#### Министерство науки и высшего образования Российской Федерации

федеральное государственное автономное образовательное учреждение высшего образования

### «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

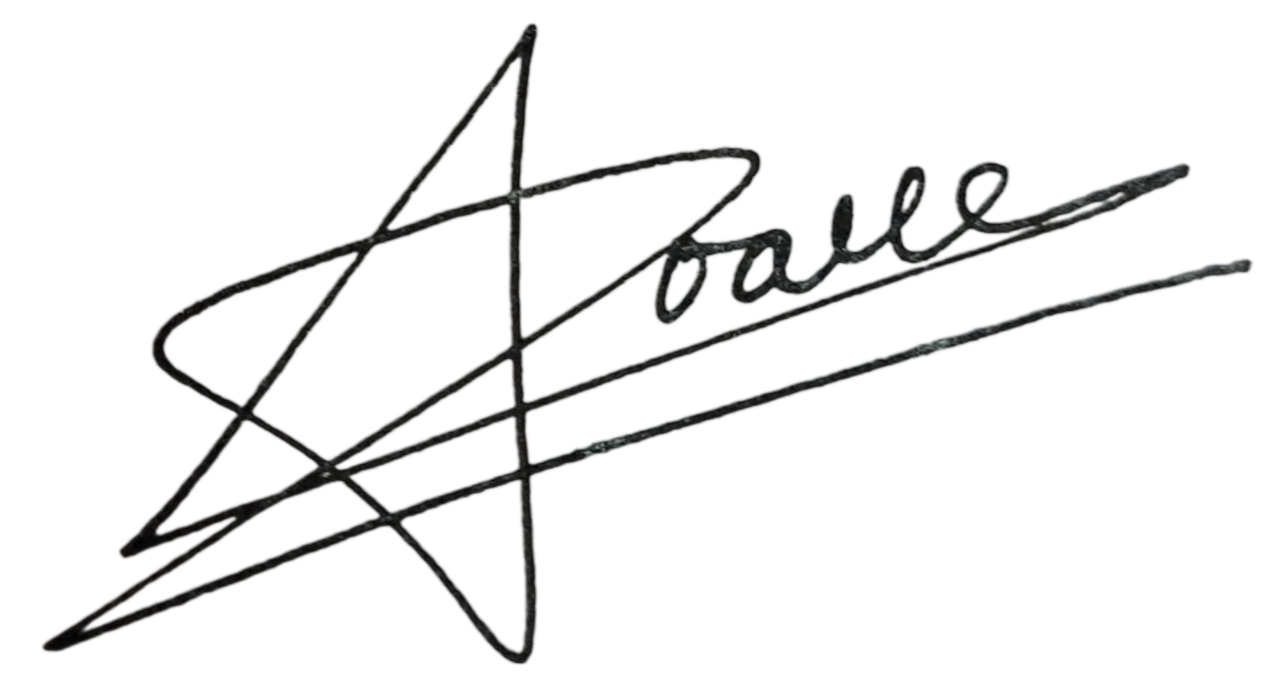
#### Дисциплина:

« Курс по ревёрс-инжинирингу»

### ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

**Выполнил студент(ы):**

группа: N3347



\_\_\_\_Чу Ван Доан \_\_\_\_\_\_\_\_/\_\_\_\_\_\_\_\_\_\_

*ФИО Подпись*

**Проверил:**

Ханов Артур Рафаэльевич \_/\_\_\_\_\_\_\_\_\_\_

*ФИО Подпись*

Санкт-Петербург

2024 г.

# ЗАДАНИЯ

Разобрать вирус Win32.Maya.4254

1. Как вирус восстанавливает таблицу адресов импорта
2. Как вирус заражает другие файлы
3. Каков payload вируса

Для выполнения лабораторной работы был выбран вирус «Virus.Win32.Maya.4254».

Запустим «Virus.Win32.Maya.4254» в отладчике x32dbg.

