#### Министерство науки и высшего образования Российской Федерации

федеральное государственное автономное образовательное учреждение высшего образования

### «НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО»

**Факультет безопасности информационных технологий**

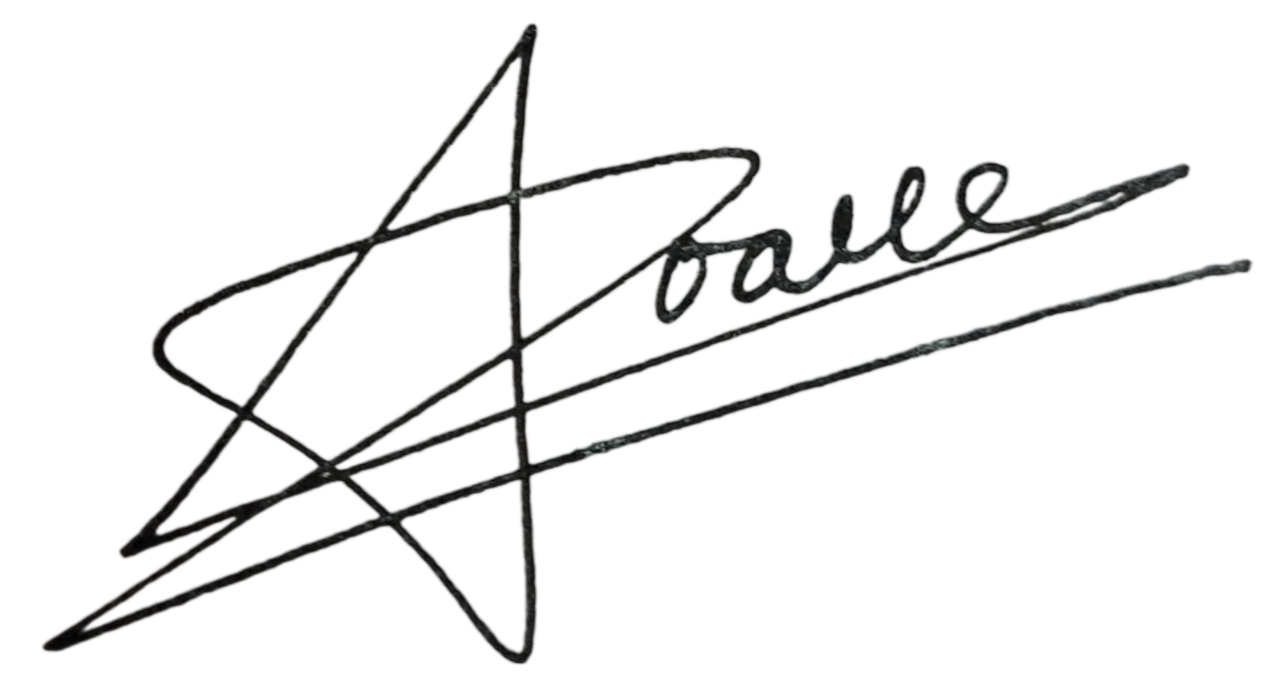
#### Дисциплина:

« Курс по ревёрс-инжинирингу»

### ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2

**Выполнил студент(ы):**

группа: N3347



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

*ФИО Подпись*

**Проверил:**

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

*ФИО Подпись*

Санкт-Петербург

2024 г.

Для выполнения лабораторной работы был выбран троян «554a804cd725c2094b2738f991faec6d».

Запустим троян 554a804cd725c2094b2738f991faec6d в отладчике x32dbg.

Установим breakpoints на функции:

* bp VirtualAllocEx;
* bp VirtualProtectEx;
* bp CreateProcessA;
* bp CreateProcessW;
* bp Process32First;
* bp ResumeThread;
* bp CreateRemoteThread;
* bp SetThreadContext;
* bp WriteFile;
* bp WriteProcessMemory;

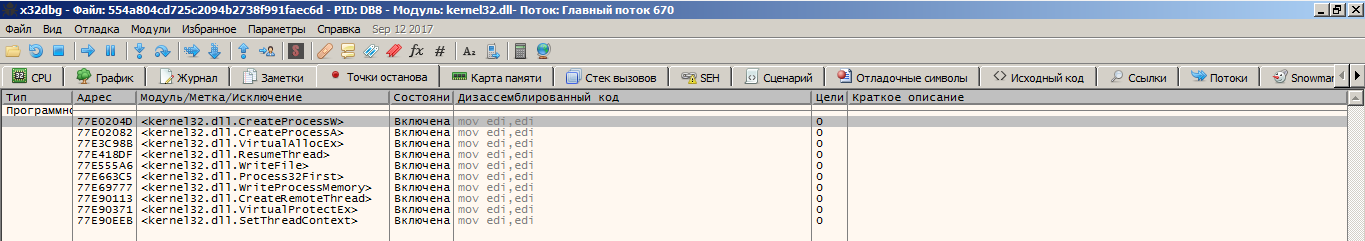


Рисунок 1 – Breakpoints

После установки шагаем с помощью кнопки F9 и смотрим какие функции использовал вирус (рисунок 2).

