#### 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: Нгуен Кхань Ли– Студентка группы N3347A close-up of a signature  Description automatically generated

Преподаватель: Ханов Артур Рафаэльевич

Санкт-Петербург 2024

**СОДЕРЖАНИЕ**

[**ЗАДАНИЯ** 3](#_heading=h.gjdgxs)

[**ХОД РАБОТЫ** 4](#_heading=h.30j0zll)

1. [**Как вирус восстанавливает таблицу адресов импорта** 4](#_heading=h.1fob9te)
2. [**Как вирус заражает другие файлы** 6](#_heading=h.3znysh7)

[**3 Каков payload вируса** 7](#_heading=h.2et92p0)

[**ВЫВОД** 11](#_heading=h.tyjcwt)

# ЗАДАНИЯ

Разобрать вирус Win32.Maya.4114

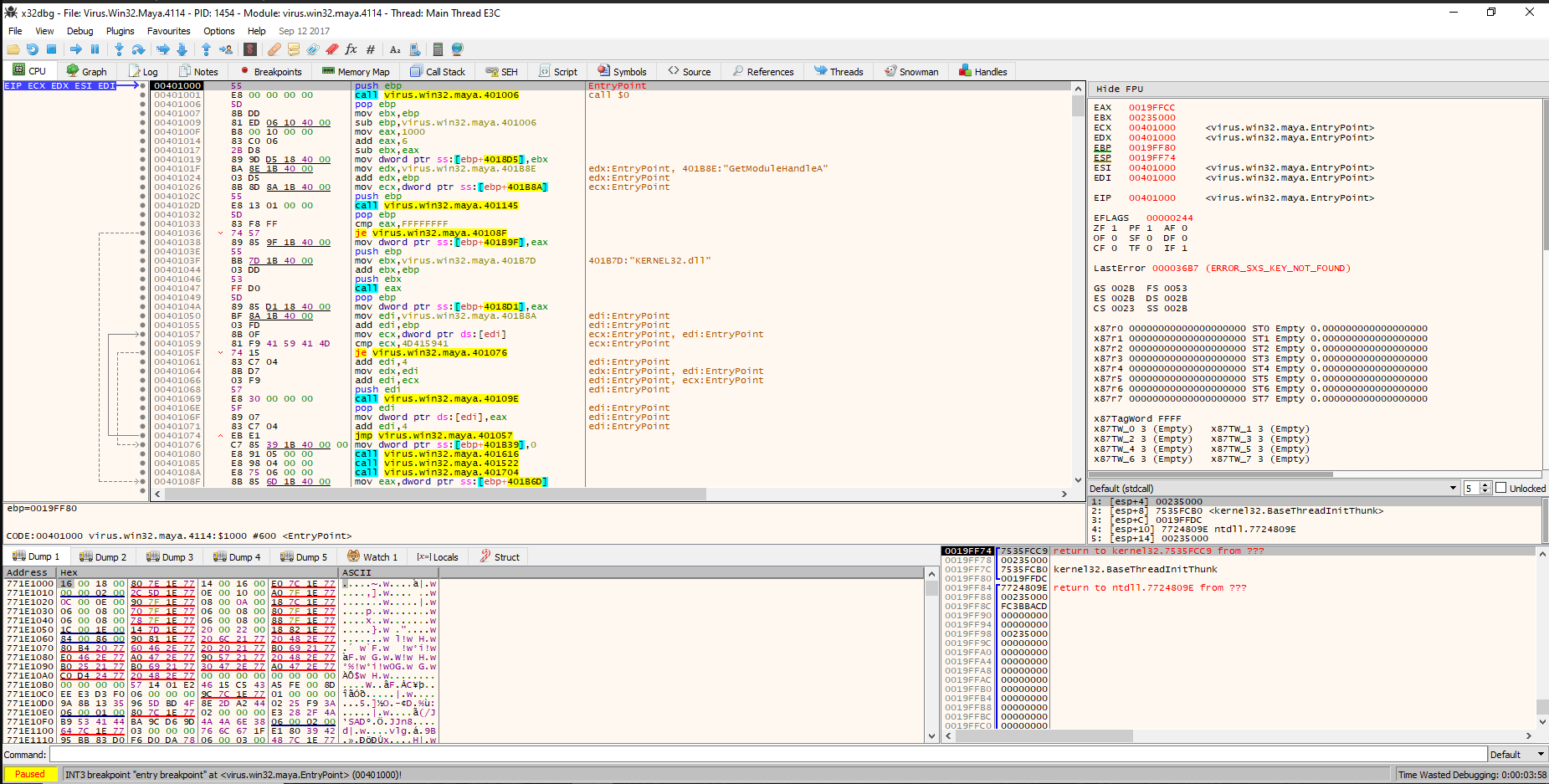
1. Как вирус восстанавливает таблицу адресов импорта
2. Как вирус заражает другие файлы
3. Каков payload вируса

