УДК 004.021

АЛГОРИТМЫ ОБФУСКАЦИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, РАЗРАБАТЫВАЕМОГО НА ЯЗЫКАХ C/C++

Лаврентьев С.А. , Дудкин А.С., Андрушкевич С.С.
Научный руководитель – кандидат технических наук, Дудкин А.С.
(Военно-космическая академия им. А.Ф.Можайского)

Введение. Обфуска́ция - приведение исходного текста или исполняемого кода программы к виду, сохраняющему её функциональность, но затрудняющему анализ, понимание алгоритмов работы и модификацию при декомпиляции.

Одним из основных методов взлома программного обеспечения является исследование кода, полученного в результате работы дизассемблера на предмет уязвимостей. На основе такого когда нетрудно, например, составить программу генерации ключей активации коммерческого программного обеспечения или, наоборот, внести в исполняемый файл изменение - патч, позволяющий злоумышленникам отключить "нежелательные" модули исходной программы.

Всему вышеперечисленному как раз и может противодействовать специальная программа - обфускатор. Как понятно из вышесказанного, методы обфускации должны усложнить код, преобразовав его таким образом, чтобы скрыть от третьих лиц логику его работы.

В идеале хотелось бы, чтобы программа, прошедшая обфускацию, давала бы не больше информации нежели чёрный ящик, имитирующий поведение исходной программы [1].

Основная часть. В предлагаемом подходе будет применяться обфускация вызова функций — это метод скрытия библиотек DLL и внешних функций, которые будут вызываться во время выполнения. Для этого будут использоваться стандартные функции Windows API, такие как GetModuleHandle и GetProcAddress. Первый возвращает обработанную указанную библиотеку DLL, а второй позволяет получить адрес памяти нужной функции, которая экспортируется из этой библиотеки DLL. Имя экспортируемой функции изначально будет зашифровано функцией XOR(исключающее ИЛИ) [2]. Также адреса функций WinAPI буду находить по их хэшу через перечисление экспортированных функций WinAPI.

Выводы. Проведен анализ существующих алгоритмов обфускации исходного кода программ на C/C++ и разработан комплексный подход.

Список использованных источников:

1. Обфускация как метод защиты программного обеспечения // Хабр URL: https://habr.com/ru/post/533954/ (дата обращения: 17.02.2023).
2. AV engines evasion // URL: https://cocomelonc.github.io/tutorial/2021/09/06/simple-malware-av-evasion-2.html (дата обращения: 17.02.2023).

Лаврентьев С.А. (автор) Подпись

Андрушкевич С.С. (автор) Подпись

Дудкин А.С. (научный руководитель) Подпись