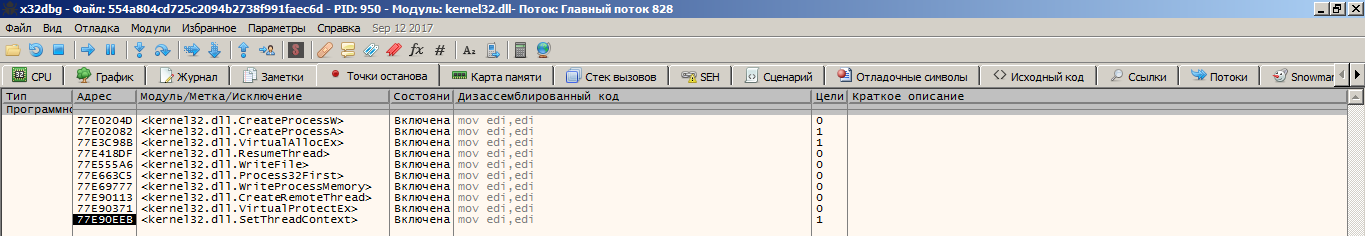


Рисунок 2 – Использованные функции

Вирус использовал следующие функции:

* CreateProcessA – Создает новый процесс и его основной поток. Новый процесс выполняется в контексте безопасности вызывающего процесса.
* VirtualAllocEx – Резервирует, фиксирует или изменяет состояние области памяти в виртуальном адресном пространстве указанного процесса.
* SetThreadContext – Устанавливает контекст для указанного потока.

Делаем вывод, что вирус создает новый процесс самого себя. Новый адрес этого процесса указан в регистре ecx (рисунок 3).

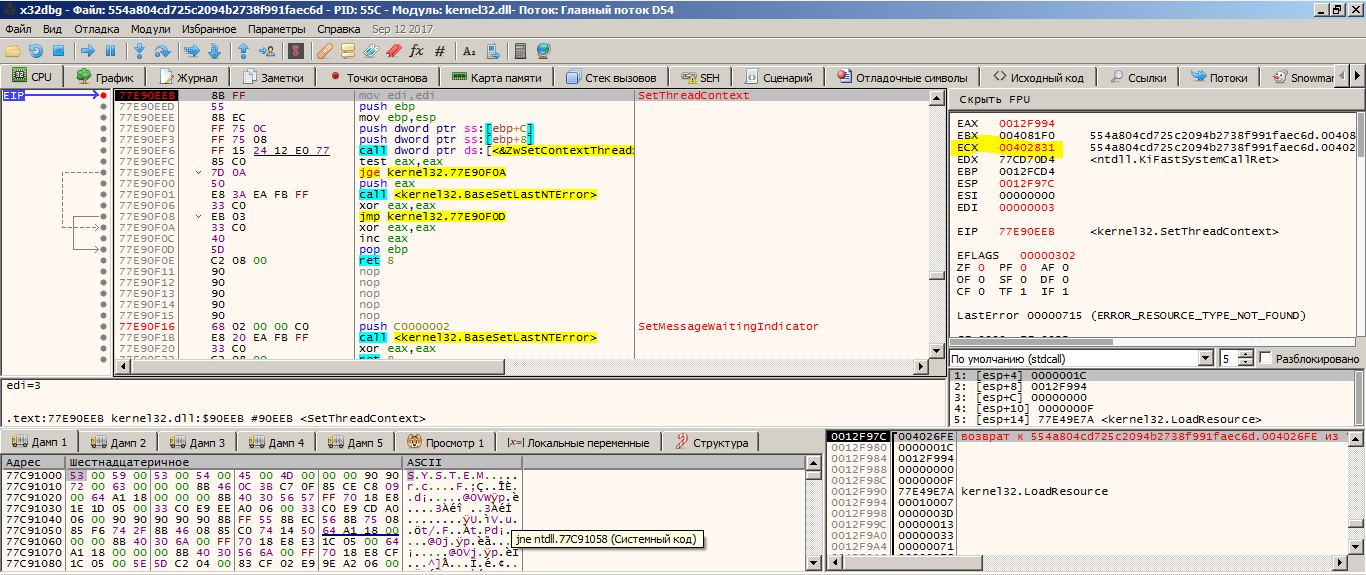


Рисунок 3 - Регистр ecx

Найдем адрес точки входа в новом процессе – 00402831 – и присоединяемся к нему.

Для этого откроем еще один отладчик x32dbg и присоединимся к новому процессу 554a804cd725c2094b2738f991faec6d.