# ХОД РАБОТЫ

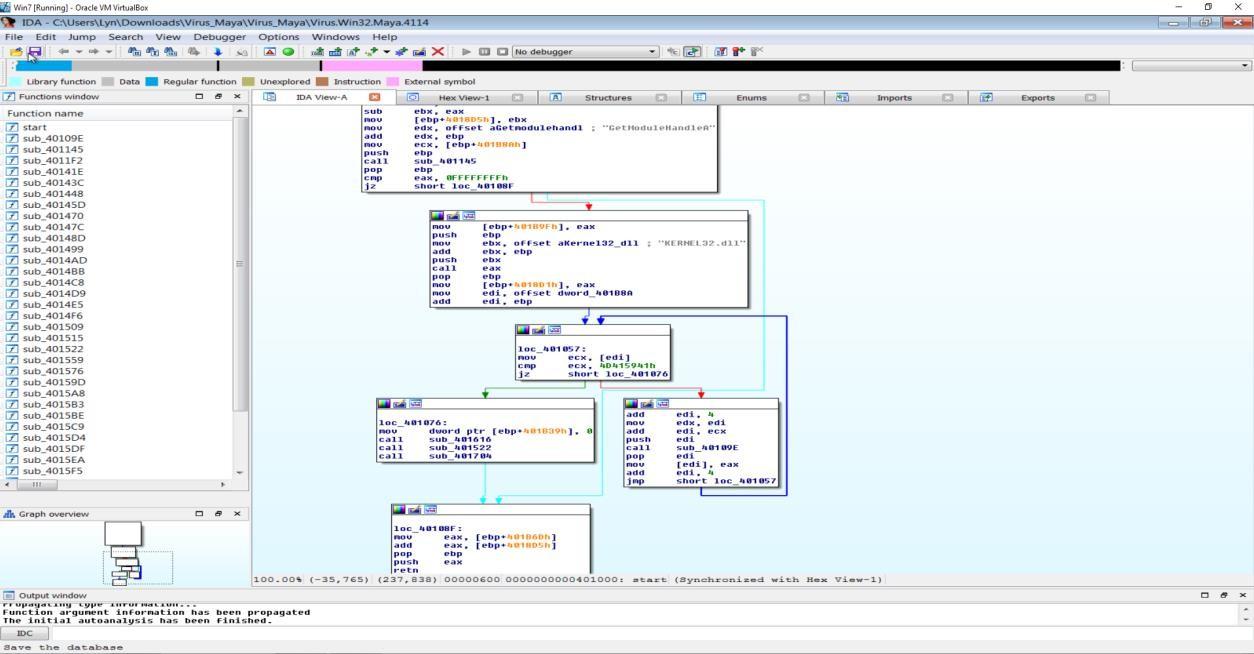
## Как вирус восстанавливает таблицу адресов импорта

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

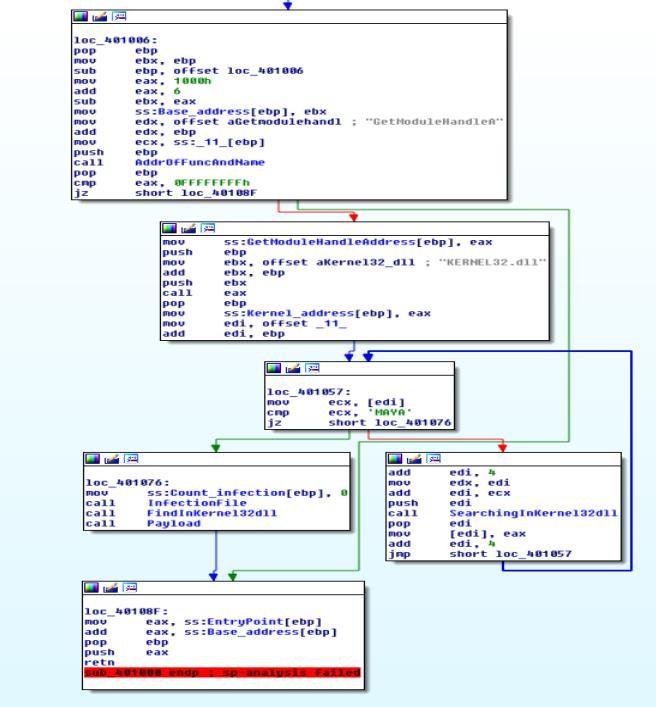
Запустим «Virus.Win32.Maya.4254» в отладчике x32dbg.