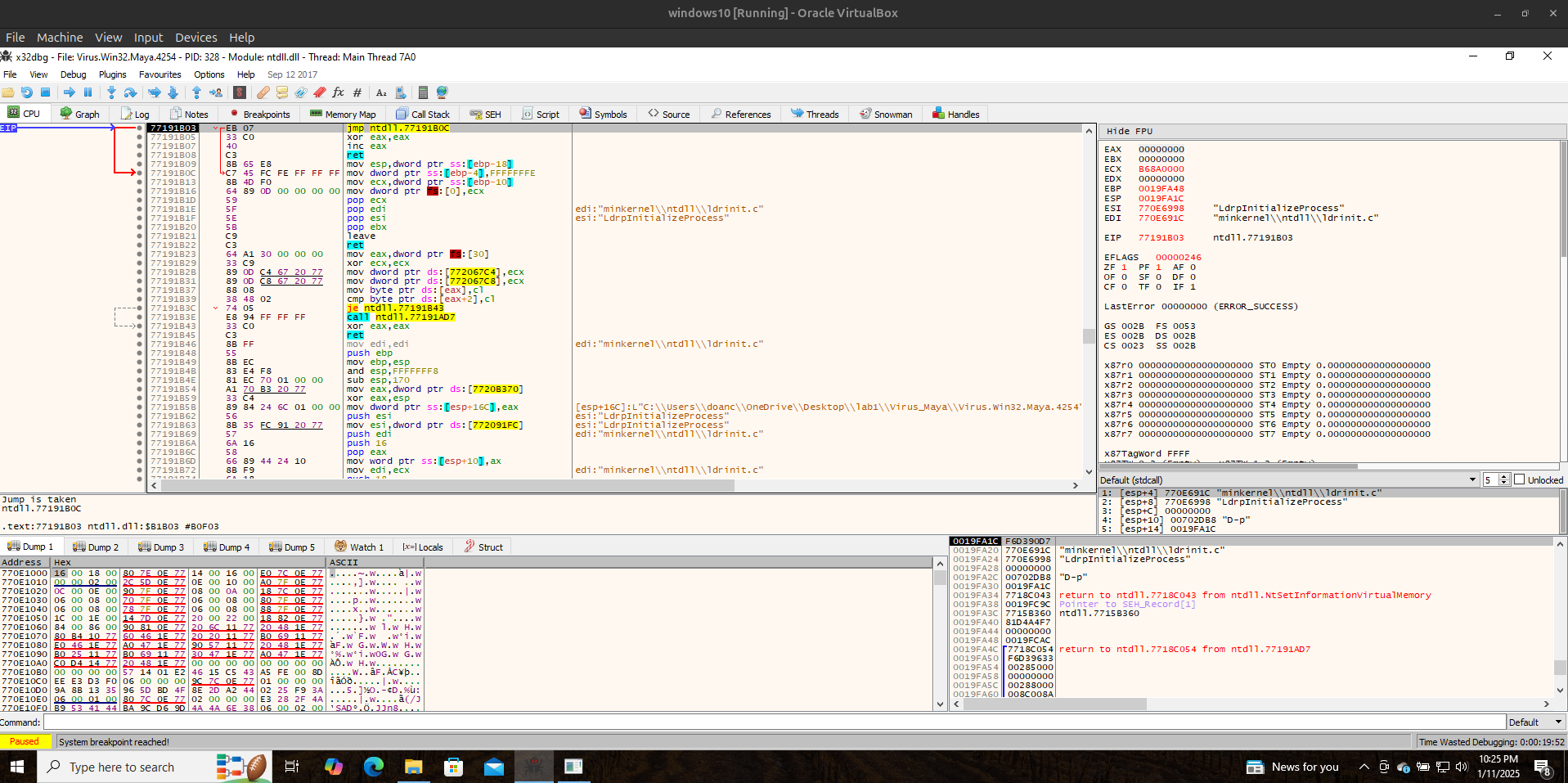


Рисунок 1 - Запуск «Virus.Win32.Maya.4254»

После нажатия на F9 происходит выполнение программы до точки останова – EntryPoint.

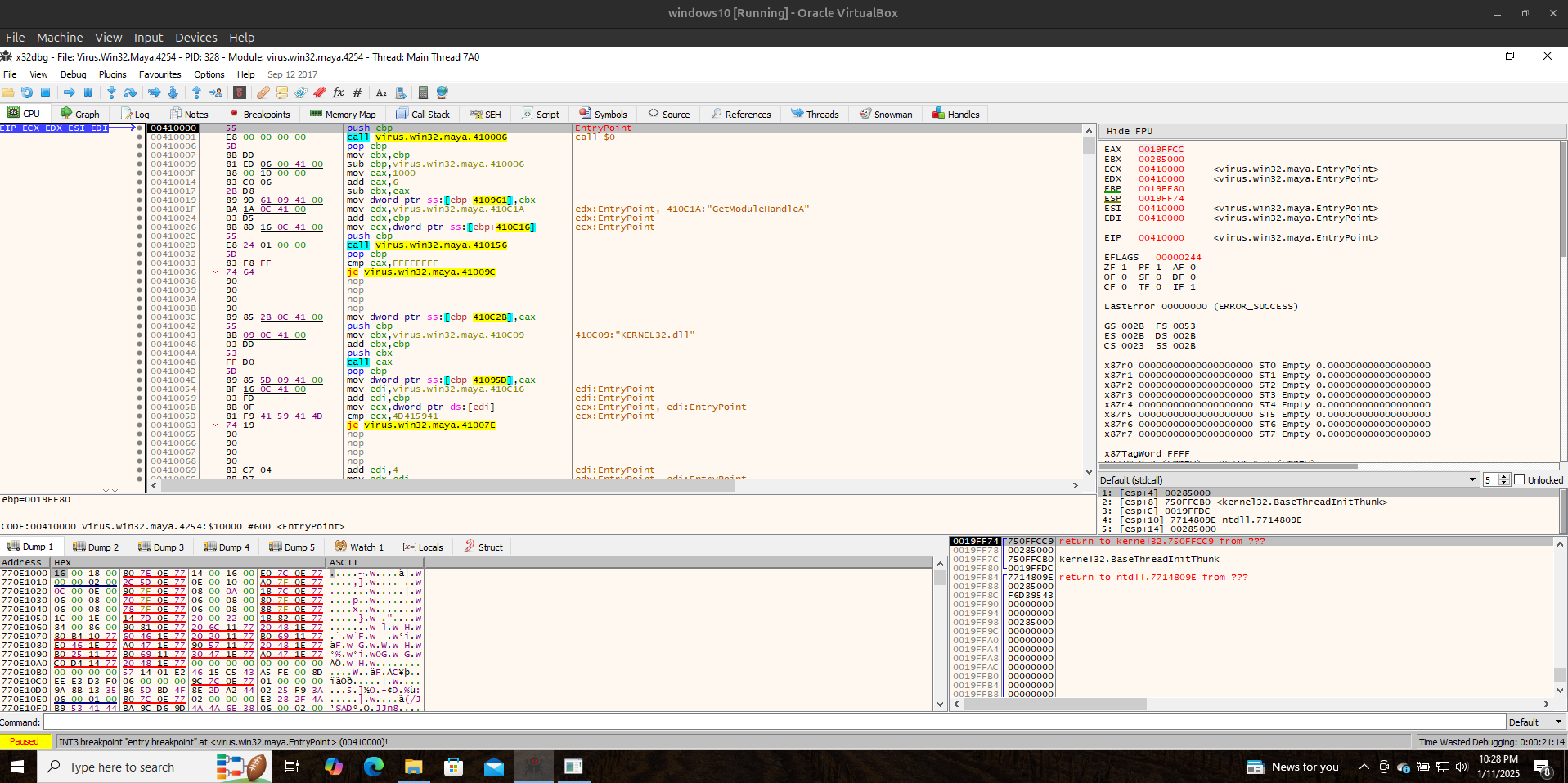


Рисунок 2 - EntryPoint в отладчике

Запускаем IDA Disassembler c «Virus.Win32.Maya.4254» и нажимаем пробел – отображается блок-схема программы.

