

Forum:[Hack Forums](#)

Thread: [Extreme Protector \(VB6/C/ASM\) No Dependencies Compatible Native/.Net/x86/x64](#)

darkshadowss - May 22, 2018, 10:19 am

This is not sell thread, is a preview for your comments, ideas and opinions about my private protector that i will sell the full project, source codes and binaries. Cant post images and links sorry.

Jabber: d4rksh4d0w@jabber.calyxinstitute.org

General description:

Extreme Protector is made and improved for more than 1 year by experienced coder/reverser in this field for more than 6 years. It is a 100% private project never used nor released made as cryptographic and educational purposes. Code has been tested, modded and improved for many many times until every feature is working 100% together others features. Working on all Windows from Windows xp to Windows 10. Stub code is optimized, reduced, as fast as possible for efficiency and removed most dependencies to work properly on most windows, stub size goes from 32kb to 450kb. Protector or client is made in pure VB6 and the different stubs are made in pure VB6 and others one mixing VB6 with full ASM and C, i mean fully integrated ASM and C, not inline one, developed with ThunderVB, a powerful tool to mix perfectly ASM and C with VB6 with no limits. There are 11 stubs and here their characteristics:

Pure VB6:

- 1-Basic(VB6): Only VB6 without anything
- 2-Basic + anti emulation-debug(VB6): Only VB6 with anti emulation.
- 3-Basic + invokes(VB6): Only VB6 with apis taken via asm inline invoke, most apis used are not declared in code.
- 4-Stub Inside Program P-Code: Basic(VB6) stub inside or mixed with real program VB6 source compiled in P-Code.
- 5-Stub Inside Program P-Code + anti emulation-debug: Basic + anti emulation-debug(VB6) stub inside or mixed with real program VB6 source compiled in P-Code.
- 6-Stub Inside Program Native Code-Small: Basic(VB6) stub inside or mixed with real program VB6 source compiled in Native-Code.

VB6/C/ASM mixed:

- 7-Basic + ASM: Basic(VB6) stub with VB6 procedures replaced by pure ASM like instrt, len, mid, some strings, strptr, varptr, left, right, api calls among many others. This applies by default for next ASM stubs.
- 8-Basic + ASM + C + anti emulation + anti debug: Basic + ASM stub with anti emulation and debug made in VB6, C and ASM code.
- 9-Stub Inside Program Native Code-Small + ASM + C + anti emulation + anti debug: Basic + ASM + C + anti emulation + anti debug stub inside or mixed with real program VB6 source compiled in Native-Code.
- 10-Basic + ASM + C + anti emulation + anti debug + experimental compilation: Basic + ASM + C + anti emulation + anti debug stub with uncommon compilation parameters like custom DOS stub, sections merge etc. This is possible due to custom compilation parameters in C code and changing VB6 linker and compiler parameters in the VB6 project file.
- 11-Basic + ASM + C + anti emulation + anti debug + runpe nt simple: Basic + ASM + C + anti emulation + anti debug stub with nt apis runpe, most apis called by ASM code.

Detailed information

Stubs Features:

Optional:

- +Advanced anti VBox/VMware:check 6 critical places with 2 methods to detect if the file is running under virtual machine.
- +Advanced anti Sandboxie:check process and dlls to detect if the file is running under sandboxie.
- +Advanced anti Analysis:check with 15 procedures to detect if the file is running under analysis environment.
- +9 different injections options
- +2 different storage file methods:End of File and Resources.
- +Fake error message: can select if you dont want show the message when the file runs at startup.
- +Run as Admin:run file as with Admin privileges.
- +Install:can choose folder to install(user/alluser/commonprogramfiles/appdata/temp) with custom filename.
- +Hidden startup:run file every time system starts,the start key is hidden from msconfig.
- +Delay:Delay the execution of the file in seconds.
- +Binder that can run 2 files binded:
 - Executable file wich is executed on memory.There are 9 different injections options.
 - Any custom file wich is executed normally.
- For both binded files there are these options:
 - +Anti Sandboxie
 - +Anti VBox/VMWare
 - +Pump bytes
 - +Dont run the binded file at startup
- +2 different storage file methods:End of File or random resources

Forced:

- +Anti Dump:3 different methods of anti dump(ASM/C)
- +Anti Emulation:many different methods of anti emulation(VB6/ASM/C)
- +Remove ZoneID:remove automatically ZoneID of the installed file when install option is activated(VB6/ASM).
- +Random RC4 password to decrypt the protected files.

Client Features:

- +Clone assembly:can change protected file cloning information and icon from other PE files(exe,dll,scr,ocx).
- +Custom icon:can change the icon with any custom icon
- +2 different methods to clone information and icon or change custom icon you can choose:
 - +Resource method:Resource Hacker method
 - +Code method:With internal code
- +Add KBs:add random kilobytes to the protected file with 2 methods automatically:
 - +If storage method is resources the extra kilobytes will be added to resources and if storage method is End of File the extra kilobytes will be added in the End of File.This apply to main file and 2 binded files too.
- +EOF:Detect automatically if the file to be protected has overlay and put that data to the protected file.
- +Realign EOF: Realign End of File data with headers.
- +Realign PE: Realign Portable Executable Headers.
- +FixChecksum:Fix the checksum of the file.
- +Null Icon>Delete full icon of the protected file.

- +Null Info:Delete full Information of the protected file.
- +Zero EntryPoint:Set the EntryPoint of the file to 0.
- +Change OEP:Change Original EntryPoint to another place.
- +UPX:Compress the protected file with UPX.
- +Erase Paddings:Erase "XPADDING" strings from the resources.
- +Add Section:Add custom section to protected file.
- +No comdlg32.ocx dependence for working.
- +Autodetect if file is native or .NET and select automatically the proper injection for working properly.This apply for main file and binded executable file too.
- +Error proof:if something is wrong with your options before protect, protector will warning you or change/disable options to avoid errors in protection process.
- +RC4 encryption with different random password generated every protection.
- +ID and type resources are randomly generated every protection automatically.
- +Real random process to generate random strings, passwords etc.
- +Drag and drop for all fields.

malson - May 23, 2018, 9:31 am

very good 6 yr in experiencing bro !! I heard whiteshadowss is as good as u at reversung bro need learn crypters with asm cooode.

darkshadowss - May 23, 2018, 9:28 pm

(May 23, 2018 09:31 AM)malson Wrote: [\[CITE\]](#) very good 6 yr in experiencing bro !! I heard whiteshadowss is as good as u at reversung bro need learn crypters with asm cooode.

There is no many asm crypters code examples on net from what i know,take time learn asm but it deserves the worth, i prefer asm over the rest languages.