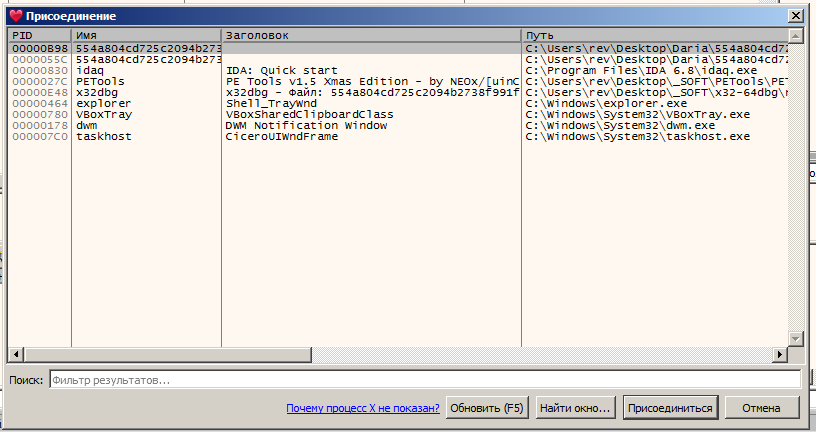


Рисунок 4 – Присоединение к новому процессу

Затем ищем адрес, который был указан в регистре ecx (рисунок 5).

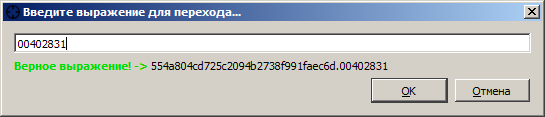


Рисунок 5 - Поиск адреса в новом процессе

И ставим в данном адресе breakpoint. Этот адрес новая точка входа вируса (рисунок 6).

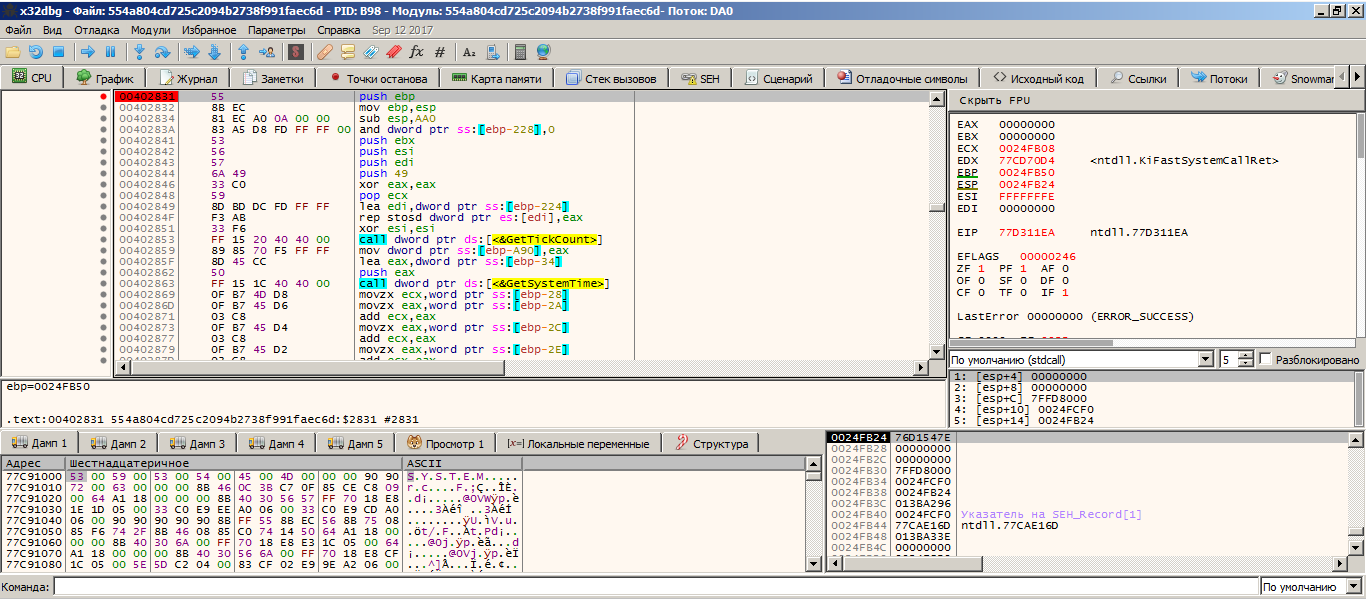


Рисунок 6 – Новая точка входа

Теперь кнопкой F9 завершаем работу вируса в первом отладчике, а затем переходим на breakpoint во втором отладчике.

В новом отладчике также смотрим какие функции использует новый процесс (рисунок 7 и 8).