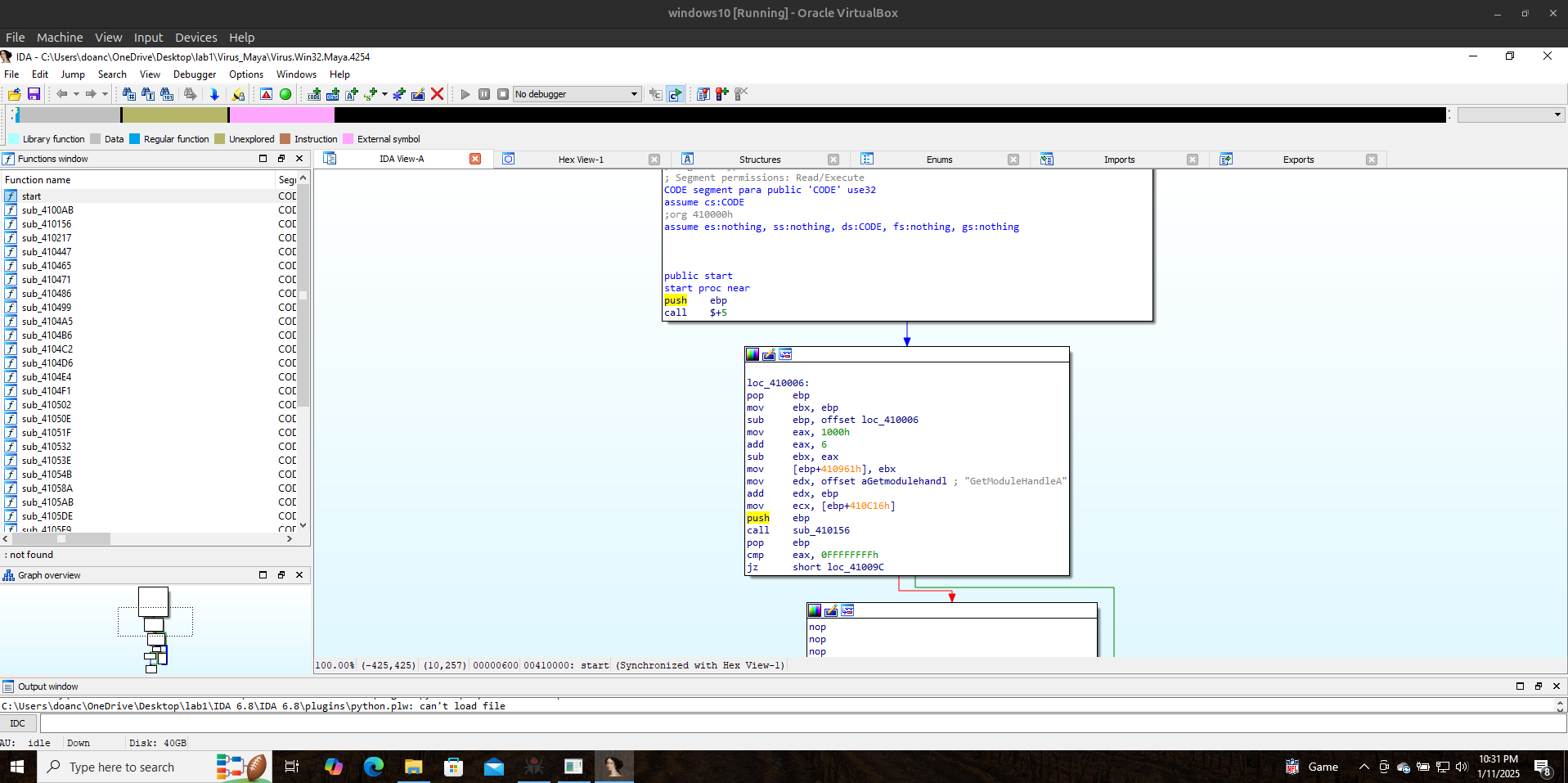


Рисунок 3 - Образ вируса открытый в IDA Disassembler

Далее в отладчике выполняем последовательно шаги программы, нажимая F8, и переименовываем dword (или пишем соответствующие комментарии в IDA Disassembler).

С помощью программы IDA Disassembler мы можем рассмотреть все основные этапы работы вируса, представленные на рисунке 4.

