Автор: Алексей Пешков - Обновлено 06.06.2015 22:57

Наверное у каждого пользователя на компьютере установлена программа устанения опечаток при наборе текста, например всем известная программа Punto Switch, разработанная Yandex'ом. В этой небольшой статье речь пойдет именно о ней - ПунтоСвитч. Программа конечно очень удобная, но

как оказалось не очень безопасная....

Далее текст взят форума forum.ixbt.com

Еще в процессе установки программы автоматического распознавания и переключения раскладки клавиатуры Punto Switcher 3.1.1 на один из компов Аутпост Файерволл сообщил, что Свичер пытается получить доступ к Фоновой Интеллектуальной Службе Передачи Файлов (Background Intelligent Transfer Service, BITS). По умолчанию эта служба стартует в автомате и используется для отправки инфы о системе и получения файлов при автообновлении.

Я ответил "запретить".
Более того, зная что у свитчера при установке включен режим поиска обновлений, после установки галку "искать обновления" убрал.
И думал что на этом все.
ОШИБСЯ.

Через несколько минут svchost.exe "ломанулся" по 80 порту аж на два сервера яндекса и продолжал пытаться это делать с регулярным постоянством.
Само собой что я пресек попытки файерволлом, но не насовсем (запретить доступ к сайту xxx), а командой "блокировать однократно".
Стал искать причину, перерыл весь реестр, удалил из него в ключах Свичера линки на сервера обновления и помощи яндекса.
Подумал, что теперь то уж точно все и перезагрузился.
ЕЩЕ РАЗ ОШИБСЯ.

Попытки коннекта продолжились.Полностью деинсталлировал Свитчер, стер все его хвосты с диска, прогнал очистку реестра несколькими программами, стер все из темпа. еще раз перезагрузился, считая что УЖ ТЕПЕРЬ-ТО ТОЧНО СОВСЕМ ОКОНЧАТЕЛЬНО ВСЕ!

И ЕЩЕ РАЗ ОШИБСЯ!!!

Попытки соединения с яндексом через svchost.exe не прекратились ДАЖЕ ПОСЛЕ УДАЛЕНИЯ пунто-свичера!!!

(г-да пунто-программеры, в приличном обществе за такие несанкционированные пользователем обращения в интернет - плюют в рожу,
а уж за оставленные после ан-инсталла хвосты - вообще, канделябрами бьют !!!)

Полез еще раз в реестр. и таки нашел причинное место и победил.

1. Открываем Мой компьютерУправлениеСлужбыостанавливаем службу BITS (временно или совсем запрещаем старт, учтите, что без нее не работает автообновление винды)

2. Идем в папку c:Documents and SettingsAll UsersApplication DataMicrosoftNetworkDownloader
удаляем два файла
qmgr0.dat
qmgr1.dat
(можно посмотреть любым редактором - ссылка на сайты яндекса находится там) доступ к файлам блокируется процессом svchost.exe, так что используйте Unlocker Assistant или нечто подобное.
(убивать свцхост процесс-киллером нельзя - начнется перезагрузка. надо именно лишь разблокировать доступ к файлам!)

3. Рестартуем BITS
Проверяем: файлы появятся вновь, но уже пустые, без ссылок на яндекс.проверяем результат (имеющий аутпост файерволл или нечто подобное, да увидит) - svchost.exe больше не лезет в инет на эти сайты.

4. СУГУБО ИМХО.
эта папка и два этих файла в обычном случае вообще не нужны..
во всяком случае на машине без Пунто-Свичера ничего такого нет,
при том что БИТС выполняется автоматом .поэтому "для добивания шпиёна" открываем regeditищем ключевое слово BITS_metadataи в трех местах удаляем из реестра "на фиг с пляжа"

запись о таком параметре со ссылкой как раз на эту папку:
c:Documents and SettingsAll UsersApplication DataMicrosoftNetworkDownloaderв моем реестре такого параметра ключа никогда не было и нет,
на вылеченном компе теперь тоже
какие еще подарочки, не удаляемые при ан-инсталле, успел подкинуть Свичер в систему

(какие-нибудь длл-ки, либ-ы, драйверы и т.д.) - пока не знаю.
очень хочется надеяться, что никаких.
но "Будем искать!"(с)

Ну и вопрос к пунто-программерам и руководству яндекса:
- зачем вам понадобилось закладывать такую гадость в Свичер?
- что еще кроме собственно Свичера устанавливается в систему?
- какие данные вы запрашиваете или передаете через БИТС?

П.С. знаю что сейчас появилось много готовых сборок винды в которых заранее включен Свичер и люди ими пользуются.
использующие такие сборки - вы тоже "в списке стукачей" яндекса.
уже проверено на практике. в машине знакомого так и было. удалили по моей методе.

Добавление от 01.09.2010 17:54:

П.П.С. Эту мою инструкцию о том как вылечить машину,
я поместил на страничку Пунто-Клуба сайта ЯНДЕКС в ответ на вопрос одного из пользователей, зачем Свичер лезет в интернет.
ОНА НЕ ПРОВИСЕЛА НА САЙТЕ ЯНДЕКСА И ПЯТИ МИНУТ!!!
даже без ответа типа, "спасибо за найденную ошибку в нашей программе, в ближайшее время она будет исправлена".

Мой вывод:

вполне возможно, что ЭТО все-таки НЕ ОШИБКА, а СКРЫТАЯ ФУНКЦИЯ программы Punto-Switcher от компании Яндекс!
и ЯНДЕКСУ или его заказчику НЕ НУЖНО, ЧТОБЫ ЛЮДИ ЗНАЛИ КАК ОТКЛЮЧИТЬ ЭТУ ФУНКЦИЮ!!!