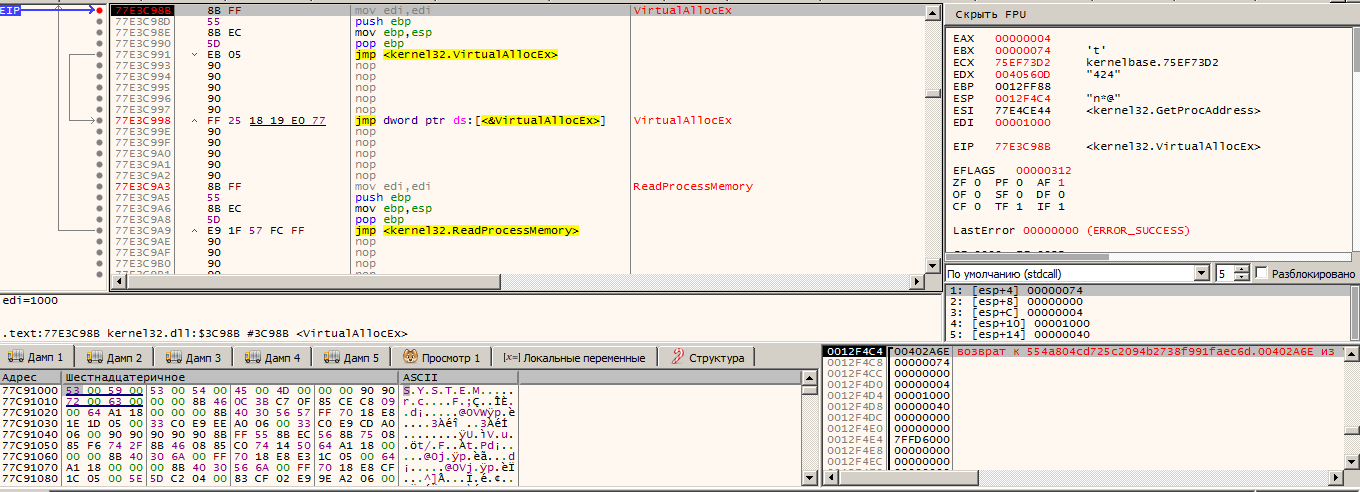


Рисунок 7 – Новый процесс в отладчике

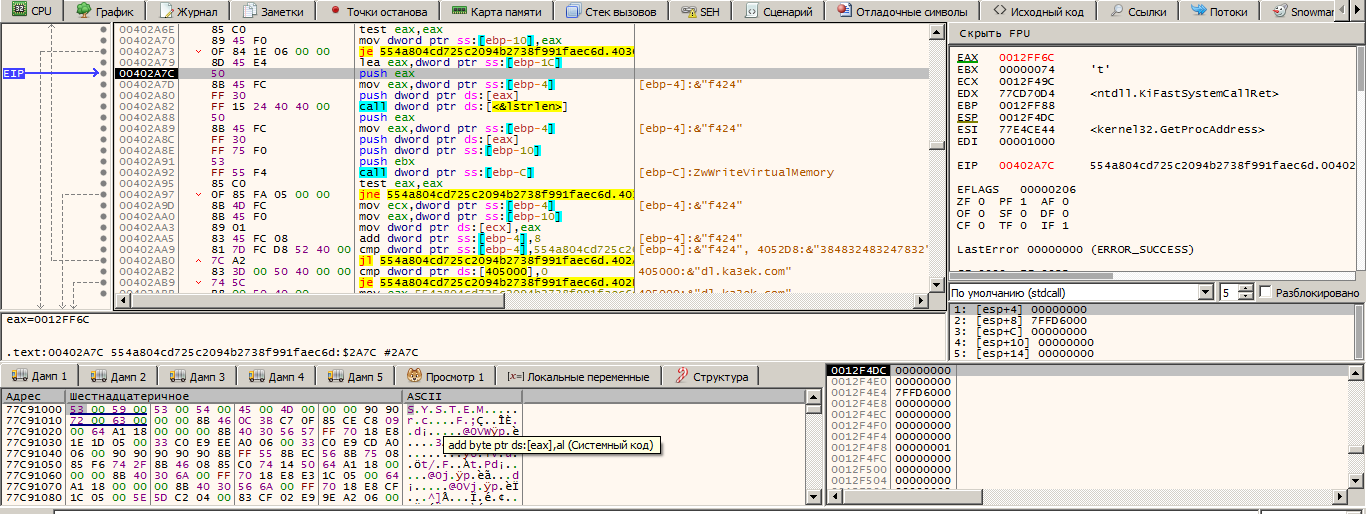


Рисунок 8 – Просмотр нового процесса в отладчике

Также использовались следующие функции (рисунок 9)

