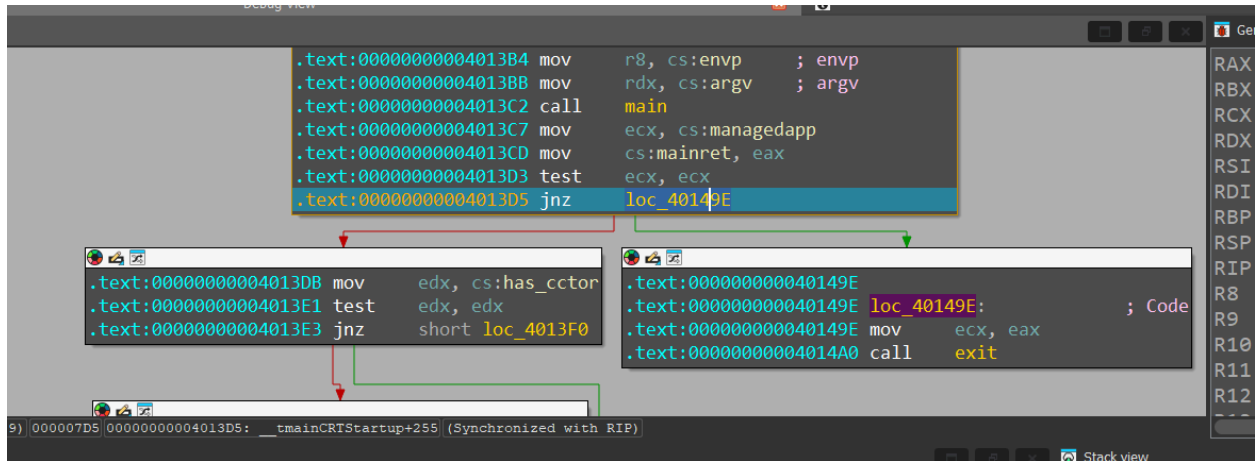




Название :	Три Лица Тени
Категория :	Реверс-инжиниринг
Уровень :	Средний
Очки :	1000
Описание :	<p>Расклад "Три Лица Тени"</p> <p>(Карты легли на стол странным узором...)</p> <p>1. Правящая Сила (Перевернутая) "То, что кажется защитой — лишь маска. Ищи там, где стражник поворачивается спиной. Его меч ржавеет от лунного света..."</p> <p>2. Тройка Мечей "Три удара в пустоту. Третья рана — невидима. Она в том, что никогда не истекает кровью, но всегда открыта..."</p> <p>3. Отшельник (В зеркальном отражении) "Одинокий свет во тьме. Не следуй за ним — он ведёт к обрыву. Истина в его тени, что тянется назад, к началу всех дорог..."</p> <p>4. Пятерка Пентаклей "Монеты с выщербленными краями. Они звенят фальшиво. Настоящее богатство замуровано в стене — там, где камень теплеет под пальцами..."</p> <p>5. Башня (Покрытая инеем) "Высокие врата рухнули. Но в подземелье, куда не ступала нога, дрожит последний факел. Его свет пишет слово на влажных камнях..."</p> <p>Совет Духов: "Когда увидишь девять воронов — считай до десяти. Когда найдёшь все двери — стучи в стену. Когда прочтёшь все надписи — смотри на промежутки между буквами."</p>
Теги :	Патчинг, обфускация

Прохождение :

Весь код в `main` и арт в TXT-файле лишь отвлекающий элемент. Описание задачи и абсурдность всего в функции `main` явно намекают на это. Посмотрим, что выполняется после `main` в отладчике.



```
.text:00000000004013B4 mov     r8, cs:envp      ; envp
.text:00000000004013BB mov     rdx, cs:argv      ; argv
.text:00000000004013C2 call    main
.text:00000000004013C7 mov     ecx, cs:managedapp
.text:00000000004013CD mov     cs:mainret, eax
.text:00000000004013D3 test     ecx, ecx
.text:00000000004013D5 jnz     loc_40149E

.text:00000000004013DB mov     edx, cs:has_ctor
.text:00000000004013E1 test     edx, edx
.text:00000000004013E3 jnz     short loc_4013F0

.text:000000000040149E loc_40149E:
.text:000000000040149E mov     ecx, eax
.text:00000000004014A0 call    exit
```

9) | 000007D5 | 00000000004013D5: \_\_tmainCRTStartup+255 (Synchronized with RIP)

В этот момент обычно программы идут направо. А тут код пропатчен и ведёт к левому блоку.

```
.text:00000000004013E3 jnz     short loc_4013F0
.text:00000000004013E5 call    _cexit
.text:00000000004013EA mov     eax, cs:mainret
.text:00000000004013F0 loc_4013F0:
.text:00000000004013F0 add     rsp, 98h
.text:00000000004013F7 pop     rbx
.text:00000000004013F8 pop     rsi
.text:00000000004013F9 pop     rdi
.text:00000000004013FA pop     rbp
0007E5|00000000004013E5: __tmainCRTStartup+265 (Synchronized with RIP)
```

Эта функция пропатчена.

```
.text:00000000004054C8
.text:00000000004054C8
.text:00000000004054C8 ; Attributes: thunk
.text:00000000004054C8
.text:00000000004054C8 ; void __cdecl cexit()
.text:00000000004054C8 public _cexit
.text:00000000004054C8 _cexit proc near
.text:00000000004054C8 jmp     _cexit_0
.text:00000000004054C8 _cexit endp
.text:00000000004054C8
```

