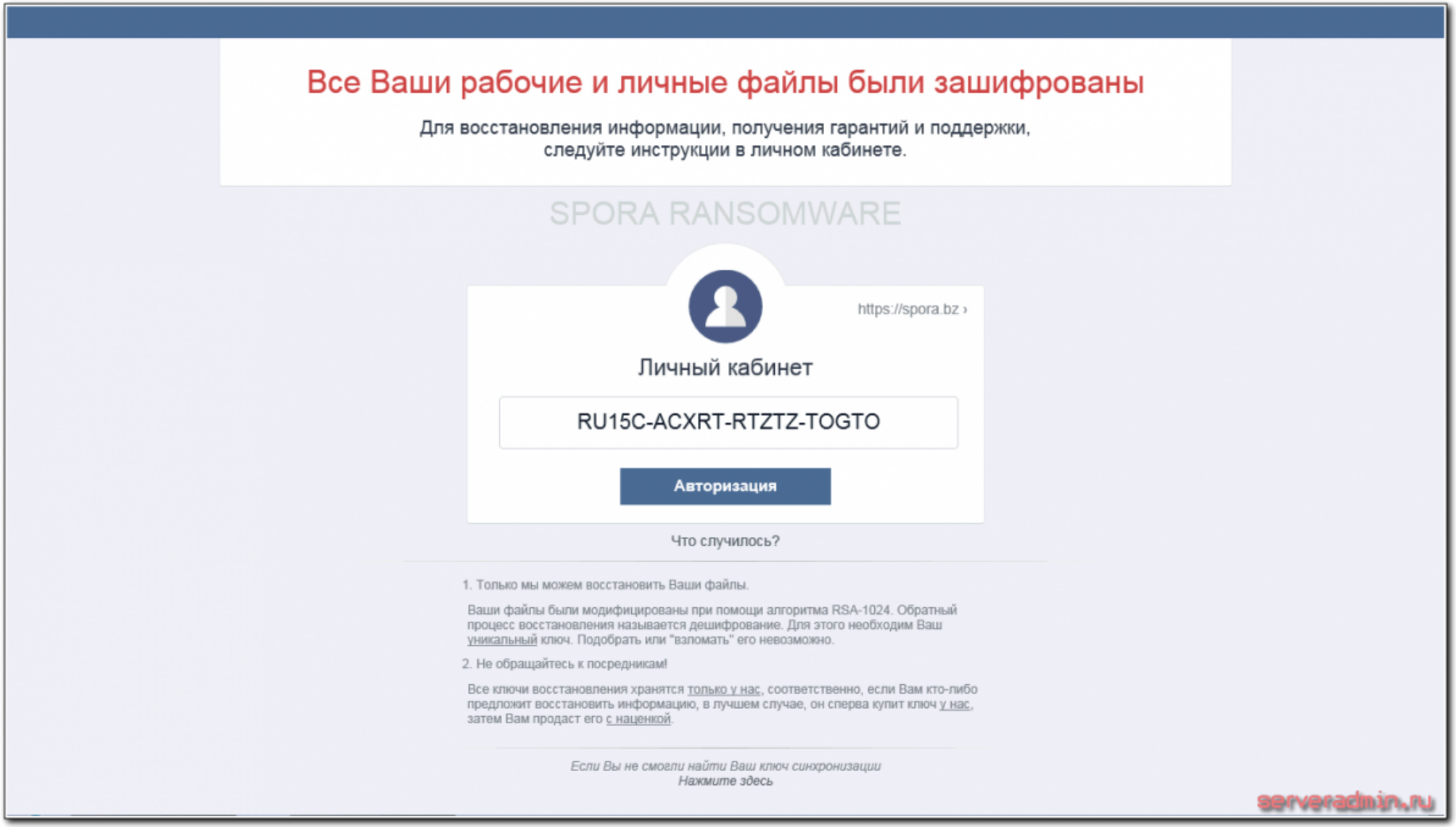

Все Ваши рабочие и личные файлы были зашифрованы
Для восстановления информации, получения гарантий и поддержки,
следуйте инструкции в личном кабинете.
SPORA RANSOMWARE
https://spora.bz ›
Личный кабинет
RU15C-ACXRT-RTZTZ-TOGTO
Авторизация
Что случилось?
1. Только мы можем восстановить Ваши файлы.
Ваши файлы были модифицированы при помощи алгоритма RSA-1024. Обратный процесс восстановления называется дешифрование. Для этого необходим Ваш уникальный ключ. Подобрать или "взломать" его невозможно.
2. Не обращайтесь к посредникам!
Все ключи восстановления хранятся только у нас, соответственно, если Вам кто-либо предложит восстановить информацию, в лучшем случае, он сперва купит ключ у нас, затем Вам продаст его с наценкой.
Если Вы не смогли найти Ваш ключ синхронизации
Нажмите здесь
serveradmin.ru

Месяц назад столкнулся с очередным шедевром вирусоделов, который оказался не похож на все то, что я видел ранее. Я расскажу вам о продвинутом вирусе вымогателе-шифровальщике **spora ransomware**, о способах расшифровки файлов и лечении. Хакеры разработали принципиально новый подход к разводу пользователей на приличные деньги. Далее расскажу обо всем по порядку.

Содержание:

Описание вируса шифровальщика spora ransomware

Расскажу подробно о том, что это такое - spora ransomware. Назвать его просто вирусом шифровальщиком, подобно ранее известным vault, da_vinci_code, enigma, no_more_ramsom язык не поворачивается. По сути это целый программный комплекс, состоящий из:

1. Непосредственно вируса, который шифрует пользовательские файлы.
2. Сайта для взаимодействия с инструментами расшифровки.
3. Модуля приема оплаты в биткоинах.
4. Чата для техподдержки пострадавшим.

Все сделано на очень высоком техническом уровне, начиная от самого трояна-вымогателя, заканчивая самим сайтом. Работа по шифрованию файлов сделана очень аккуратно и незаметно. Если раньше шифровальщики заменяли расширения файла, что сразу указывало на то, что файл зашифровали, то теперь криптолокер действует хитрее - он шифрует файлы, не изменяя название файлов и их расширение. Это позволяет ему оставаться незаметным до тех пор, пока он не закончит свою работу. Особенно это актуально с сетевыми дисками, где сразу не догадаешься, что идет шифрование, если работают с файлами разные пользователи по сети.

Но я забегаю вперед. Расскажу обо всем по порядку, начиная от заражения компьютера, заканчивая вариантами расшифровки и восстановления файлов.

> Важное замечание сделаю сразу же. Данный шифровальщик шифрует в том числе и сетевые диски, до которых сможет добраться. Как только заподозрили на компьютере вирус - сразу же отключайте его от сети. А лучше полностью выключите.

Как вирус вымогатель spora шифрует файлы

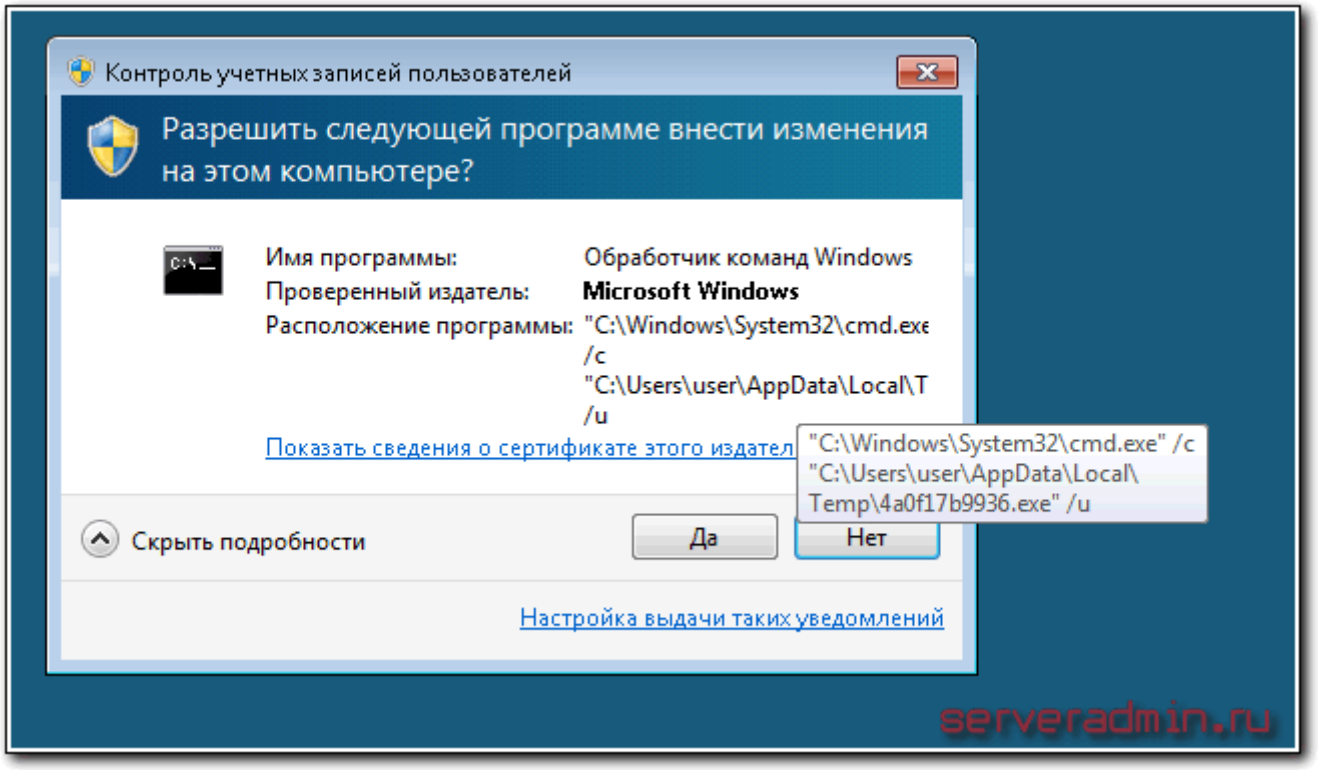
Начинается все, как обычно со всеми вирусами шифровальщиками - с письма на почту. Письмо это будет специально подобрано по содержанию, чтобы максимально напоминать рабочую переписку, если рассылка ведется по корпоративной базе почтовых ящиков. К примеру, там может быть просьба от какого-то контрагента сверить бухгалтерские документы, или посмотреть счет фактуру, либо что-то еще. Если рассылка идет по личным ящикам пользователей, то оно будет замаскировано под письмо от сбербанка, налоговой или какой-то еще популярной в народе службы.