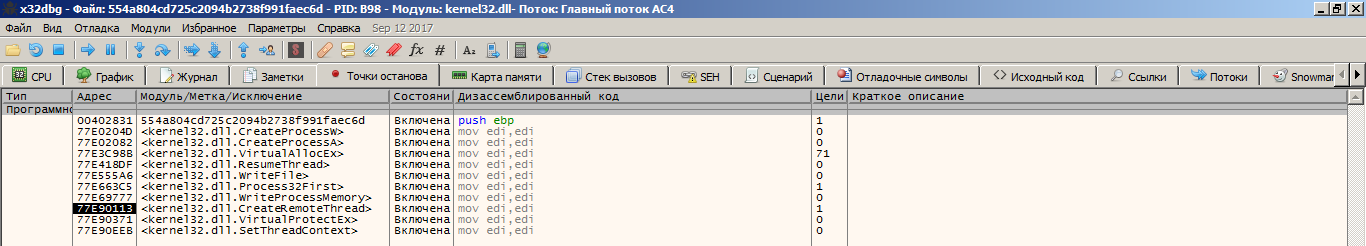


Рисунок 9 – Используемые функции

* VirtualAllocEx;
* CreateRemoteThread – Создает поток, который работает в виртуальном адресном пространстве другого процесса.

Делаем вывод, что далее вирус создает поток в процессе explorer.exe. в 4-ом параметре функции CreateRemoteThread указывается адрес, с которого вирус продолжит свою работу в процессе explorer.exe (рисунок 10).

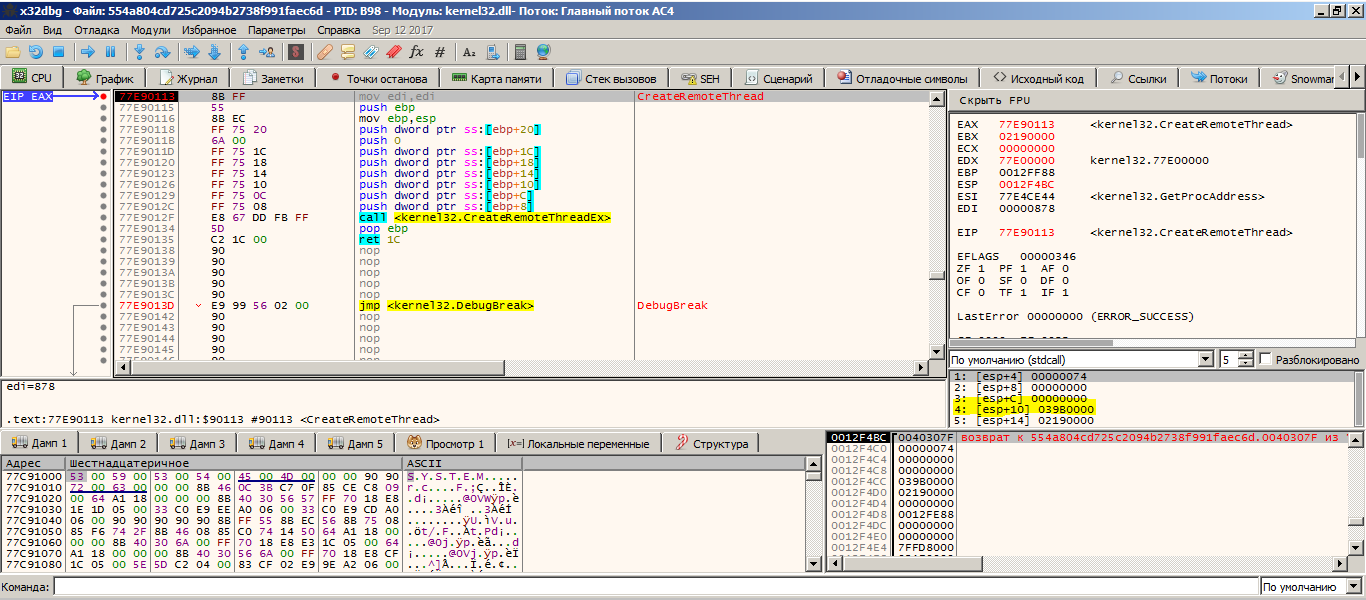


Рисунок 10 – 4 параметр функции CreateRemoteThread

Запускаем еще один отладчик и присоединяемся к процессу explorer.exe (рисунок 11).

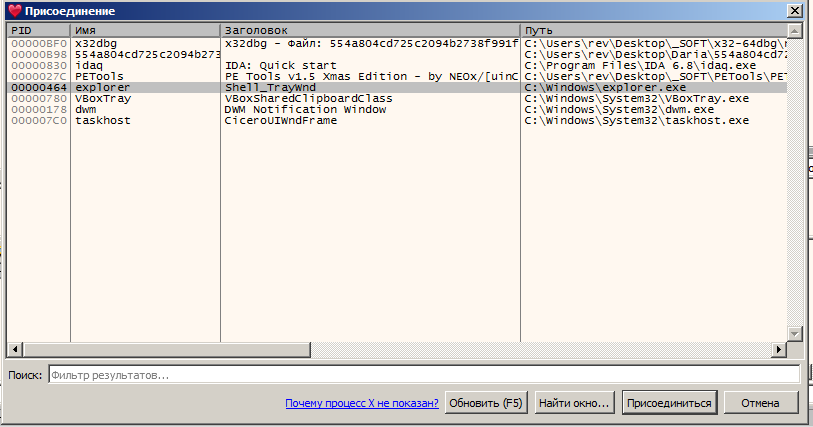


Рисунок 11 – Присоединение к explorer.exe

Находим адрес, который был указан в 4-ом параметре функции CreateRemoteThread (039B0000), и ставим на нем breakpoint (рисунок 12).

