Почистил hosts но проблема не изчезла

Послан Alex009 - 07.07.2010 12:24

Почистил hosts но проблема не изчезла (ноутбук босса очень нужна ваша помощь)

Система- windows vista home
Сражу скажу что систему переустанавливать нельзя

Всё началось с какого-то приложения из вконтакта.
Благо ОС не блокировалась, «вирус» работал просто: блокировал самые популярные сайты, в том числе поисковики, сайты антивирусов и электронной почты. При запросах в окне браузера появлялось

http://img-fotki.yandex.ru/get/8/ait-it.2/0_4a121_cf2ad41d_L.jpg

Естественно, первое, что приходит на ум: «левые» процессы, сегодня уже упомянутые AVZ, HiJackThis. С этим всё оказалось в порядке, но разум дал о себе знать — идём в c:/windows/system32/drivers/etc. Там hosts и hosts.txt. С первым на первый взгляд всё чисто, а во втором я вижу заботу создателя о наших с вами финансах:
127.0.0.1 localhost
#Отправьте смс и не мучайтесь… Реальная стоимость смски 100 рублей, а вызов программиста рублей 500 минимум:)

Так-то. Снова открыв файл hosts я увидел, что это ещё не конец файла, через полсотни символов перевода строки следует длинный список тех самых популярных сайтов:

http://img-fotki.yandex.ru/get/4212/ait-it.2/0_4a122_b23b3861_L.jpg

Почистил все что ниже localhost , проверил kaspersky live cd, нашел 2 вируса один в вирус в папке документ энд сетингс был, а второй вирус был в самом hosts –всех их вылечил.
НО ПРОБЛЕМА НЕ ИЗЧЕЗЛА!!!
При запросах в окне браузера появлялось

http://img-fotki.yandex.ru/get/8/ait-it.2/0_4a121_cf2ad41d_L.jpg

Так же не открывается ни один сайт.
Повторю систему переустанавливать нельзя, может быть поможет восстановление системы, с помощью загрузочного диска vista ?
Может кто сделает хорошее дело и не пошлет на куй, а даст дельный совет?
Нужна именно ваша помощь

==========

RE: Почистил hosts но проблема не изчезла

Послан Эцио Аудиторе Де Фиренце - 07.07.2010 12:56

хм.... может попробовать вам удалить hosts,а затем снова создать его,вставив после этого оригинальное содержимое этого файла

a hosts.txt УДАЛИТЬ!!!!!!!!!!!!

==========

RE: Почистил hosts но проблема не изчезла
Послан Эцио Аудиторе Де Фиренце - 07.07.2010 13:01

_____

ах,да! что это за приложение?

==========

RE: Почистил hosts но проблема не изчезла
Послан Гоша Компьютерный - 07.07.2010 13:47

_____

так а как тут написано - http://www.yachaynik.ru/content/view/279/31/ - вы пробовали делать?

==========

RE: Почистил hosts но проблема не изчезла
Послан Эцио Аудиторе Де Фиренце - 07.07.2010 13:50

_____

http://www.yachaynik.ru/content/view/281/31/ а если не получится,то вот еще одна полезная прога))

==========

RE: Почистил hosts но проблема не изчезла
Послан zzsnn - 07.07.2010 17:29

_____

Удалением и чисткой файлов hosts проблему не решишь. Автор данного троя прав. Лучше послать 100 рублей, чем вызывать профи.
Что бы выловить данный трой нужно начинать с чистки компа от временных файлов, чистки автозагрузки. Но не msconfig смотреть, а использовать более профессиональные проги. В частности нужно использовать, как миниум, AutoRuns и Process Explorer отсюда http://technet.microsoft.com/ru-ru/sysinternals/default.aspx . Возможно придёться ковырять и Process Monitor . А для работы с такими прогами нужно уже уровень и опыт достаточно опытного админа.
Если сможешь хотя бы с Process Explorer разобраться, и выловить что у тебя работает, без твоего ведома, тогда помогу разобраться с AutoRuns . А так слишком много объяснять и показывать нужно будет. На уровне чайника не пройдёт. Нужно повыше уровень.

==========

RE: Почистил hosts но проблема не изчезла
Послан Эцио Аудиторе Де Фиренце - 07.07.2010 23:54

Я конечно извеняюсь,но ты,zzsnn,-ИДИОТ!!!!!!!!!!:angry: он отправит смс,которое все деньги сжерёт в 80%(потому,что для некоторых троянов вобще не предусмотрен код) случаев пришлёт код(которого хватит на столько времени по тарифу,сколько было денег),а потом-всё начнётсяя снова!

==========

RE: Почистил hosts но проблема не изчезла
Послан zzsnn - 08.07.2010 03:01

Возможно я и идиот. Но:
1. Я сталкивался с данным троем. И посылка смс как раз и стоило 100 руб, и код присылали.
2. Данный трой можно вылечить ручками. Там особо ничего сложного. Нужно только опыт. И умение работать с соотвествующими инструментами.
3. Так как такого опыта у топикастера точно нет, то я предожил более дешевый способ для него.

4. Если ты знаешь более простой способ, более дешевый - посоветуй. А топикастер выберет. Это его дело.
А так, визжать, не предлагая ничего для решения проблемы - это изображать из себя жигули на Формуле-1. Визгу много, а даже проехать не может, рассыпается.

