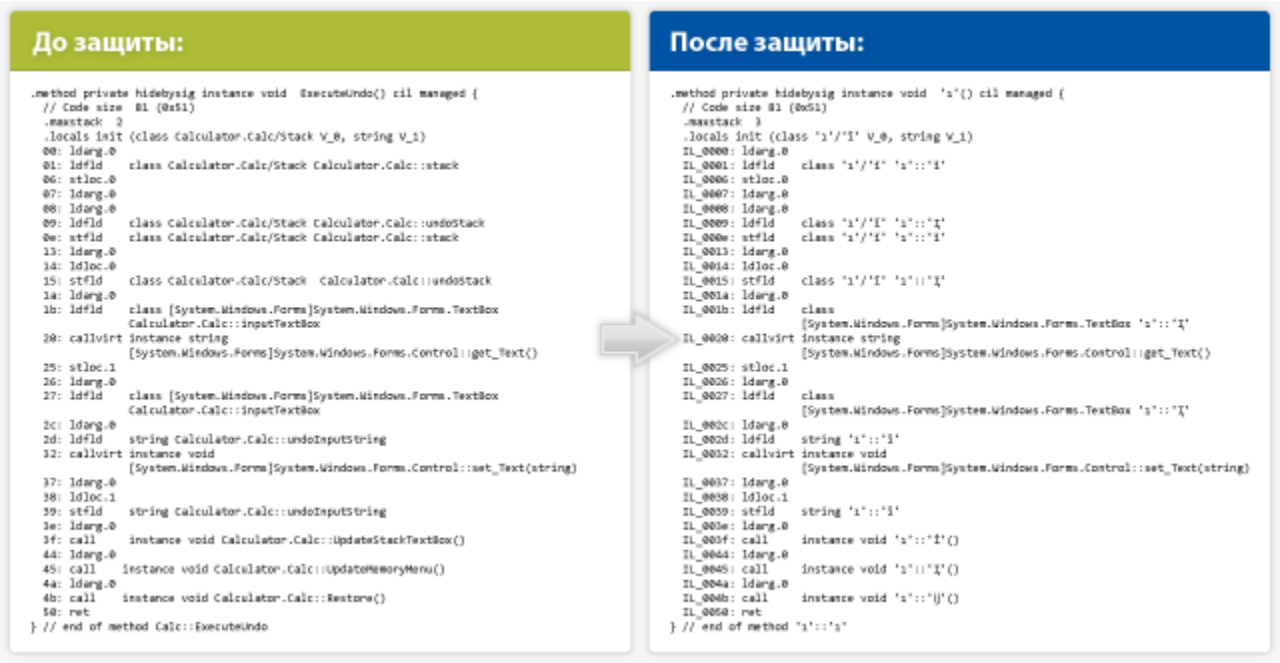
Обфускация

Символьная обфускация

Символьная обфускация — наиболее простой способ запутать злоумышленника, анализирующего код. Она позволяет переименовать имена типов, событий, свойств, методов. При этом может использовать непечатный набор символов, что очень помешает т.н. статическому анализу. Данная операция необратима, и код получается очень трудночитаемый.

Результат работы символьный обфускации MSIL кода:

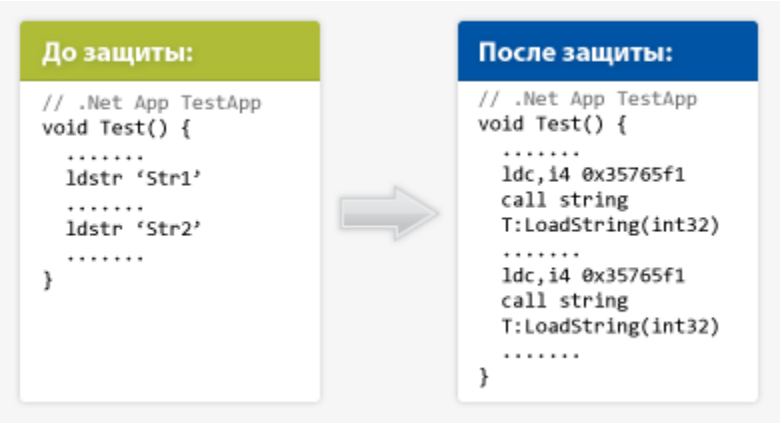


Важно!
Будьте внимательны, если вы используете **Reflection API.** Типы и методы, доступ к которым происходит с его использованием, обфусцировать нельзя.

Шифрование строк

В процессе обфускации все текстовые строки в исходном тексте зашифровываются с использованием электронного ключа и помещаются в защищенный **native–контейнер.** Метод применяется для сокрытия важной информации, которая может заинтересовать злоумышленника или поможет ему найти нужный фрагмент кода. Используя **Reflection API** для вызова функций, данный механизм позволяет зашифровать имена методов и типов.

Результат работы режима шифрования строк:



Обфускация графа потока управления

Обфускация графа потока управления (начиная с версии ***Guardant SDK 6.0***) предоставляет возможность разбить код методов на несколько блоков, добавить фальшивые и скрыть от анализа последовательность их исполнения. Последовательность исполнения блоков в этом случае будет зашифрована с использованием электронного ключа Guardant. При этом в реальных функциях количество блоков легко превышает 10, делая невозможным статический анализ кода.

Результат работы режима обфускации графа потока управления: