

11.01.2024

Курс:

Практическая работа к уроку № Lesson_8

--

Антиотладочные приемы

Задание:

Дана программа task-5. Необходимо получить ключ для вашего имени, который успешно примет программа.

Пример запуска программы:

task-5.exe

```
Name: <your name>
License Key: <license key>
```

Антиотладочный прием – это способ обнаружения того, что программа выполняется под управлением отладчика. Основной целью является замедление или предотвращение процесса реверс - инжиниринга.

Запускаем в CMD *task-5.exe*

Insert name: Andrew

License key: aaaabbbbccccdddd

```
C:\Users\Администратор\Documents\GB>task-5.exe
Insert your name: Andrew
Insert key: qwerty
ERROR. Your key is incorrect.
```

License key: **aaaabbbbccccdddd**

Запускаем *task-5.exe* под отладчиком в OllyDbg

OllyDbg - task-5.exe - [CPU - main thread, module task-5]

File View Debug Plugins Options Window Help

LEMTWHC / KBR... S

```

00401000 55 PUSH EBP
00401001 8BEC MOV EBP,ESP
00401003 83EC SUB ESP,8
00401006 C745 F8 000000 MOV DWORD PTR SS:[EBP-8],0
0040100D C745 FC 000000 MOV DWORD PTR SS:[EBP-4],0
00401014 EB 09 JMP SHORT task-5.0040101F
00401016 8B45 FC MOV EAX,DWORD PTR SS:[EBP-4]
00401019 83C0 02 ADD EAX,2
0040101C 0FBE 02 MOV SX EAX, BYTE PTR DS:[EDX]
0040101F 8B4D 08 MOV ECX,DWORD PTR SS:[EBP+8]
00401022 51 PUSH ECX
00401023 E8 A8810000 CALL task-5.00409100
00401028 83C4 04 ADD ESP,4
0040102B 3945 FC CMP DWORD PTR SS:[EBP-4],EAX
0040102E 77 11 JA SHORT task-5.00401041
00401030 8B55 08 MOV EDX,DWORD PTR SS:[EBP+8]
00401033 8355 FC ADD EDX,DWORD PTR SS:[EBP-4]
00401036 0FB6 02 MOV SX EAX, BYTE PTR DS:[EDX]
00401039 8345 F8 ADD EAX,DWORD PTR SS:[EBP-8]
0040103C 8945 F8 MOV DWORD PTR SS:[EBP-8],EAX
0040103F EB D5 JMP SHORT task-5.00401016
00401041 8B45 F8 MOV EAX,DWORD PTR SS:[EBP-8]
00401044 8BEC MOV EBP,ESP
00401046 5D POP EBP
00401047 C3 RETN
00401048 CC INT3
00401049 CC INT3
0040104A CC INT3
0040104B CC INT3
0040104C CC INT3
0040104D CC INT3
0040104E CC INT3
0040104F CC INT3
00401050 55 PUSH EBP
00401051 8BEC MOV EBP,ESP
00401053 91EC 90000000 SUB ESP,90
00401059 56 PUSH ESI
0040105A FF15 00704100 CALL DWORD PTR DS:[<&KERNEL32.IsDebuggerPresent]
00401060 8945 F8 MOV DWORD PTR SS:[EBP-8],EAX
00401063 837D F8 00 CMP DWORD PTR SS:[EBP-8],0
00401066 74 14 JE SHORT task-5.0040107D
00401069 68 00E04100 PUSH task-5.0041E000
0040106E E8 AD010000 CALL task-5.00401220
00401073 83C4 04 ADD ESP,4
00401789 task-5.00401789

```

Registers (FPU)

EAX 0019FFC0 task-5.<ModuleEntryPoint>
ECX 004014E1 task-5.<ModuleEntryPoint>
EDX 004014E1 task-5.<ModuleEntryPoint>
EBX 003C8000
ESP 0019FF74
EBP 0019FF80
ESI 004014E1 task-5.<ModuleEntryPoint>
EDI 004014E1 task-5.<ModuleEntryPoint>
EIP 004014E1 task-5.<ModuleEntryPoint>