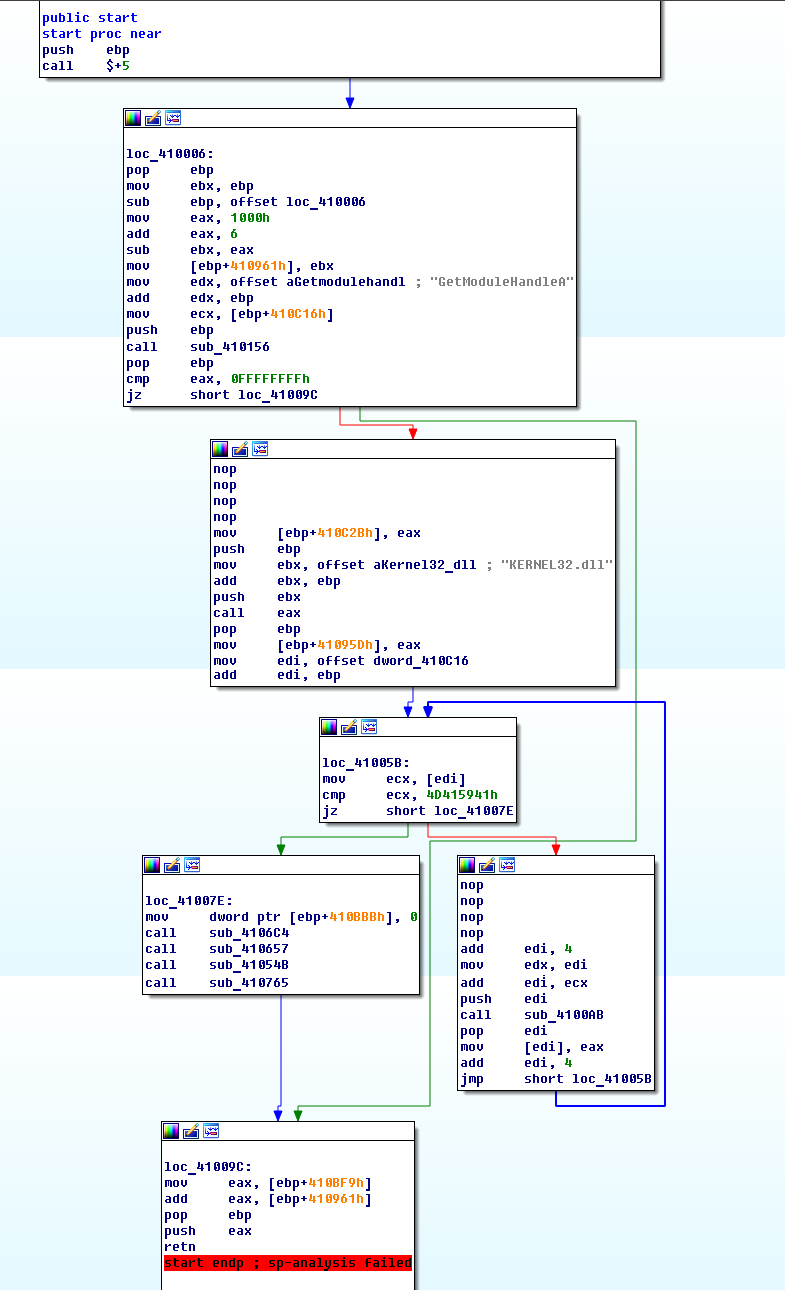


Рисунок 4 – Схема работы вируса

Далее переименовываем функции и переменные в соответствии с работой вируса.

Представленная на рисунке 5 функция «CopyAddressAndNameOfFunction» с помощью таблицы импорта находит адрес функции и имя и копирует в себя адреса и имена функций из библиотеки kernel32.dll. Она находит сигнатуру MZ-заголовка и от неё переходит к PE-заголовку. Затем идёт переход к таблице импорта и проверка имени на совпадение с kernel32.dll. Если имя не совпадает, то функция переходит к следующей таблице и повторяет проверку до тех пор, пока не найдёт kernel32.dll. После этого в таблице адресов идёт сравнение содержимого этой таблицы и перебор имен функции.

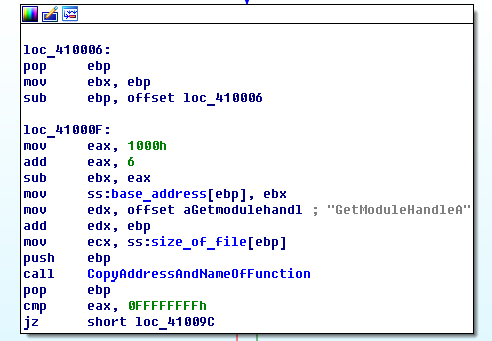


Рисунок 5 - Функция «CopyAddressAndNameOfFunction»

