Клавиатурные шпионы. Принципы работы и методы обнаружения

* В феврале 2005 года бизнесмен из Флориды Джо Лопес (Joe Lopez) подал иск против Bank of America: неизвестные хакеры украли у американского предпринимателя с его банковского счета в Bank of America 90 тыс. долларов, которые каким-то образом были переведены в Латвию.
* В результате расследования выяснилось, что на компьютере Лопеса присутствовал вирус Backdoor.Win32.Apdoor (Backdoor. Coreflood), который фиксирует все клавиатурные нажатия пользователя и через Интернет направляет их злоумышленникам. Именно таким образом к хакерам попали пароль и логин Джо Лопеса, который регулярно работал через Интернет со своим счетом в Bank of America.
* Однако суд отказал истцу в возмещении ущерба, указав на то, что г-н Лопес пренебрег элементарными мерами предосторожности при работе со своим банковским счетом через Интернет: детектирование указанного вируса было добавлено в антивирусные базы почти всех производителей антивирусного ПО еще в 2003 году.
* Исчезновению 90 тыс. долларов со счета Джо Лопеса помог обычный кейлоггер.

Что такое кейлоггер?

В переводе с английского keylogger — это регистратор нажатий клавиш.

Кейлоггер (клавиатурный шпион) — программное обеспечение, основным назначением которого является скрытый мониторинг нажатий клавиш и ведение журнала этих нажатий.

Причины для использования «легальных» кейлоггеров:

* для родителей: отслеживание действий детей в Интернете и оповещение родителей в случае попыток зайти на сайты «для взрослых»;
* для ревнивых супругов: отслеживание действий своей половины в Сети в случае подозрения на «виртуальную измену»;
* для службы безопасности организации: отслеживание фактов нецелевого использования персональных компьютеров, их использования в нерабочее время;

* для службы безопасности организации: отслеживание фактов набора на клавиатуре критичных слов и словосочетаний, которые составляют коммерческую тайну организации, и разглашение которых может привести к материальному или иному ущербу для организации;
* для различных служб безопасности: проведение анализа и расследования инцидентов, связанных с использование персональных компьютеров;
* другие причины.

Все кейлоггеры можно условно разделить на аппаратные и программные.

Аппаратные представляют собой небольшие устройства, которые могут быть закреплены на клавиатуре, проводе или в системном блоке компьютера.

Программные — это специально написанные программы, предназначенные для отслеживания нажатий клавиш на клавиатуре и ведения журнала нажатых клавиш.

Наиболее популярные технические подходы к построению программных кейлоггеров:

* системная ловушка на сообщения о нажатии клавиш клавиатуры (устанавливается с помощью функции WinAPI SetWindowsHook, для того чтобы перехватить сообщения, посылаемые оконной процедуре, — чаще всего пишется на C);
* циклический опрос клавиатуры (с помощью функции WinAPI Get(Async)KeyState, GetKeyboardState — чаще всего пишется на VisualBasic, реже на Borland Delphi);
* драйвер-фильтр стека клавиатурных драйверов ОС Windows (требует специальных знаний, пишется на C).