Главная задача такого письма - заставить пользователя запустить вложение. В случае с spora, во вложении будет zip архив, внутри которого файл с расширением .**hta**. После запуска этого файла, во временной директории пользователя создается новый файл с расширением .js, в который записывается зашифрованный JScript и выполняется. Сам скрипт с вирусом зашифрован стандартными системными алгоритмами, чтобы его не обнаружили антивирусы.

После выполнения скрипта, во временной директории пользователя *C:\Users\user\AppData\Local\Temp* появятся два файла:

- **4a0f17b9936.exe**
- **doc_113fce.docx**

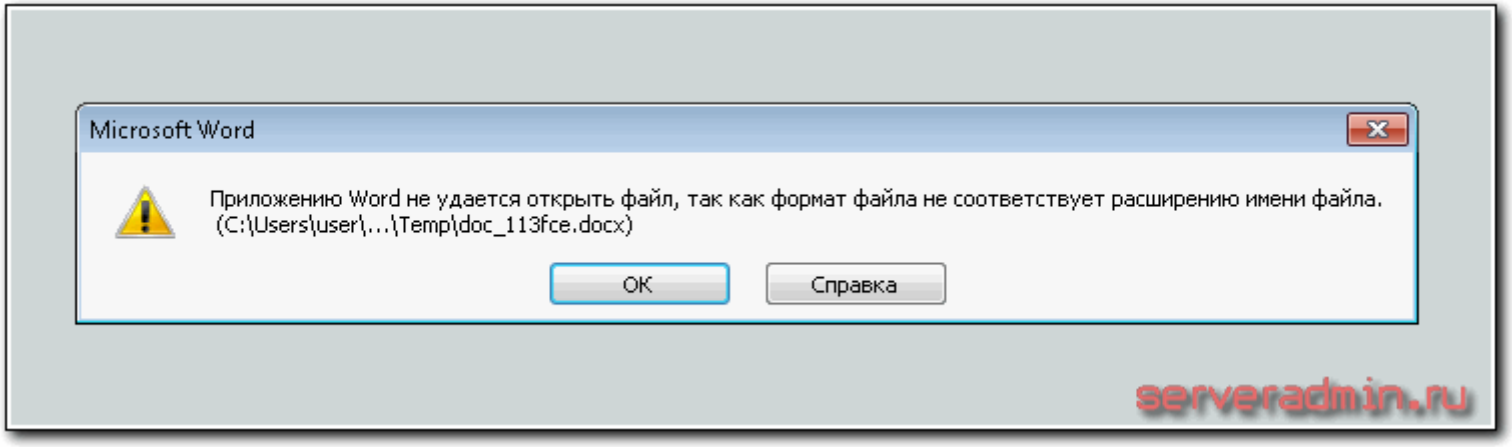
Имена файлов скорее всего в каждом конкретном случае будут разными, но по типу будут такие же. Первое это исполняемый файл, который и является шифровальщиком. Сразу после создания, он запускается и начинает свою черную работу по шифрованию файлов.



Если у вас включен UAC, то вы увидите запрос на выполнение файла. Вирус пытается удалить все теневые копии, а для этого нужно подтверждение. Если не подтвердите запуск файла, то считайте, что вам повезло, и ваши теневые копии останутся. А если подтвердите выполнение, или если у вас вообще отключен UAC, то ваши теневые копии будут удалены командой:

```
vssadmin.exe delete shadows /all /quiet
```

Второй файл является пустышкой, который замаскирован под файл формата word, но при этом открывается с ошибкой.



Он сделан, скорее всего, для того, чтобы запутать пользователя. Человек может подумать, что просто файл повредился. Это может побудить его еще раз открыть вложение из письма, чтобы убедиться, что письмо не открывается. Особо сообразительные люди отправляют письмо коллегам с просьбой проверить, открывается ли у них этот файл. Сам лично наблюдал такое поведение. В итоге шансы у вируса-вымогателя выполнить свою работу увеличиваются.

После того, как вирус запустился и зашифровал все файлы, которые смог найти, он создает 2 файла на рабочем столе пользователя:

- **RU15C-ACXRT-RTZTZ-TOGTO.HTML**
- **RU15C-ACXRT-RTZTZ-TOGTO.KEY**

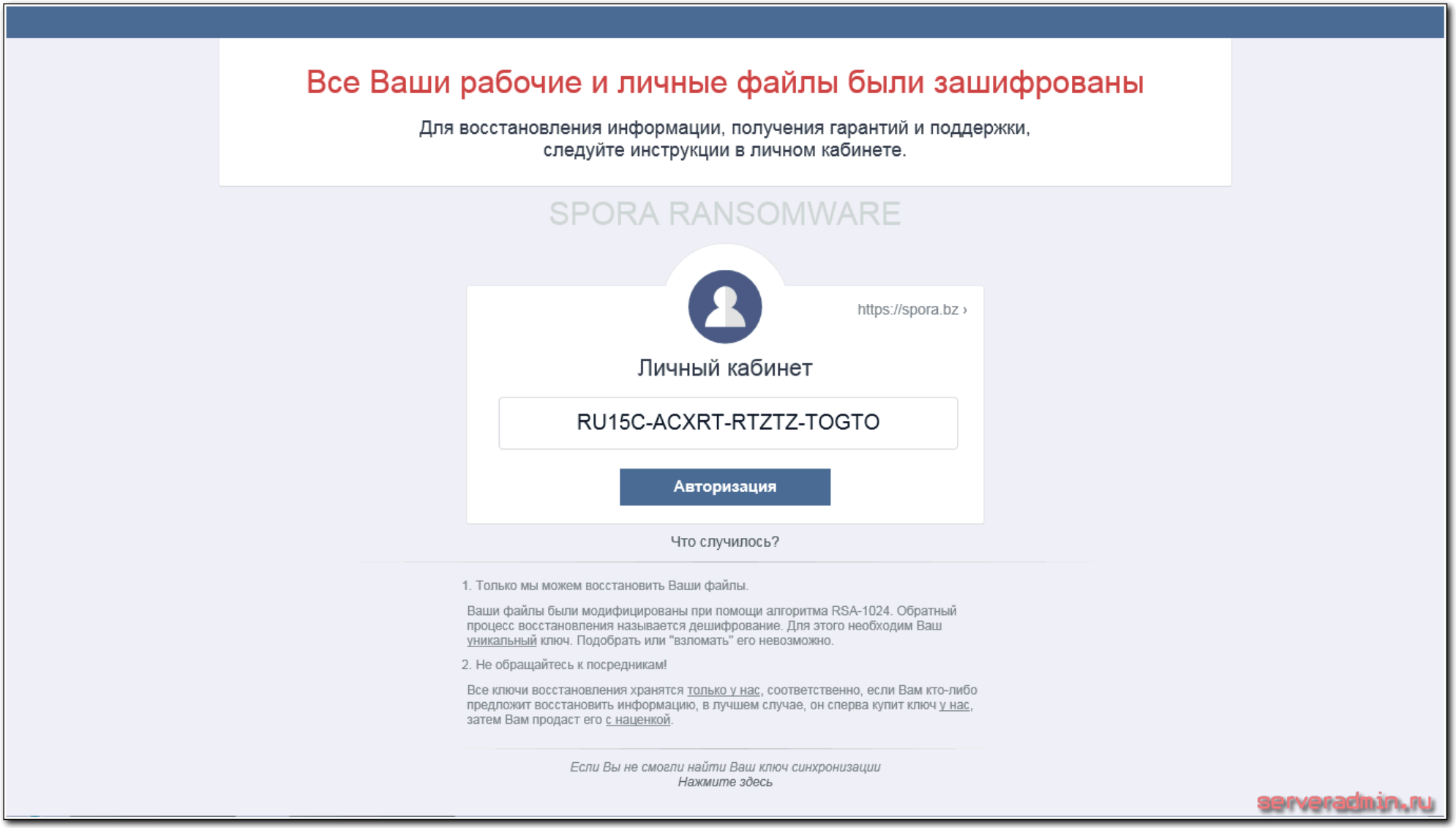
Первый файл - html страничка, которая автоматически запускается. Она содержит в себе краткую информацию о том, что произошло на компьютере:

```
Все ваши рабочие и личные файлы были зашифрованы.
Для восстановления информации, получения гарантий и поддержки, следуйте инструкции в личном кабинете.

1. Только мы можем восстановить Ваши файлы.

Ваши файлы были модифицированы при помощи алгоритма RSA-1024. Обратный процесс восстановления называется дешифрование.
```

```
Для этого необходим Ваш уникальный ключ. Подобрать или "взломать" его невозможно.
2. Не обращайтесь к посредникам!
Все ключи восстановления хранятся только у нас, соответственно, если Вам кто-либо предложит восстановить информацию, в
лучшем случае, он сперва купит ключ у нас, затем Вам продаст его с наценкой.
```