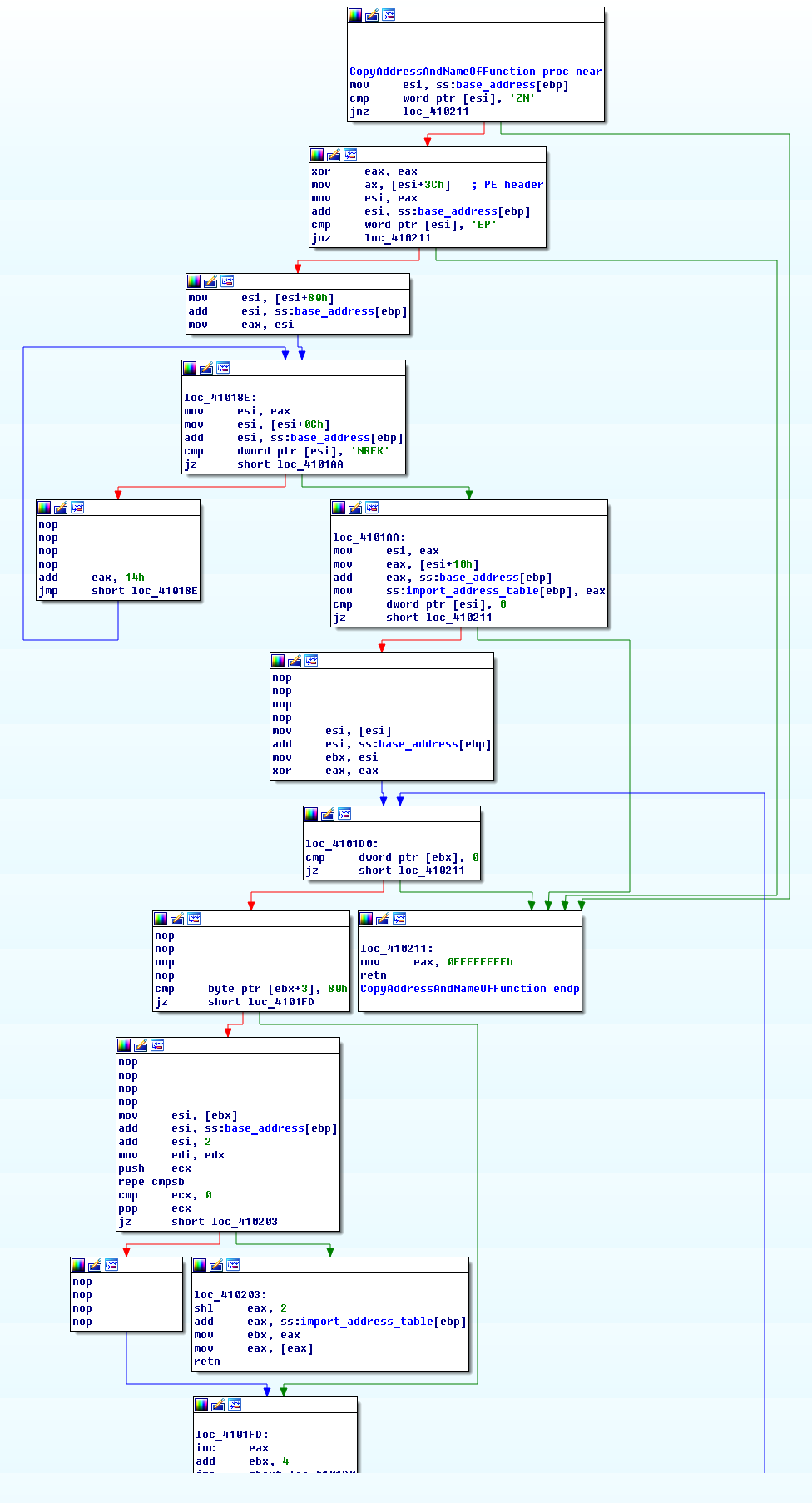


Рисунок 6 - Функция «CopyAddressAndNameOfFunction»

В блоке, представленном на рисунке 7, функция get\_module\_handle извлекает адрес экспортируемой функции из динамически подключаемой библиотеки Kernel32.dll.

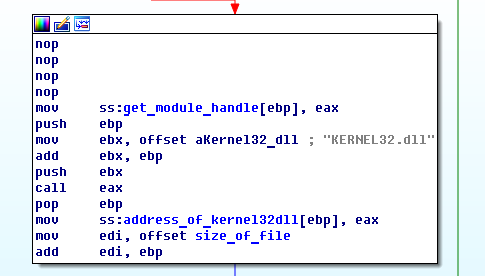
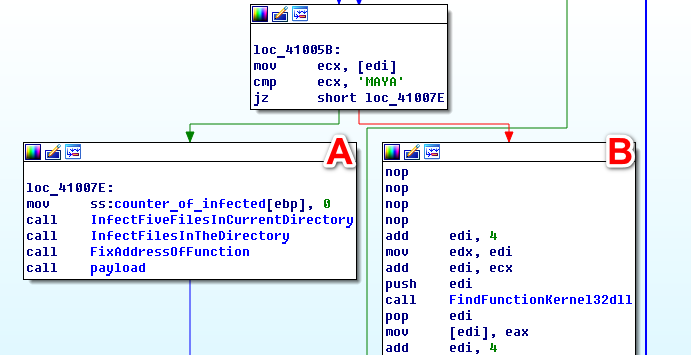


Рисунок 7

На следующем рисунке показано как происходит сравнение: если функция MAYA не найдена, то переходим в блок A, в противном случае выполняется переход в блок B.



В блоке B с помощью функции FindFunctionKernel32dll производится поиск адреса и имени функции с помощью таблицы импорта (поиск заражающей функции по имени). Шаг в 4 байта обеспечивает проход по всей таблице. Когда функция нашлась или таблица закончилась происходит выход из функции и возвращение к Блоку A для проверки.

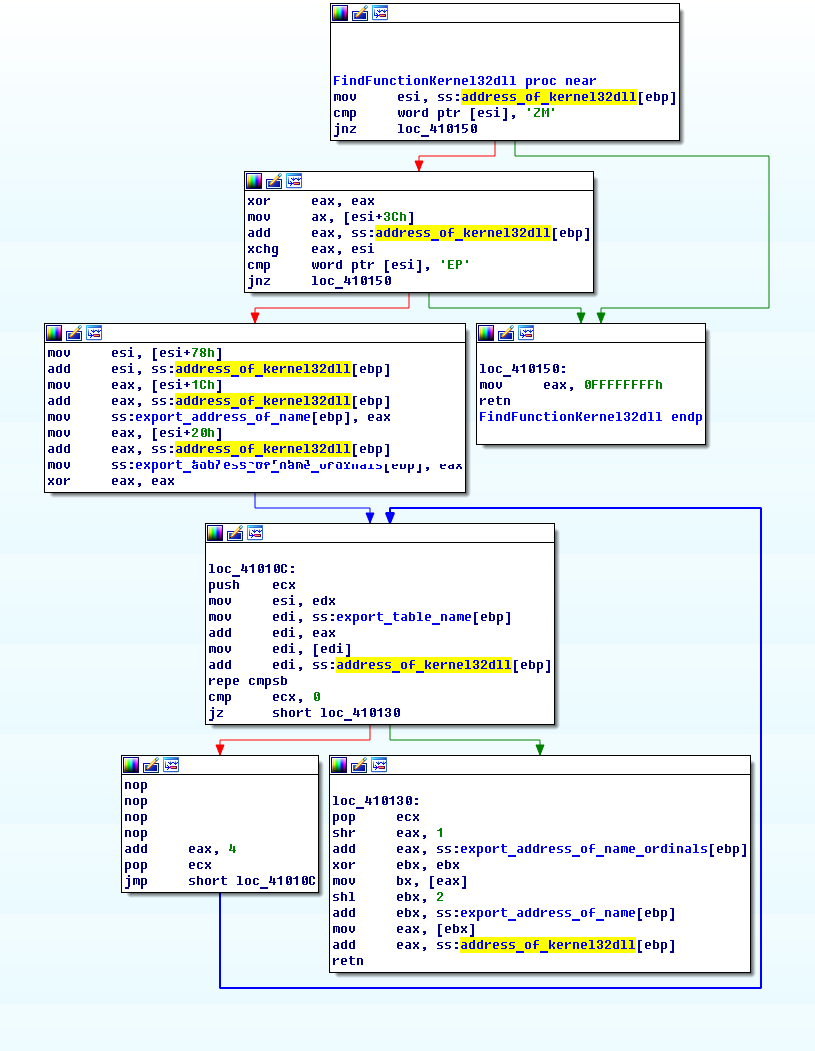


Рисунок 8 - Функция «FindFunctionKernel32dll»

В блоке А находятся основные действия вируса. Рассмотрим функции из этого блока.