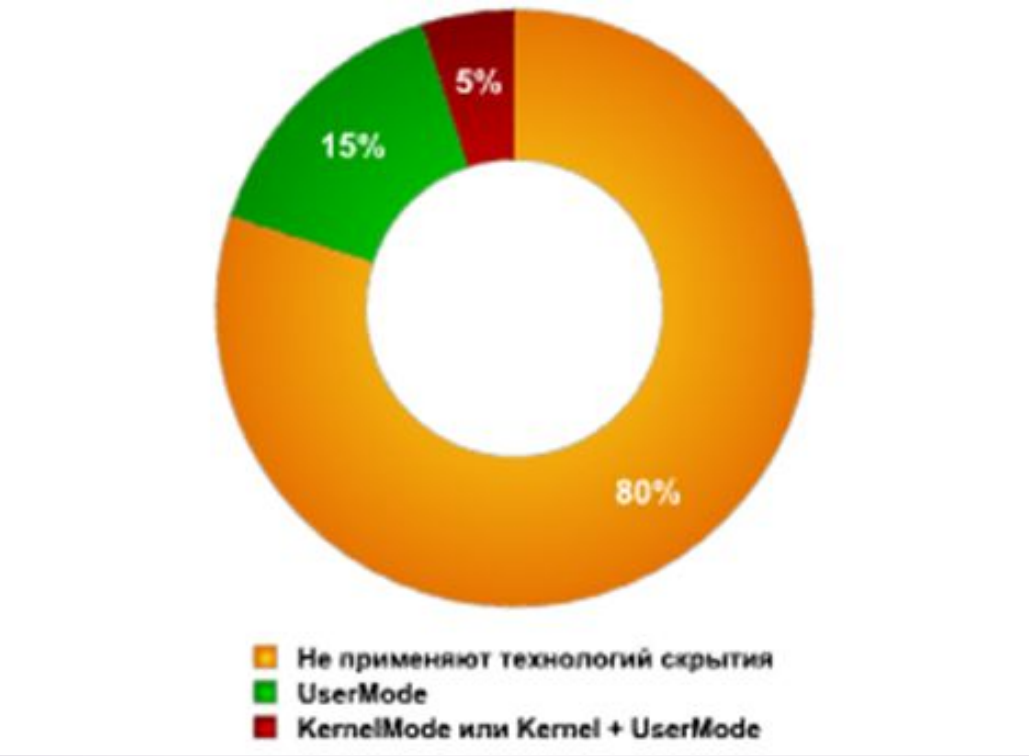
Примерное распределение указанных типов кейлоггеров показано на следующей диаграмме:

В последнее время отмечается тенденция использования в кейлоггерах ***методов сокрытия (маскировки) своих файлов*** — так, чтобы их нельзя было найти вручную или с помощью антивирусного сканера. Такие методы принято называть rootkit-технологиями.

Можно выделить **два основных типа технологий сокрытия**, используемых кейллоггерами:

* с использованием методов сокрытия пользовательского режима (UserMode);
* с использованием методов сокрытия режима ядра операционной системы (KernelMode).

Примерное распределение используемых кейлоггерами технологий сокрытия показано на следующей диаграмме:

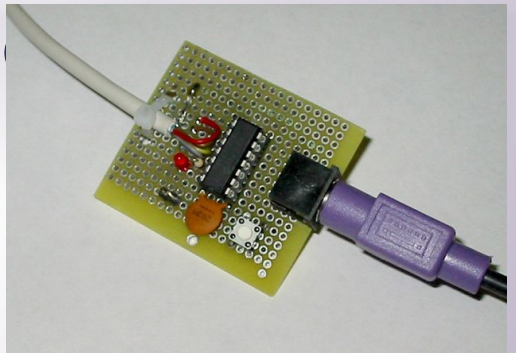


Способы распространения кейлоггеров

* при открытии файла, присоединенного к электронному письму;
* при запуске файла из каталога, находящегося в общем доступе в peer-to-peer сети;
* с помощью скрипта на веб-страницах, который использует особенности интернет-браузеров, позволяющие программам запускаться автоматически при заходе пользователя на данные страницы;
* с помощью ранее установленной вредоносной программы, которая умеет скачивать и устанавливать в систему другие вредоносные программы.

Аппаратные клавиатурные шпионы

* Установка устройства слежения в разрыв кабеля клавиатуры (например, устройство может быть выполнено в виде переходника PS/2);
* Встраивание устройства слежения в клавиатуру;
* Считывание данных путем регистрации ПЭМИН (побочных электромагнитных излучений и наводок);
* Ви лю иатур