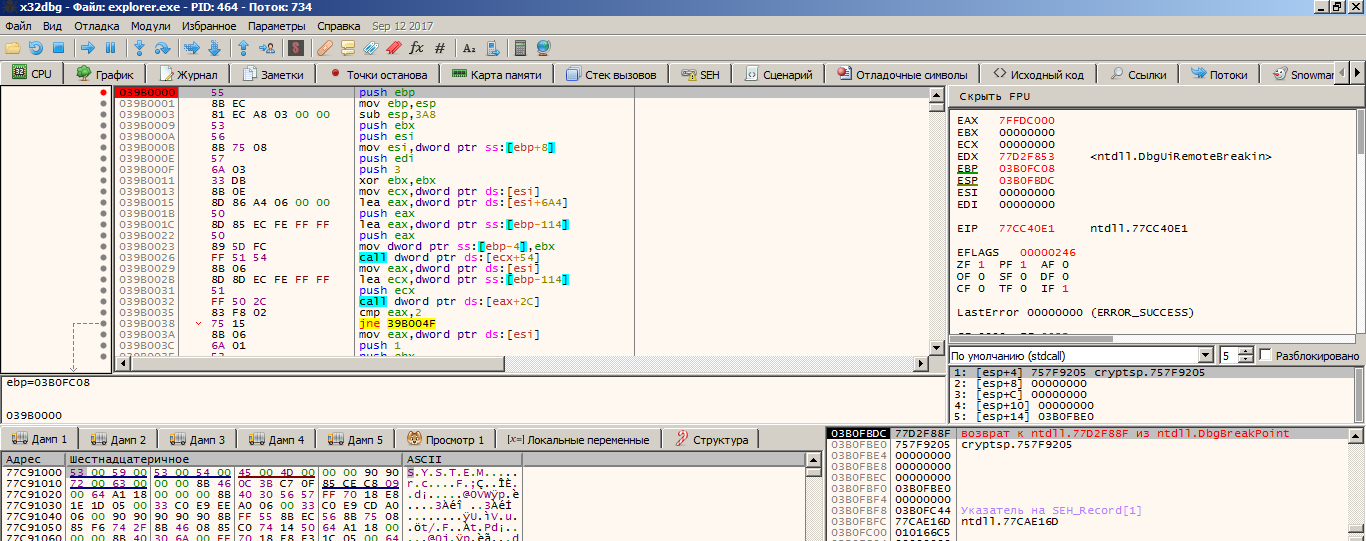


Рисунок 12 – Новая точка входа

Завершаем работу вируса во 2-ом отладчике и переходим на breakpoint в новом отладчике. Затем с помощью программы PE Tools снимаем дамп памяти, чтобы проанализировать работу вируса (рисунок 13).