C 0 ES 002B 32bit 0(FFFFFFFF)
P 1 CS 0023 32bit 0(FFFFFFFF)
A 0 SS 002B 32bit 0(FFFFFFFF)
Z 1 DS 002B 32bit 0(FFFFFFFF)
S 0 FS 0053 32bit 3CB000(FFF)
T 0 GS 002B 32bit 0(FFFFFFFF)
D 0
O 0
LastErr ERROR_SEM_NOT_FOUND (000000B8)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty 0.0
ST1 empty 0.0
ST2 empty 0.0
ST3 empty 0.0
ST4 empty 0.0
ST5 empty 0.0
ST6 empty 0.0
ST7 empty 0.0

FST 0000 Cond 0 0 0 0 Err 0 0 0 0 0 0 0 0 (GT)
FCW 027F Prec NEAR,S3 Mask 1 1 1 1 1 1

0019FF74 76190419 RETURN to KERNEL32.76190419
0019FF78 003C8000
0019FF7C 76190400 KERNEL32.BaseThreadInitThunk
0019FF80 0019FFDC
0019FF84 76ED662D RETURN to ntdll.76ED662D
0019FF88 003C8000
0019FF8C 1FF950B

Address Hex dump ASCII

0041E000 0A 44 65 62 75 67 67 65 72 20 68 61 73 20 62 65 .Debugger has be
0041E010 65 64 65 74 65 63 74 65 64 21 0A 00 00 00 en detected....
0041E020 0A 49 6E 73 65 72 74 20 79 6F 75 72 20 6E 61 6D .Insert your nam
0041E030 65 3A 20 00 25 73 00 00 0A 49 6E 73 65 72 74 20 e: .%s...Insert
0041E040 68 65 79 3A 20 00 00 00 25 73 00 00 0A 45 52 52 key: ...%s...ERR
0041E050 4F 5F 2F 20 63 6F 7E 73 73 2A 68 65 74 20 68 65 Your key is

Окно Memory

OllyDbg - task-5.exe - [Memory map]

File View Debug Plugins Options Window

LEMTWHC / KBR... S

Address	Size	Owner	Section	Contains	Type	Access	Initial	Mapped as
00010000	00010000				Map	Rw	Rw	
00040000	0001A000				Map	R	R	
00095000	0000B000				Priv	Rw	Guar	Rw
0019B000	00002000			stack of ma	Priv	Rw	Guar	Rw
0019D000	00003000				Priv	Rw	Guar	Rw
001A0000	00004000				Map	R	R	
001B0000	00002000				Priv	Rw	Rw	
003C7000	00004000				Priv	Rw	Rw	
003CB000	00001000			data block	Priv	Rw	Rw	
00400000	00001000	task-5		PE header	Image	R	RWE	
00401000	00016000	task-5	.text	code	Image	R	RWE	
00417000	00007000	task-5	.rdata	imports	Image	R	RWE	
0041E000	00002000	task-5	.data	data	Image	R	RWE	
00420000	00005000				Map	R	R	\Device\HarddiskVolume2\Windows\System32\locale.nls
00540000	00006000				Priv	Rw	Rw	
00700000	00005000				Priv	Rw	Rw	
748A0000	00001000	KERNELBA		PE header	Image	R	RWE	
748A1000	001C3000	KERNELBA	.text	code,export	Image	R	RWE	
74A64000	00004000	KERNELBA	.data	data	Image	R	RWE	
74A65000	00003000	KERNELBA	.idata	imports	Image	R	RWE	