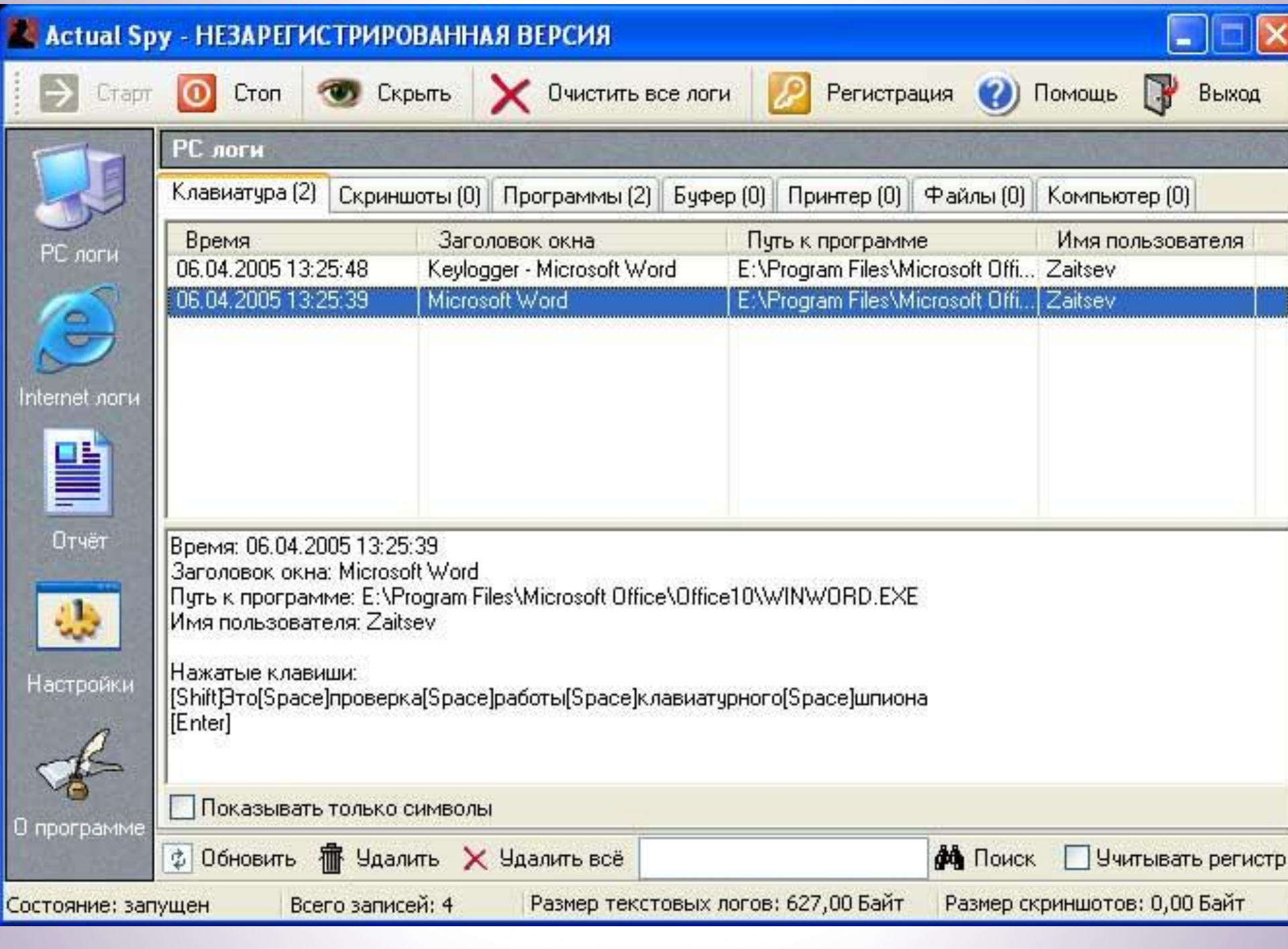


Программные клавиатурные шпионы

Распространенная коммерческая программа ActualSpy (http://www.actualspy.ru).

Возможности:

может регистрировать клавиатурный ввод (с регистрацией заголовка окна и имени программы), снимать скриншоты экрана по расписанию, регистрировать запуск/останов программ, следить за буфером обмена, принтером, создаваемыми пользователем файлами. Кроме того, в программе реализовано слежение за Интернет-соединениями и посещаемыми сайтами.


Actual Spy - НЕЗАРЕГИСТРИРОВАННАЯ ВЕРСИЯ
Старт
Стоп
Скрыть
Очистить все логи
Регистрация
Помощь
Выход
PC логи
Internet логи
Отчёт
Настройки
О программе
PC логи
Клавиатура (2)
Скриншоты (0)
Программы (2)
Буфер (0)
Принтер (0)
Файлы (0)
Компьютер (0)
Время
Заголовок окна
Путь к программе
Имя пользователя
06.04.2005 13:25:48
Keylogger - Microsoft Word
E:\Program Files\Microsoft Offi...
Zaitsev
06.04.2005 13:25:39
Microsoft Word
E:\Program Files\Microsoft Offi...
Zaitsev
Время: 06.04.2005 13:25:39
Заголовок окна: Microsoft Word
Путь к программе: E:\Program Files\Microsoft Office\Office10\WINWORD.EXE
Имя пользователя: Zaitsev
Нажатые клавиши:
[Shift]Это[Space]проверка[Space]работы[Space]клавиатурного[Space]шпиона
[Enter]
Показывать только символы
Обновить
Удалить
Удалить всё
Поиск
Учитывать регистр
Состояние: запущен
Всего записей: 4
Размер текстовых логов: 627,00 Байт
Размер скриншотов: 0,00 Байт