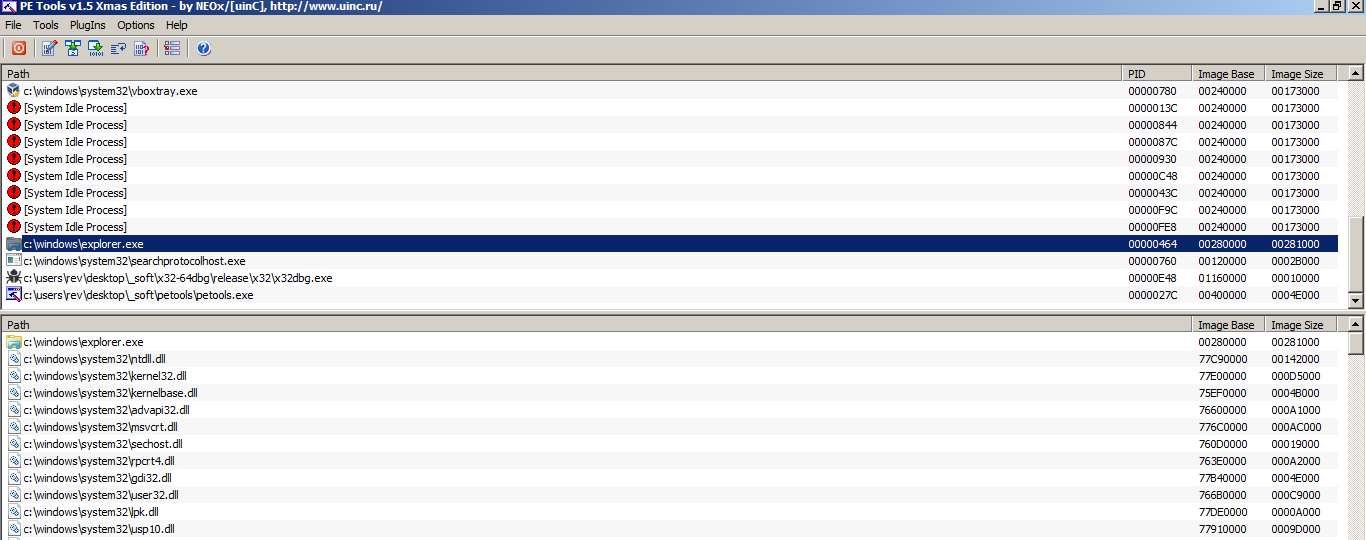


Рисунок 13 PE Tools

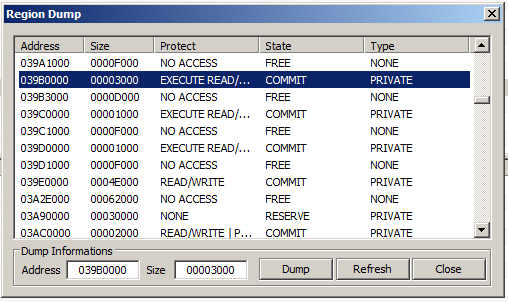


Рисунок 14 – Снятие дампа

Делаем dump region и дальше откроем дамп региона в IDA (рисунок 15), изменив значение loading\_offset на значение из названия дампа региона. Будем подписывать все вызываемые функции.

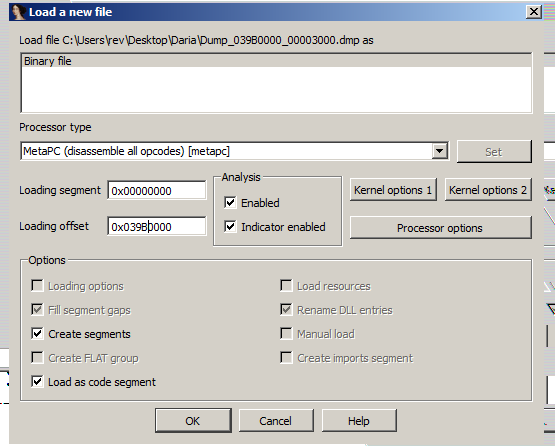


Рисунок 15 – Открытие дампа в IDA

В IDA перейдем к первому push и нажмем p. Это необходимо, чтобы начать интерпретировать команды как функции. После этого можно переходить в режим схемы нажатием пробела.

Сначала вирус использует следующие функции (рисунок 16 и 17):

* lstrcpynA – Копирует указанное количество символов из исходной строки в буфер.
* GetDriveTypeA – Определяет, является ли дисковод съемным, фиксированным, CD-ROM, RAM-диском или сетевым диском.
* CreateMutexA – Создает или открывает именованный или безымянный объект мьютекса.
* WaitForSingleObject – Ожидание, пока указанный объект не окажется в сигнальном состоянии или пока не истечет время ожидания.

