



ОНЛАЙН-ОБРАЗОВАНИЕ

Меня хорошо слышно
&& видно?



Напишите в чат, если есть проблемы!

Ставьте если все хорошо

Перехват API функций

PE Loader



Подмена IAT

Подмена
EAT

Подмена VAT

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
```

```
82edd68a 4e423001     ror    byte ptr [ebp+30h],1
82edd68b 46           jnc    eax
82edd68e 7401         je     nt!NtCreateProcess+0xe (82edd689)
82edd68f 4e423001     ror    byte ptr [ebp+30h],1
```

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
```

```
82edd692 83c802   or      eax,2
82edd694 83c802   or      eax,2
82edd696 83c802   or      eax,2
82edd698 83c802   or      eax,2
82edd69a 83c802   or      eax,2
```

Можно взять пример:

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

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

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

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

Используем

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

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

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

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

Результат:

```
Выбрать D:\MyPrograms\Windows-IAT-Hook\Debug\Windows-IAT-Hook.exe
```

```
Current PID: 19176
```

```
Base virtual address(DOS_HEADER) of Process :00E10000
```

```
NT_HEADER Address : 00E100F0
```

```
OPTIONAL_HEADER Address : 00E10108
```

```
IMPORT_DIRECTORY_TABLE address 00E2B1C8
```

```
IMPORT DIRECROTY ENTRY : KERNEL32.dll
```

```
    ---> GetCurrentProcessId was found with address : 0x764D3C00
```

```
Current PID: 10000
```

```
Для продолжения нажмите любую клавишу . . .
```

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

Вопросы???





Пакулов Артур

A.Pakulov.Otus@Gmail.com

Спасибо
за внимание!