Программа имеет простейшую маскировку от обнаружения – она не видна в стандартном списке задач Windows. Для анализа собранной информации программа формирует протоколы в формате HTML. Принцип работы программы ActualSpy основан на ловушке, регистрирующей события клавиатуры.

Другие примеры:

SpyAgent (http://www.spytech-web.com),

ActMon (http://www.actmon.com),

SpyBuddy (http://www.actmon.com),

PC Activity Monitor (http://www.keyloggers.com),

KGB Spy (http://www.refog.ru/) и др.

Методики поиска клавиатурных шпионов

* Поиск по сигнатурам. Сигнатурный поиск позволяет однозначно идентифицировать клавиатурные шпионы, при правильном выборе сигнатур вероятность ошибки практически равна нулю. Однако сигнатурный сканер сможет обнаруживать заранее известные и описанные в его базе данных объекты;

* Эвристические алгоритмы. Эвристический поиск носит вероятностный характер. Этот метод наиболее эффективен для поиска клавиатурных шпионов самого распространенного типа – основанных на ловушках. Однако подобные методики дают много ложных срабатываний, например, существуют сотни безопасных программ, не являющихся КШ, но устанавливающих ловушки для слежения за клавиатурным вводом и мышью;

* Мониторинг API функций, используемых клавиатурными шпионами. Данная методика основана на перехвате ряда функций, применяемых клавиатурным шпионом. Вызов данных функций каким либо приложением позволяет вовремя поднять тревогу, однако проблемы многочисленных ложных срабатываний будут аналогичны предыдущему методу;

* Отслеживание используемых системой драйверов, процессов и сервисов. В простейшем случае можно применять программы типа Kaspersky Inspector или Adinf, которые отслеживают появление в системе новых файлов.

Методы защиты от кейлоггеров

* Любой антивирусный продукт. Все антивирусы в той или иной мере могут находить клавиатурные шпионы;
* Утилиты, реализующие механизм сигнатурного поиска и эвристические механизмы поиска. Примером может служить утилита AVZ, сочетающая сигнатурный сканер и систему обнаружения клавиатурных шпионов на базе ловушек;
* Специализированные утилиты и программы, предназначенные для обнаружения клавиатурных шпионов и блокирования их работы. Подобные программы наиболее эффективны для обнаружения и блокирования клавиатурных шпионов, поскольку как правило могут блокировать практически все разновидности клавиатурных шпионов.

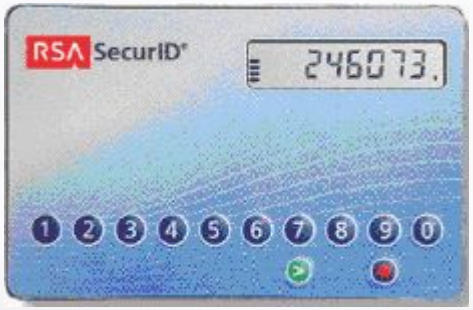
Методы защиты от неизвестных кейлоггеров:

* использование одноразовых паролей / двухфакторная аутентификация,
* использование систем проактивной защиты, предназначенных для обнаружения программных кейлоггеров,
* использование виртуальных клавиатур.

