

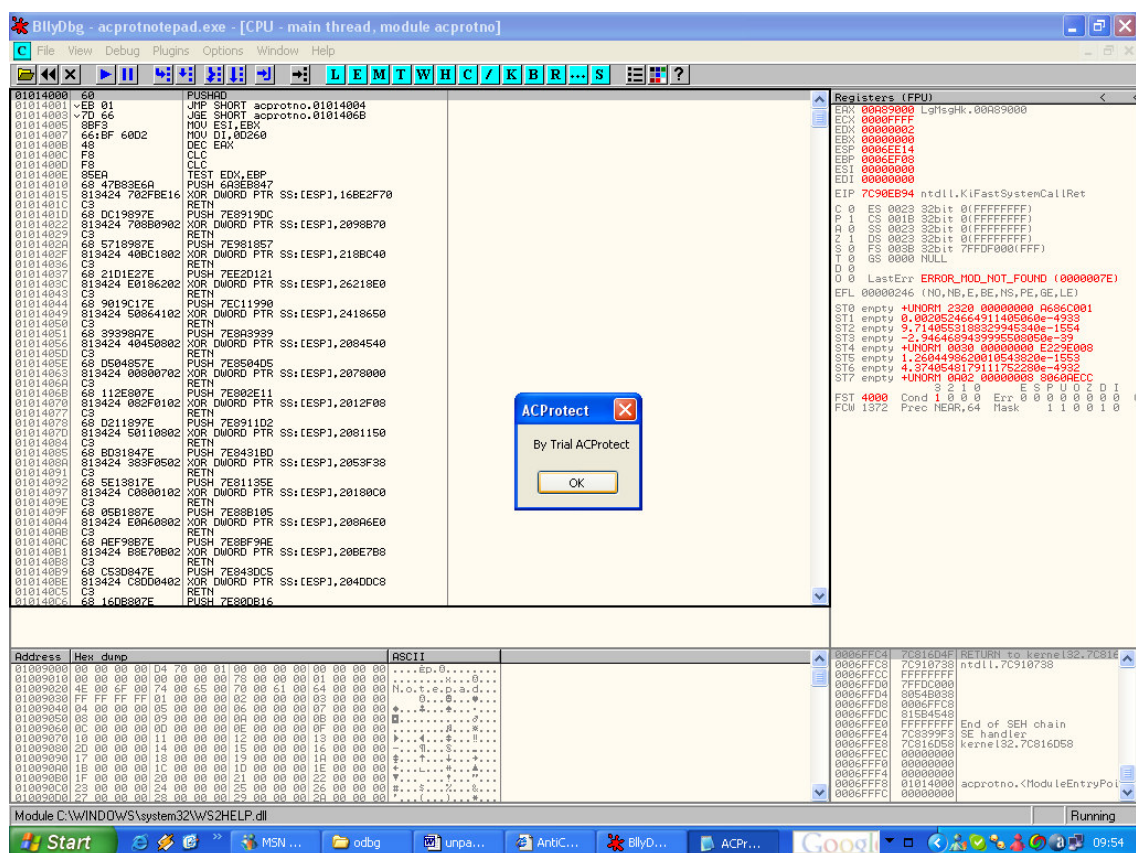
## Manually unpacking AntiCrack Protector v1.41

Stardate: 2005-12-05  
Target: Anything that's protected with Acprotector v1.41 (eg. notepad.exe)  
Protector URL: <http://www.siskinsoft.com/protector/downloads.html>  
Tools needed: Olly, IMPrec with ACprotect plugin, a hammer and nails  
Difficulty: Depends on your current state of knowledge :-P  
Author: potassium / ARTeam

Hello readers!

