Updating MakeMethodInstance

by Peter Sokolov

Back in Issue 18 (February 1997), an article by John Chaytor described a unit called `MakeMIC`, which contained a set of procedures for creating wrappers around class methods so they could be used as standard Windows callback procedures. I've found them to be really useful. However, after some recent in-depth debugging on one of my projects which used John's code, I located a serious but hard to find bug.

This brief article describes the problem and the solution. `MakeMIC` uses a `VirtualXXX` function to allocate memory for procedure wrapping code. The call is simple. In the function `MakeMethodInstance`:

```
Result := VirtualAlloc(nil, sizeof(TJumpBlock), MEM_COMMIT,
  PAGE_EXECUTE_READWRITE);
```

Later in `MakeMethodInstance32Reg` we find:

```
Result := VirtualAlloc(nil, sizeof(TJumpBlockOpt3), MEM_COMMIT,
  PAGE_EXECUTE_READWRITE);
```

This memory is freed in `FreeMethodInstance`:

```
VirtualFree(Instance, 0, MEM_DECOMMIT);
```

The problem lies in the virtual memory implementation in Win32. Virtual memory must first be reserved then committed. In the above calls the `MEM_RESERVE` flag is not included, but memory is reserved nevertheless! In the call to `VirtualFree`, memory is just de-committed, not released ('unreserved'). If you call these functions frequently, more and more virtual memory will be reserved until the program cannot allocate any more. Although program memory consumption (as seen, for example, in Task Memory) is very low, since reserved but uncommitted memory is not shown, but calls to `VirtualAlloc` still return `ERROR_NOT_ENOUGH_MEMORY`.

The fix is very simple: explicitly `RESERVE` and `RELEASE` memory. The above calls should be changed to:

```
Result := VirtualAlloc(nil, sizeof(TJumpBlock), MEM_RESERVE OR
  MEM_COMMIT, PAGE_EXECUTE_READWRITE);
```

and:

```
Result := VirtualAlloc(nil, sizeof(TJumpBlockOpt3), MEM_RESERVE or
  MEM_COMMIT, PAGE_EXECUTE_READWRITE);
```

and finally:

```
VirtualFree(Instance, 0, MEM_RELEASE);
```

The updated version of the `MakeMIC` unit, together with John Chaytor's original article (in Adobe Acrobat format), is included on this month's disk.

Peter Sokolov works for FAB d.o.o. in Slovenia.