Загружаем образец в IDA (далее – программа с женщиной)



В программе с женщиной переименуем все call (названия функций берем из программы с паучком)

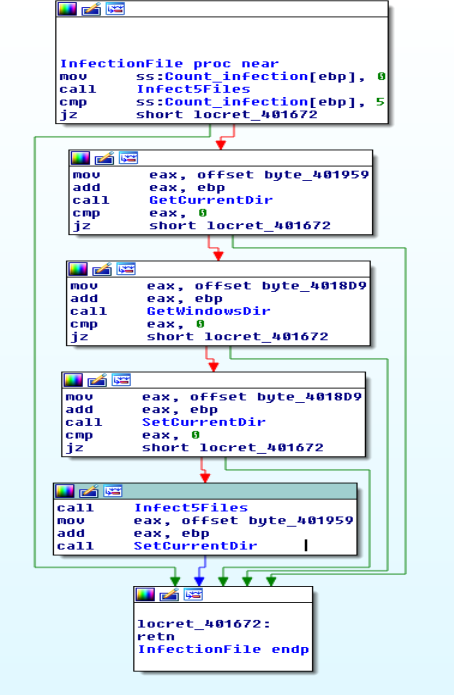


#### Алгоритм работа вируса:

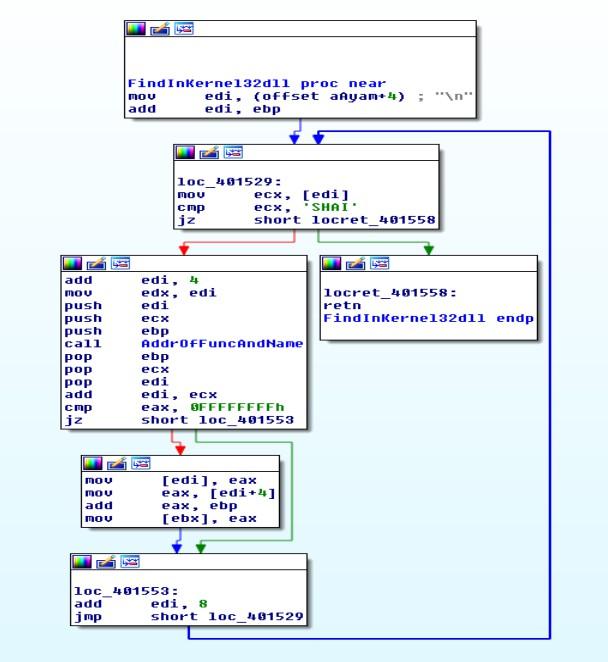
* 1. Узнает где находится Base\_address;
  2. При помощи функции AddrOfFuncAndName находит GetModuleHandle, через нее находит местонахождение остальных функций
  3. Вирус проходит по списку функций до того момента пока не найдет "MAYA".
  4. Вирус получает адреса функции при помощи SearchingInKernel32 (Находит нужные функции через экспорт kernel32).
  5. После осуществляется вызов функций InfectionFile, FindInKernel32dll, Payload
  6. Заражение происходит в функции InfectFile
  7. FindInKernel32dll производит восстановление таблицы адресов и имен так, чтобы зараженная программа могла обращаться к функциям из таблицы адресов.
  8. Payload – проверяет текущее время и дату, изменяет фон рабочего стола на SLAM.bmp каждое первое число, а также выводит окно с сообщением: “Virus Alert! Win32.Maya (c) 1998 The Shaitan [SLAM]”.

## Как вирус заражает другие файлы

Процесс заражения изображен на рисунке ниже:

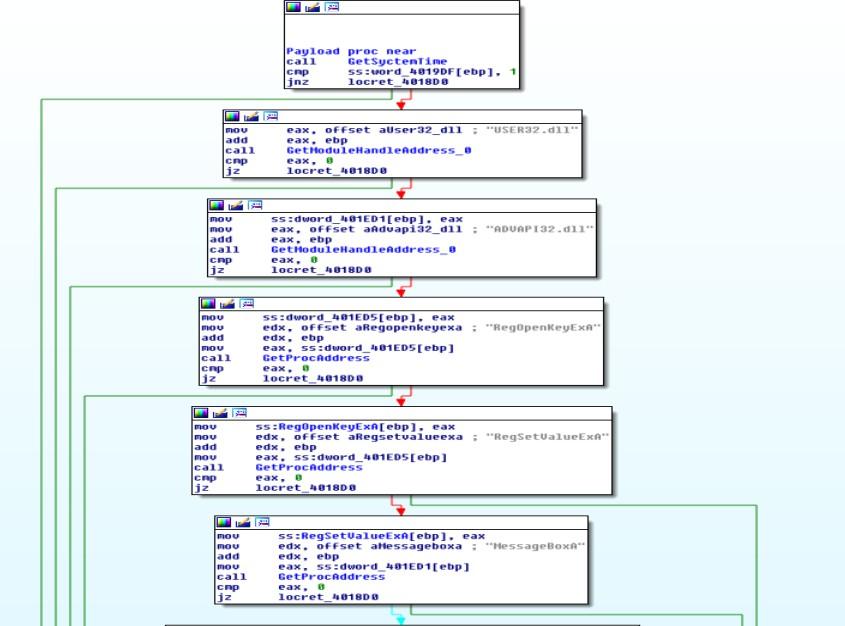


Восстановление таблицы адресов и имен изображено на рисунке ниже:



## 3 Каков payload вируса

Алгоритм работы Payload изображен на рисунке ниже:





# ВЫВОД

В этой лабораторной работе мы анализировали вирус Maya с помощью декомпилятора IDA и отладчика x32dbg.