Функция «InfectFiveFilesInCurrentDirectory» при помощи счетчика заражает 5 исполняемых файлов в текущей директории.

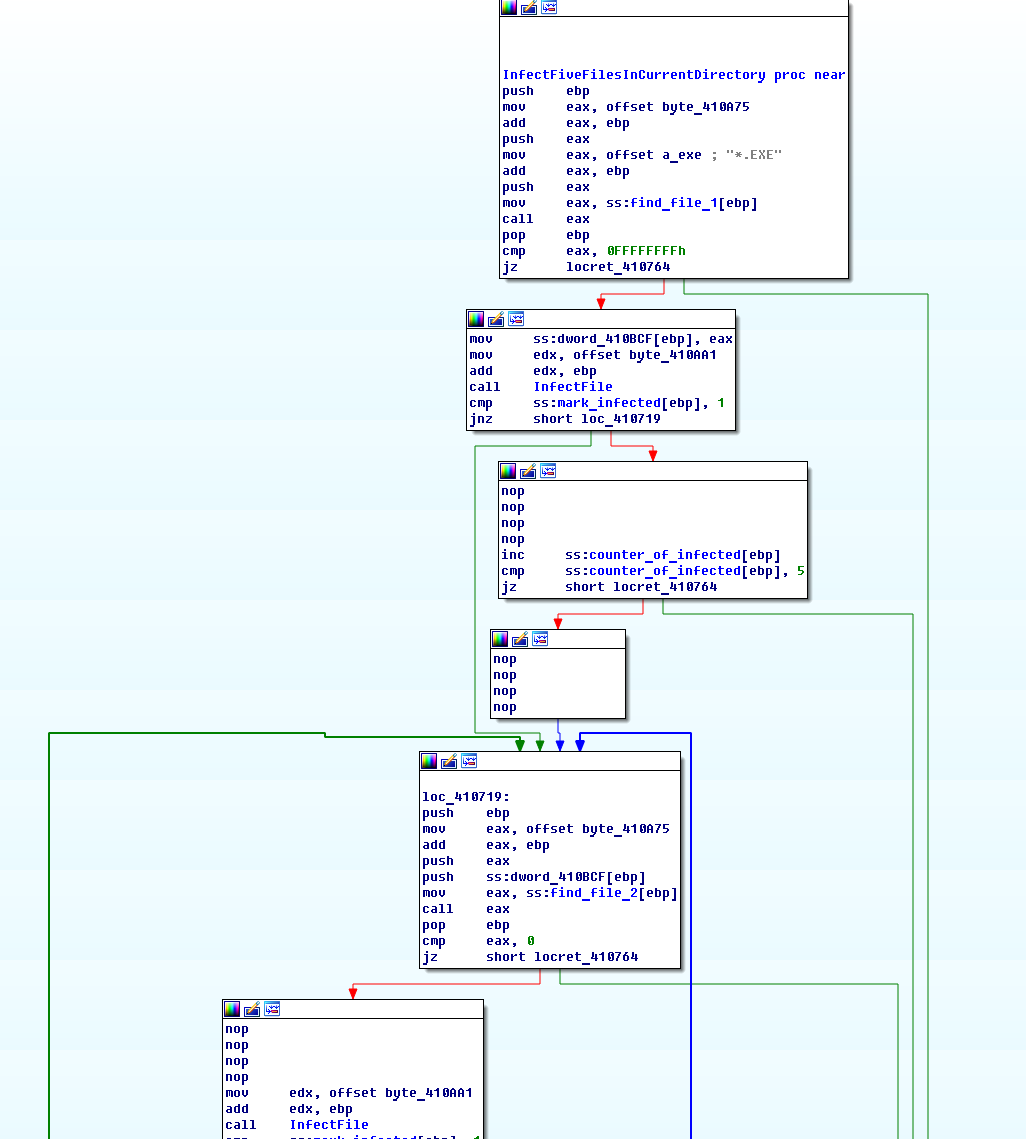


Рисунок 9 - Функция «InfectFiveFilesInCurrentDirectory»

В функции InfectFilesInTheDirectory, происходит заражение еще 5 (или дополнение до 5) файлов в текущей (или Windows) директории.