Секция кода находится по адресу 00401000

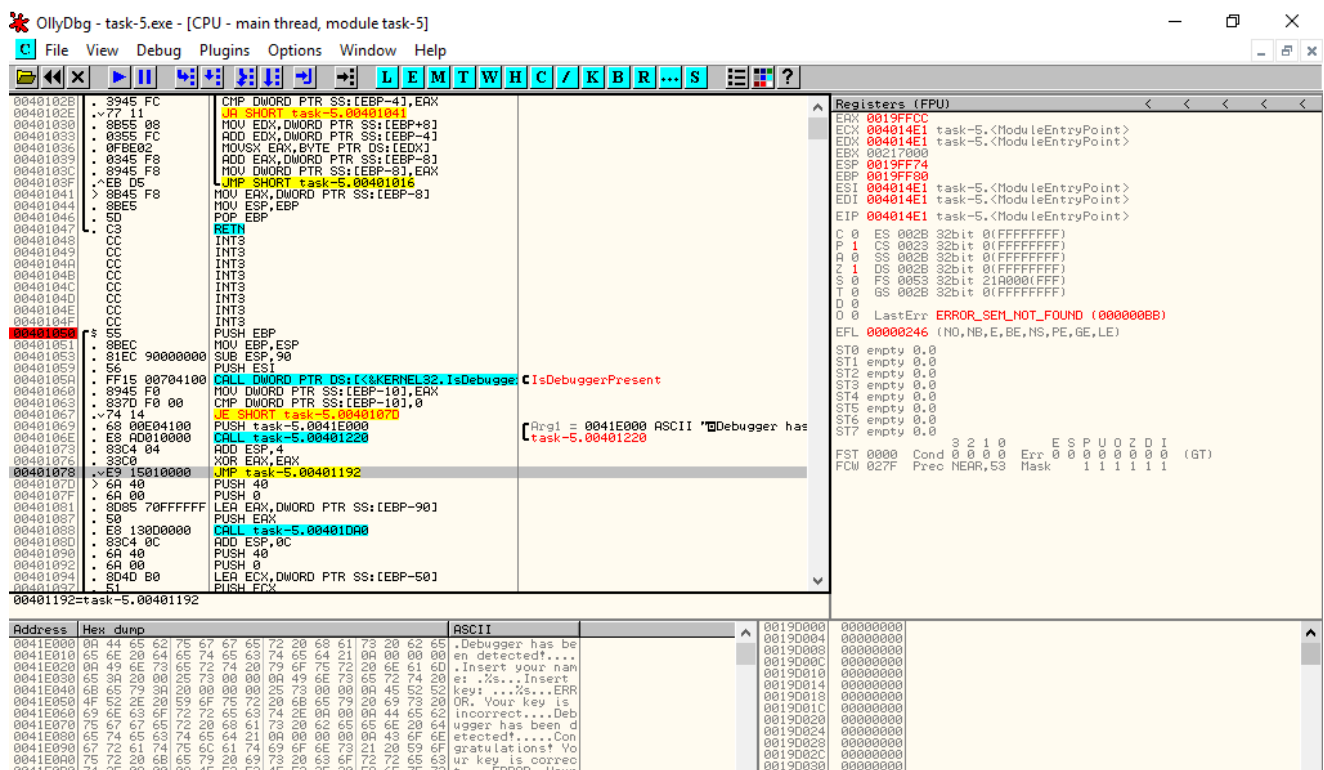
Переходим по этому адресу (C)

