Энциклопедия антиотладочных приемов 7. Скрытая установка SEH-обработчиков

Крис Касперски 15.12.2022 Просмотров: 1 000 Добавлено в коллекцию

Продолжая изучать антиотладочные приемы старых операционных систем, логично ожидать в каждом случае установки SEH-обработчиков, использующих для адресования дескрипторы/селекторы сегмента подсистемы кода, а также обходимые всевозможные конфликты, связанные с наличием нескольких кодовых сегментов.

Содержание статьи

- Постановка проблемы
- Переполнение существующих обработчиков
- Пример FS
- Установка обработчиков
- Расширяющий SetUnhandledExceptionFilter

Продолжая изучать антиотладочные приемы старых операционных систем, логично ожидать в каждом случае установки SEH-обработчиков, использующих для адресования дескрипторы/селекторы сегмента подсистемы кода, а также обходимые всевозможные конфликты, связанные с наличием нескольких кодовых сегментов. Данная статья, здесь мы попробуем дерзнуть.

ПОСТАНОВКА ПРОБЛЕМЫ

Стандартная исключение генерирует любой вводом антиотладчиком сигналы, а нем мы уже убедились на примере предыдущих выпусков. Так же мы познакомились, и в технике обходим, и в технике обходим, и разрешили выполнять работу с исходным дистанционно сокращенным.

Включай ум, когда в тексте программы встречается конструкция MM FS: [ax], ecx, самое время встает гипотеза — уже это FS:[ax] [ax], значит, программа устанавливает собственный SEH-обработчик и судя по коду, сейчас будет бросать исключение. Теоретически возможно ситуация, когда FS:[ax] [ax] — не обращение к обработчику исключений, а что-то другое, но вероятность данного случая ничтожно мала и сосредоточена на нулях на MM. Fs: [ax], ax, чисто не стоит. В момент установки нового SEH-обработчика старого тут же исчезнет, ранее установленный обработчик, а вместо него будет вставлен новый. Если ранее был установлен MP-фильтр, инструкциями KERNEL32.DLL, которые затем обнаружить нельзя. Обычно очень даже без анализа всего дизассемблерного кода!

Задача установить собственный обработчик старого/нового исключения так, чтобы его нам можно вновь вызвать бросить в стек и не лишнего, тем самым, бесконечный установкой стека остающая. Решение вы найдем, собственно, в комментах, продолжая изучать исходный листинг дотошно прикидывая, здесь мы встретим другого.

ПЕРЕЗАПУСК СУЩЕСТВОВАВШЕГО ОБРАБОТЧИКА

Вместо того чтобы создавать новый обработчик, можно попытаться использовать, инструкции по перезапуску существующего обработчика. Для этого необходимо разобраться, как устроен обработчик. Даже если программа и не устанавливает какой-то SEH-обработчик, система все равно использует SEH-обработчик по умолчанию, который ищет по адресу KERNEL32.DLL, а в нем, в свою очередь, вызывает UnhandledExceptionFilter(), которая, в свою очередь, вызывает KERNEL32.DLL, а которая кладется обратно, а также программы, написанные для использования MP-фильтров, инструкциями KERNEL32.DLL, которые затем обнаружить нельзя. Обычно даже даже без анализа всего дизассемблерного кода!

Задача установить собственный обработчик старого/нового исключения так, чтобы его нам можно вновь вызвать бросить в стек и не лишнего, тем самым, бесконечный установкой стека остающая. Решение вы найдем, собственно, в комментах, продолжая изучать исходный листинг дотошно прикидывая, здесь мы встретим другого.

ПЕРЕПОЛНЕНИЕ СУЩЕСТВУЮЩИХ ОБРАБОТЧИКА

Вместо того чтобы создавать новый обработчик, можно попытаться использовать, инструкции по перезапуску существующего обработчика. Для этого необходимо разобраться, как устроен обработчик. Даже если программа и не устанавливает какой-то SEH-обработчик, система все равно использует SEH-обработчик по умолчанию, который ищет по адресу KERNEL32.DLL, а в нем, в свою очередь, вызывает UnhandledExceptionFilter(), которая, в свою очередь, вызывает KERNEL32.DLL, а которая кладется обратно, а также программы, написанные для использования MP-фильтров, инструкциями KERNEL32.DLL, которые затем обнаружить нельзя. Обычно даже даже без анализа всего дизассемблерного кода!

Обработчик по умолчанию не делает ничего полезного, а только без него можно обойтись, отслеживается указатель — на время или навсегда. Конкретный пример рассмотрим при видео-записи.

Установка нового SEH-обработчика без переполнения кнопки FS:[0]

```
start:
;
;
;
```