ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно && видно?

Напишите в чат, если есть проблемы!

Ставьте + если все хорошо

OTUS

Перехват API функций

PE Loader

Пакулов Артур

Типы перехватов

Метод сплайсинга

Вставка в начало функции инструкции перехода

```
kd> u ZwCreateProcess
nt!ZwCreateProcess:
82c3d404 b84f000000      mov     eax,4Fh
82c3d409 8d542404        lea     edx,[esp+4]
82c3d40d 9c              pushfd
82c3d40e 6a08            push    8
82c3d410 e869220000      call    nt!KiSystemService (82c3f67e)
82c3d415 c22000          ret     20h
nt!ZwCreateProcessEx:
82c3d418 b850000000      mov     eax,50h
82c3d41d 8d542404        lea     edx,[esp+4]
kd> u NtCreateProcess
nt!NtCreateProcess:
82edd67b 8bff            mov     edi,edi
82edd67d 55              push    ebp
82edd67e 8bec            mov     ebp,esp
82edd680 33c0            xor     eax,eax
82edd682 f6451c01        test    byte ptr [ebp+1Ch],1
82edd686 7401            je      nt!NtCreateProcess+0xe (82edd689)
82edd688 40              inc     eax
82edd689 f6452001        test    byte ptr [ebp+20h],1
```

Метод сплайсинга

Вставка в начало функции инструкции перехода

```
> u NtCreateProcess
nt!NtCreateProcess:
82edd67b 8bff            mov     edi,edi
82edd67d 55              push    ebp
82edd67e 8bec            mov     ebp,esp
82edd680 33c0            xor     eax,eax
82edd682 f6451c01        test    byte ptr [ebp+1Ch],1
82edd686 7401            je      nt!NtCreateProcess+0xe (82edd689)
82edd688 40              inc     eax
82edd689 f6452001        test    byte ptr [ebp+20h],1
kd> eb nt!NtCreateProcess 0xe9
kd> u NtCreateProcess
nt!NtCreateProcess:
82edd67b e9ff558bec      jmp     6f792c7f
82edd680 33c0            xor     eax,eax
82edd682 f6451c01        test    byte ptr [ebp+1Ch],1
82edd686 7401            je      nt!NtCreateProcess+0xe (82edd689)
82edd688 40              inc     eax
82edd689 f6452001        test    byte ptr [ebp+20h],1
82edd68d 7403            je      nt!NtCreateProcess+0x17 (82edd692)
82edd68f 83c802          or      eax,2
```

Перехват IAT

Можно взять пример:

```
void HookFunction(char* funcName, SIZE_T function)
{
    PSIZE_T pOldFunction = FindFunctionAddress(funcName);
    DWORD accessProtectionValue, accessProtec;

    int vProtect = VirtualProtect(pOldFunction, sizeof(PSIZE_T), PAGE_EXECUTE_READWRITE, &accessProtectionValue);
    *pOldFunction = function;
    vProtect = VirtualProtect(pOldFunction, sizeof(PSIZE_T), accessProtectionValue, &accessProtec);
}

DWORD WINAPI HookedGetCurrentProcessId(VOID)
{
    return 10000;
}
```

https://github.com/KooroshRZ/Windows-IAT-Hook

Перехват IAT

OTUS

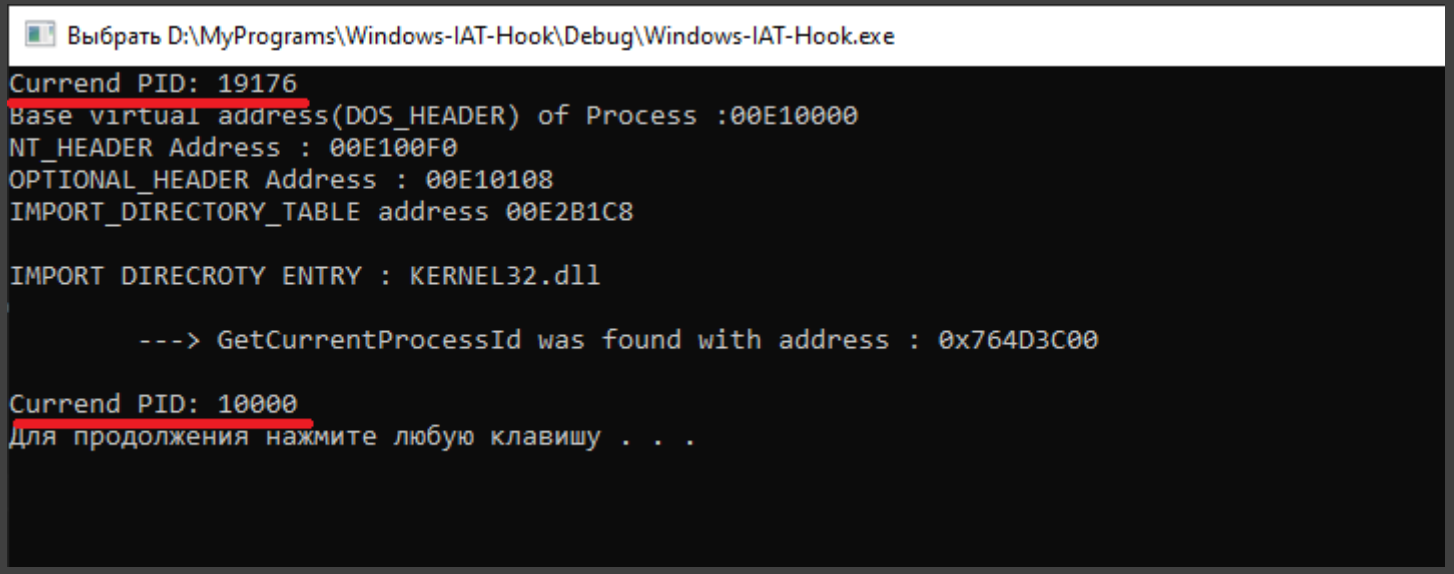
Используем

```
int main()
{
    DWORD pid = GetCurrentProcessId();
    printf("Currend PID: %d\n", pid);

    HookFunction("GetCurrentProcessId", (DWORD)&HookedGetCurrentProcessId);
    pid = GetCurrentProcessId();
    printf("Currend PID: %d\n", pid);

    system("pause");
    return 0;
}
```

https://github.com/KooroshRZ/Windows-IAT-Hook

Перехват IAT

Результат:



https://github.com/KooroshRZ/Windows-IAT-Hook

OTUS

Вопросы???

Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!