Все Ваши рабочие и личные файлы были зашифрованы
Для восстановления информации, получения гарантий и поддержки,
следуйте инструкции в личном кабинете.
SPORA RANSOMWARE
https://spora.bz ›
Личный кабинет
RU15C-ACXRT-RTZTZ-TOGTO
Авторизация
Что случилось?
1. Только мы можем восстановить Ваши файлы.
Ваши файлы были модифицированы при помощи алгоритма RSA-1024. Обратный процесс восстановления называется дешифрование. Для этого необходим Ваш уникальный ключ. Подобрать или "взломать" его невозможно.
2. Не обращайтесь к посредникам!
Все ключи восстановления хранятся только у нас, соответственно, если Вам кто-либо предложит восстановить информацию, в лучшем случае, он сперва купит ключ у нас, затем Вам продаст его с наценкой.
Если Вы не смогли найти Ваш ключ синхронизации
Нажмите здесь
serveradmin.ru

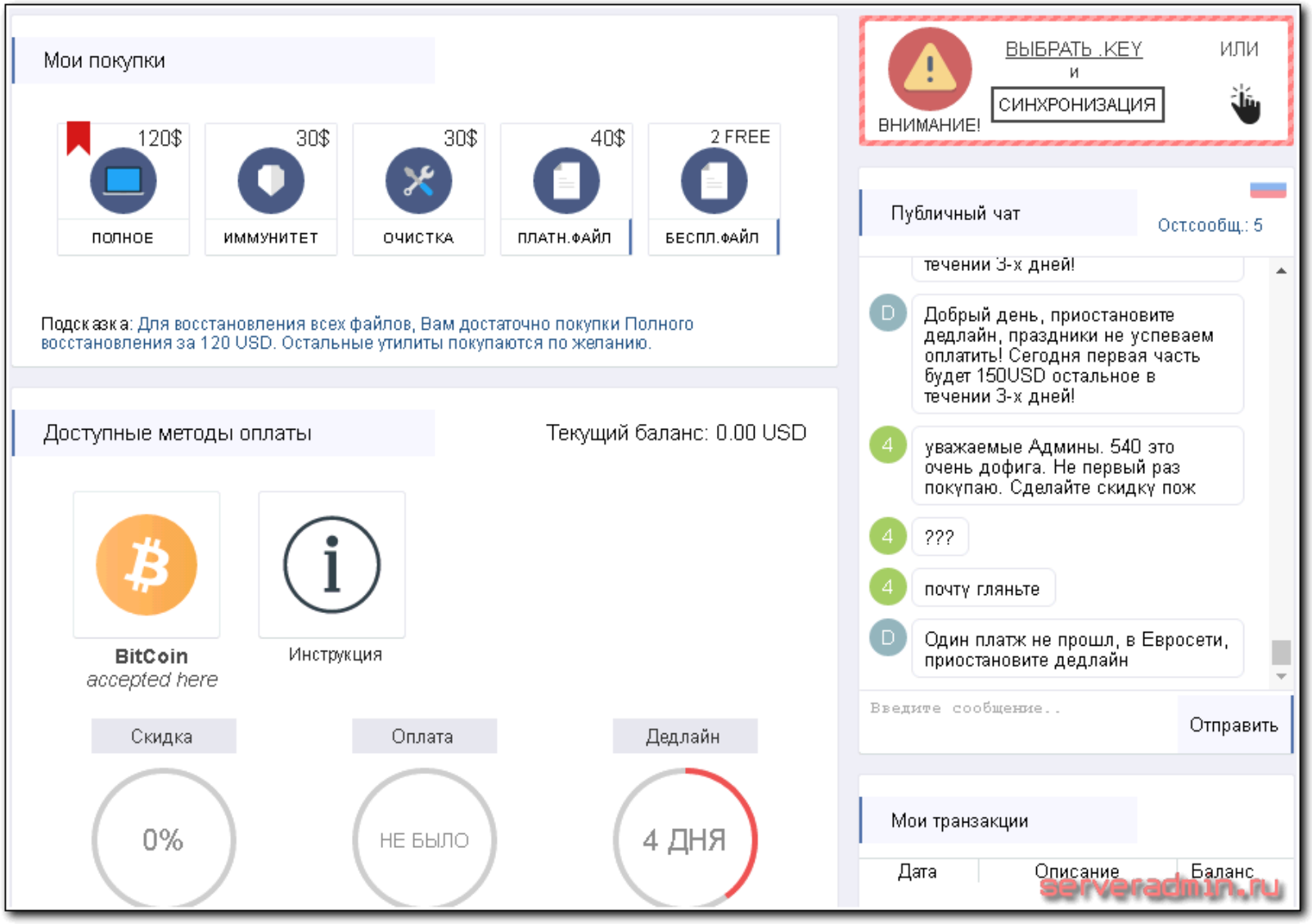
На странице есть форма ввода, куда уже введен ваш идентификатор, с помощью которого вы можете авторизоваться на сайте https://spora.bz.

Второй файл необходим для того, чтобы вы смогли получить дешифратор от злоумышленников. Его нужно сохранить, если вы рассчитываете расшифровать файлы.

> Особенностью работы данного вируса шифровальщика является то, что ему для своей работы не требуется доступ в интернет. После того, как вы его запустите из почты, он начнет свою работу, даже если у вас антивирус или firewall контролирует подозрительный сетевой трафик.

Если вы увидели в своем браузере описанную выше страничку, значит все ваши файлы уже зашифрованы, хотя внешне кажется, что все в порядке. Но при попытке открыть файл, вы получите ошибку. Дальше нужно действовать аккуратно и внимательно, если хотите получить свои данные обратно. Шансы сделать это бесплатно хоть и небольшие, но есть.

Можно зайти в личный кабинет указанного выше сайта и посмотреть, как там все устроено.