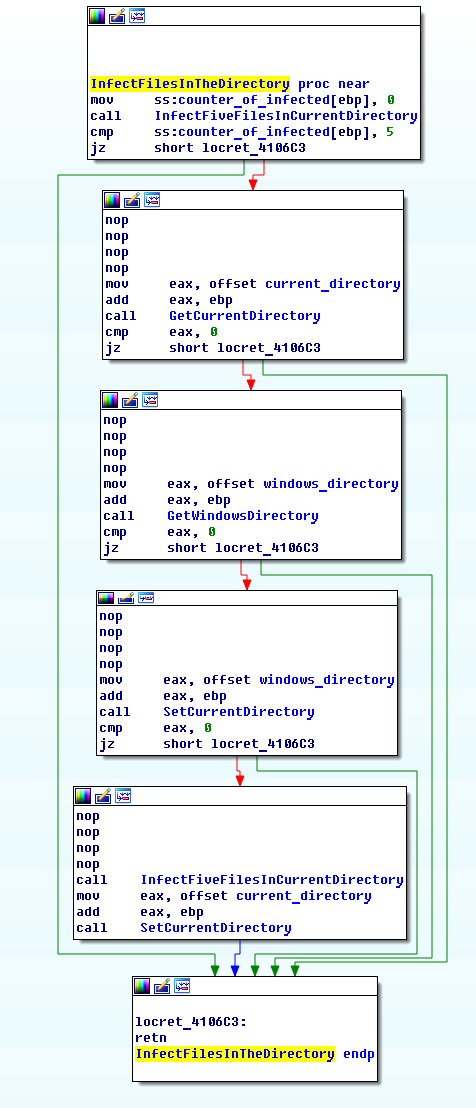


Рисунок 10 - Функция InfectFilesInTheDirectory

В функции «FixAddressOfFunction» восстанавливается таблица адресов функций и их имён.

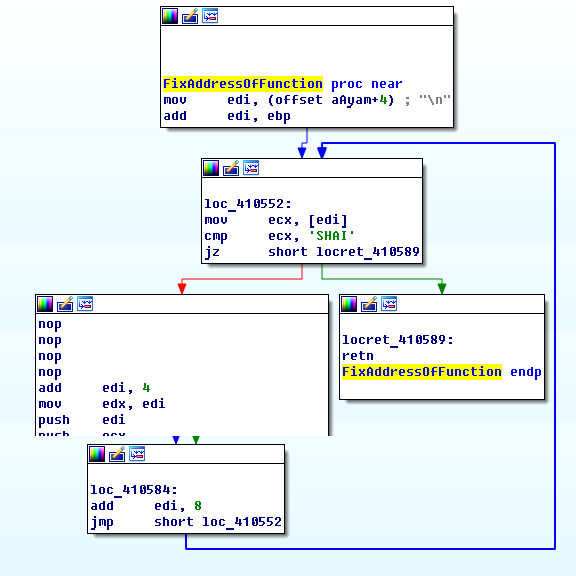


Рисунок 11 - Функция «FixAddressOfFunction»

В функции «Payload» идет переход к библиотекам USER32.dll и ADVAPI32.dll, с помощью функций которых происходит следующее: вирус проверяет системное время и по первым числам ежемесячно меняет "обои" экрана: заполняет экран текстом "SLAM". Затем вирус выводит окно сообщения: «Virus Alert! Win32.Maya (c) 1998 The Shaitan [SLAM]».

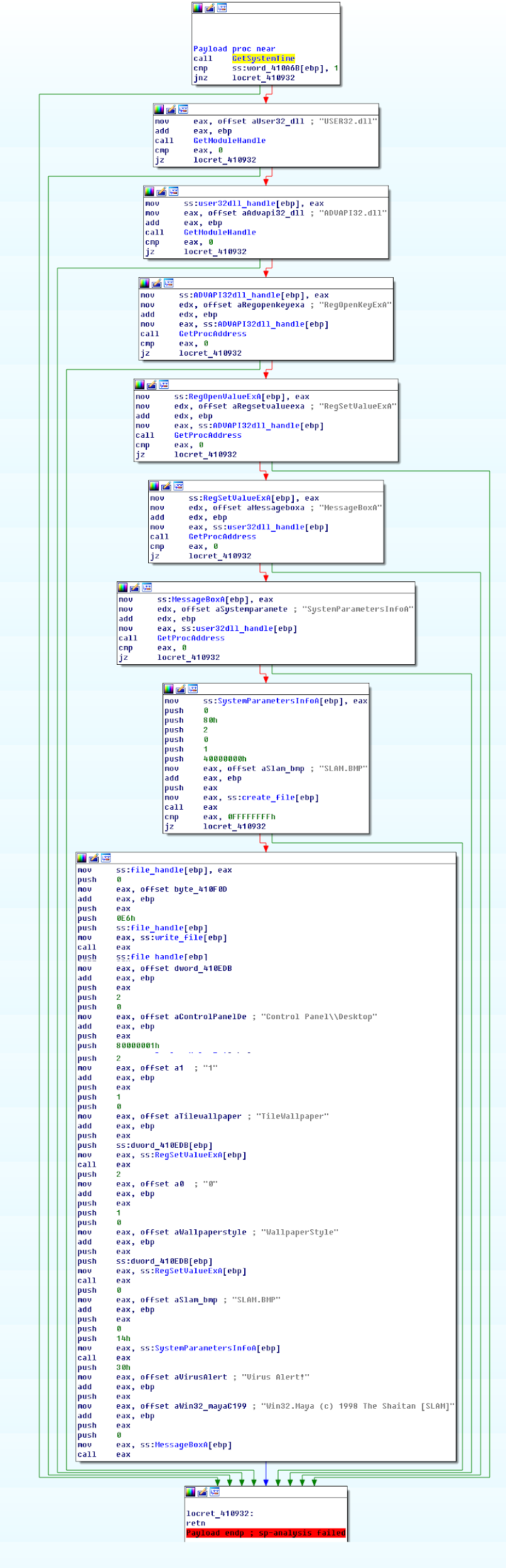
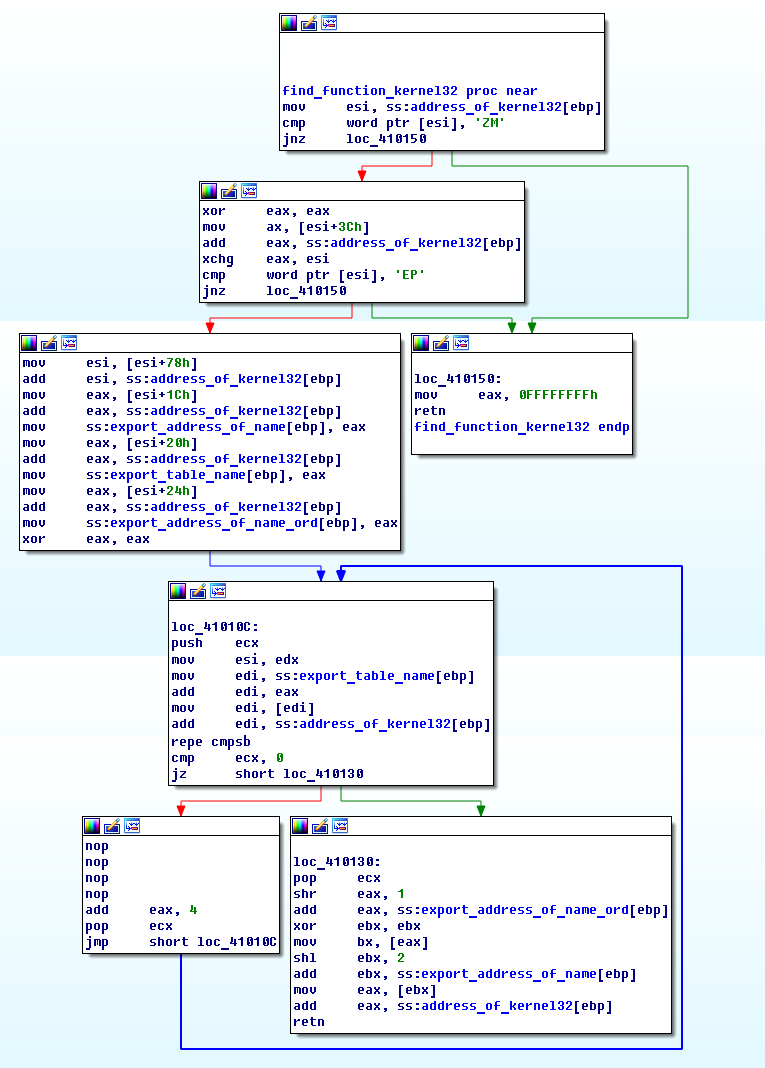