Для получения одноразовых паролей могут использоваться специальные аппаратные устройства:

* в виде брелка (например, Aladdin eToken NG OTP):

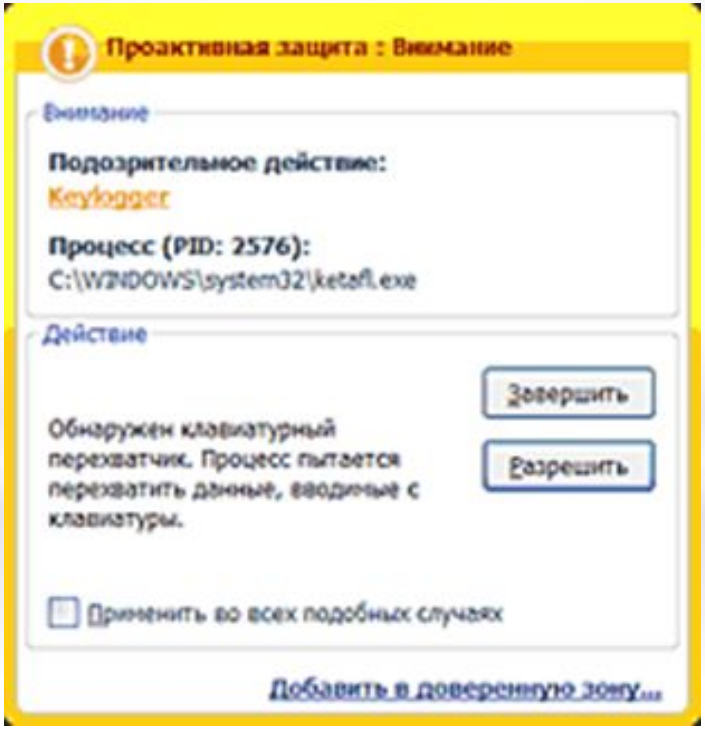
* в виде «калькулятора» (например, RSA SecurID 900 Signing Token):



* системы, основанные на посылке SMS с мобильного телефона, зарегистрированного в системе, и получения в ответ PIN-кода, который нужно вводить вместе с персональным кодом при аутентификации.

Более дешевым решением является использование систем проактивной защиты на стороне клиентов банка (провайдера и т.д.), которые могут предупредить пользователя об установке или активизации программных кейлоггеров.

Пример срабатывания проактивной защиты Kaspersky Internet Security



* Виртуальная клавиатура представляет собой программу, показывающую на экране изображение обычной клавиатуры, в которой с помощью мыши можно «нажимать» определенные клавиши.