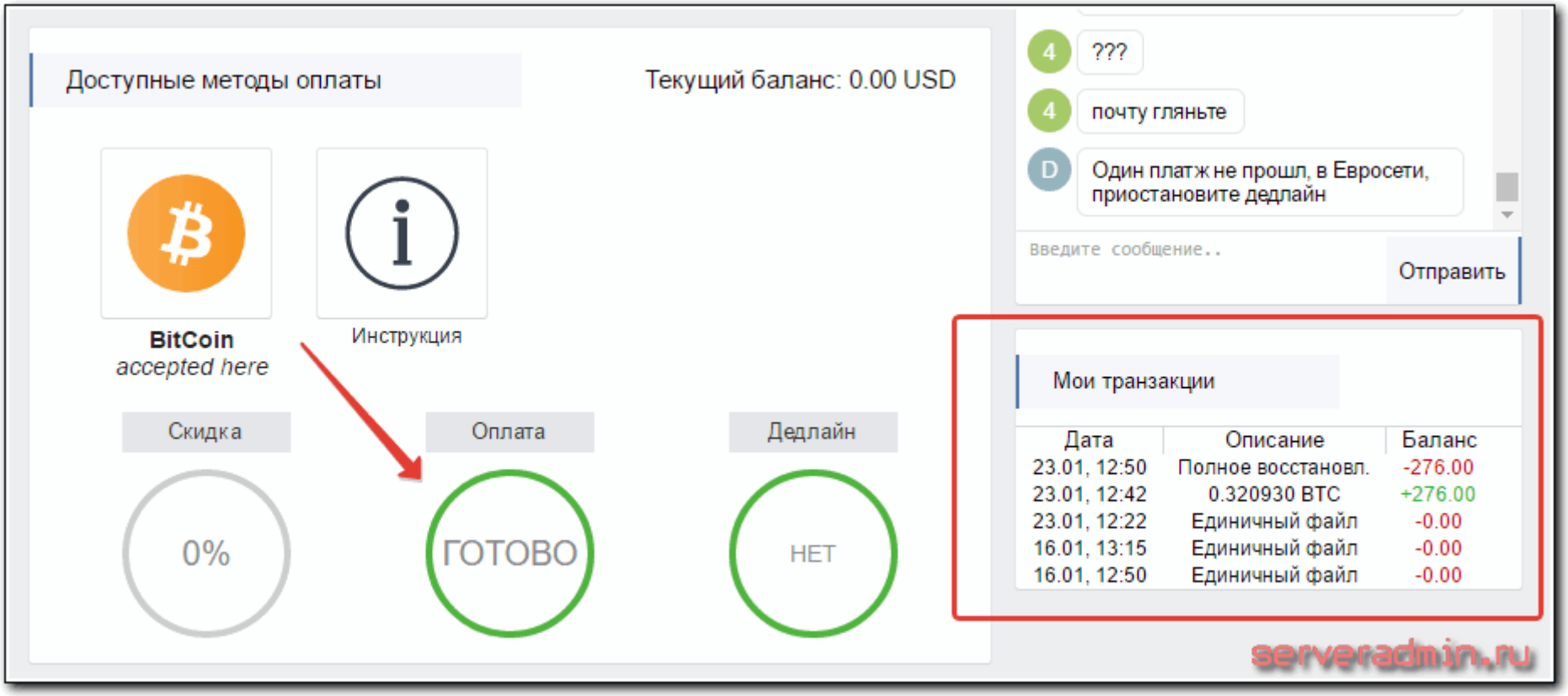

Мои покупки
120$
ПОЛНОЕ
30$
ИММУНИТЕТ
30$
ОЧИСТКА
40$
ПЛАТН.ФАЙЛ
2 FREE
БЕСПЛ.ФАЙЛ
Подсказка: Для восстановления всех файлов, Вам достаточно покупки Полного восстановления за 120 USD. Остальные утилиты покупаются по желанию.
Доступные методы оплаты
Текущий баланс: 0.00 USD
BitCoin
accepted here
Инструкция
Скидка
0%
Оплата
НЕ БЫЛО
Дедлайн
4 ДНЯ
ВНИМАНИЕ!
ВЫБРАТЬ .KEY
и
СИНХРОНИЗАЦИЯ
ИЛИ
Публичный чат
Ост.сообщ.: 5
течении 3-х дней!
Добрый день, приостановите дедлайн, праздники не успеваем оплатить! Сегодня первая часть будет 150USD остальное в течении 3-х дней!
уважаемые Админы. 540 это очень дофига. Не первый раз покупаю. Сделайте скидку пож
???
почту гляньте
Один платж не прошл, в Евросети, приостановите дедлайн
Введите сообщение..
Отправить
Мои транзакции
Дата
Описание
Баланс
serveradmin.ru

После заражения у вас есть 5 дней, чтобы оплатить расшифровку. После этого, она станет дороже в 2 раза. Имейте это ввиду, если решитесь платить деньги. Я знаю, что многие платят, так как нет выхода, поэтому сразу предупреждаю. Цена через 5 дней реально будет в 2 раза выше.

Поражает набор услуг, которые вы можете приобрести в "магазине". Тут и иммунитет от шифровальщика, и очистка компьютера. У вас есть возможность расшифровать 2 файла бесплатно. Если у вас пропало не более пары нужных файлов, считайте что вам повезло, сможете их расшифровать. Но имейте ввиду, что это не всегда срабатывает. Если злоумышленники посчитают, что файл очень ценен, то могут отказать в бесплатной расшифровке.

На сайте предусмотрен чат с техподдержкой вируса. Первое время не было ограничения на количество сообщений, теперь оно есть - не более пяти. Так что внимательно следите за тем, что пишите, если у вас реально есть необходимость общаться.

Вы можете тут же внести оплату за расшифровку. На сайте есть подробные инструкции. После зачисления денег, информация в личном кабинете изменится.



Если деньги сразу не придут, нужно написать в техподдержку, они вручную проверят поступление и подтвердят его. Масштабы деятельности, честно говоря, поражают. Очень занимательный чат. Я прям зачитался, когда первый раз попал в личный кабинет.

Как лечить компьютер и удалить вымогатель spora ransomware

После того, как вы узнали, что все ваши файлы зашифрованы, нужно определиться, что вы будете делать дальше. Если у вас есть бэкапы и расшифровка

файлов вам не требуется, то можно смело переходить к лечению компьютера и удалению вируса. Как и все остальные вирусы шифровальщики, удалить из системы его не трудно. Та модификация, что попалась мне, вообще ничего особенного с системой не делала, нигде себя не прописывала - ни в реестре, ни в автозапуске. Все, что сделал вирус, это создал несколько файлов. 3 файла в папке с профилем пользователя *C:\Users\user\AppData\Roaming*:

- **RU15C-ACXRT-RTZTZ-TOGTO.HTML** - html страничка с информацией о заражении и входе в личный кабинет на сайте злоумышленников.
- **RU15C-ACXRT-RTZTZ-TOGTO.KEY** - файл с ключами, на основе которых можно купить дешифратор.
- **RU15C-ACXRT-RTZTZ-TOGTO.LST** - файл со списком ваших зашифрованных файлов.

Эти же 3 файла будут продублированы в папке *C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates*. На рабочем столе пользователя будут лежать первые два файла из списка. Все эти файлы носят информационный характер и непосредственной опасности не представляют. Сам вирус будет находиться в папке *C:\Users\user\AppData\Local\Temp*. Вот список файлов оттуда, относящиеся к spora:

- **4a0f17b9936.exe** - непосредственно вирус.
- **close.js** - javaScript-файл, который создает исполняемый файл с вирусом.
- **doc_113fce.docx** - поддельный документ.
- **1C.a01e743_pdf.hta** - вложение из почты.

Этот список файлов представляет непосредственную опасность и его в первую очередь надо удалить. Ни в коем случае не копируйте эти файлы на флешку или куда-то еще. Если случайно запустите на другом компьютере, то потеряете и там все данные. Если вам нужно сохранить для последующего разбора файлы с вирусами, то добавьте их в зашифрованный архив.

Удаления этих файлов достаточно для того, чтобы избавиться от вируса шифровальщика. Но хочу обратить внимание, что модификации могут быть разные. Я видел в интернете информацию о том, что этот вирус иногда ведет себя как троян, создает копии системных папок в виде ярлыка, скрывает настоящие системные папки, а в свойствах запуска ярлыков добавляет себя. Таким образом, после расшифровки файлов, ваша карета снова может превратиться в тыкву.

После ручного удаления вируса, рекомендую воспользоваться бесплатными инструментами от популярных антивирусов. Подробнее об этом я уже рассказывал ранее на примере вируса no_more_ransom. Можете воспользоваться приведенными там рекомендациями. Они актуальны и для вируса spora.

Я рекомендую после расшифровки файлов, сразу же переустановить систему Windows. Только это может дать 100% гарантию, что на компьютер очищен полностью.

Если вам необходимо любой ценой восстановить зашифрованные файлы, а самостоятельно вы это сделать не можете, рекомендую сразу обращаться к профессионалам. Неправильные ваши действия могут привести к тому, что файлы вы вообще не сможете получить назад. Как минимум, вам нужно снять

посекторный образ системы и сохранить его, прежде чем вы сами начнете что-то делать. Как сделать образ системы рассказывать не буду, это выходит за рамки данной статьи.

Подведем итог. После того, как ваш компьютер был зашифрован, правильная последовательность действий для возможной расшифровки файлов и лечения компьютера следующая:

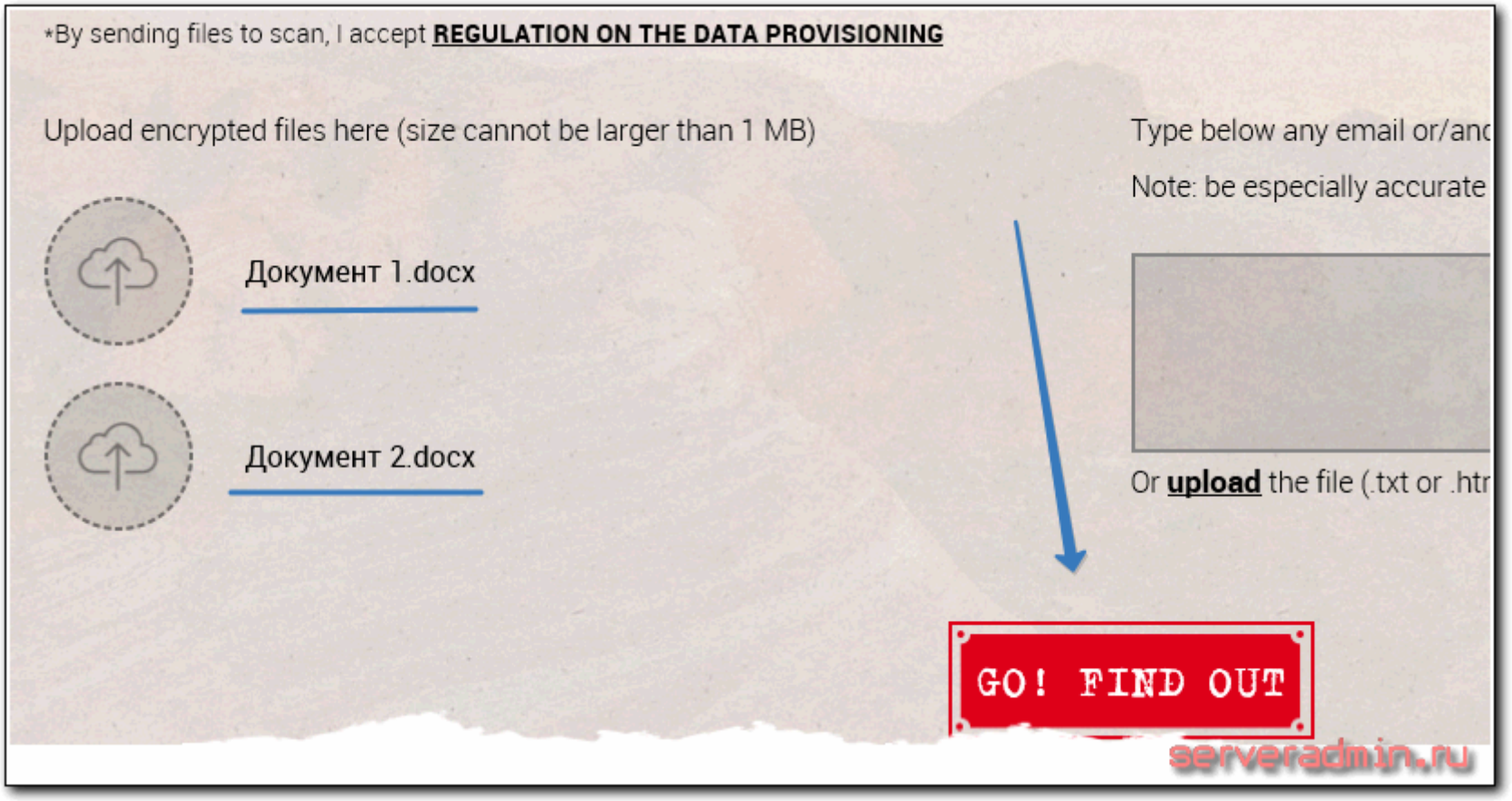
1. Отключаем компьютер от сети.
2. Сохраняем файлы с расширением .KEY и .LST.
3. Делаем полный посекторный образ дисков с информацией, загрузившись с Live CD.
4. Удаляем вирус с компьютера.
5. Пробуем восстановить файлы самостоятельно.
6. Переустанавливаем Windows.

Где скачать дешифратор spora ransomware

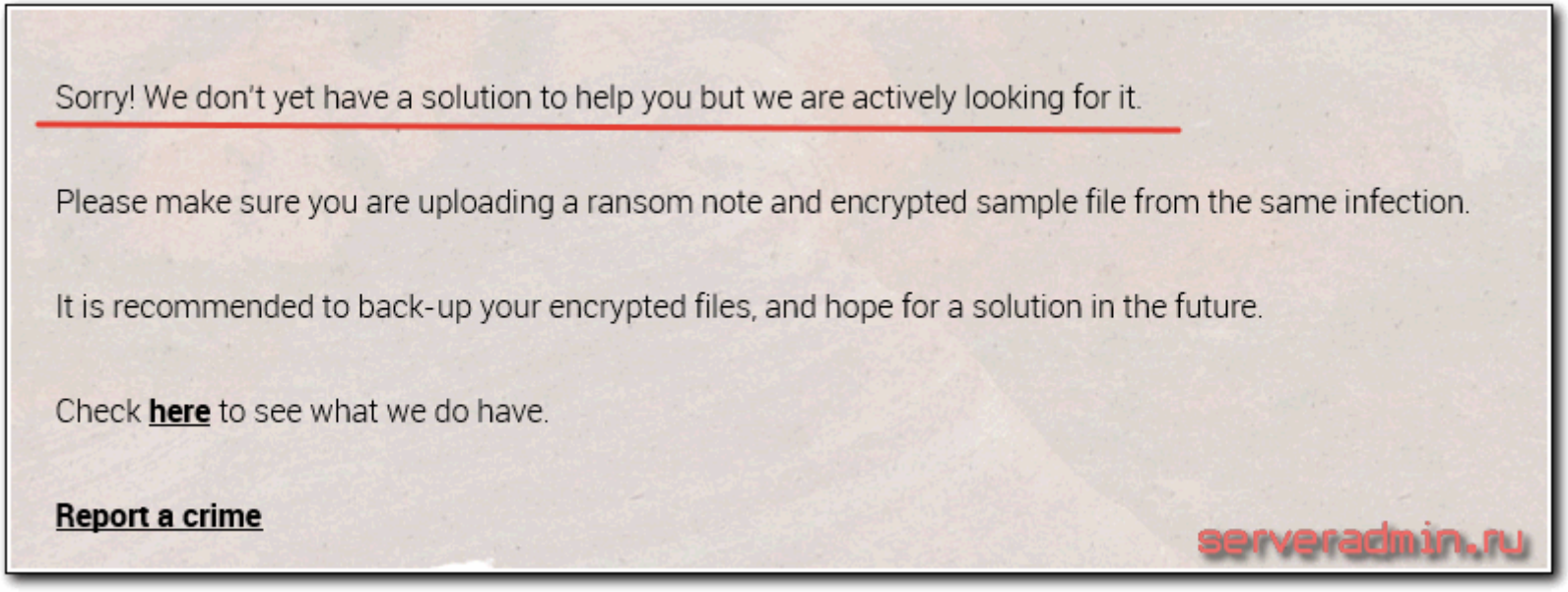
Прежде чем начинать восстанавливать файлы самостоятельно, можно попробовать поискать дешифратор для spora ransomware. Существует сайт https://www.nomoreransom.org, на котором собраны дешифраторы для некоторых шифровальщиков. Можно попытать счастья и проверить, есть ли там рабочий дешифратор для spora, который позволит очень быстро и просто расшифровать файлы.

Сразу хочу предупредить, что шансов найти рабочий дешифратор не много, но вдруг повезет? Попытка не пытка. Идем на сайт, на главной странице нажимаем на YES.

Выбираем парочку зашифрованных файлов и отправляем их на сервер для подбора дешифратора.



Мне не повезло. На момент написания статьи дешифратор для spora ransomware отсутствовал.



Список существующих дешифраторов для шифровальщиков можно посмотреть в отдельном разделе https://www.nomoreransom.org/decryption-tools.html. Возможно, когда-нибудь там появится что-то и для spora. Наличие такого количества готовых дешифраторов позволяет думать, что теоретически это возможно, хотя я и не очень представляю как это возможно с текущей реализацией алгоритма шифрования.

Есть ли еще возможность найти рабочий дешифратор для шифровальщика spora ransomware я не знаю. Думаю, что нет. А если кто-то будет предлагать его продать, да еще и по небольшой цене, то скорее всего это будет мошенник.

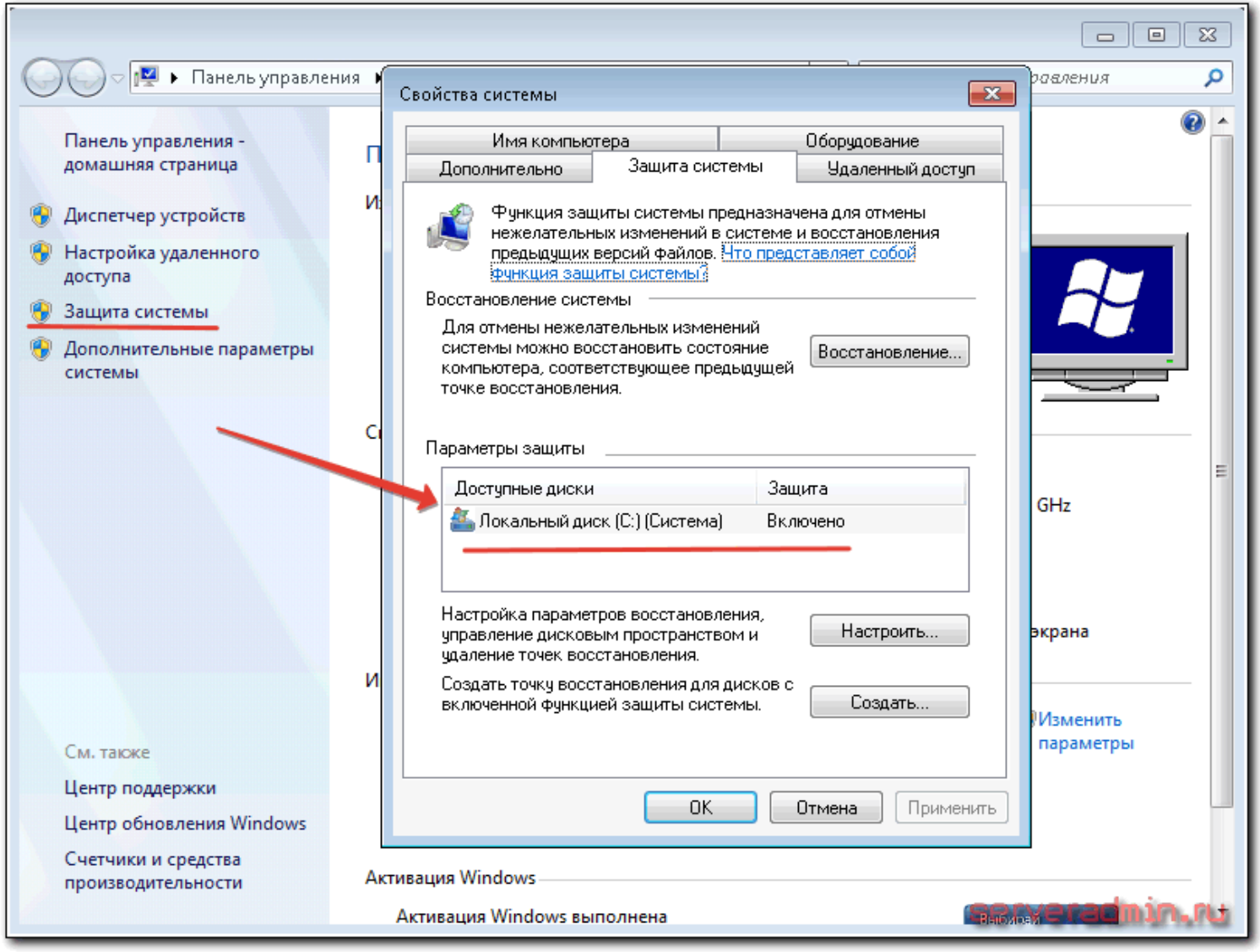
> Никогда не покупайте дешифраторы, если вам предварительно не предоставят 100% гарантии его работы на примере нескольких, а еще лучше всех файлов.