Рисунок 12 - Функция «Payload»



*Рисунок 13 Функция «find\_function\_kernel32»*

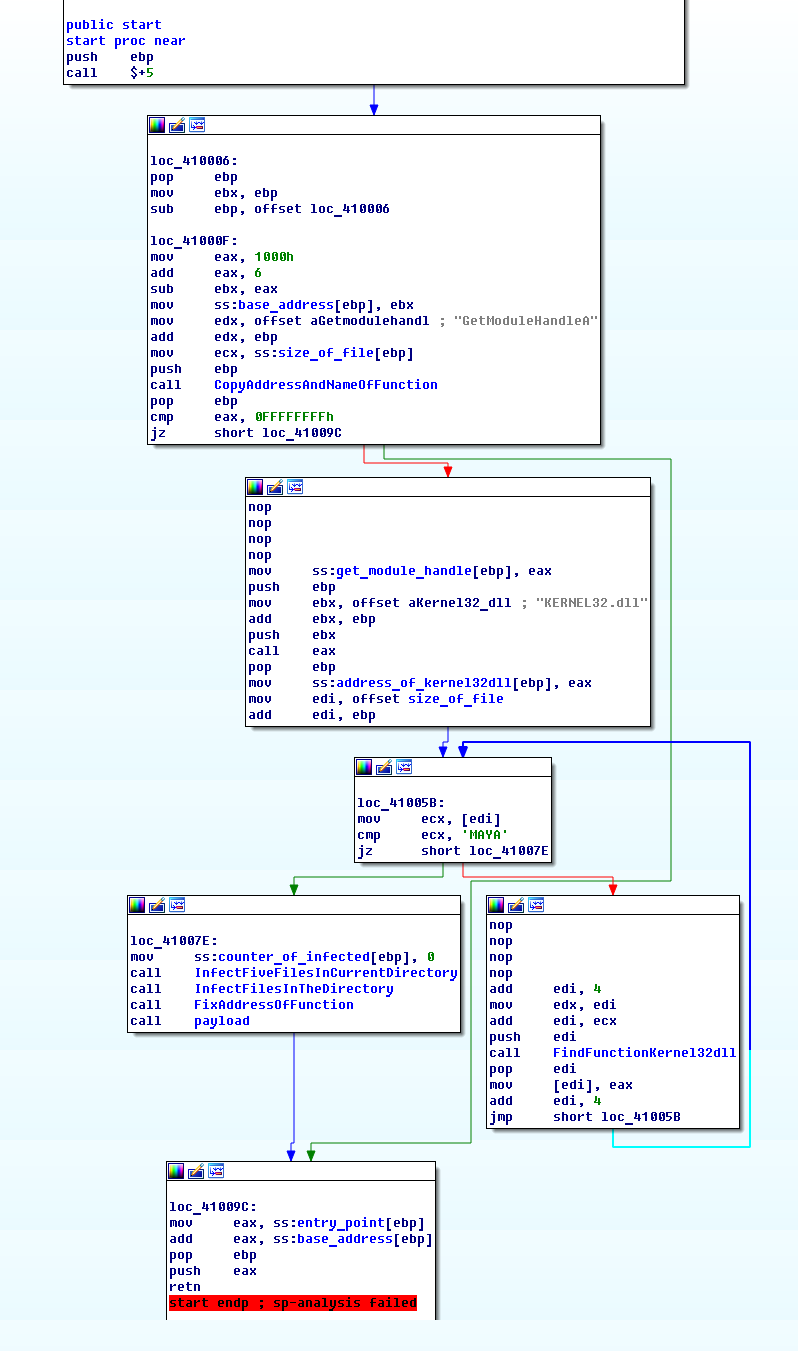


Рисунок 14 - Схема работы вируса с переименованными функциями и переменными