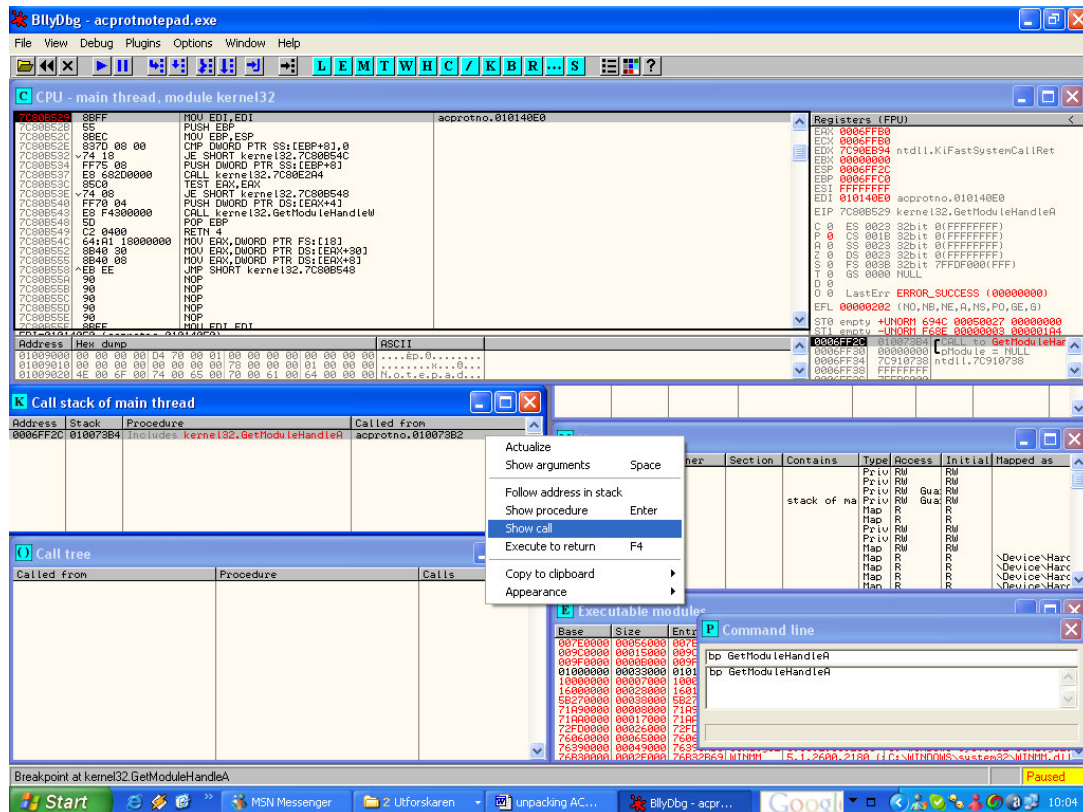
Today I am presenting a method to unpack the trial version of AntiCrack Protector, and thus automatically removing the trial nag.

First of all, carefully prepare the target by protecting it with Acprotect.  
Then load it into olly and run it!

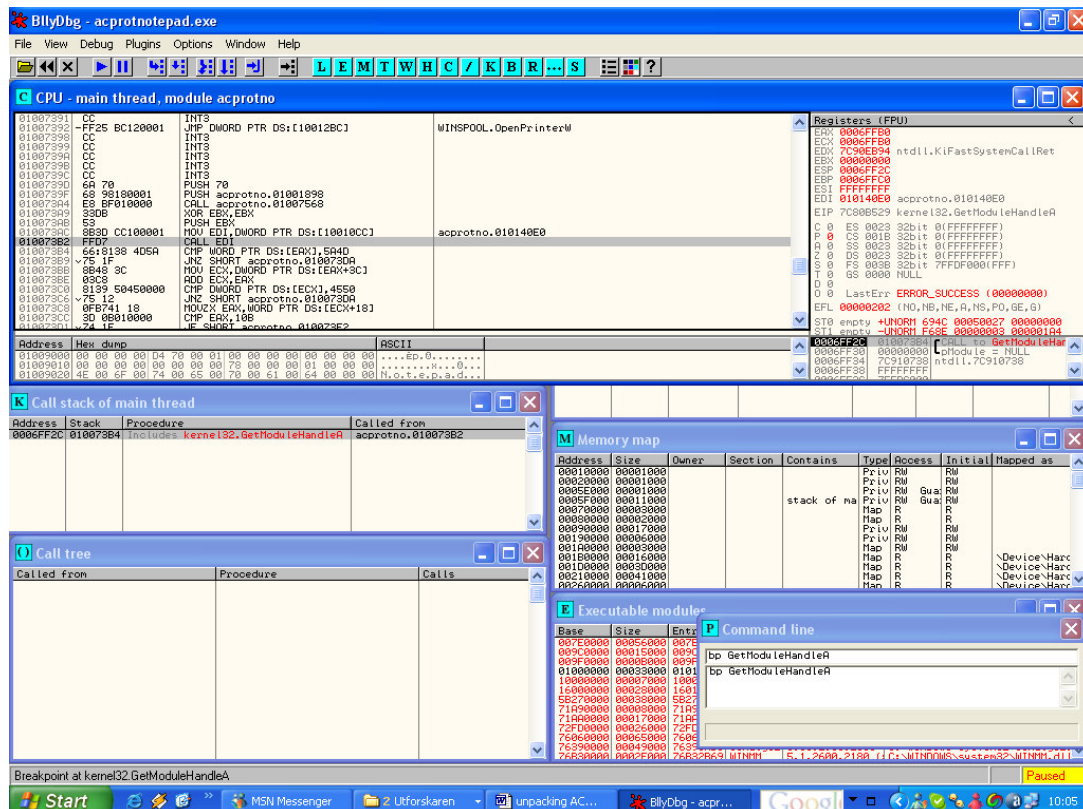


Ahaa, there is the nag. Now, set breakpoint on an appropriate API, in this case I know it is GetModuleHandleA, but it could of course be something completely different in your target. The most common alternatives would be GetVersion and GetModuleHandleA.