Как расшифровать и восстановить файлы после вируса spora ransomware

Что делать, когда вирус spora ransomware зашифровал ваши файлы? Вы можете расшифровать бесплатно 2 файла в личном кабинете. Как это сделать показано в видео в конце статьи. Если вам этого мало, то читайте дальше о том, как расшифровать остальные файлы. Точнее не расшифровать, а восстановить. 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

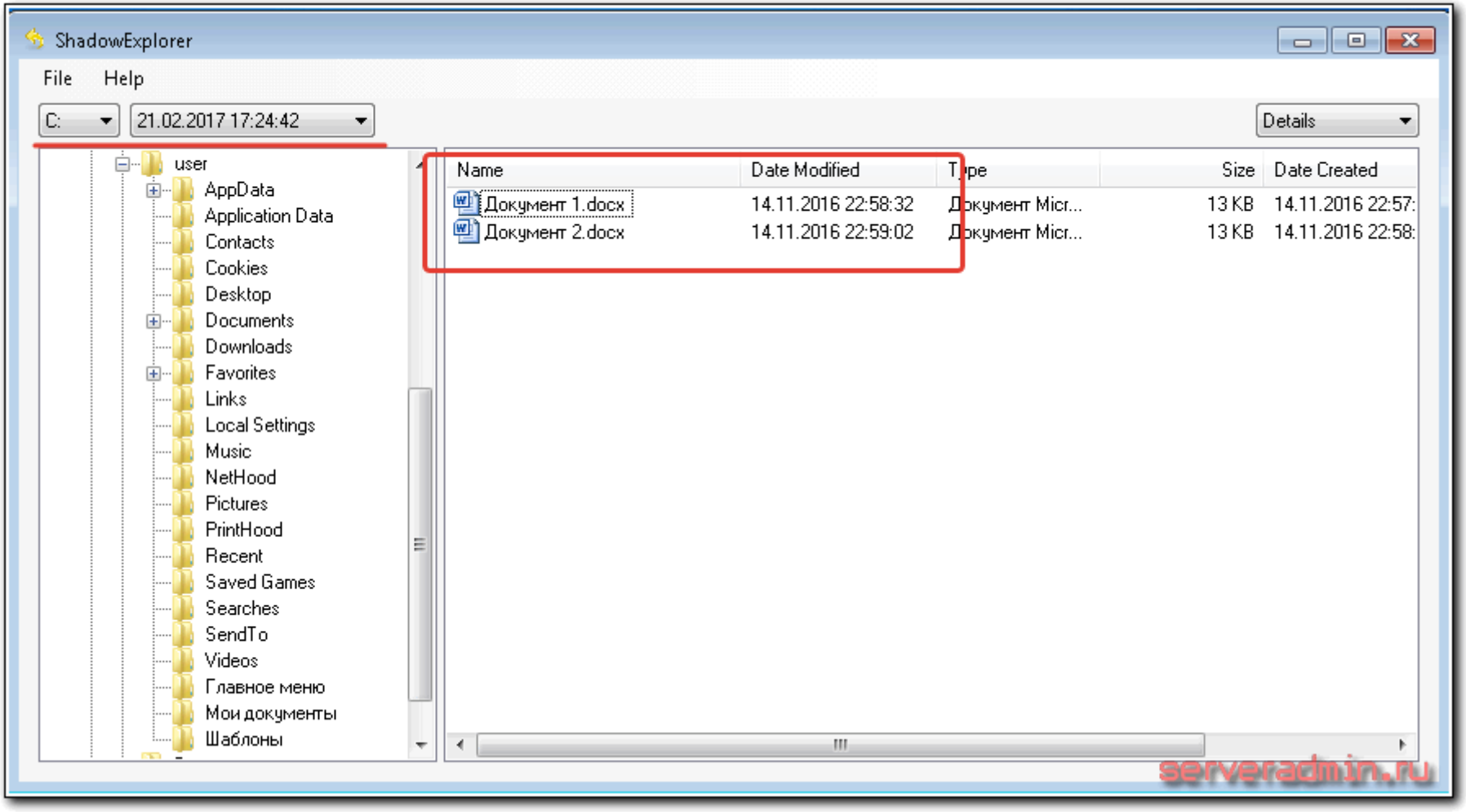
Для начала проверим, включены ли у нас теневые копии. Этот инструмент по-умолчанию работает в windows 7 и выше, если вы его не отключили вручную. Для проверки открываем свойства компьютера и переходим в раздел защита системы.


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

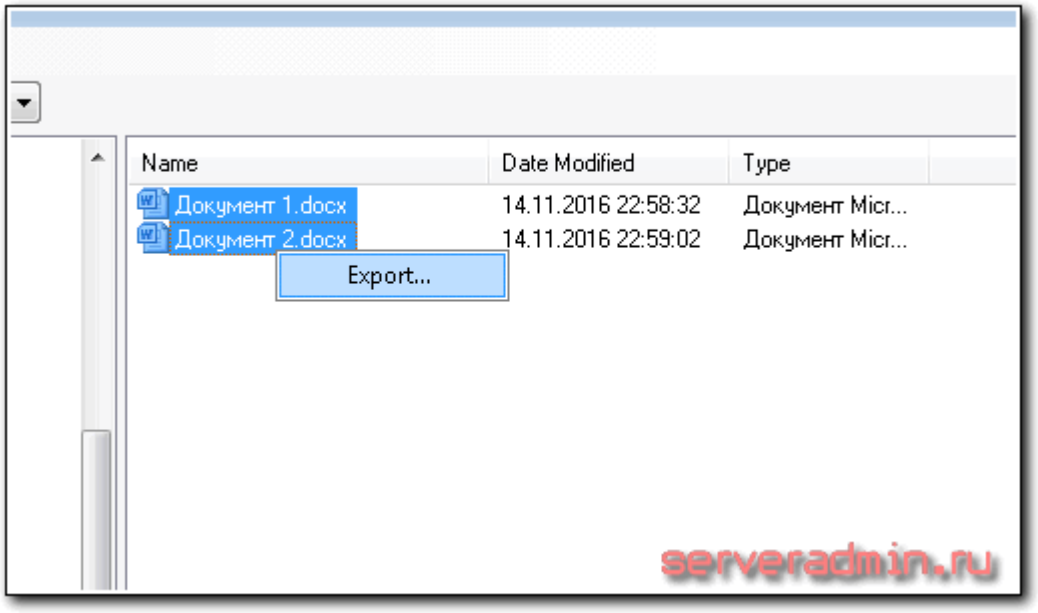
Если вы во время заражения не подтвердили запрос UAC на удаление файлов в теневых копиях, то какие-то данные у вас там должны остаться. Подробнее об этом запросе я рассказал в начале повествования, когда рассказывал о работе вируса.

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.



