Вирус
Послан Natvlad - 02.06.2010 15:23

Сегодня столкнулась с новой (для меня) модификацией autorun.inf Также создает корзину, но под именем ISPRED. А в самом файле запуск из-под корзины файл menekrug.exe. Кто подскажет, что за зверь и как с ним бороться. Avira и Касперский эти файлы не видят, но при показе скрытых файлов их не возможно удалить с компьютера и с флешки в этот момент. На другом компьютере эти файлы с флешки вручную удаляются.

==========

RE: Вирус
Послан ЛЁПА - 05.06.2010 04:15

тоже похожая проблема - вот такая у друга проблема : вирус определяется на всех съемных носителях, когда их вставляешь в компьютер.
Затем вирус удаляется, а когда вставляется устройство заново, он опять там появляется.
троянская программа Trojan.Win32.AutoRun.ahz
Файл: G:autorun.inf
буду признателен за совет

==========

RE: Вирус
Послан Natvlad - 05.06.2010 05:50

В своём случае я не придумала ничего умнее и просто переставила систему - в отпуск уходила. Какое содержимое файла autorun.inf? Его смотрят с помощью блокнота. Смотрим процессы, там может быть запущен процесс csrcs.exe, то его останавливаем.НЕ ПУТАТЬ с процессом csrss.exe - это необзодимый процесс!! Можно запустить Касперского, этого гада он удаляет.
http://www.windxp.com.ru/ - вот здесь можно посмотреть про последствия. На сайтах касперского и доктора веба много про вирусы написано.

==========

RE: Вирус
Послан zzsnn - 05.06.2010 07:20

начнём с того, что вирусов типа autorun.inf громадное количество и многие из них используют вполне разрешенные действия. Дело в том, что наличие данного файла на CD, или флешке позволяет выполнять операцию автозапуска программы на CD, или флешке. Чаще всего - это просто набор команд по запуску файла на носителе. Понятное дело, что антивири тут, почти всегда бессильны. Обычные команды - запуск файла- файл запущен пользователем - делает копии каких-то файлов на диск - прописывает себе в автозагрузку. Никаких запрёщенных действий. Антивири не работают.

Но защититься от этой напасти несложно. Но нужно защищать, прежде всего, флешку, потом комп. И тут немного мозгами пошевелить нужно, а не расчитывать на антивири. Твоя защита - в твоих руках.
В данном случае нужно использовать мониторинг автозапуска, процессов, и тогда можно будет прикинуть где и что у тебя наделал данный autorun.inf.
Для мониторинга можно использовать программы с этого сайта http://technet.microsoft.com/ru-ru/sysinternals/default.aspx . Но тут опыт нужен.

==========

RE: Вирус
Послан Гоша Компьютерный - 05.06.2010 08:42

ЛЁПА писал(а):
тоже похожая проблема - вот такая у друга проблема : вирус определяется на всех съемных носителях, когда их вставляешь в компьютер.
Затем вирус удаляется, а когда вставляется устройство заново, он опять там появляется.
троянская программа Trojan.Win32.AutoRun.ahz
Файл: G:autorun.inf
буду признателен за совет
Собственно , ничего нового , кроме написанного здесь: http://www.yachaynik.ru/content/view/37/1/ добавить не могу

==========

RE: Вирус
Послан zzsnn - 05.06.2010 09:04

Добавить можно.
Можно добавить как закрыть флешку (хоть и не на 100%, но достаточно хорошо) от данной гадости. И как комп закрыть от подобной напасти.
В принципе ничего сложного. Флешка - форматировать в NTFS- закрыть доступ в корень - разрешить доступ в отдельную папку. На 90% сработает.
В компе можно тоже или правами пользователя поиграть, или использовать возможности настройки самой WinXP.

==========

RE: Вирус
Послан Гоша Компьютерный - 05.06.2010 09:10

В целом нормальная ситуация на компьютере когда пользователь работает с ограниченными правами. И где то там далеко существует учетная запись администратора к которой мы обращаемся только в случае установки программ или настройки системы
Но так уж сложилось исторически ,что пользователи windows выходят в интернет, работают с флешками из под учетной записи администратора.

Когда мы научимся ограничивать себе права на компьютере и будем считать это нормой, тогда ситуация с вирусами начнет исправляться.

==========

RE: Вирус
Послан hell - 05.06.2010 16:15

_____

:) можно долго плясать с бубном вокруг ОС, ограничивать себе доступ и права, ставить пароли и т.д.
самое лучшее решение: отключить автозапуск всех дисков, флешек и т.п. либо в Настойках автозапуска самой ОС (в Висте есть, есть ли в 7-ке - не знаю) или при подключении флешки / вставки диска в привод держать нажатой клавишу Shift на клавиатуре.
лично я его давно уже отключила и никакие ауторaны меня не беспокоят :) к тому же диски быстрее открываются. а в случае чего можно диск просмотреть (если без авторана не можете) так: щелкнуть по нему правой кнопкой и выбрать Открыть.

==========

RE: Вирус
Послан zzsnn - 05.06.2010 18:14

_____

Увы, но отключение автозапуска часто не помогает. Проблема в том, что при отключении автозапуска отключается возможность автоматического запуска какого-то файла на флещке.
Но при этом остаётся:
1. Вероятность заражения флешки (и часто намного опаснее банального авторана).
2. Запуск пользователема фала-вируса.
3. Пользование Корзиной при включенной флешке с вирусом.
4. Даже запуск песни с заражённой флешке может привести к проблемам.
И это всё при отключенно автозапуске.
А вот работа под пользователем, а не админом очень и очено хорошо помогает в этом случае.

==========

RE: Вирус
Послан ЛЁПА - 07.06.2010 18:25

_____

Огромное спасибо ВСЕМ за советы , с проблемой разобрался ,
автозапуск и касперский

==========

RE: Вирус
Послан DreadLord - 08.06.2010 01:35

_____

hell писал(а):
:) можно долго плясать с бубном вокруг ОС, ограничивать себе доступ и права, ставить пароли и т.д.
самое лучшее решение: отключить автозапуск всех дисков, флешек и т.п. либо в Настойках автозапуска самой ОС (в Висте есть, есть ли в 7-ке - не знаю) или при подключении флешки / вставки диска в привод держать нажатой клавишу Shift на клавиатуре.
лично я его давно уже отключила и никакие ауторaны меня не беспокоят :) к тому же диски быстрее открываются. а в случае чего можно диск просмотреть (если без авторана не можете) так: щелкнуть по нему правой кнопкой и выбрать Открыть.

В 7 винде есть это есть,я это уже знаю(У меня у самого стоит семёрка)

==========

RE: Вирус
Послан hell - 08.06.2010 07:42

_____

zzsnn писал(а):
Увы, но отключение автозапуска часто не помогает. Проблема в том, что при отключении автозапуска отключается возможность автоматического запуска какого-то файла на флещке. Но при этом остаётся:
1. Вероятность заражения флешки (и часто намного опаснее банального авторана).
2. Запуск пользователема фала-вируса.
3. Пользование Корзиной при включенной флешке с вирусом.
4. Даже запуск песни с заражённой флешке может привести к проблемам.
И это всё при отключенно автозапуске.
А вот работа под пользователем, а не админом очень и очено хорошо помогает в этом случае.
это хорошо работает с вирусами авторанерами. в смысле зараженную флешку можно воткнуть в ПК и отформатировать вместе с вирусом. или при подключении зараженной флешки увидеть там файл авторан, которого там и быть не должно и удалить его. :))

==========