Oreans Technologies Code Virtualizer v3.14.0 + CRACK

2025-06-12 08:43:30 label 我要反馈 下载页面

Code Virtualizer is a highly effective code obfuscation program for Windows, Linux, and Mac OS X software, which aids programmers in securing their sensitive code places against Reverse Engineering with quite powerful obfuscation code on code virtualization.

Code Virtualizer will convert your initial code (Intel x86/x64 directions) to Virtual Opcodes, only known through an inner digital Machine. Those digital Opcodes and the Virtual Machine are exceptional for every protected program, preventing an overall assault over Code Virtualizer.

Code Virtualizer can safeguard your sensitive code places in almost any x32 and x64 native PE/ELF/Mach-O documents (such as adware files/EXEs, system solutions, DLLs, OCXs, ActiveX controls, shared items, screen savers, and device drivers).

Once an application has been made, the compiler will compile the program source code to many object files made from machine language. Then, the records are linked together to make the executable.

Once an attacker attempts to decode a compiled program, he'll use a decompiler tool that will decompile the system language code into a broader code (such as assembly code or a greater programming language), performing his research within the decompiled code.

After the attacker gets a fantastic understanding of the target program, he could alter the compiled program to change its behavior. By way of instance, the attacker may skip the routine which checks for the trial period within an application and allow it to run indefinitely, or worse, cause the program to act as though it had been registered.

Code virtualization is made from transforming code from a particular machine into a distinct binary code that's recognized by another device. In other words, the instruction set in the particular machine has been converted into a new instruction set that's understood by another machine. This picture represents the transformation in the cube of Intel x86 instructions into a new instruction set for another device (especially a RISC 32-bit CPU):

Code Virtualizer can create numerous kinds of virtual machines using another instruction set for everyone. This usually means that a particular block of Intel x86 instructions could be transformed into various instruction sets for every device, preventing an attacker from recognizing some established virtual opcode following the transformation out of x86 directions. This picture represents how the block of Intel x86 directions is converted into various sorts of virtual opcodes, which might be emulated by various virtual machines.

Once an attacker attempts to decompile a code block that has been shielded by Code Virtualizer, he won't locate the first x86 instructions. Rather, he'll come across an entirely new instruction set that's not recognized by any other specific decompiler. This may force the consumer to experience the tough job of identifying how every opcode is implemented and how the particular digital machine functions for every protected program. Code Virtualizer completely obfuscates the implementation of these digital opcodes and analyzes every distinctive digital machine to prevent somebody from analyzing how the digital opcodes are implemented.

Code Virtualizer could be embedded within your Win32 and Win64 software and device drivers easily. You have to select which Code Virtualizer will guard regions on your source code. The next example demonstrates how it is possible to shield a block of code at a C program.

The VIRTUALIZER_START/VIRTUALIZER_END macros are dummy macros that do not interfere with implementing their first program. It is simply in protection-time if Code Virtualizer will comprehend those regions of code and convert them to specific digital opcodes, which are subsequently emulated by a digital server once the protected software is operating.

去下载

标签

Applications Tools

This picture represents the picture of a first compiled program (before being shielded) and how it's altered when Code Virtualizer shields it:

As the picture shows, Code Virtualizer should embed the virtual server to conclude the protected software to emulate the digital opcodes when they are implemented.

Code Virtualizer is a powerful technology that may stop somebody from scrutinizing your sensitive code, like your patterns, which support an input key to registering your program. Additionally, Code Virtualizer slightly simplifies the secure program's header, which means that you could place a compressor or other applications shield at the top of Code Virtualizer without any issues.

If you're a Windows device driver programmer and felt failed when there wasn't any remedy to safeguard your device drivers, Code Virtualizer supplies you with the same technology to do this (for 32-bit and 64-bit drivers) in precisely the same manner as your programs and DLLs.

Try Code Virtualizer now and begin integrating the most recent software security to your Windows, Linux, and Mac OS X software and device drivers!

Oreans Technologies Code Virtualizer Great Features:

- Obfuscation via multiples Virtual Machines
- Unique coverage for Each protected program
- Security of almost any x32 and x64 program and Apparatus Driver
- Advanced mutation motor
- Code move to Safeguard DLLs and Device Drivers
- Emulation of almost any Intel x86 opcode interior unique Digital Machines
- Unique Digital opcodes for each protected program
- Complete compatible with almost any compressor/protector
- Command-line defense

资源列表

download Oreans Technologies Code Virtualizer v3.14.0

inve 产品数量

已有 42647个

grou 付费会员

已有 1676位

anal 价值评估

商业价值约 ￥6635.87万元

dow 下载数量

已下载 222908次