==========

RE: Почистил hosts но проблема не изчезла
Послан Sumerechnyi - 08.07.2010 05:35

Уж не ты ли автор данного троя? =)

==========

RE: Почистил hosts но проблема не изчезла
Послан Эцио Аудиторе Де Фиренце - 08.07.2010 07:21

хД может и он =))

==========

RE: Почистил hosts но проблема не изчезла
Послан zzsnn - 08.07.2010 13:52

Да нет. В принципе, такие трои пишуться достаточно несложно. Достаточно знать немного VB. И в реестре разбираться немного. Самое сложное - замаскировать под какой-то процесс. Остальное дело опыта и техники.

И защита от таких троев тоже несложная. Кстати на антивирь надежды, при подобных троях, почти никакой. Защиту нужно организовывать на уровне распределения прав пользователей. Проще - не работать постоянно под административной учётной записью. И тогда трои, да и вирусы, в 80% случаев пролетают даже без антивиря. Это верно для Windows. В Linux такая защита по умолчанию.
Тут тоже можно попробовать сработать по разрешению прав пользователей. Изменить файл hosts, и сразу закрыть доступ для возможного изменения всем. Как системной учетной записи, так и админу, так и всем остальным. Трой не проверяте постоянно файл host, а с определенной периодичностью. Это обычно. Тогда достаточно попасть в промежуток времени, когда трой не работает с hosts и спокойно его защитить.
Но это пройдёт, если защита троя организована по периодическому контролю. А если по событию, то тут нужно гнать мониторингом Windows. Тогда ещё проще получиться. Можно будет сразу выловить тело троя. И задавить его.

==========

RE: Почистил hosts но проблема не изчезла
Послан Филатова Марина - 11.07.2010 18:59

_____

У меня тоже фигня какая-то...сидела вконтакте, потом меня вышибло написано страница заблокирована и предоставляется возможность отправить смс на короткий номер, я дура отправила,деньги со счета ушли и вместо кода ответом мне было, что сервис заблокирован за нарушение партнерских условий((Дальше началось веселье...internet explorer не пускает меня на поисковые сайты, такие как яндекс, мейл и рамблер, а стартовой страницей у него стала страница из котнакта с надписью о блоке...папку hosts открыла, там никаких надписей нет о контакте и что делать не знаю. Касперским сделала полную проверку, ничего не нашел.

==========

RE: Почистил hosts но проблема не изчезла
Послан Гоша Компьютерный - 11.07.2010 19:18

_____

http://www.yachaynik.ru/content/view/279/31/ - делаем так как написано здесь

==========

RE: Почистил hosts но проблема не изчезла
Послан Филатова Марина - 11.07.2010 20:00

_____

Господи, Гоша, спасибо Вам огромное, были бы рядом-расцеловала бы, честное слово)))) Вы делаете людей счастливыми, счастье, что Вы и этот сайт есть!!!!!! СПАСИБО!!!!!

==========

RE: Почистил hosts но проблема не изчезла
Послан юлькин - 14.07.2010 16:51

У меня тоже самое!!!Я все почистила, сто раз все поменяла!Я перепробовала все!!!и resert hosts и какую-то программу online. и скачивала hosts и старый удаляла!!!!Вообщем, помогите мне!!!!!!!!!!Мне срочно надо!!!!!

==========

RE: Почистил hosts но проблема не изчезла
Послан Гоша Компьютерный - 15.07.2010 00:48

так а вы попробовали поднять глаза и попробовать воспользоваться советом который я чуть выше писал?

==========

RE: Почистил hosts но проблема не изчезла
Послан Эцио Аудиторе Де Фиренце - 15.07.2010 01:18

---

http://www.yachaynik.ru/content/view/281/31/ тогда удалите им

==========

RE: Почистил hosts но проблема не изчезла
Послан юлькин - 15.07.2010 04:40

Спасибо вам огромное!!!!У меня все получилось!!!:woohoo: :woohoo: :woohoo: :woohoo: :woohoo: :woohoo:

==========

RE: Почистил hosts но проблема не изчезла
Послан xarius - 15.07.2010 09:45

Приветствую всех! Проблема аналогичная, не могу зайти на авито... Попроборал и Резет Хост и удалил Хост через Тотал Коммандер.... Не заходит хоть ты тресни. Неужели только переустановка?

==========

RE: Почистил hosts но проблема не изчезла
Послан Эцио Аудиторе Де Фиренце - 15.07.2010 10:09

попробуй LiveCD от Dr.Wed

==========

RE: Почистил hosts но проблема не изчезла

Послан Dariya Sergeevna - 15.07.2010 17:37

_____

я всё сделала!и почистаила и установила!всё равно не могу зайти!!а когда открываю online.exe там становится всё бульше лишних строчек,я опять редактирую,сохраняю,потом открываю либо ничё не поменялось,либо ещё больше...короче пипец!!!!!!что делать Гоша!!!!!!!!!!!!!!!!!!!!!!!!!!!!:ohmy:

==========

RE: Почистил hosts но проблема не изчезла

Послан Sumerechnyi - 15.07.2010 22:45

_____

http://www.yachaynik.ru/content/view/279/31/

вот так пробовали?

==========