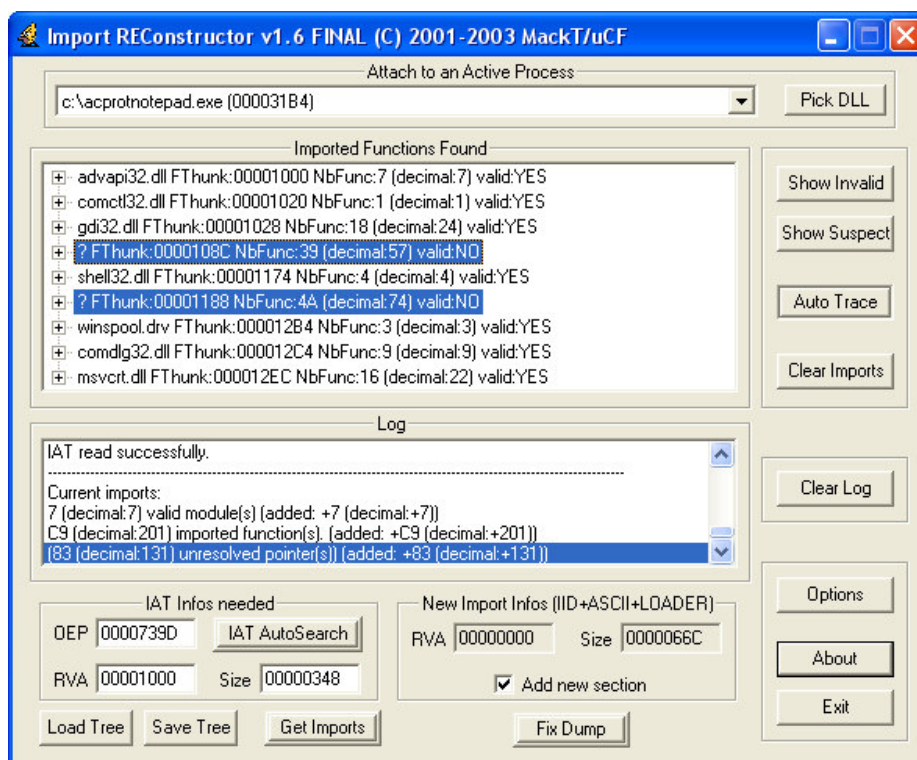
When breakpoint is set on GetModuleHandleA Olly will break a couple of times, just press F9 till nothing more happens then press the nag 'ok' button and you should end up here:



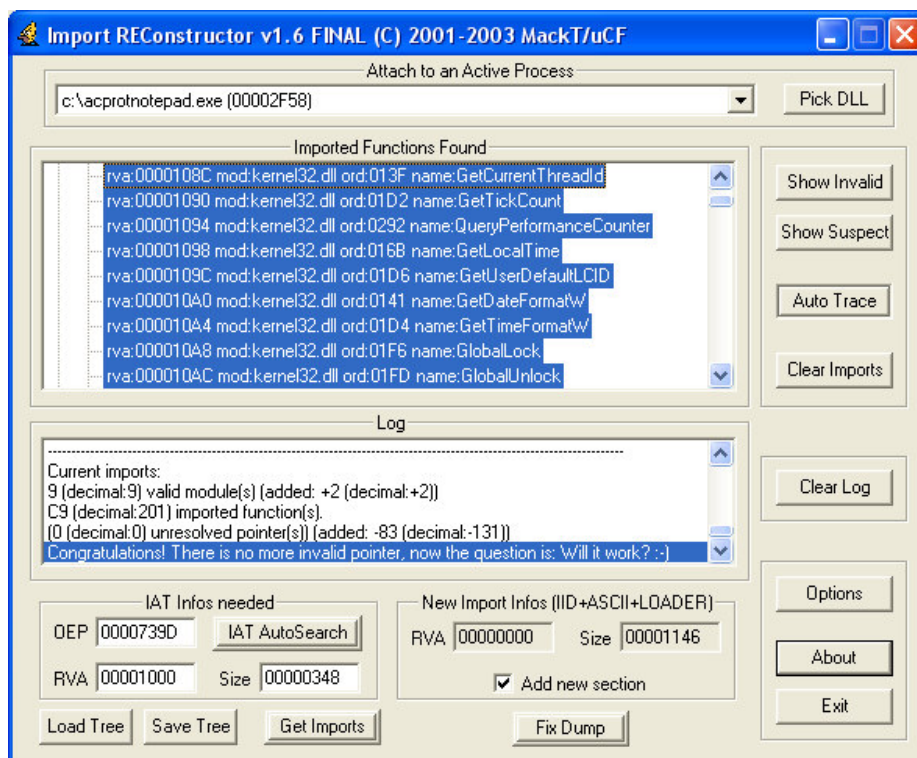
Bring up the call stack window (alt-k) and press Show call, this is where you end up. Scroll up a little bit And here is our beloved OEP! (PUSH 70)



Mark the row of the OEP and set as new origin and dump the target with ollydump (without the rebuild option).  
Now launch Imprec and fix the target:



As you can see we have to invalid thunks, fix these with the Acprotect plugin and fix the dump.



And, there it is, success!! It runs! Have a nice day.

/potassium