TITLE: DoDi's Protection Test
FILENAME: OVERTEST.EXE
KEYS: decompiler source code reverse engineering discompiler VB security protection
DESCRIPTION:
Test the protection of your Windows programs before shipping!
Even well known companies sometimes ship their programs with debug information, and this tool quickly tests any single module or whole directories, and alerts you if debug information is found in a module.

In the first version, only the debug information in VB programs is detected, the next release will include detection of Microsoft and Borland debug information.

The name OVERTEST is derived from a so called protection tool, that does some woodoo to make users beleive that their programs were protected afterwards. Gamblers may appreciate to give it a 'risk level' and try to protect a VB3 program with the methods for VB4 (don't wonder, there is no working code for VB4). You should test the result of tools like OVERWRITE with OVERTEST before wasting your money and nevertheless giving away your sources for free.

But I appreciate competition, and was inspired to improve my own protection mechanisms while ROTFLing about the 20 lines of 'protection' code in OVERWRITE, and while writing OVERTEST. No, honestly, I didn't adopt any of Marty's 'algorithms', but I'm angry that he promises to protect programs against decompilers. It's only 1 line of sourcecode in a decompiler to detect overwritten names and use a synthesized name instead, so this method is inappropriate at all.

However, VBDis3 is designed to demonstrate all the unnecessary informations about your source code in a VB executable, and will reject to deal with overwritten programs (only if it happens to detect this, of course). But there exist more decompilers, which certainly are not so polite.

Serious programmers possibly prefer a complete automatic protection for their VB programs, based on the knowledge of the author who also wrote the best public VB decompiler, VBDis3. Overwriting the names of forms and controls is no protection against a decompiler, since these names can be easily synthesized, and the changes can be edited into valid names with a hex editor. A hacker equipped with a decompiler will also have a hex editor and know how to use it. Therefore other techniques must be used to make any decompiler crash or (sometimes better) produce wrong sources.

Reasonable protection against all kinds of decompilers is available with DoDi's Project Manager, contained in DoDi's Developer Tools for Visual Basic. Demo versions of DoDi's VB-Tools are available in the CompuServe DDJ forum (VBDIS*.ZIP), the last upload was VBDIS11E.ZIP, and version 18 or higher will come after the currently known bugs are fixed.

The unrestricted versions of DoDi's VB-Tools are available in CompuServe with SWREG #7807. For questions about protection of VB programs ask Microsoft or Dr. Hans-Peter Diettrich (DoDi for short) on CIS 100752,3277 (Internet: 100752.3277@compuserve.com).