Технология

spyware

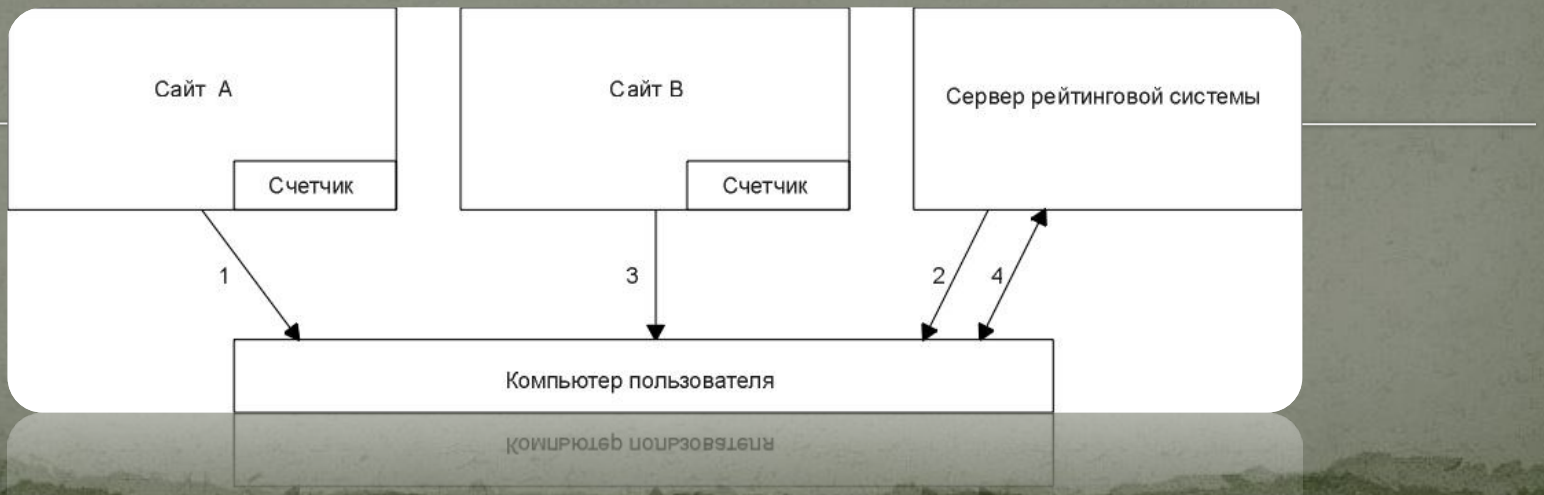
Что такое SpyWare?

Программой-шпионом (альтернативные названия - Spy, SpyWare, Spy-Ware, Spy Trojan) принято называть программное обеспечение, собирающее и передающее кому-либо информацию о пользователе без его согласия.

Информация о пользователе может включать его персональные данные, конфигурацию его компьютера и операционной системы, статистику работы в сети Интернет.

Виды SpyWare. AdWare

Шпионское ПО применяется для ряда целей, из которых основным **являются маркетинговые исследования и целевая реклама.** В этом случае информация о конфигурации компьютера пользователя, используемом им программном обеспечении, посещаемых сайтах, статистика запросов к поисковым машинам и статистика вводимых с клавиатуры слов позволяет очень точно определить род деятельности и круг интересов пользователей.



Виды SpyWare

Однако собранная информация может использоваться не только для рекламных целей - например, **получение информации о ПК пользователя** может существенно упростить хакерскую атаку и взлом компьютера пользователя. А если программа периодически обновляет себя через Интернет, то это делает компьютер очень уязвимым - элементарная атака на DNS может подменить адрес источника обновления на адрес сервера хакера - такое "обновление" приведет к внедрению на ПК пользователя любого постороннего программного обеспечения.

Цели (задачи) SpyWare

- собирать информацию о привычках пользования Интернетом и наиболее часто посещаемые сайты (программа отслеживания);
- запоминать нажатия клавиш на клавиатуре (keyloggers) и записывать скриншоты экрана (screen scraper) и в дальнейшем отправлять информацию создателю spyware;
- несанкционированно и удалённо управлять компьютером (remote control software) backdoors, botnets, droneware;
- инсталлировать на компьютер пользователя дополнительные программы;
- использоваться для несанкционированного анализа состояния систем безопасности (security analysis software) сканеры портов уязвимостей и взломщики паролей;
- изменять параметры операционной системы rootkit, перехватчики управления (hijackers) и пр. результатом чего является снижение скорости соединения с Интернетом или потеря соединения как такового, открывание других домашних страниц или удаление тех или иных программ;
- перенаправлять активность браузеров, что влечёт за собой посещение Web-сайтов вслепую с риском заражения вирусами.

Как бороться?

В случае заражения проверить ПК на вирусы. Теперь общие рекомендации:

1. Установить антивирус
2. Использовать обновленные базы антивируса
3. Раз в месяц делать проверку ПК на вирусы
4. Не скачивать подозрительные файлы и не заходить на подозрительные сайты
5. Установить на свой любимый браузер плагин AdBlock