HOOK

Системные ловушки

- Ловушка (hook) - это механизм Windows, позволяющий перехватывать события, предназначенные некоторому приложению, до того как эти события до этого приложения дойдут.
- Функции-фильтры - это функции, получающие уведомления о произошедшем событии от ловушки.
- В зависимости от типа ловушки функции-фильтры могут изменять события, отменять их или просто реагировать на них. Таким образом, когда мы говорим "установил ловушку" мы подразумеваем процесс прикрепления функции-фильтра к выбранному нами типу ловушки.

SetWindowsHookEx

- function SetWindowsHookEx(idHook: integer; lpfn: TFNHookProc; hmod: HINST; dwThreadID: DWORD): HHOOK; stdcall;

- *idHook*: описывает тип устанавливаемой ловушки.

idHook

WH_CALLWNDPROC - Фильтр процедуры окна. Функция-фильтр ловушки вызывается, когда процедуре окна посылается сообщение. Windows вызывает этот хук при каждом вызове функции SendMessage.

WH_CALLWNDPROCRET - Функция-фильтр, контролирующая сообщения после их обработки процедурой окна приемника.

idHook

- WH_CBT - В литературе встречаются следующие названия для этого типа фильтров: "тренировочный" или "обучающий". Данная ловушка вызывается перед обработкой большинства сообщений окон, мыши и клавиатуры.

- WH_DEBUG - Функция-фильтр, предназначенная для отладки. Функция-фильтр ловушки вызывается перед любой другой ловушкой Windows. Удобный инструмент для отладки и контроля ловушек.

idHook

- WH_GETMESSAGE - Функция-фильтр обработки сообщений. Функция-фильтр ловушки вызывается всегда, когда из очереди приложения считывается любое сообщение.
- WH_HARDWARE - Функция-фильтр, обрабатывающая сообщения оборудования. Функция-фильтр ловушки вызывается, когда из очереди приложения считывается сообщение оборудования.

idHook

- WH_JOURNALPLAYBACK - Функция-фильтр вызывается, когда из очереди системы считывается любое сообщение. Используется для вставки в очередь системных событий.
- WH_JOURNALRECORD - Функция-фильтр вызывается, когда из очереди системы запрашивается какое-либо событие. Используется для регистрации системных событий.

idHook

- WH_KEYBOARD - Функция-фильтр "обработки" клавиатуры. Наверное, наиболее часто используемый тип ловушки. Функция-фильтр ловушки вызывается, когда из очереди приложения считывается сообщения wm_KeyDown или wm_KeyUp.

- WH_KEYBOARD_LL - Низкоуровневый фильтр клавиатуры.

idHook

WH_MOUSE - Функция-фильтр, обрабатывающая сообщения мыши. Функция-фильтр ловушки вызывается, когда из очереди приложения считывается сообщение мыши.

WH_MOUSE_LL - Низкоуровневый фильтр мыши.

idHook

- WH_MSGFILTERФункция-фильтр специального сообщения. Функция-фильтр ловушки вызывается, когда сообщение должно быть обработано диалоговым окном приложения, меню или окном приложения.

- WH_SHELLФильтр приложения оболочки. Функция-фильтр ловушки вызывается, когда создаются и разрушаются окна верхнего уровня или когда приложению-оболочке требуется стать активным.

lpfn

- *lpfn* : это адрес функции-фильтра, которая является функцией обратного вызова.
- Функция-фильтр имеет тип TFNHookProc, определение которого выглядит следующим образом:

- TFNHookProc = function (code: Integer; wparam: WPARAM; lparam: LPARAM): LRESULT stdcall;

hmod

- *hmod*: данный параметр должен иметь значение hInstance в EXE или DLL-файлах, в которых содержится функция-фильтр ловушки.
- Если речь идёт о глобальных ловушках, то данный параметр может принимать только дескриптор DLL, из которой устанавливается ловушка.

dwThreadID

- *dwThreadID*: данный параметр идентифицирует поток, с которым будет связана ловушка. Мы ведём речь о глобальных ловушках, поэтому данный параметр будет всегда равен 0, что означает, что ловушка будет связана со всеми потоками в системе.

SetWindowsHookEx

SetWindowsHookEx(WH_SHELL, **@ShellHook**, HInstance, 0);

в данном случае ShellHook - это и есть функция-фильтр.

В дальнейшем, под словосочетанием "установили ловушку" будем понимать присоединение функции-фильтра к ловушке.