# Осторожно, вирус!

## Spyware
## Программа-шпион

Выполнила: Кузнецова Елизавета
Студентка 321 группы

# 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.

# Терминология

- Нарушитель (англ. *user violator*)пользователь, осуществляющий
- Несанкционированный доступ к информации. Несанкционированный доступ к информации (англ. *unauthorized access to information*)доступ к информации, осуществляемый с нарушением правил разграничения доступа.
- Правила разграничения доступа (англ. *access mediation rules*)часть политики безопасности, регламентирующая правила доступа пользователей и процессов к пассивным объектам.
- Политика безопасности информации (англ. *information security policy*)совокупность законов, правил, ограничений, рекомендаций, инструкций и т. д., регламентирующих порядок обработки информации.

# 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, dronеware;
- инсталлировать на компьютер пользователя дополнительные программы;

# Spyware могут осуществлять широкий круг задач, например:

- 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.

# Законные виды применения

- *Tracking Software* (программы отслеживания) широко и совершенно законно применяются для мониторинга персональных компьютеров.
- *Adware* может открыто включаться в состав бесплатного и условно-бесплатного программного обеспечения. Пользователь соглашается на просмотр рекламы, чтобы иметь какую-либо дополнительную возможность (например — пользоваться данной программой бесплатно). В таком случае наличие программы для показа рекламы должно явно прописываться в соглашении конечного пользователя (EULA).
- *Программы удалённого контроля и управления* могут применяться для удалённой технической поддержки или доступа к собственным ресурсам, которые расположены на удалённом компьютере.

# Законные виды применения

- *Дозвонщики* (диалеры) могут давать возможность получить доступ к ресурсам, нужным пользователю (например — дозвон к Интернет-провайдеру для подключения к сети Интернет).
- *Программы для модификации системы* могут применяться и для персонализации, желательной для пользователя.
- *Программы для автоматической загрузки* могут применяться для автоматической загрузки обновлений прикладных программ и обновлений ОС.
- *Программы для анализа состояния системы безопасности* применяются для исследования защищённости компьютерных систем и в других совершенно законных целях.
- *Технологии пассивного отслеживания* могут быть полезны для персонализации веб-страниц, которые посещает пользователь.

# Образцы spyware

- CoolWebSearch. Группа программ, использующая уязвимости в Internet Explorer. Перенаправляет трафик на рекламу на веб-сайтах, включая *coolwebsearch.com*. Выдаёт всплывающие рекламные окна, переписывает результаты поисковых запросов и изменяет файл hosts инфицированного компьютера для перенаправления DNS на эти веб-сайты.
- *HuntBar*, также *WinTools* или *Adware.Websearch*. Инсталлируется совместно с загрузкой ActiveX с партнёрских сайтов или посредством всплывающих окон, выдаваемых другой spyware (пример того, как одна spyware может инсталлировать ещё больше spyware).
- *Internet Optimizer*, также известный как *DyFuCa*. Перенаправляет в Internet Explorer страницы с ошибками на рекламу. Когда пользователь вводит нерабочую ссылку или набирает неправильный URL, то видит страницу с рекламой. *Internet Optimizer* также классифицируется как *загрузчик*, то есть программа, способная загружать, инсталлировать и запускать другие программы без ведома пользователя.

# Образцы spyware

- Zango (прежде *180 Solutions*). Передаёт детальную информацию рекламодателям о веб-страницах, посещаемых пользователем. Также меняет HTTP-запросы со ссылок на веб-сайты партнёрских рекламодателей, которые, в свою очередь, дают возможность нечестных доходов для *180 Solutions*. Открывает всплывающие окна, перекрывающие веб-страницы компаний-конкурентов.
- Trojan.Zlob (англ.) или просто *Zlob*. Загружается на компьютер через кодек ActiveX и докладывает на сервер такую информацию, как история поиска, веб-сайты, которые вы посещали, и даже нажатия клавиш. Недавно выяснилось, что *Zlob* способен аннулировать установки роутеров.

# 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.
- Использование антивирусных программ с максимально «свежими» вирусными базами.

# Программы анти-spyware

Программы, такие как Ad-Aware (бесплатно для некоммерческого использования, дополнительные услуги платные) от Lavasoft и Spyware Doctor от PC Tools (бесплатное сканирование, удаление spyware платное) стремительно завоевали популярность как эффективные инструменты удаления и, в некоторых случаях, препятствия внедрению spyware. В 2004 году Microsoft приобрела GIANT AntiSpyware, переименовав её в Windows AntiSpyware beta и выпустив её как бесплатную загрузку для зарегистрированных пользователей Windows XP и Windows Server 2003. В 2006 году Microsoft переименовала бета-версию в Windows Defender который был выпущен для бесплатной загрузки (для зарегистрированных пользователей) с октября 2006 года и включён как стандартный инструмент в Windows Vista.