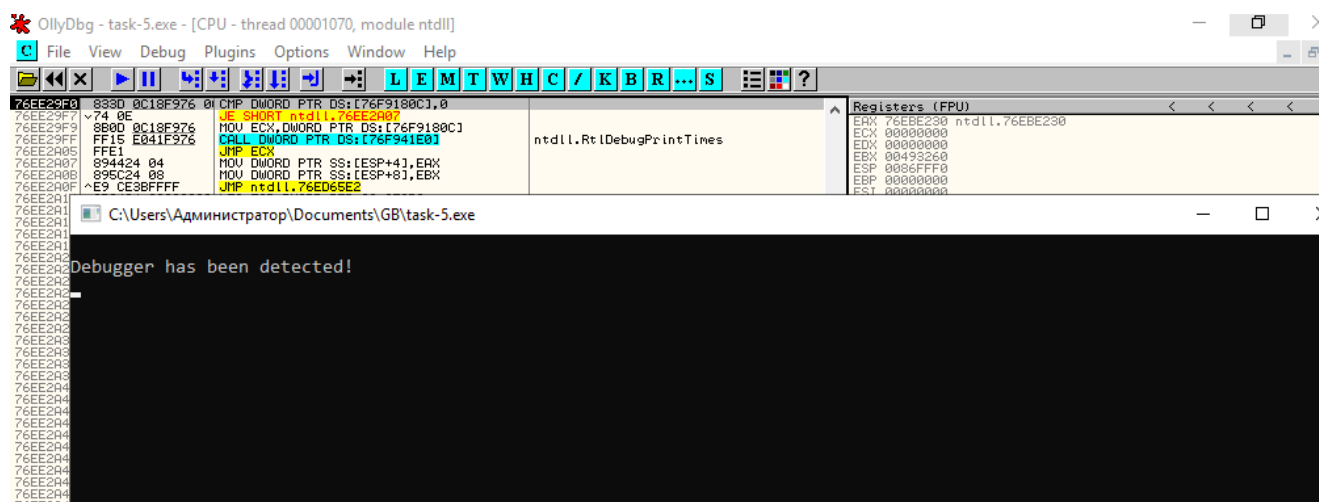
Ctrl+G 00401000

Переходим в функцию main и ставим точку остановки - break point (F2) 0040105

и запускаем программу (F9)

DebuggerPresent - определение наличия отладчика. Применяем здесь несколько инструкций...





Будем для обхода использовать плагин *HideOD*

Option

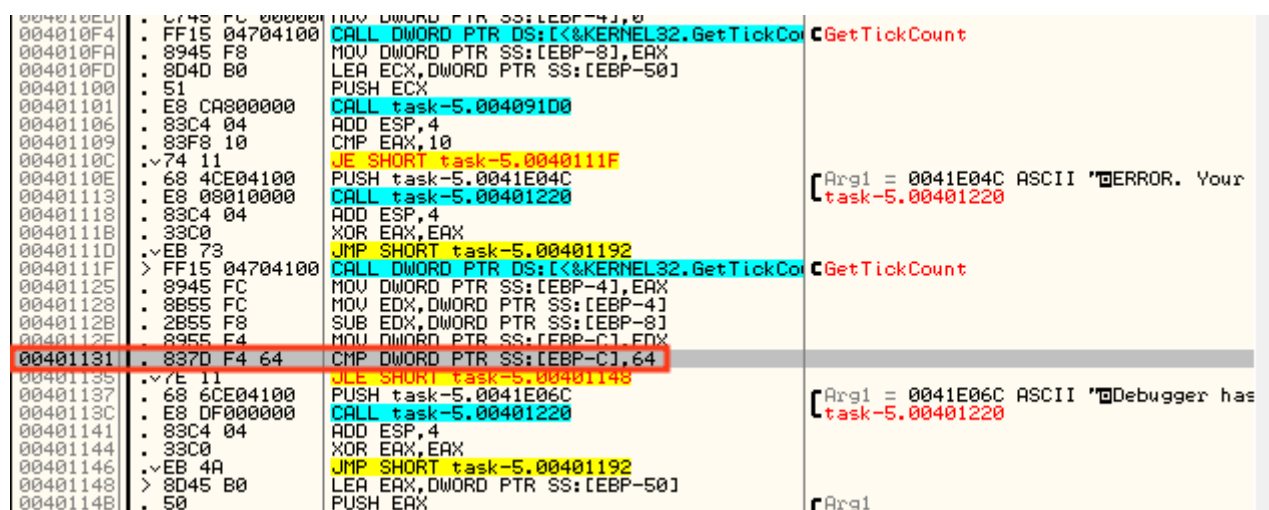
-> Auto Run HideOD

-> HideNrDebugBit

Видим, вызывается дважды *GetTickCount*

Проходит проверка на длину ключа *CMP EAX, 10*

Далее видим *CMP*, 64 (число 100), т.е. если разница более 100 мили сек., должен сработать отладчик



Enter expression to follow in Dump (local 3)

- видим содержится число *B1770000*, больше 64, следовательно проверку не проходим.

Ставим точку останова на втором *GetTickCount*

Проверяем содержимое ячейки, оно равно 0.

Смотрим регистры.

Для корректировки нужно меньше на 1С байт.

меняем первый байт на Е (большое = 14)

License key: **Eaaabbbbccccdddd**

проходит проверку

Использование специальных плагинов

<https://github.com/JackAston/OllyDbg1plugins/tree/master/>

.DLL скачать и поместить в директорию Plugins

<https://at0m2k.narod.ru/soft.html>

- ScyllaHide <https://github.com/x64dbg/ScyllaHide>
- HideOD <https://www.aldeid.com/wiki/OllyDbg/HideOD>
- HideDebugger <https://www.aldeid.com/wiki/OllyDbg/HideDebugger>

Выполнил: **AndreiM**