Отличить системный процесс от вируса.

Послан serg11011 - 22.05.2009 08:07

Открыл доступ к скрытым папкам и выяснилось что на диске D немогу открыть папку System Volume Information с помощью сторонних программ узнал что доступ закрыт процессом C:WINDOWSSYSTEM 32svchost.exe Хочется узнать зачем системному процессу закрывать доступ к папке если это вирус то подскажите как от него избавиться.Касперский со всеми обновлениями и сканер для Windows от Dr.Web ни чего не выявляют.

==========

RE: Отличить системный процесс от вируса.

Послан admin - 22.05.2009 10:58

Папка System Volume Information — это скрытая системная папка, которая используется программой восстановления системы для хранения своих данных и точек восстановления. Папка создается в каждом разделе жесткого диска.

По умолчанию эта папка блокируется системой. И это в принципе хорошо, потому что доступ туда затруднен не только пользователю , но и вредоносной программе. Однако , если вы все таки хотите получить туда доступ , можно сделать так, как советуют на сайте Microsoft

http://support.microsoft.com/kb/309531/

==========

RE: Отличить системный процесс от вируса.

Послан hell - 22.05.2009 12:33

В Windows есть папки и файлы, доступ к которым запрещен пользователю, т.к. изменив там что-либо вы можете нанести непоправимый вред системе. Процесс svchost.exe - системный, он занимается в папке System Volume Information своими делами, а именно сохраняет туда копии важных системных файлов, когда вы что-то устанавливаете на компьютере или меняете важные настройки системы. Это нужно для того, чтобы в случае сбоя вы могли откатить систему на дату, предшествующую этим изменениям.
Создаваемые в System Volume Information копии называются точками восстановления системы.
Думаю, Касперскому и DrWeb можно верить, если ни один из них ничего не нашел, то не стоит волноваться. Для большей уверенности можете просканировать весь диск в безопасном режиме - при загрузке ПК нажимайте на клавиатуре F8, и в списке режимов загрузки ОС выберите Безопасный режим.
А вот отличить системный процесс от вируса очень сложно, даже маститые сисадмины могут тут прогадать, т.к. вирус необязательно бывает в виде процесса. Вирусы уже дано научились внедрять в системные процессы свои компоненты, и с виду процесс кажется нормальным.

==========

RE: Отличить системный процесс от вируса.
Послан serg11011 - 22.05.2009 16:36

Выполнил рекомендации Microsoft но доступ к папке так и неполучил.Буду надеятся на антивирусы,появятся видимые изменения или проблеммы в работе системы напишу.

==========

RE: Отличить системный процесс от вируса.
Послан admin - 22.05.2009 16:41

Хорошо) Кстати говоря, в Linux системах вам вообще ни одну системную папку не изменить через стандартный проводник. И это я считаю, как раз правильной политикой

==========

RE: Отличить системный процесс от вируса.
Послан hell - 23.05.2009 16:20

---

serg11011 писал(а):
Выполнил рекомендации Microsoft но доступ к папке так и неполучил.Буду надеятся на антивирусы,появятся видимые изменения или проблеммы в работе системы напишу.
Если вам очень хочется посмотреть, что в этой папке, то сделайте так:
1. В меню Сервис любого окна выбираем Свойства папки. Переходим на вкладку Вид. Снимаем галочку "Использовать простой общий доступ к файлам (рекомендуется)". Жмем OK.
2. Теперь идем в Мой компьютер на диск D. По папке System Volume Information щелкаем правой кнопкой мышки и выбираем Свойства.
2. Переходим на вкладку Безопасность. Там вверх в "Группы или пользователи" должно быть SYSTEM, т.е. система. Это значит, что только ОС разрешен доступ к этой папке.
3. Добавляем себя в список этих групп и пользователей: жмем "Добавить", в открывшемся окошке жмем "Дополнительно", а потом кнопку "Поиск".
4. выделяем имя пользователя, под которым вы работаете в Windows и жмем OK, потом еще раз OK.
5. Выделяем в списке "Группы или пользователи" добавленного пользователя и ниже в разделе "Разрешения" ставим галочку "Полный доступ". Жмем OK.
Теперь можете зайти в папку и посмотреть, что там. Но НИЧЕГО ТАМ НЕ УДАЛЯЙТЕ!
После того как посмотрите папку, выделите добавленного пользователя в списке "Группы или пользователи" и нажмите кнопку "Удалить" рядом. Потом OK.
Также прилагаю скриншот содержимого папки System Volume Information. Ничего сверхъестественного там нем. Можете проверить эти папки антивирусом, чтобы было спокойнее.
http://www.yachaynik.ru/images/fbfiles/images/0-25eac0dae7e0e5ac9fe1ee7229a35ffd.png

==========

RE: Отличить системный процесс от вируса.
Послан serg11011 - 24.05.2009 19:32

Спасибо большое за доступное подробное обьяснение.

==========

RE: Отличить системный процесс от вируса.

Послан hell - 25.05.2009 09:01

Рада была помочь! Удачи! :)

==========

RE: Отличить системный процесс от вируса.

Послан admin - 28.05.2009 21:16

---

http://www.yachaynik.ru/content/view/163/1/
Постарались ответить на ваш вопрос в этой статье

==========

RE: Отличить системный процесс от вируса.

Послан serg11011 - 31.05.2009 06:05

Хорошая статья,подробная,обязательно воспользуюсь.

==========