Символьная обфускация .NET-сборок

Символьная обфускация позволяет усложнить жизнь злоумышленнику, так как все осмысленные имена внутри защищаемого приложения превращаются в набор случайных символов, и обратный анализ такого кода становится гораздо сложнее. Если осмысленные имена больше не используются, то поиск по ключевым словам становится невозможным. Например, **«SerialNumberCheck(uint licenseID, byte[] serialNumber)** в виде обфусцированного имени будет выглядеть, как **"abb(uint zxd, byte[] skf)".**

Технология перегрузки имен, также использованная в обфускаторе, позволяет присвоить одно и то же имя большому количеству сущностей внутри защищаемого приложения, что позволяет еще сильнее усложнить его обратный анализ.

Еще одним элементом защиты, который реализуется посредством обфускации, является шифрование строковых констант с использованием аппаратного алгоритма электронного ключа. Этот механизм позволяет обращаться к ключу в процессе выполнения, причем для каждого защищаемого приложения такая схема работы с ним будет уникальной, так как обращение к строковым константам происходит в разных местах обфусцированного кода.

Обфускатор Guardant предоставляет следующие возможности для защиты .NET-приложений:

- Обфускация исполняемых файлов (.exe) и библиотек (.dll)
- Символьная обфускация имен (типы, методы, поля, свойства, события, параметры методов и обобщений)
- Перегрузка полей, методов (присваивание одного и того же имени объектам с разными сигнатурами)
- Поддержка нескольких алфавитов (символы, цифры, символы и цифры, непечатные символы)
- Тонкая настройка параметров обфускации при помощи конфигурационного файла
- Сохранение в файл отображения обфусцированных имен в оригинальные
- Сохранение статистики обфускации (покрытие оригинального кода обфусцированным)
- Шифрование строк с использованием электронного ключа
- Обфускация графа потока управления

- Задать собственные сообщения вакцины
- Запретить вывод сообщений защищенного приложения
- Запретить вывод сообщений утилиты на экран