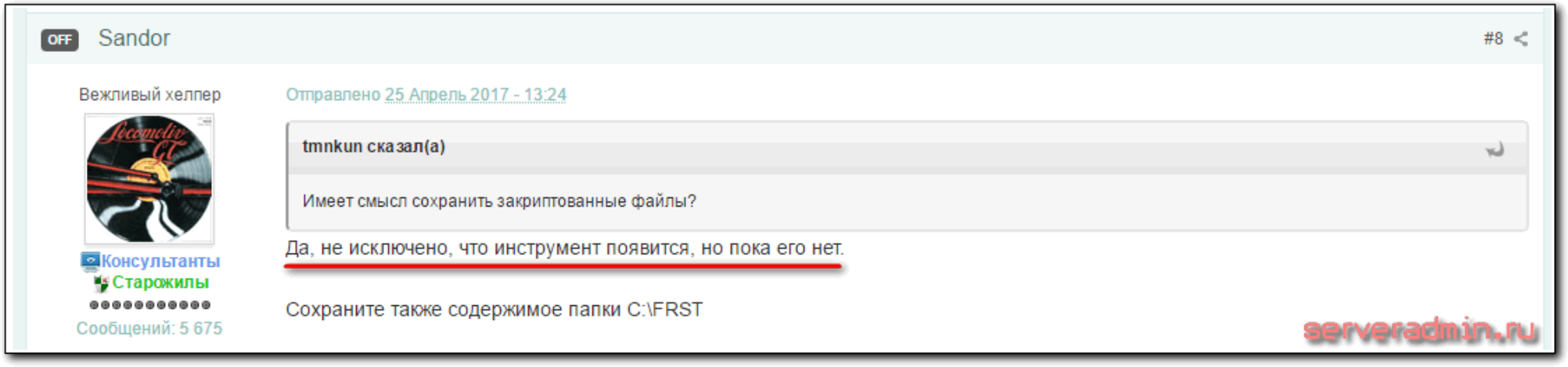
- R.saver
- Starus File Recovery
- JPEG Recovery Pro
- Active File Recovery Professional

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

Весь процесс восстановления файлов подробно показан в видео в самом конце статьи.

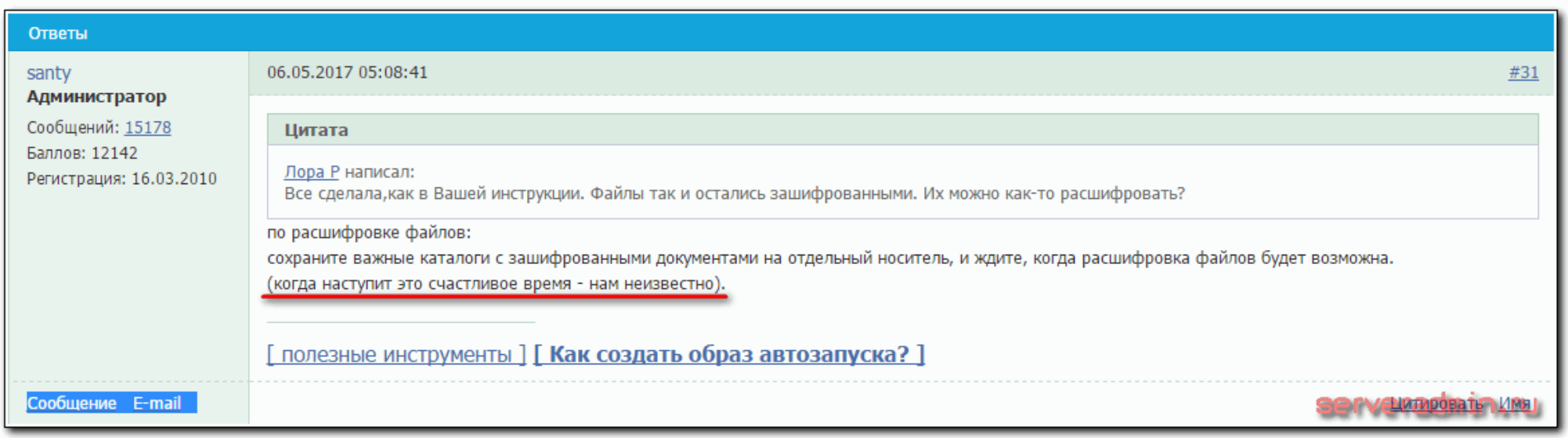
Касперский, eset nod32 и другие в борьбе с шифровальщиком Filecoder.ED

Популярные антивирусы определяю шифровальщик CRYPTED000007 как **Filecoder.ED** и дальше может быть еще какое-то обозначение. Я пробежался по форумам основных антивирусов и не увидел там ничего полезного. К сожалению, как обычно, антивирусы оказались не готовы к нашествию новой волны шифровальщиков. Вот сообщение с форума Kaspersky.



https://forum.kasperskyclub.ru/index.php?showtopic=55324

Вот результат подробного обсуждения шифровальщика CRYPTED000007 на форуме антивируса Eset nod32. Обращений уже очень много, а антивирус ничего не может поделать.


Ответы

santy
Администратор
Сообщений: 15178
Баллов: 12142
Регистрация: 16.03.2010

06.05.2017 05:08:41 #31

Цитата

Лора Р написал:
Все сделала,как в Вашей инструкции. Файлы так и остались зашифрованными. Их можно как-то расшифровать?

по расшифровке файлов:
сохраните важные каталоги с зашифрованными документами на отдельный носитель, и ждите, когда расшифровка файлов будет возможна.
(когда наступит это счастливое время - нам неизвестно).

[полезные инструменты] [Как создать образ автозапуска?]

Сообщение E-mail

Цитировать Имя

http://forum.esetnod32.ru/forum35/topic13688/?PAGEN_1=27

Антивирусы традиционно пропускают новые модификации троянов-шифровальщиков. И тем не менее, я рекомендую ими пользоваться. Если вам повезет, и вы получите на почту шифровальщика не в первую волну заражений, а чуть позже, есть шанс, что антивирус вам поможет. Они все работает на шаг позади злоумышленников. Выходит новая версия вымогателя, антивирусы на нее не реагируют. Как только накапливается определенная масса материала для исследования по новому вирусу, антивирусы выпускают обновление и начинают на него реагировать.

Что мешает антивирусам реагировать сразу же на любой процесс шифрования в системе, мне не понятно. Возможно, есть какой-то технический нюанс на эту тему, который не позволяет адекватно среагировать и предотвратить шифрование пользовательских файлов. Мне кажется, можно было бы хотя бы предупреждение выводить на тему того, что кто-то шифрует ваши файлы, и предложить остановить процесс.

Куда обратиться за гарантированной расшифровкой

Мне довелось познакомиться с одной компанией, которая реально расшифровывает данные после работы различных вирусов-шифровальщиков, в том

числе CRYPTED000007. 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 CRYPTED000007

Как защититься от работы шифровальщика и обойтись без материального и морального ущерба? Есть несколько простых и эффективных советов:

1. Бэкап! Резервная копия всех важных данных. И не просто бэкап, а бэкап, к которому нет постоянного доступа. Иначе вирус может заразить как ваши документы, так и резервные копии.
2. Лицензионный антивирус. Хотя они не дают 100% гарантии, но шансы избежать шифрования увеличивают. К новым версиям шифровальщика они чаще всего не готовы, но уже через 3-4 дня начинают реагировать. Это повышает ваши шансы избежать заражения, если вы не попали в первую волну рассылки новой модификации шифровальщика.
3. Не открывайте подозрительные вложения в почте. Тут комментировать нечего. Все известные мне шифровальщики попали к пользователям через почту. Причем каждый раз придумываются новые ухищрения, чтобы обмануть жертву.
4. Не открывайте бездумно ссылки, присланные вам от ваших знакомых через социальные сети или мессенджеры. Так тоже иногда распространяются вирусы.
5. Включите в windows отображение расширений файлов. Как это сделать легко найти в интернете. Это позволит вам заметить расширение файла на вирусе. Чаще всего оно будет **.exe**, **.vbs**, **.src**. В повседеневной работе с документами вам вряд ли попадаются подобные расширения файлов.

Постарался дополнить то, что уже писал раньше в каждой статье про вирус шифровальщик. А пока прощаюсь. Буду рад полезным замечаниям по статье и вирусу-шифровальщику CRYPTED000007 в целом.

Видео с расшифровкой и восстановлением файлов

Здесь пример предыдущей модификации вируса, но видео полностью актуально и для CRYPTED000007.

Watch this video on YouTube

Помогла статья? Подписывайся на telegram канал автора

Анонсы всех статей, плюс много другой полезной и интересной информации, которая не попадает на сайт.