Всем! Всем! Всем! Или как победить страшный вирус

Послан strelok - 27.01.2010 05:53

Сегодняшнее раннее морозное утро преподнесло мне "подарок"! Придя на работу я включил комп. и вместо рабочего стола увидел белое полотно с предложением получить доступ к сайту эротического содержания и соответственно отправить для этого СМС. Ниже была еще одна устрашающая запись, что все попытки обмануть это предложение прведут к полной порче компьютера..... Я так понял, что это и есть новый вирус (или что-то иное), о чем сейчас много говорят, но я про все это слышал пока только краем уха. И вот оно у меня!. (Как ко мне попала эта зараза - сам не могу понять.) Единственное подозрение на то, что при вчерашнем посещении страниц интернета периодически всплывали окна с предложением перейти на порно сайты, которые я закрывал или блокировал.

Так вот, это белое окно закрывало свшые 90% рабочего стола, никак не удалялось и работа на комп. была невозможна. Не помогала и перезагрузка компьютера. Вообще то эта бяка не очень меня напугала, так как у меня для подобных случает припасено очень мощное оружие - программа Acronis True Image Home, которая позволила бы выполнить полное восстановление системы и всех программ, что меня уже неоднократно выручало. Но сначала я попробовал другие способы избавления от этой заразы. Вошел в безопасный режим и попробовал выполнить стандартное восстановление системы. Оно не заработало! То ли эта функция вообще не работает в безопасном режиме, (у меня win7) то ли была заблокирована этим вирусом. Тогда я (так же в безопасном режиме) попробовал запустить программу Рево инсталлер. (о ней я пишу и её можно скачать здесь http://loshckarev2010.narod.ru/programmi_2.htm). Что интересно! Эта программа также не запустилась. Но к счастью на диске D у меня была портативная версия этой программы и она заработала!. В программе рево инсталлер я заблокировал абсолютно все записи автозагрузки, среди которых были и две новые, незнакомые мне, и которые впоследствии куда-то исчезли (как они назывались я теперь не вспомню.Но по-моему мнению они и были причиной инцидента!)После этого я сделал быструю проверку системы антивирусом касперского (как недавно мне советовала это сделать hell)И вот это все помогло! Белое окно исчезло после перезагрузки компьютера! Что именно сыграло решающую роль - удаление записей автозагрузки или проверка антивирусом или и то и другое сказать теперь трудно. После "лечения" компьютера нужные мне записи автозагрузки я восстановил, за исключение двух, которых я раньше не видел. Но в них по-моему никакого криминала нет. (см. криншот) http://www.yachaynik.ru/images/fbfiles/images/Snap_2010-e48a031c4be5eec68aba0c303e2f0495.jpg

==========

RE: Всем! Всем! Всем! Или как победить страшный вирус

Послан hell - 28.01.2010 14:39

да, абсолютно безвредные записи. всего лишь панель Google :) А вот запись Windows Update Servise как-то не очень похожа на обновлялку ОС :(скажите, пожалуйста, что за файлик в папке system32 она обозначает?

==========

RE: Всем! Всем! Всем! Или как победить страшный вирус

Послан strelok - 28.01.2010 14:49

А вот это интересный вопрос! Этой записи вроде бы тоже ранее не было. Сначала я подумал что он и отвечает за обновление win. Но эта запись как видите у меня отключена. а win. все равно обновляется. тут и правда что - то не то! Сейчас посмотрю куда эта запись меня приведет!

==========

RE: Всем! Всем! Всем! Или как победить страшный вирус

Послан hell - 28.01.2010 14:55

_____

за обновление Windows отвечает центр обновлений. Насколько я знаю он работает под одним из процессов svchost.exe и запускается в виде службы. в автозагрузке его вообще быть не должно :)

==========

RE: Всем! Всем! Всем! Или как победить страшный вирус

Послан strelok - 28.01.2010 15:12

_____

Программа Рево инсталлер предлагает открыть папку, куда ведет эта запись. такой папки нет. Еще есть предложение посмотреть соответствующую запись реестра см. скриншот Я пробовал включить эту запись и перезагрузить комп. Ничего ни хорошего. ни плохого не произошло. Я думаю теперь эта запись вообще пустая и я её вовсе удалил. Но может быть она и запускала этот баннер? И еще хочу напомнить, что до лечения компьютера были еще две. совершенно не знакомые и очень позрительные активные записи, которые я своевременно заблокировал, и которые потом сами собой пропалиhttp://www.yachaynik.ru/images/fbfiles/images/Snap_2010-3c57f0bbeada0672bdd6bc0ba6f56e42.jpg

==========

RE: Всем! Всем! Всем! Или как победить страшный вирус

Послан hell - 28.01.2010 15:24

_____

вирусы были уничтожены, поэтому записи пропали :) спасибо антивирусу. жаль, что он не предотвратил заражение, но хоть вылечил :) и на это ему спасибо!

==========

RE: Всем! Всем! Всем! Или как победить страшный вирус

Послан strelok - 28.01.2010 15:26

_____

Не меньшее спасибо я хочу сказать программе Рево Инсталлер!

==========