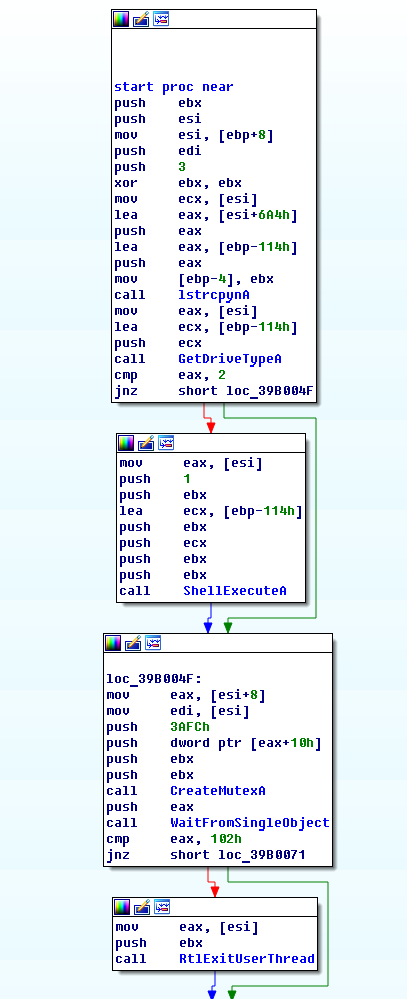


Рисунок 16 – Используемые функции

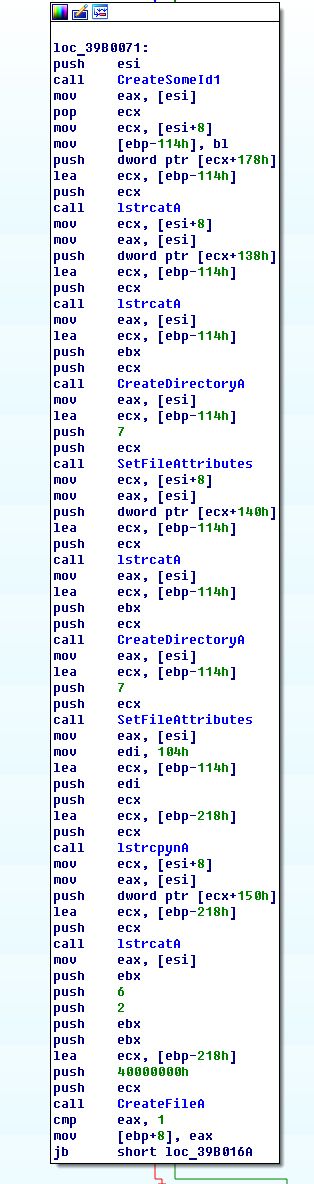


Рисунок 17 – Используемые функции при создании файлов

* lstrcatA – конкатенация строк.
* CreateDirectoryA – создание директории.
* SetFileAttrubitesA – установка атрибутов для директории. Видно, что создается 2 файла с атрибутом 7 в C:\\RECYCLER\\R-1-5-... .
* CreateFileA – создание или открытие файла.

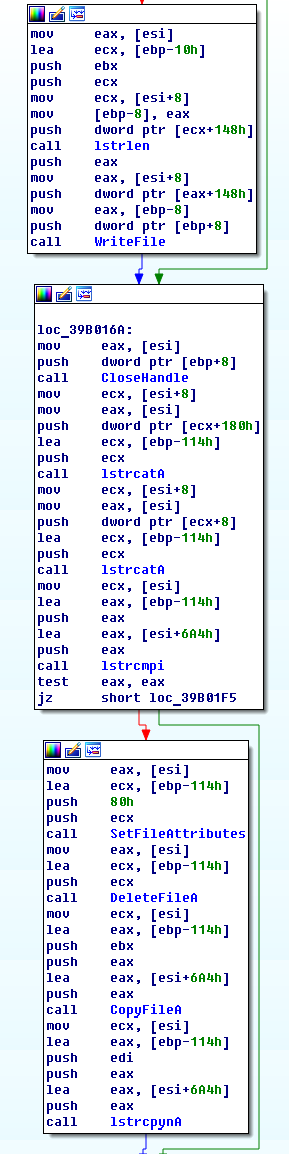


Рисунок 18 – Создание файлов

* Lstrlen – возвращает длину указанной строки в байтах.
* WriteFile – запись данных в файл.
* Lstrcmpi – осуществляет лексикографическую проверку двух строк.
* DeleteFileA – удаление файла.
* CopyFileA – копирование файла

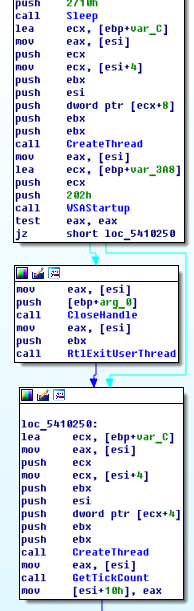


Рисунок 19 – Создание потока

* Sleep – приостановление выполнения текущего потока.
* CreateThread – создание потока.
* WSAStartup – инициирует использование Winsock DLL.
* GetTickCount – извлекает число миллисекунд, которые истекли, с тех пор как система была запущена.

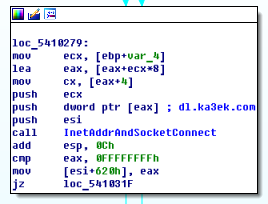


Рисунок 20 – функция установки соединения

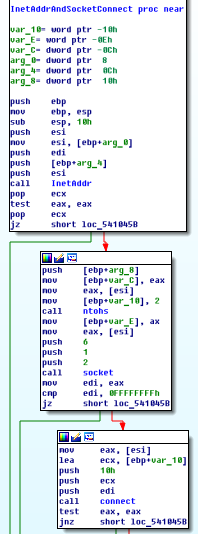


Рисунок 21 – тело функции InetAddrAndSocketConnect

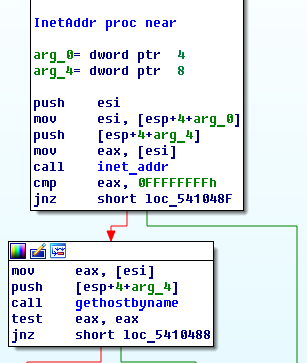


Рисунок 22 – тело функции InetAddr

Происходит обращение к dl.ka3ek.com. используются следующие функции:

* Inet\_addr – формирование адреса.
* Gethostbyname – получение IP по DNS.
* Socket – определение сокета (порт 3321).
* Connect – соединение.

Дальнейшее изучение требует внедрение механизма перебора и создания ответа от сервера, т.к. вирус зацикливает сам себя и без данных полученных с сервера невозможно выполнить дальнейшие действия. Сам explorer.exe продолжает работу.