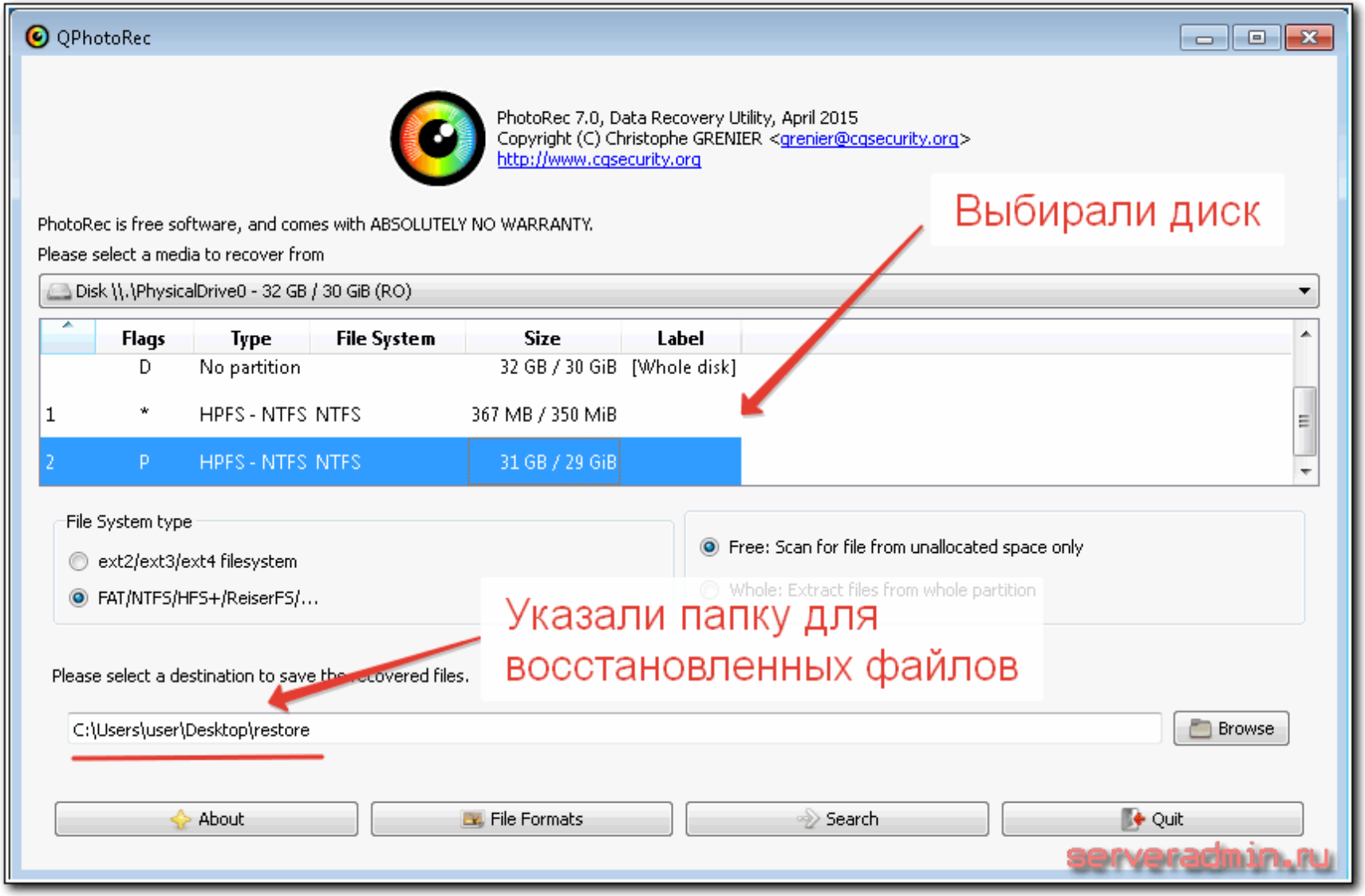
Мне удалось восстановить эти файлы. Для этого я их выбрал, нажал правой кнопкой мыши, выбрал Export и указал папку, куда их восстановить.



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.

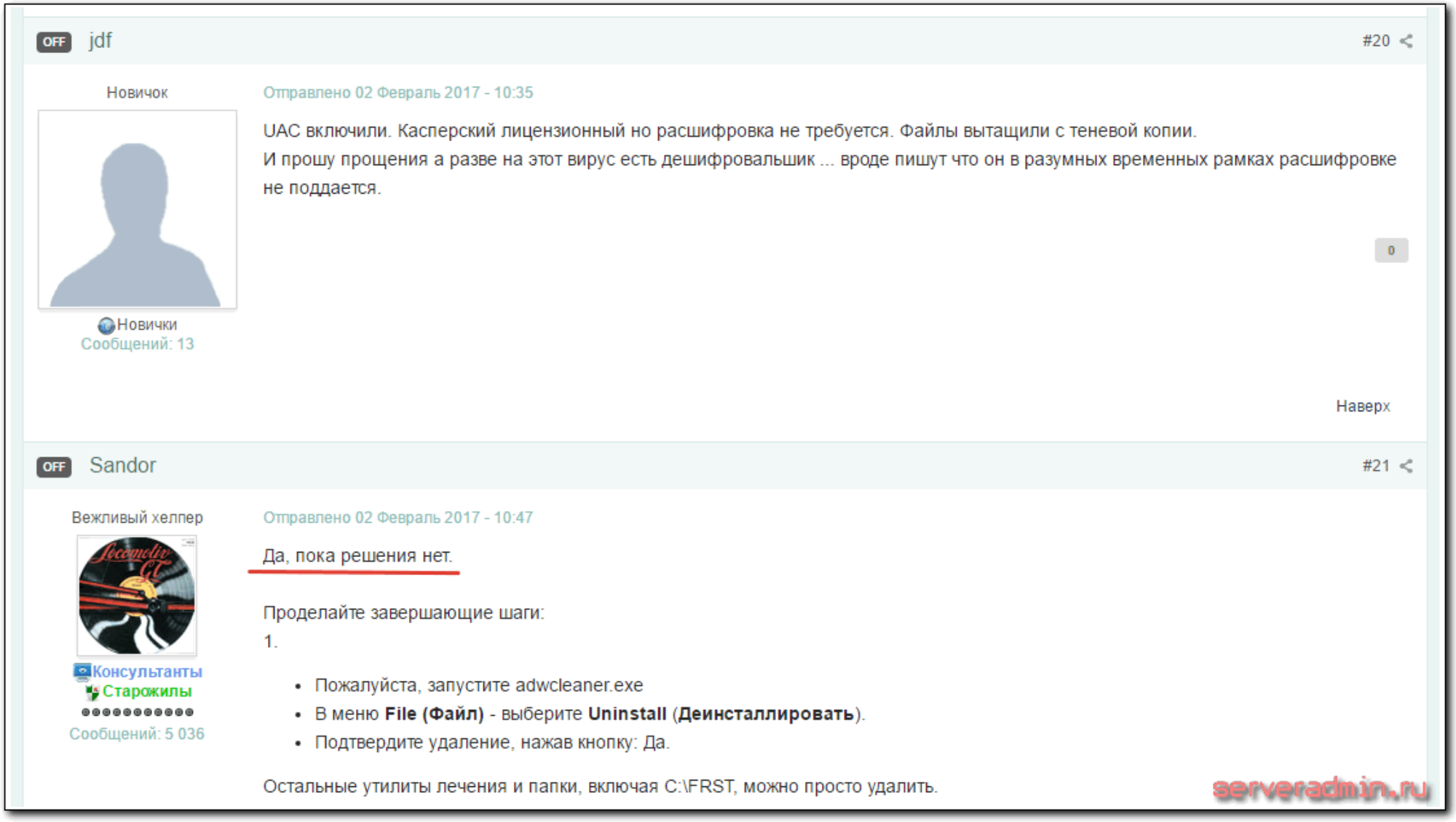
Весь процесс восстановления файлов подробно показан в видео в самом конце статьи.

Касперский, eset nod32 и другие в борьбе с шифровальщиком Trojan-Ransom.Win32.Spora

Сейчас старые модификации вируса определяются антивирусами как Win32/Filecoder.Spora.A, Win32/Filecoder.NJI и д.р. Может меняться последняя буква на b, f и т.д. Filecoder иногда заменяется на trojan. К сожалению, все это применимо только к старым версиям вирусов. Постоянно выходят новые, которые антивирусы не способны быстро определить.

Пробежимся по форумам популярных на сегодняшний день антивирусов и посмотрим, что они могут предложить в борьбе с шифровальщиком spora.

К сожалению, как и раньше - НИЧЕГО. Смотрим сообщение с сайта forum.kasperskyclub.ru, куда отправляют с официального форума kaspersky делать заявки на лечение от вирусов.



OFF jdf #20

Новичок

Новички
Сообщений: 13

Отправлено 02 Февраль 2017 - 10:35

UAC включили. Касперский лицензионный но расшифровка не требуется. Файлы вытащили с теневой копии.
И прошу прощения а разве на этот вирус есть дешифровальшик ... вроде пишут что он в разумных временных рамках расшифровке не поддается.