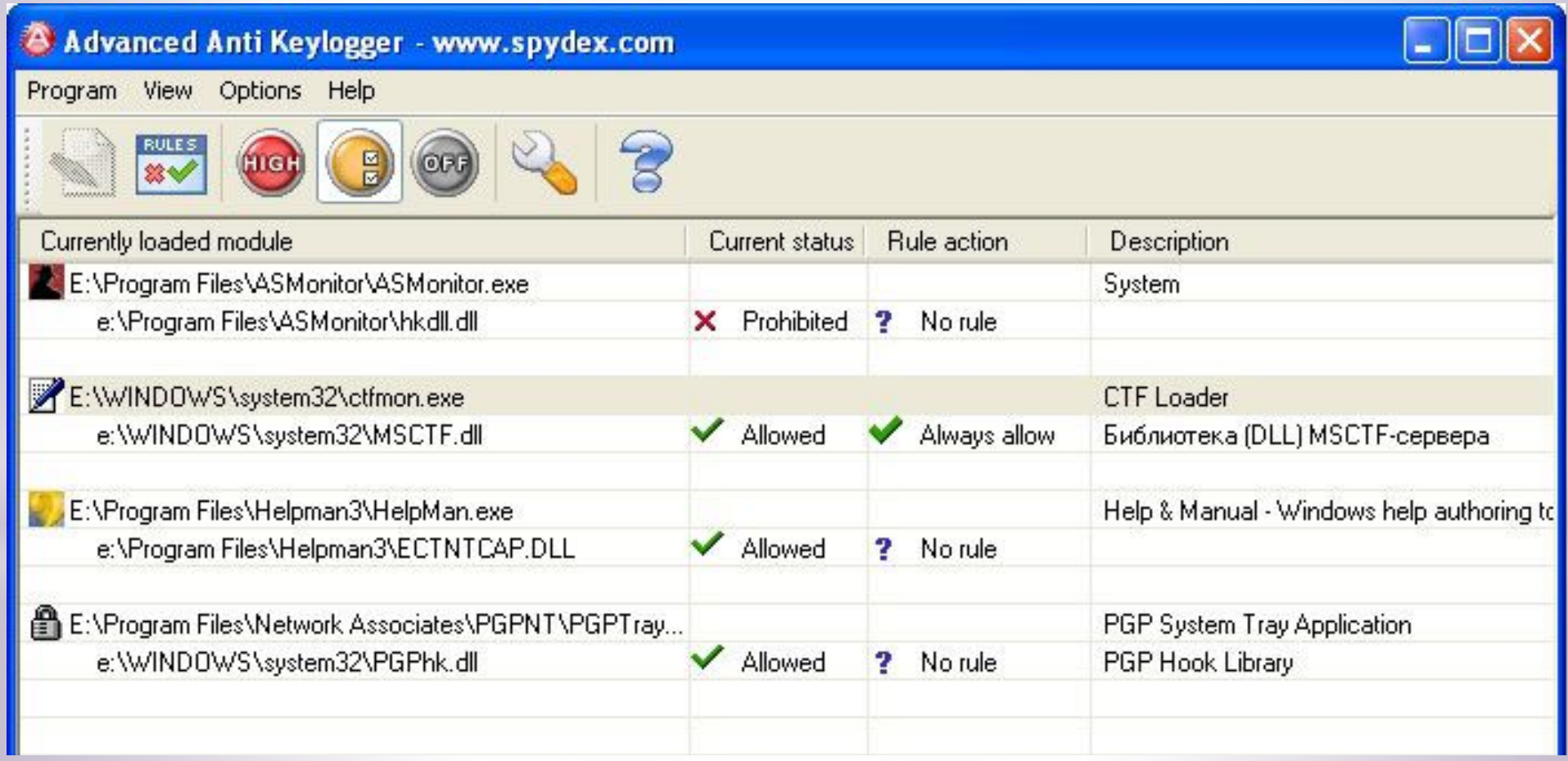
* Однако встроенная в Windows экранная клавиатура плохо применима для обмана кейлоггеров, так как она создавалась не как средство защиты, а для помощи людям с ограниченными возможностями, и передача данных после ввода с помощью данной клавиатуры может быть очень легко перехвачена вредоносной программой. Экранная клавиатура, которая может быть использована для того, чтобы обойти кейлоггеры, должна быть разработана специальным образом, исключающим перехват вводимых данных на любой стадии их ввода и передачи.

Из специализированных программ интерес могут представлять коммерческие продукты PrivacyKeyboard и Anti-keylogger (http://www.bezpeka.biz/). Интерфейс программы Anti-keylogger показан на рисунке:

Программа Anti-keylogger работает в фоновом режиме и производит обнаружение программ, подозреваемых в слежении за клавиатурой. В случае необходимости можно вручную разблокировать работу любой из обнаруженных программ (например, на рисунке видно, что в список «шпионов» попали MSN Messanger и программа закачки из Интернет FlashGet).

Для обнаружение клавиатурных шпионов не применяются базы сигнатур, обнаружение ведется эвристическими методами.

Другим примером может служить программа Advanced Anti Keylogger (http://www.anti-keylogger.net).



В режиме обучения данная программа по логике работы напоминает Firewall – при обнаружении подозрительной активности выводится предупреждение с указанием имени и описания программы. Пользователь может выбрать действие на сеанс (разрешить, запретить), или создать постоянное правило для правило для приложения. Настройки программы защищаются паролем, который задается в ходе инсталляции.

*Выводы

- Несмотря на то что производители кейлоггеров позиционируют их как легальное ПО, большинство кейлоггеров может быть использовано для кражи персональной информации пользователей и осуществления экономического и политического шпионажа.
- В настоящее время кейлоггеры, наряду с фишингом и методами социальной инженерии, являются одним из главных методов электронного мошенничества.
- Компании, работающие в сфере компьютерной безопасности, фиксируют стремительный рост числа вредоносных программ, имеющих функциональность кейлоггера.
- Отмечается тенденция добавления в программные кейлоггеры rootkit-технологий, назначение которых — скрыть файлы кейлоггера так, чтобы они не были видны ни пользователю, ни антивирусному сканеру.
- Обнаружить факт шпионажа с помощью кейлоггеров можно только с использованием специализированных средств защиты.
- Для защиты от кейлоггеров следует использовать многоуровневую защиту.

Спасибо за внимание!!!