Презентация на тему: «Технология spyware (шпионские программы)»

Spyware (шпионское программное обеспечение, программа-шпион) — программа, которая скрытным образом устанавливается на компьютер с целью сбора информации о конфигурации компьютера, пользователе, пользовательской активности без согласия последнего. Также могут производить другие действия: изменение настроек, установка программ без ведома пользователя, перенаправление действий пользователя. В настоящий момент существует множество определений и толкований термина spyware. Организация «Anti-Spyware Coalition», в которой состоят многие крупные производители антишпионского и антивирусного программного обеспечения, определяет его как мониторинговый программный продукт, установленный и применяемый без должного оповещения пользователя, его согласия и контроля со стороны пользователя.

Особенности функционирования

- ✔*Spyware могут осуществлять широкий круг задач, например:*
- ✔*собирать информацию о привычках пользования Интернетом и наиболее часто посещаемые сайты (программа отслеживания);*
- ✔*запоминать нажатия клавиш на клавиатуре (кейлоггеры) и записывать скриншоты экрана (screen scraper) и в дальнейшем отправлять информацию создателю spyware;*
- ✔*несанкционированно и удалённо управлять компьютером (remote control software) — бэкдоры, ботнеты, droneware;*
- ✔*инсталлировать на компьютер пользователя дополнительные программы;*
- ✔*использоваться для несанкционированного анализа состояния систем безопасности (security analysis software) — сканеры портов и уязвимостей и взломщики паролей;*
- ✔*изменять параметры операционной системы (system modifying software) — руткиты, 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 веб-сайтов вслепую с риском заражения вирусами.*

Отличие от других видов программ

Adware

«Adware» — программа, демонстрирующая рекламу с или без согласия пользователя. Такие программы не являются spyware, но могут действовать скрытно. Многие adware являются spyware по другим причинам: они показывают рекламные заставки, базирующиеся на результатах шпионской деятельности на компьютере пользователя. Примеры: Gator Software от Claria Corporation и Exact Advertising от BargainBuddy. При посещении некоторых веб-сайтов Gatorможет быть установлен тайным способом, доход от демонстрации всплывающих окон получает сайт и Claria Corporation.

Программы отслеживания

Широкое распространение spyware бросает тень подозрения на другие программы, отслеживающие посещения страниц веб-сайтов с целью исследований и статистики. Некоторые обозреватели описывают Alexa Toolbar (плагин для Internet Explorer) как spyware и ряд программ анти-spyware, таких как Ad-Aware, классифицируют его как spyware. Это происходит благодаря участившимся случаям обнаружения у приложений предназначенных для отслеживания недокументированных функций аудита, сбора и передачи информации пользователя. Весьма показательными в этом отношении являются разработки компании Carrier IQ предназначенные для передачи операторам связи метрик с мобильных устройств, но в действительности имеющие посредника в виде мобильной платформы разведки MSIP, а также показанные исследователем Тревором Экхартом факты сбора пользовательской информации (нажатий клавиш мобильного устройства, захват паролей и т. д.), получившие широкое освещение в СМИ.

В отличие от вирусов и сетевых червей, spyware обычно не саморазмножается. Подобно многим современным вирусам, spyware внедряется в компьютер преимущественно с коммерческими целями (демонстрация рекламных всплывающих окон, кража персональной информации, например, номеров кредитных карт), отслеживание привычки посещения веб-сайтов или перенаправление адресного запроса в браузере на рекламные или порносайт).

Вирусы и сетевые черви

Spyware и некоторые adware сходны с вирусами в том, что они злонамеренны по своей природе.

Аналогичным образом, программы, поставляемые в комплекте с бесплатными программами с рекламной поддержкой, бывают spyware (поскольку при деинсталляции удаляется только «материнская» программа, а рекламный модуль остаётся). Тем не менее, пользователи добровольно скачивают и устанавливают эти программы. Это представляет дилемму для создателей анти-spyware, чьи инструменты удаления могут безвозвратно привести в неработоспособность нужные пользователю программы. Например, недавние результаты теста показали, что комплектная программа WhenUSaveигнорируется Ad-Aware (но удаляется как spyware большинством сканеров), потому что она является частью популярного клиента eDonkey. Для решения этой проблемы Anti-Spyware Coalition работает над постройкой единого мнения внутри индустрии анти-spyware касательно того, что́ является приемлемым поведением программы.

В отличие от вирусов и сетевых червей, spyware обычно не саморазмножается. Подобно многим современным вирусам, spyware внедряется в компьютер преимущественно с коммерческими целями (демонстрация рекламных всплывающих окон, кража персональной информации, например, номеров кредитных карт), отслеживание привычки посещения веб-сайтов или перенаправление адресного запроса в браузере на рекламные или порносайт).

Spyware и cookies

Анти-spyware часто отмечают cookies как spyware. Хотя куки не всегда злонамеренны по своей сути, многие пользователи возражают против того, чтобы третьи стороны использовали их личную информацию, а также дисковое пространство, в своих деловых интересах, поэтому многие анти-spyware предлагают удалять cookies.

Если угроза со стороны spyware становится более чем назойливой, существует ряд методов для борьбы с ними. Среди них программы, разработанные для удаления или блокирования внедрения spyware, также как и различные советы пользователю, направленные на снижение вероятности попадания spyware в систему.

Тем не менее, spyware остаётся дорогостоящей проблемой. Когда значительное число элементов spyware инфицировало ОС, единственным средством остаётся сохранение файлов данных пользователя и полная переустановка ОС.

Меры по предотвращению заражения

Использование браузеров, отличных от Internet Explorer — Opera, Mozilla Firefox и др. Хотя нет совершенно безопасного браузера, Internet Explorer представляет бóльший риск по части заражения из-за своей обширной пользовательской базы.

Использование файрволов и прокси-серверы для блокировки доступа к сайтам, известным как распространители spyware.

Использование hosts-файла, препятствующего возможности соединения компьютера с сайтами, известным как распространители spyware. Однако spyware легко могут обойти этот тип защиты, если производят соединение с удалённым хостом по IP-адресу, а не по имени домена.

Скачивание программ только из доверенных источников (предпочтительно с веб-сайтов производителя), поскольку некоторые spyware могут встраиваться в дистрибутивы программ.