0

Наверх

OFF Sandor #21

Вежливый хелпер

Консультанты
Старожилы

Сообщений: 5 036

Отправлено 02 Февраль 2017 - 10:47

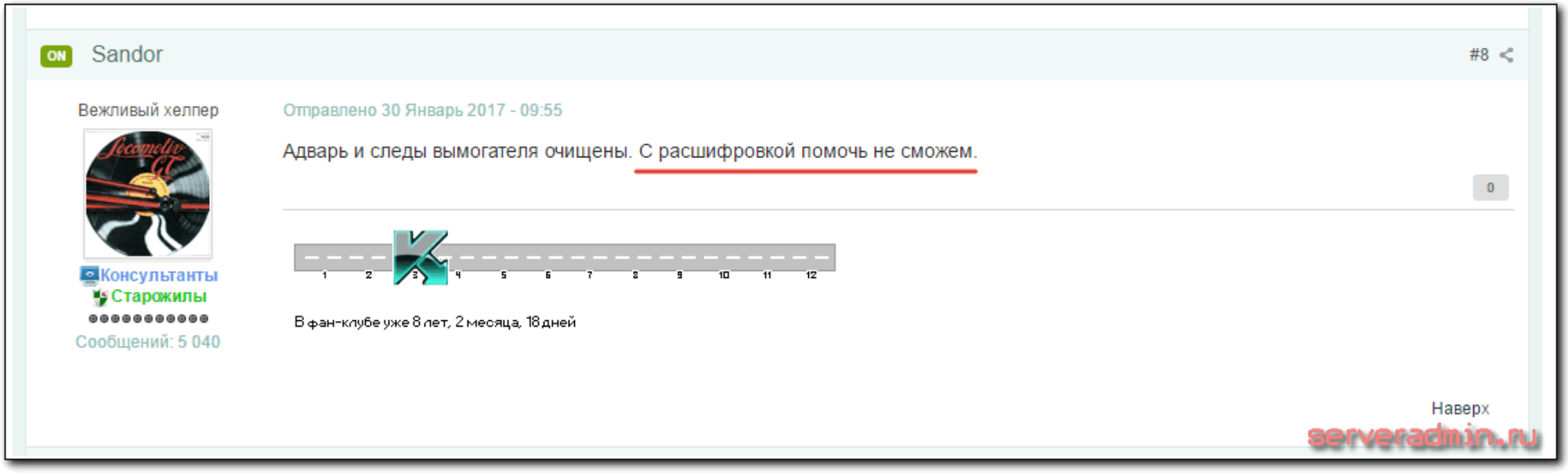
Да, пока решения нет.

Проделайте завершающие шаги:
1.

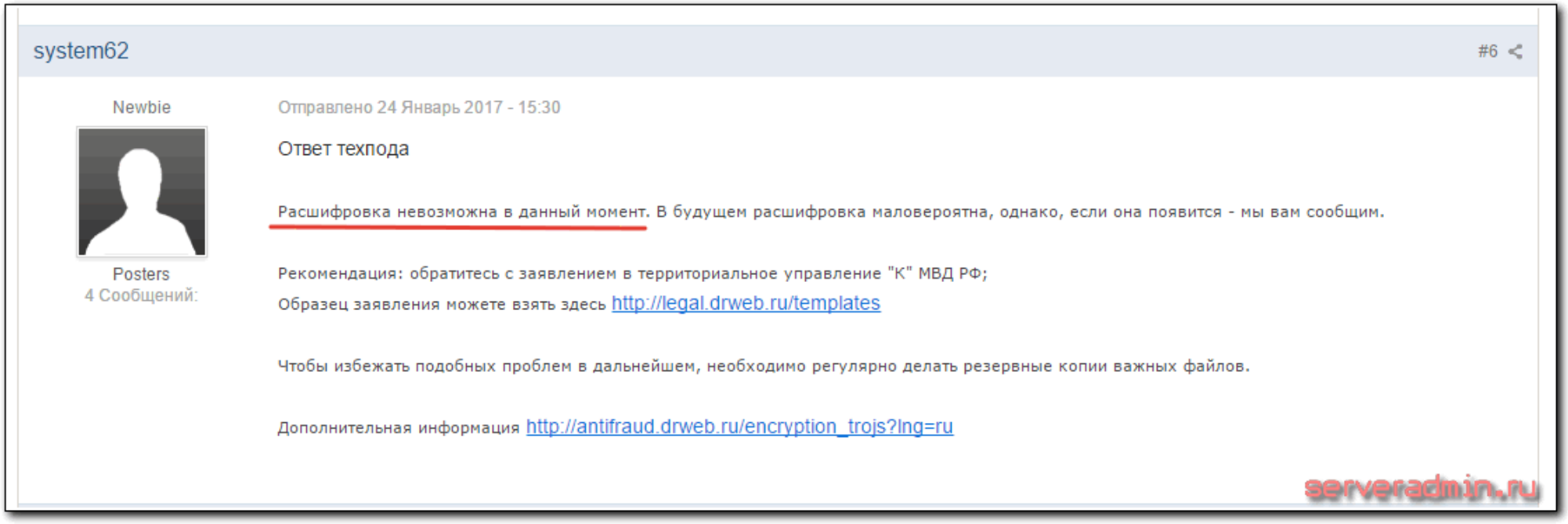
- Пожалуйста, запустите adwcleaner.exe
- В меню **File (Файл)** - выберите **Uninstall** (**Деинсталлировать**).
- Подтвердите удаление, нажав кнопку: Да.

Остальные утилиты лечения и папки, включая C:\FRST, можно просто удалить.

Вот еще оттуда же https://forum.kasperskyclub.ru/index.php?showtopic=54138&p=795414



Вот пострадавший от такого же вируса spora на форуме dr.web. Ответ техподдержки доктора веба тоже неутешительный:

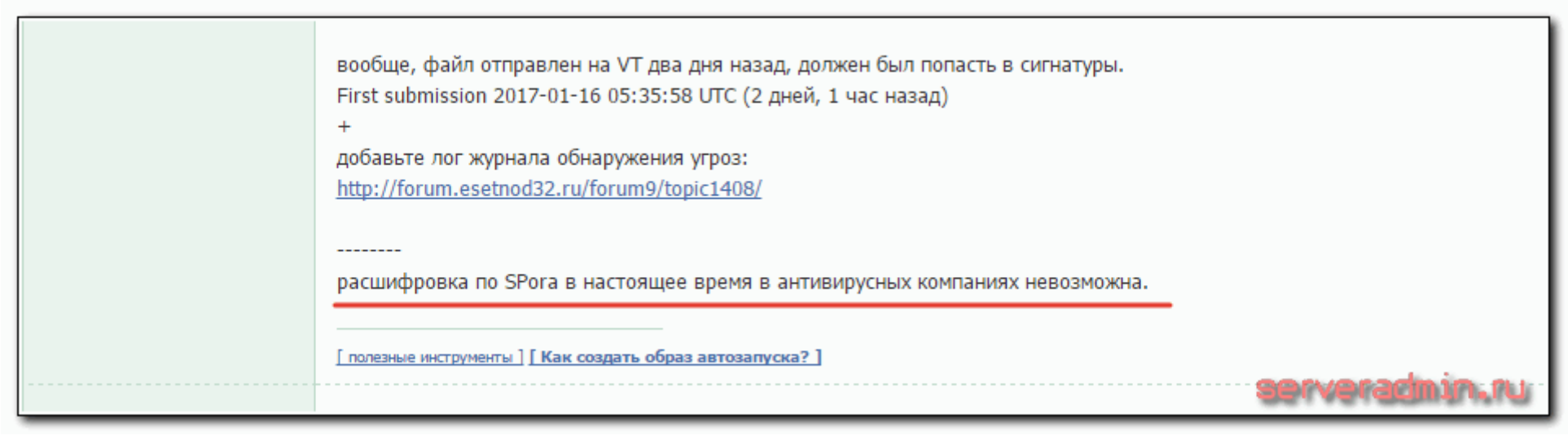


Расшифровка невозможна в данный момент. В будущем расшифровка маловероятна, однако, если она появится - мы вам сообщим.

Рекомендация: обратитесь с заявлением в территориальное управление "К" МВД РФ;
Образец заявления можете взять здесь http://legal.drweb.ru/templates

Чтобы избежать подобных проблем в дальнейшем, необходимо регулярно делать резервные копии важных файлов.

Заглянул к еще одному крупному игроку рынка антивирусных решений - ESET NOD32, что там у него есть на тему spora ransomware. Как водится, тоже есть упоминания о столь популярном сейчас вирусе. Вот большая тема оттуда - зашифровано в Spora. Сообщение администратора на 2-й странице обсуждений:



Все как всегда со всеми предыдущими шифровальщиками, за исключением Энигмы. Ее обещали расшифровывать. А текущий нет и пока не предвидится. Так что тут каждый сам за себя.

Методы защиты от вируса шифровальщика

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.

На этом у меня все. Будьте внимательны за компьютером. Не открывайте подозрительные файлы, не переходите по сомнительным ссылкам, делайте регулярно бэкапы всех важных данных.

Видео с 100% расшифровкой и восстановлением файлов

Я записал видео, где на тестовой машине заразился вирусом, успешно восстановил все файлы, вылечил компьютер и удалил вирус из системы.

Watch this video on YouTube