Дополнительная защита кода, обфусцированного посредством виртуальной машины

Выполнил: Ниценко Г.Ю.

Научный руководитель: ст. пр. Сартасов С.Ю.

Рецензент: Мордвинов Д.А.

Предметная область

- Обфускация программ
- Обфускация с помощью виртуальной машины

Предметная область

- Анализ потока системных вызовов для деобфускации (Kevin Coogan, 2011)
- Системные вызовы в операционных системах Windows NT для процессоров Intel x86

Постановка задач

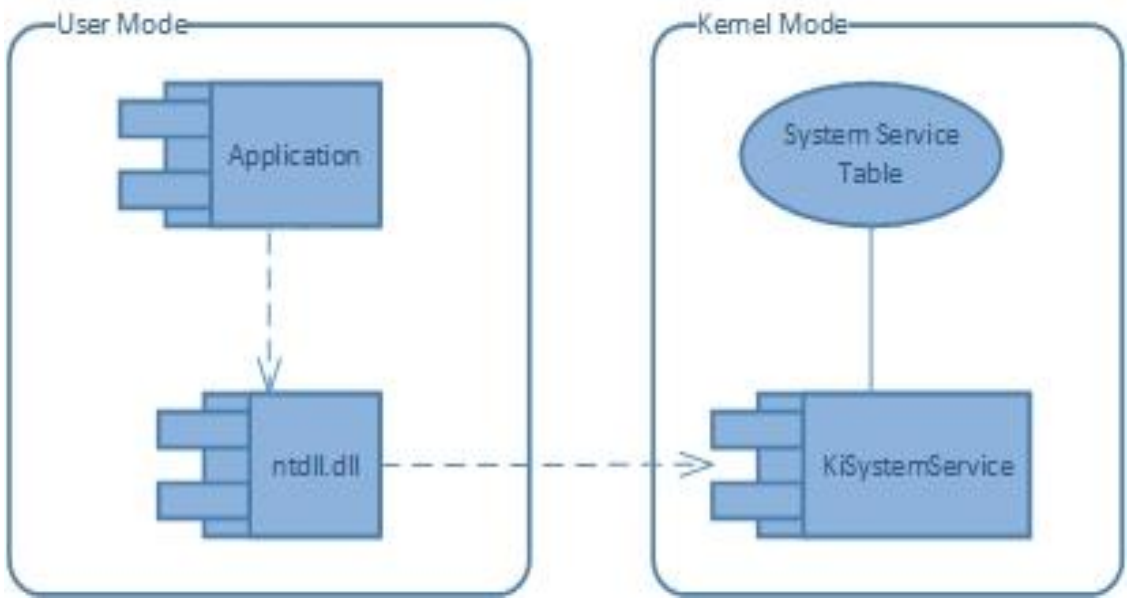
- Цель
  - Разработка программной компоненты для защиты программ, обфусцированных посредством ВМ, от деобфускации посредством анализа потока системных вызовов
- Задачи
  - Изучить предметную область: подходы к обфускации/деобфускации, системные вызовы (Windows NT, Intel x86)
  - Разработать подход для защиты от анализа потока системных вызов
  - Создать программную компоненту, реализующую данный подход

Системные вызовы

- Native API – посредник при взаимодействии между процессами и ядром ОС
- Библиотека ntdll.dll – реализация Native API, набор «заглушек» (stubs) системных вызовов. «Заглушка» содержит:
  1. идентификатор системного вызова,
  2. указатель на параметры системного вызова,
  3. вызов прерывания для запуска режима исполнения ядра,
  4. вызов возврата в режим пользователя.

Системные вызовы

- KiSystemService – обработчик прерывания
- Ядро исполняет системный вызов посредством поиска его номера по идентификатору в System Service Table



Решение

- Генерация системных вызов для создания шума, препятствующего анализу потока системных вызов
- Разработка драйвера для создания системных вызовов
- Эффективность алгоритма доказана теоретически: препятствие созданию множества релевантных системных вызов для дальнейшего анализа

Реализация

- Подмена обработчика исключения KiSystemService на собственный
- Создание системного вызова при каждой обработке прерывания

Результаты

- Изучена предметная область: подходы к обфускации/деобфускации, системные вызовы (Windows NT, Intel x86).
- Разработан подход для защиты кода, обфусцированного посредством ВМ, от деобфускации с помощью анализа потока системных вызовов
- Создан драйвер (Windows NT, Intel x86), реализующую данный подход